Saku Tolvanen

Tietoturvallisuuden häiriönhallinta pienissä yrityksissä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

11.5.2016

Metropolia

Tekijä Otsikko Sivumäärä Aika	Saku Tolvanen Tietoturvallisuuden häiriönhallinta pienissä yrityksissä 36 sivua + 1 liite 11.5.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	
Ohjaaja	Lehtori Erik Pätynen

Insinöörityössä selvitettiin tietoturvallisuuden häiriönhallinnan toteuttamista pienissä yrityksissä ja organisaatioissa. Tietoturvallisuuden häiriöiden yleistyminen ja tarve suomenkieliselle ohjeistukselle niiden selvittämiseksi oli havaittu omien työtehtävien ja häiriöiden lisääntyneen julkisuuden kautta. Työtä voi käyttää häiriöiden hoitamiseen ja niihin varautumiseen.

Työssä selvitettiin miksi tietoturvallisuuden häiriönhallintaa pitää tehdä, miten tekemiseen varaudutaan ja miten sitä tulee tehdä. Työ tehtiin tutustumalla saatavilla oleviin materiaaleihin ja muokkaamalla niistä ja käytännön kokemuksista asian ymmärtämistä helpottavia esimerkkejä ja ohjeita. Työssä ohjattiin yritystä tutustumaan tiettyihin lähdemateriaaleihin, jotta yritykselle tulisivat tutuiksi häiriönhallinnanperuskäsitteet ohjeet.

Häiriönhallintaa koskevaa lainsäädäntöä käytiin läpi esimerkein ja lainsäädännön aiheuttamien vaatimusten kautta. Samoin muistutettiin muista yritystä koskevista vaatimuksista, kuten Internet-yhteyden sopimusehtojen vaatimuksista. Yrityksen toiminnan kehittämiselle annettiin työkaluja tietoturvallisuuden osalta ja selvitettiin miten tietoturvallisuuden häiriönhallintaa ylläpidetään.

Työn aihealueeseen liittyvään materiaaliin ja kirjoittajan työkokemuksen perusteella todettiin, että yrityksen liiketoiminnan jatkuvuuden kannalta merkittävimmät asiat ovat yrityksen tärkeiden tietojen ja omaisuuden tunnistaminen, liiketoiminnan jatkuvuuden kannalta tärkeiden tietojen riittävän kattava varmuuskopiointi ja ihmisten tietoturvatietoisuuden parantaminen. Liiketoiminnan jatkuvuuden kannalta merkittävien kohteiden lisäksi selvitettiin sitä, mihin muuhun yrityksen kannattaa keskittää tietoturvallisuuden häiriönhallinnan kehitystoimet. Ylläpidossa korostettiin henkilöiden kouluttamista ja ympäristön muutoshallintaa.

Yritykset tulevat kokemaan tietoturvallisuuden häiriöitä, ja niistä toivutaan valmistautumalla tilanteisiin etukäteen ja turvaamalla kriittisen omaisuuden tietoturvallisuus. Yrityksien tehtäväksi jätettiin yksityiskohtaisemman ja omiin ympäristöihin soveltuvan toteutuksen miettiminen. Toteutuksessa tulee huomioida sopivien käytäntöjen ja järjestelmien luominen häiriöiden havaitsemiseen, reagoimiseen, palautumiseen ja kehittämiseen.

Avainsanat	tietoturvallisuus, häiriö, varmuuskopio, lokitieto, varautuminen

Author Title Number of Pages Date	Saku Tolvanen Information security incident handling in small companies 36 pages + 1 appendix 11 May 2016
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	
Instructor	Erik Pätynen, Senior Lecturer

This thesis analyses how information security incident management can be implemented in small companies and organizations. Information security incidents have become more common and a need for Finnish guidance was noticed by observing past public and non-public incidents and increased publicity of incidents. The thesis can be used for handling security incidents and in preparing to handle them.

The thesis explains why information security incident management must be done, how to prepare for incident management and how it should be done. The study was carried out by reading publicly available material and drawing up case examples and guides based on the material and personal knowledge gained from hands on work experience. The thesis suggests companies to familiarize themselves with some further reading and guides about basic concepts of information security incident management.

The thesis gives examples regarding legislation on incident management and other requirements mandated by legislation. Companies are also reminded about other requirements, like the terms of contract of their Internet service provider. Development tools of company operations regarding information security are described and it is explained how information security management is maintained.

Based on the reviewed material and the writer's work experience, It is suggested that the most relevant issues regarding business continuity are recognizing critical data and assets, sufficient backups of business critical data and information security awareness of people. In addition to the most relevant issues concerning business continuity, other main development targets of information security incident management are noted. In terms of maintenance of incident management, the training of personnel and change management is emphasized.

Companies will experience information security incidents and recovery from them is done by preparing in advance and securing the information security of critical assets. It is left for the companies to decide and implement how to build the management in their environments. Implementation must pay attention to creating proper practices and systems for detecting, reacting, recovery and development of information security incidents.

Keywords	information security, incident, backup, logs, preparedness

Sisällys

Lyhenteitä ja käsitteitä

CIA	Tietoturvan kolmio: luottamuksellisuus (Confidentiality), eheys (Integrity) ja saatavuus (Availability)
IDS/IPS	Tunkeutumisen havaitsemisen järjestelmä (Intrusion Detection System) ja Tunkeutumisen estämisen järjestelmä (Intrusion Prevention System) käytetään havaitsemaan ja estämään omiin järjestelmiin tunkeutumista ja muuta poikkeavaa toimintaa.
ITIL	Information Technology Infrastructure Library on IT-palveluiden johtamisen ja hallinnan käytäntöjä kuvaava prosessikehys.
juurisyy	ITIL Palvelutuotannon mukaan häiriön tai ongelman taustalla oleva alkuperäinen syy.
koventaminen	Laitteen tai sovelluksen aiotun käytön mukaiselle toiminnalle tarpeettomien ohjelmien, osien ominaisuuksien ja asetusten poistaminen. Englanniksi hardening.
loki	Tiedosto, johon tehdään aikajärjestyksessä merkinnät tapahtumista ja niiden aiheuttajista. Loki kerätään yleensä automaattisesti, ja samaan järjestelmään liittyviä lokeja voi olla useita, esimerkiksi vikaloki, laskutusloki, turvaloki.
lokitieto	Tietojärjestelmästä automaattisesti kirjautuva tapahtumatieto. Lokitieto voi sisältää erilaisia tunnistamistietoja ja koskea muun muassa sitä, kuka järjestelmää on käyttänyt, miten ja milloin järjestelmää on käytetty ja millaista tietoa erilaisista virhetilanteista on saatu.
RAID	Redundant Array of Independent Disks. Tekniikka kiintolevyjen vikasietoisuuden parantamiseksi tai nopeuden kasvattamiseksi.
replikointi	Tiedostojen tai tietueiden automaattinen kopiointi toiseen kohteeseen.

SIEM	Tietoturvan häiriöiden tapahtumien hallinta. Lokien ja muiden tietolähteiden keskitetty tallennus ja analysointi tilannekuvan luomiseksi ja häiriöiden hallitsemiseksi.
SOC	Security Operations Center. Tietoturvan operatiivinen keskus tilannekuvan, häiriönhallinnan ja operatiivisen tietoturvan tekemiseen.

1 Johdanto

Insinöörityön tarkoituksena on tukea pienten yritysten ja organisaatioiden tietoturvan häiriönhallintaa ja antaa välineitä tietoturvallisuuden häiriötilanteisiin reagoimista varten. Työssä kuvatut tavat soveltuvat myös isommille organisaatioille erityisesti silloin, jos tietoturvan häiriönhallinnasta ei ole aiempaa kokemusta ja oman organisaation resurssit ongelmien käsittelemiseksi ovat pienet.

Käytän termistönä Information Technology Infrastructure Libraryn ITIL:n version 3 mukaisia termejä ja niiden virallisia suomennoksia [Hyvönen ym. 2011]. Valitsemastani termistöstä vuoksi käytän käsitettä *tietoturvallisuuden häiriönhallinta* (information security incident management) enkä vaihtoehtoista käsitettä *tietoturvallisuuden poikkeamien tai ongelmien hallinta*. Käyttämällä käsitettä *häiriö* pyrin laskemaan kynnystä tutustua aiheeseen niiden lukijoiden kohdalla, joille tietoturvan häiriönhallinta on uusi asia. Tietoturvan häiriön selvittäminen on periaatteiltaan samanlaista toimintaa kuin minkä tahansa häiriöntilanteen selvitys organisaatiossa. Selvittäjällä tulee olla hallussaan tietyt tiedot häiriön kohteena olevasta ympäristöstä, selvityksessä käytössä olevista työkaluista ja selvitystyöhön mahdollisesti vaikuttavista tekijöistä, kuten viranomaisten määräyksistä ja lainsäädännöstä.

Insinöörityön ensisijainen tavoite on antaa lukijalle suomen kielellä riittävät tiedot häiriönhallinnan aloittamiseksi. Lukuun 5 on kerätty ne toimenpiteet, joiden avulla käynnissä olevaa häiriötilannetta voidaan hoitaa. Sitä aiemmissa luvuissa käydään läpi välineitä, prosesseja ja työtapoja, joilla häiriönhallintaa kannattaa tehdä. Lukijalle tarjotaan myös tietoa alan kirjallisuudesta, johon tutustumalla lukija voi saada tarkempaa tietoa tässä insinöörityössä käsitellyn kokonaisuuden tarkemmista yksityiskohdista.

2 Tietoturvallisuuden häiriönhallinta

Tietoturvallisuuden häiriönhallinnalla tarkoitetaan yrityksen tietoturvallisuudesta huolehtimista tavanomaisin häiriönhallinnan keinoin. Tietoturvallisuudella tarkoitetaan yrityksen luottamuksellisen tiedon ja omaisuuden suojaamista kontrolloimalla sen käytettävyyttä, eheyttä ja luottamuksellisuutta. Käytännössä tavallisessa häiriönhallinnassa selvitettävästä häiriöstä voi tulla tietoturvallisuuden häiriönhallinnan häiriö selvityksen

aikana. Toisaalta tietoturvallisuuden häiriöistä voi tulla tavallisia häiriötilanteita käsittelyn edetessä. Tämän vuoksi tietoturvallisuuden häiriönhallinta on häiriönhallinnan prosessin osa, jonka suurimmat eroavaisuudet tulevat aiheuttajasta eli inhimillisen toiminnan tuloksena. Tietoturvan häiriön syynä on harvemmin koneen vikaantuminen, joskin koneessa tai sovelluksessa oleva vika voi mahdollistaa siihen kohdistuvan hyökkäyksen onnistumisen. Myös inhimillinen erehdys sovelluksen ylläpidossa voi poistaa joitain turvakontrolleja käytöstä ja siten helpottaa hyökkäyksen onnistumista.

2.1 Tahallinen ja tahaton toiminta tietoturvallisuuden häiriöiden taustalla

Tietoturvallisuuden häiriöiden synty on karkeasti jaettavissa kahteen luokkaan: tahallisen ja tahattoman toiminnan aikaansaamat häiriöt. Tahallisella toiminnalla syntyneiden häiriöiden aiheuttajia ovat muun muassa palvelunestohyökkäykset, haittaohjelmien aiheuttamat ongelmat ja tietomurrot. Tahallisen toiminnan häiriön yhtenä aiheuttajana on aina ihminen. Tahallisena toimintana voidaan pitää myös tilannetta, jossa esimerkiksi tulipalon suorat ja välilliset vahingot ovat yrityksen riskienhallinnassa tehtyä arviointia suurempia, koska annettuja ohjeita palavien materiaalien varastoinnista ei ollut huomioitu asianmukaisesti. Tahallista toimintaa vastaan pystytään varautumaan toimivan riskienhallinnan ja riittävien ohjeiden avulla tahatonta toimintaa helpommin.

Tahattomalla toiminnalla syntyviä tietoturvallisuuden häiriöitä tai niitä mahdollistavia tilanteita ovat muun muassa varmuuskopioiden tekemisen unohtaminen, päivitysten asentamisen unohtaminen, vesivahingot ja puuttuvat tietoturvakäytännöt. Tietoturvallisuuden häiriön juurisyy voi myös alkaa tahattomasti esimerkiksi tilanteessa, jossa yrityksessä unohdetaan päivittää järjestelmät. Päivittämisen unohtamisen eli tahattoman toiminnan kautta syntyneitä aukkoja voidaan hyödyntää tahallisen toiminnan kautta. Tahattomalta häiriöltä suojautuminen on pääasiassa riskienhallinnan kautta tehtävää liiketoiminnan jatkuvuuden suunnittelua.

2.2 Syitä tietoturvallisuuden häiriöihin

Pienten ja suurten yritysten edustajilta kuulee usein kysymyksen: ”Miksi meitä vastaan hyökätään?” Kysymykseen ei ole yhtä oikeaa tai väärää vastausta. Käytännössä jokaisella henkilöllä ja yrityksellä on jotain luottamuksellista tietoa, jota ei haluta muiden

tietävän tai konkreettista tai immateriaalista omaisuutta (ITIL V3 mukainen määritys engl. asset), jota ei toivota muiden saavan oikeudetta haltuunsa. Konkreettista omaisuutta voi olla esimerkiksi yrityksen verkkokapasiteetti, jota hyökkääjä käyttää luvatta esimerkiksi roskapostien lähettämiseen. Immateriaalisen omaisuuden kohdalla hyökkääjän tavoitteena voi olla yrityksen kehittämän sovelluksen tietojen ja koodin varastaminen.

Suurimmalla osalla yrityksistä on jonkinlaista tarvetta tietotekniikan käyttöön, sillä vähintään yrityksen rahaliikenne on riippuvainen tietotekniikasta. Suomessa ei vielä ole koettu toistuvia laajamittaisia hyökkäyksiä maksuliikennettä kohtaan, mutta ongelma yleistyy ja tapaukset voivat olla merkittäviä. Esimerkiksi itähelsinkiläisen kahvilan tapauksessa [itähelsinkiläinen kahvila 2010] yli 100 000 luottokorttitietoa päätyi rikollisten käsiin. Yksittäisellä PK-yrittäjällä ei yleensä ole resursseja selvittää vastaavaa tapausta. Pitkäkestoisten tapausten osalta myös isojen yritysten tietotaito ja resurssit voivat olla yksinään riittämättömiä.

Pienelle yritykselle yksikin onnistunut hyökkäysyritys voi olla uhka liiketoiminnan jatkumiselle, mikäli korvausvelvollisuudet tai selvityskulut kasvavat kohtuuttoman suuriksi. Uhista johtuvat mahdolliset riskit tulisi kartoittaa ja niiden perusteella arvioida yrityksen toiminnan jatkuvuuden mahdollisuuksia eri tilanteissa. Arvion perusteella tulisi laatia jatkuvuussuunnitelma, jonka avulla varaudutaan liiketoiminnan jatkuvuuteen.

Kun arvioidaan tietoturvallisuutta vain haittaohjelmien määrän näkökulmasta, Suomi on pärjännyt hyvin verrattaessa havaintoja saastuneista koneista muissa maissa tehtyihin havaintoihin [Microsoft SIR 2012]. Tilanne on ollut sama jo useana peräkkäisenä vuotena. Vaikka tilanne on tästä näkökulmasta parempi kuin monessa muussa maassa, on yksikin yrityksen omaan verkkoon päässyt haittaohjelma riski yrityksen toiminnalle. Koska haittaohjelmien määrä kasvaa hyvin nopeasti, kuten F-Securen [F-Secure 2016] artikkelista käy ilmi, eivät virustorjuntaohjelmat edes aina tunnista niitä.

Poliisille tulleet tietokoneisiin liittyvät rikosilmoitukset ovat kuitenkin kasvussa esimerkiksi palvelunestohyökkäysten osalta [Kuusela: 22]. Pienetkin yritykset ovat yhä useammin kohteina [Sopanen 2016]. Pienilläkin häiriöillä voi olla merkitystä yrityksen maineen kannalta. Tilanteessa, jossa yrityksen tietoturvallisuuteen kohdistuu sen asiakkaille näkyvä häiriö, on yrityksen arvioitava myös maineeseensa kohdistuvat vahingot. Yrityksen maineeseen kohdistuvien vahinko voi olla tietoturvahäiriön ainoa pitkäaikai-

nen vaurio, joka kohdistuu yhtiön liiketoimintaan. Maineen vaurioitumista on hankala arvioida ja mitata, mutta viimeistään siinä vaiheessa sitä tapahtuu, kun ulkopuoliset toimijat kertovat häiriöstä julkisesti. Jatkossa EU:n lainsäädäntö pakottaa yritykset kertomaan henkilötietoihin kohdistuneet tietomurrot viranomaisille [EU Tietosuoja-asetus lehdistötiedote 2015]. Tietosuojaa koskevan lainsäädännön tiukentaminen korostaa tietosuojan merkitystä, mutta Suomen keskivertoa tiukemman yksityisyyden suojan vuoksi pohjatyötä on jo tehty esimerkiksi henkilörekisterien käsittelyn osalta. Kaikki henkilörekisterit tulee nykyisen henkilötietolain [Henkilötietolaki 1999] ja 2018 voimaan tulevan EU:n tietosuoja-asetuksen mukaisesti suojata mahdollisilta väärinkäytöksiltä. Lainsäädäntö koskee sekä paperisia että sähköisiä tietoja [Henkilötietolaki 1999 5 §].

Yhtenä syynä yritykseen kohdistuviin tietoturvavaatimuksiin voi olla yrittäjän asiakkaiden tai tavarantoimittajien yleistyvät vaatimukset, jotka koskevat tietoturvallisuutta ja tietosuojaa. PK-yrityksissä vaatimustenmukaisuudet koskevat lähinnä rahaliikenteen hoitamista ja televerkkojen käyttämistä. Esimerkkeinä vaatimuksista ovat Netsin (entinen Luottokunta) valvomat vaatimukset turvallisesta korttimaksamisesta [Nets korttimaksaminen 2016] ja teleoperaattoreiden sopimusehtojen [Elisa YSE 2016: 1; Sonera toimitusehdot 2016: 1] vaatimukset tietoturvallisesta televerkon käyttämisestä. Nämä vaatimukset juontavat juurensa teleoperaattoreita koskevasta velvoittavasta lainsäädännöstä, joka pakottaa teleoperaattorit huolehtimaan verkkojensa turvallisuudesta. Jos operaattorin asiakas ei saa tietoturvallisuuden häiriötään kuriin, operaattori voi katkaista verkkoyhteyden sopimusehtojen nojalla. Erilaisia vaatimuksia on myös potilas- ja henkilötietojen käsittelyssä erityisesti silloin, kun yritys toimittaa palveluita terveydenhuoltoalalle.

Tapahtuneesta tietoturvan häiriöstä tulee aina ylimääräisiä kustannuksia. Joissain tapauksissa kustannukset ovat pieniä. Siten ne voidaan katsoa riskienhallinnan kautta tehdyn arvion perusteella jäännösriskin arvoisiksi. Pahimmillaan kustannukset ajavat yrityksen konkurssiin, kun sopimussanktiot, sakot ja keskeytynyt tuotanto kuluttavat yrityksen kassan. Yrityksen liiketoiminta voi keskeytyä tai pahimmassa tapauksessa päättyä hoitamattomaan tietoturvallisuuden häiriöön. Kyseessä voi olla vain näennäisesti viaton virhe, kuten varmuuskopioiden puuttuminen haittaohjelman saastuttamasta koneesta tai sähköiseen kauppapaikkaan kohdistuva tietoturvahyökkäys, joka estää kaupankäynnin.

2.3 Tietoturvan häiriönhallinta

Tietoturvasta huolehtimisen tulee olla osa yrityksen tavallista liiketoimintaa. Tietoturvallisuuden häiriöihin kannattaa varautua ja varautuminen kannattaa tehdä riskiarviointien kautta. Yrityksellä tulee olla yleisempi turvallissuunnitelma ja sitä tietoturvallisuuden osalta täydentävä tietoturvallisuuspolitiikka. Yrityksen henkilöstön tulee myös tuntea näiden dokumenttien sisältö vähintään siltä osin, että henkilöstö tietää kenelle he ilmoittavat havaitsemistaan poikkeamista ja keneltä saavat ohjeita tilanteen hoitamiseksi.

Yrityksen yleisen turvallisuussuunnitelman tulee kattaa turvallisuuden eri osa-alueet. Henkilöturvallisuuteen, fyysiseen kulunvalvontaan, paloturvallisuuteen ja matkustukseen liittyvät alueet tulee kuvata turvallisuussuunnitelmassa. Siltä osin kuin turvallisuuden osa-alueilla on vaikutusta yrityksen tietoturvallisuuteen, kannattaa edellä mainittuja turvallisuuden osa-alueita täydentää tietoturvapolitiikassa. Tietoturvapolitiikka voi olla osana turvallisuussuunnitelmaa, ja ylläpidon kannalta tämä on pienessä yrityksessä järkevää. Turvallisuussuunnitelmassa tulee ottaa kantaa siihen, miten usein yrityksen riskit käydään läpi ja miten yritys tekee riskienhallintaa.

Yrityksen riskienhallinnasta kannattaa tehdä säännöllistä toimintaa. Riskienhallinnassa pitää arvioida yrityksen oma toimintaympäristö, henkilöstö ja omaisuus ja niihin liittyvät riskit. Se, miten riskienhallinta tehdään, pitää määritellä turvallisuussuunnitelmassa. Riskienhallinnan tulee olla säännöllistä, ja uusiin uhkiin tulee reagoida myös suunnitelmaa päivittämällä. Riskienhallintaa kuvataan useassa teoksessa, myös IT-näkökulmasta. Esimerkiksi Ernie Jordanin ym. Strateginen IT-riskien hallinta [2006] voi toimia pohjana riskienhallinnan suunnittelussa.

Tietoturvallisuus

Tietoturvallisuudella tarkoitetaan henkilöille, yhteisöille, yrityksille ja niin edelleen. tärkeän tiedon suojaamista. Käytännössä tietoturvallisuus toteutetaan kolmen perusominaisuuden avulla noudattaen suojattavan tiedon vaatimuksia. Nämä perusominaisuudet ovat luottamuksellisuus (confidentiality), eheys (integrity) ja käytettävyys (availability). Koska jokainen ominaisuus tulee huomioida, ei tietoturvallisuutta voida toteuttaa laittamalla vain yksi osa-alue kuntoon ja luottamalla, että muut ominaisuudet hoituvat itsestään. Kolme ominaisuutta tasapainottavat toinen toistaan silloin, kun niitä pohdi-

taan ympäristön vaatimuksien kautta. Tiedon luottamuksellinen suojaaminen on helpompaa, jos sitä ei tarvitse antaa useiden ihmisten käytettäväksi tai muokattavaksi. Jos usea henkilö pystyy käsittelemään tietoa, on sen luottamuksellisuudelle asetettava erilaisia vaatimuksia kuin tiedolle, jota pystyvät käsittelemään vain harvat. Ketkä kaikki voivat muokata ja kenelle riittää vain oikeus lukea tietoa? Pitääkö tiedon käsittely estää muilta esimerkiksi muokkauksen aikana?

Yleisen määritelmän mukaan tietoturvallisuus keskittyy enemmän tiedon suojaamiseen, kun taas kyberturvallisuuden häiriönhallinnassa on mukana myös muiden häiriöiden hallinta, kuten ihmisten turvallisuus. Perinteisessä tietoturvassa painotus on enemmän käsityönä tapahtuvassa työssä. Kyberturvallisuudessa sen sijaan painotus on verkottuneen yhteiskunnan turvallisuudessa, automaatiolla tehtävissä häiriöissä ja suojaavissa toimissa. Ihminen on kuitenkin sekä tietoturvallisuudessa että kyberturvallisuudessa se lenkki, joka toisaalta määrittelee oman ympäristönsä suojaustarpeet ja toisaalta suunnittelee ja toteuttaa hyökkäykset. Ainoa suurempi ero tietoturvallisuuden ja kyberturvallisuuden välillä tulee siitä, miten helposti hyökkäys onnistuu isoissa, laajoissa ja turvalliseksi tehdyissä ympäristöissä. Perusmuotoisen palvelunestohyökkäyksen eli tietoturvallisuuteen kohdistuvan hyökkäyksen voi kuka tahansa ostaa verkosta, mutta suuren yrityksen tai maan merkittävään infrastruktuuriin kohdistuvissa kyberturvallisuuteen kohdistuvissa hyökkäyksissä tekijällä on yleensä toiminnalleen valtiollista tai vastaavan suuruusluokan rahoitusta. PK-yrityksen kannalta tietoturvallisuudessa ja kyberturvallisuudessa on kyseessä pitkälti sama asia eli oman liiketoiminnan tietojen eheyden, luottamuksellisuuden ja käytettävyyden turvaaminen.

Tietoturvallisuuden häiriönhallinta on yksi osa yrityksen tietoturvapolitiikkaa. Tietoturvapolitiikkana pidetään yrityksen yleisiä määrityksiä ja suuntaviivoja sille, miten tietoturvallisuudesta tulisi yrityksessä huolehtia. Vaihtoehtoisena nimenä tietoturvapolitiikalle on tietoturvasuunnitelma. Tämä työ keskittyy tietoturvapolitiikan niihin osiin, joilla on vaikutusta tietoturvallisuuden häiriönhallintaan. PK-yrityksen tietoturvapolitiikan laatimisen apuna kannattaa käyttää Matti Laakson insinöörityötä PK-yrityksen tietoturvasuunnitelman laatiminen [Laakso: 2010]. Häiriönhallinnan kannalta oleelliset tietoturvapolitiikan osa-alueet ovat

- lainsäädännön vaatimukset
- muut vaatimukset

- hallinnollinen tietoturva
- fyysisen tietoturvan tärkeysluokittelu ja kulunhallinta
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineiston turvallisuus
- tietoliikenneturvallisuus
- henkilöstöturvallisuus.

Lainsäädännölliset ja muut vaatimukset muodostavat tietoturvapolitiikalle perusrungon, jonka perusteella muut osa-alueet, kuten esimerkiksi yrityksen budjetti ja toimintaympäristö muokkaavat politiikasta yritykselle käyttökelpoisen. Muita vaatimuksia voivat olla esimerkiksi rahoituslaitosten ja yrityksen välisissä sopimuksissa vaaditut asiat esimerkiksi maksukorttiliikenteen tietoturvallisuudesta. Edellä mainittujen vaatimusten perusteella hallinnollista tietoturvallisuutta muokataan vastaamaan tarpeita ja määritellään muiden osa-alueiden käytännöt esimerkiksi siitä, millaisia salasanoja tulee käyttää kirjautumisissa. Tietoturvallisuuden häiriönhallinnan kannalta tulee huolehtia ja vastuuttaa tehtävät eri rooleille ympäristön vaatimustenmukaisuudesta, eri osa-alueiden turvallisuuden vaatimuksista, niiden seurannasta ja poikkeamiin reagoimisesta.

Käytännössä yrityksellä pitää olla tieto niistä laitteista, sovelluksista ja verkoista, joissa on yritykselle merkittävää tietoa. Tieto tulisi luokitella jollain tapaa vähintään yrityksen sisäiseksi ja julkiseksi tiedoksi. Ympäristön käytölle tulisi luoda työntekijöiden kanssa pelisäännöt esimerkiksi salasanojen pituuksista, yksityisten viestien käsittelystä ja omien työkalujen käytöstä. Ulkoisiin poikkeamiin on sinänsä helppo reagoida, jos ne havaitaan, mutta sisäisten poikkeamien käsittelyä sääntelee useampi laki, kuten laki yksityisyyden suojasta työelämässä [Laki yksityisyyden suojasta työelämässä 2004] ja tietoyhteiskuntakaari [Tietoyhteiskuntakaari 2014]. Luvussa 3 käsitellään tietoturvapolitiikka tarkemmin.

Tietoturvallisuuden käytäntöjä

Tietoturvapolitiikan avulla muodostetun hallinnollisen perustan jälkeen voidaan jatkaa käytännönläheisimmillä tehtävillä. Yrityksen käytössä olevat laitteet, sovellukset, henkilöt, dokumentit ja niin edelleen tulee selvittää ja ylläpitää selvityksestä syntyvää listaa.

Listaan tulee myös merkitä se, miten kriittisestä omaisuudesta on kyse yrityksen näkökulmasta katsottuna. Alussa riittää, että on olemassa tieto esimerkiksi käytössä olevista verkko-osoitteista ja niissä käytetyistä tekniikoista. Kullekin tiedon tyypille tulee olla määritelty omistaja, joka vastaa tietojen päivittämisestä. Koneita luokitellaan, jotta tiedetään millä alustalla ja sovelluksilla yritys toimii. Dokumentit ja muu vastaava aineisto luokitellaan, jotta tiedetään, mikä tieto on yritykselle suojelemisen arvoista ja missä se sijaitsee. Henkilöiden osalta tulee miettiä heidän roolinsa tietojen käyttämisessä ja käyttötarpeet.

Kun tiedot saadaan luokiteltua, voidaan paremmin varautua niihin kohdistuviin häiriöihin. Ensimmäinen askel häiriönhallinnan varautumisessa on pitää liiketoiminnalle kriittinen tieto varmuuskopioituna ja testata näiden varmuuskopioiden toimivuus säännöllisesti. Jos tiedon palautus ei onnistukaan, ei varmuuskopioilla tee mitään. Kriittistä tietoa on siis myös kuvaus ympäristöstä ja siinä käytetyistä asetuksista. Varmuuskopioista kannattaa säilyttää yhtä kappaletta muualla kuin siinä tilassa jossa tieto tuotetaan. Varmuuskopioita suojataan vähintään samalla tavalla kuin niiden sisältämää tietoa muutenkin suojattaisiin.

Jos yrityksen toiminta perustuu julkisesti saatavilla olevaan verkko-sivustoon, kuten verkkokauppaan, tulee varautumisessa ottaa huomioon myös kauppaan kohdistuvat palvelunestohyökkäykset. Yritykseen omaan toimintaan tarpeelliset yhteydet ja verkkokauppaan tarvittavat yhteydet kannattaa pitää omissa erillisissä verkoissaan ja varmistaa verkkokaupalle varaosoite, johon palvelut voidaan siirtää riittävän lyhyellä aikataululla. Omien tärkeiden tietojen ja palveluiden turvallisuuden varmistamiseksi tulee niiden tietoturvallisuutta valvoa tai vähintään reagoida muualta tuleviin ilmoituksiin, jotka koskevat palveluiden toimivuutta tai yrityksen tietojen luottamuksellisuuden menetystä.

Tietoturvallisuuden häiriöiden seuraamiseksi tulee yrityksellä olla jokin sähköpostiosoite tai muu julkisesti saatavilla oleva selkeä yhteystieto, johon ulkopuoliset tahot tai yrityksen oma henkilökunta voi ilmoittaa havaitut häiriöt. Sinne tulevia viestejä tulee seurata säännöllisesti, mieluiten päivittäin. Hyvän Internet-tavan mukaisesti yrityksen käytössä olevalla domain-nimellä tulisi löytyä myös abuse-osoite. Tällöin yksi postilaatikoista olisi osoitteessa abuse@yritys.fi. Eri palvelutoimittajille kannattaa antaa myös jokin osoite, jota seurataan säännöllisesti, jotta heidän havaitsemistaan poikkeamista tulee yritykselle tietoa. Pienellä yrityksellä ei välttämättä ole muita mahdollisuuksia valvoa ympäristönsä tietoturvallisuuden tilaa. Kattavampaa valvontaa voidaan joutua te-

kemään esimerkiksi lainsäädännön velvoittamana. Tällöin valvonta tulee toki järjestää vaatimusten mukaisesti. Jos yrityksellä on kykyä liiketoimintansa suojeluun, voidaan valvontaa tehdä myös ennakoivasti. Valvonnan parantamisessa on eri vaihtoehtoja, ja niitä käsitellään tarkemmin luvussa 4.

3 Valmistautuminen tietoturvallisuuden häiriöiden hallintaan

3.1 Tietoturvapolitiikka

Jos yrityksellä on jo olemassa tietoturvapolitiikka, sen toimivuutta voi arvioida esimerkiksi Antti Kuritun [2015] kehittämän tietoturvallisuustilanteen Tikka-kartoitustyökalun avulla. Jos politiikkaa ei ole tai kartoitustyökalun mukaan asioita pitäisi parantaa, tulee politiikka tehdä tai päivittää vastaamaan nykyisiä tarpeita. Jotta valmistautuminen tietoturvallisuuden häiriönhallintaan voidaan aloittaa, tulee yrityksen käydä häiriönhallinnan vaikutukset läpi työntekijöidensä kanssa. Selvityksen yksi osa-alue on muodostaa yritykselle toimiva tietoturvapolitiikka, jolla on johdon tuki. Tietoturvapolitiikan vaikutukset, jotka kohdistuvat työntekijöiden työtehtäviin ja yksityisyydensuojaan työelämässä, on käytävä läpi työntekijöiden kanssa.

Tietoturvapolitiikka on käytännössä yleinen kuvaus siitä, miten yrityksessä huolehditaan tietoturvallisuudesta ja mitkä roolit vastaavat, että näin tapahtuu. Tarkemmat kuvaukset siitä, miten esimerkiksi yksittäisiä laitteita käsitellään, tulee kirjata ohjeisiin. Pienessä yrityksessä turvallisuussuunnitelma, tietoturvapolitiikka ja niihin liittyvät ohjeet voivat olla yhtenäinen dokumentti, mutta ylläpidon kannalta on helpompaa, jos turvallisuussuunnitelman, tietoturvapolitiikan ja muiden ohjeiden välillä on jotain hierarkiaa eli eniten muutoksia koskevat ohjeet olisivat erillisiä muista ohjeista. Yrityksen tietoturvapolitiikan tulee huomioida häiriönhallinnan oikeudet ja velvollisuudet työntekijöiden ja yrityksen johdon kannalta sekä häiriönhallinnan kautta tapahtuva pääsy ihmisten väliseen viestintään.

Tietoturvapolitiikan on noudatettava lakia, joten sen tulee kuvata asiantuntijoiden mahdollisuudet vikatilanteen selvitykseen ja työntekijöiden velvollisuudet ja oikeudet tietoturvallisuudesta huolehtimiseksi. Politiikka voidaan kirjoittaa koskemaan nimenomaan yrityksen ympäristöä ja siinä tehtävää työtä, joten se voi olla ja sen pitää olla työntekijän näkökulmasta lakitekstiä selkeämpää.

Tietoturvapolitiikan tulee noudattaa esimerkiksi lakia yksityisyyden suojasta työelämässä [Laki yksityisyyden suojasta työelämässä 2004], joten työntekijän yksityisen viestinnän sisältöä ei saa tutkia ilman työntekijän lupaa. Käytännössä tietoturvapolitiikassa kuvataan yleisellä tasolla, että häiriönhallinnassa voidaan tutkia liikennettä vian selvittämiseksi, mutta yksityisiä viestejä ei avata ilman ennalta sovittuja käytäntöjä. Tästä syystä laitteet, joilla ei ole tarvetta tehdä yksityistä viestintää, kannattaa kuvata politiikan tai ohjeiden tasolla ja todeta, että niissä tapahtuvat poikkeamat selvitetään laitteelle merkityn omistajan tai hallinnoijan kanssa. Jos laite on yrityksen omistama, mutta yksittäisen työntekijän käytössä, tulee mahdollinen selvitys tehdä mahdollisuuksien mukaan yhdessä työntekijän kanssa tai hänen nimeämänsä edustajan läsnä ollessa. Jos laite on työntekijän omistama, mutta sitä käytetään yrityksen työtehtävien hoitoon, tulee politiikassa määritellä, miten selvitys tehdään.

Koska pieni yritys joutuu todennäköisesti ostamaan vähintään osan IT-palveluistaan ulkopuolelta, yrityksen kannattaa tutustua myös käyttämiensä palveluntarjoajien ja teleyritysten tietoturvapolitiikkaan ja sen noudattamiseen omien sopimusten osalta. Suomessa teleyritykset joutuvat Tietoyhteiskuntakaaren [2014] velvoittamina huolehtimaan tietoturvallisuudesta. Kun taas ostetaan palveluita usealta taholta, on vaikea löytää yhtä vastuullista tahoa korjaamaan häiriöitä. Siksi yrityksen kannattaa pyrkiä kirjaamaan tietoturvallisuuden vastuut sopimuksiin ja tutustua nykyisten sopimusten sopimusehtoihin sekä miettiä niille joku koordinointivastuullinen omasta yrityksestä nimeämällä vähintään koordinointivastuulllisen rooli tietoturvapolitiikassa. Tämän avulla oman tietoturvapolitiikan mukaisista vaatimuksista saadaan riittävän kattavia suhteessa tarpeeseen ja tarjolla oleviin palveluihin. Yritykselle jää kuitenkin vastuu huolehtia esimerkiksi henkilötiedoista ja muista vastaavista tiedoista, joiden väärinkäytöksistä voi seurata lakien määräämiä sanktioita.

Jos yritys käyttää ulkopuolisten toimijoiden apua tietoturvallisuuden häiriönhallinnassa, se kannattaa kirjata yrityksen tietoturvapolitiikkaan ja samalla rajata ulkopuolisten vastuut ja velvollisuudet sopimuksellisesti politiikan mukaisiksi. Osaa vastuista, kuten omaa rooliaan henkilörekisterin rekisterinpitäjänä, ei voi ulkoistaa, mutta vastuiden sisältämiä tehtäviä voi sen sijaan ulkoistaa.

3.2 Ohjeistus

Tietoturvallisuuden häiriönhallinnan ohjeistuksen tulisi olla osa tavanomaisia häiriönhallinnan ohjeita. Koska yksityisyyden suojaa koskevat lait vaikuttavat enemmän tietoturvan häiriöiden selvitykseen kuin tavallisten häiriöiden selvitykseen, tulee ohjeisiin kirjata ne kohdat, joihin asti asiantuntijat voivat lait noudattaen selvittää tilanteen. Esimerkiksi vaarantamatta yksittäisen käyttäjän yksityisyyden suojaa ei hänen koneeltaan voida yleensä selvittää sitä, mikä on aiheuttanut haittaohjelman tarttumisen koneeseen. Kun työntekijöille kerrotaan yleisellä tasolla etukäteen mahdollisista selvityksistä ja selvitystyö tehdään pelkästään aiemmin pystytettyjen järjestelmien keräämillä tiedoilla tai automatisoidusti tietokoneella, voidaan työ tehdä tavallisten politiikkojen, ohjeistusten ja käytäntöjen puitteissa. Jos tämä ei riitä, tulee toimia ohjeisiin kirjatun mukaisesti ja tulkita selvitystyö sellaiseksi, jossa voidaan mahdollisesti nähdä henkilön yksityistä viestintää.

Käytännössä rajaus tehdään tilanteeseen, jossa voivat selvitä kahden ihmisen välisen viestinnän osapuolet tai viestin sisältöä. Esimerkiksi sähköpostijärjestelmää ylläpitävän henkilön ja siihen verkkoliikennettä välittävien laitteiden ylläpidosta vastaavien henkilöiden kuuluu tietyissä, kuten häiriönhallintaan liittyvissä tehtävissä, päästä käsiksi viesteihin ja niiden sisältöön. He eivät saa kertoa saamiaan tietojaan sellaisille henkilöille, jotka eivät ole viestinnän osapuolia tai tarvitse tietoja saman häiriötilanteen selvittämiseksi [Tietoyhteiskuntakaari 2014]. Jos keskitetyssä hallinnassa oleva virustorjuntaan käytetty järjestelmä ilmoittaa, että käyttäjän lähettämässä sähköpostissa on haittaohjelma, tulee ohjeiden kuvata, että viestin lähettämisen saa estää automatisoidusti. Tämän lisäksi käyttäjän koneesta poistetaan haittaohjelma tavallisten käytäntöjen mukaan ja siten, että käyttäjän muita viestejä tai mahdollisia yksityisiä tiedostoja ei käsitellä. Jos on olemassa perusteltu syy selvittää tapauksen haittaohjelmatartunnan alkuperäinen syy, tehdään selvitys yhdessä käyttäjän tai hänen edustajansa kanssa. Selvityksessä pyritään välttämään henkilön yksityisen viestinnän näkemistä. Jos kuitenkin yksityistä viestintää joudutaan tarkastelemaan, tulee nämä kirjata erikseen talteen. Ohjeista tulee myös käydä ilmi se, missä tilanteessa tutkinta siirtyy viranomaisille ja mitä toimia se edellyttää.

3.3 Varmuuskopiot

Yrityksen tulee huolehtia liiketoiminnalleen kriittisten tietojen ja palveluiden varmuuskopioinnista. Yrityksen koosta ja toimialasta riippuen varmuuskopioitavat tiedot vaihtelevat. Perusperiaatteena voidaan pitää sitä, että kaikki sellainen tieto, jolla yrityksen toiminta pysyy käynnissä, on tärkeää, ja se on varmuuskopioitava. Yksittäisen työntekijän kannalta hänen tarvitsemansa yhteystiedot, sovellusten asetukset, työntekijän tekemät dokumentit, työtä varten muokatut ohjeistukset ja vain kyseisen henkilön vastuulla olevien asioiden hoitamiseen tarvittavat tiedot tulee varmuuskopioida. Yrityksen tasolla tulee myös huolehtia tuotantolaitteiden ja liiketoiminnan dokumenttien, kuten tilausten, varmuuskopioinnista.

Varmuuskopiointi kannattaa automatisoida niistä ympäristöistä, joissa se on mahdollista. Puhelimien automaattinen varmuuskopiointi on hankalampaa, mutta siihenkin on joitakin hallintaohjelmistoja. Näiden hallintaohjelmistojen käyttömahdollisuus riippuu osin esimerkiksi siitä, voiko yrityksen tietoja varmuuskopioida pilvipalveluihin. Varmuuskopioinnin tulee olla riittävän säännöllistä, jotta mahdollisen vahingon tapahduttua kopiota on hyödyllistä käyttää ja työntekijällä ei mene turhaa aikaa tietojen korjaamiseen nykytilaa vastaavaksi. Esimerkiksi tilanteessa, jossa työntekijä on kirjoittamassa uutta dokumenttia, varmuuskopiot kannattaa ottaa tuntien, ei päivien, välein. Toisaalta dokumentti, jota päivitetään vain harvoin, tarvitsee varmuuskopiot vain muutosten yhteydessä. Jos tiedot kopioidaan heti tiedoston muuttuessa kahdelle eri fyysiselle laitteelle, tämä helpottaa palautumista esimerkiksi laiterikoista. Yhtenä tekniikkana on peilata tiedot kahdelle tai useammalle levylle esimerkiksi Redundant Array of Indepedent Disks (RAID) -tekniikalla. Sovelluskerroksella voidaan käyttää myös tiedostojen tai muiden kohteiden, kuten tietokantojen, solujen replikointia. Jos yrityksessä on esimerkiksi dokumenttien hallintajärjestelmä, jossa käytetään tietojen replikointia, saadaan sovellustasolla hallittua sitä, mitä tietoa replikoidaan eli kopioidaan ja milloin. Tarkempaa tietoa replikoinnista ja RAID-levyjärjestelmistä on saatavilla Juha Turpeisen [2010] opinnäytetyössä Vikasietoinen virtuaalipalvelinjärjestelmä.

Varmuuskopiointi kannattaa tehdä kahdessa vaiheessa, koska pelkän täydellisen varmuuskopioinnin tekeminen jatkuvasti vie turhaa aikaa. Ensimmäisessä vaiheessa varmuuskopioidaan kaikki laitteen tuotantoon palauttamisen kannalta oleelliset tiedot. Toisessa vaiheessa otetaan talteen vain muutokset ensimmäiseen vaiheeseen ja muut laitteessa olevat tärkeät tiedot. Näitä vaiheita käydään läpi riittävän usein, esimerkiksi

ensimmäistä vaihetta viikoittain ja toista päivittäin. Näiden lisäksi kannattaa mahdollisuuksien mukaan tallentaa muutoksia edeltävät versiot jopa tunneittain. Varmuuskopiointien välinen aika riippuu kopioitavan tiedon kriittisyydestä ja siitä, kuinka usein sitä muokataan. Kriittinen, jatkuvasti muokattu tieto kannattaa varmuuskopioida mahdollisimman usein. Esimerkiksi usean henkilön käyttämä ja muokkaama tieto aiheuttaa kadotessaan useiden tuntien lisätyön, kun yritetään selvittää tehtyjä muutoksia vanhasta varmuuskopiosta alkaen. Harvakseltaan päivitetyn dokumentin osalta riittää, kunhan varmuuskopio on tehty kustakin muutoksesta.

Eri käyttöjärjestelmien ja niissä olevien ohjelmien ja tietojen varmuuskopiointi tehdään helpoiten käyttöjärjestelmän omalla varmuuskopiointiohjelmalla. Windows 7 -järjestelmän osalta alkuun pääsee Microsoftin [Windows 7 varmuuskopiointi 2013] ohjeiden mukaisella tavalla. Applen IOS -ympäristössä helpoin tapa on käyttää Time Machine -sovellusta. Jos tarpeet ovat näitä laajemmat, kannattaa tutustua avoimen lähdekoodin ja kaupallisten toimijoiden tarjoamiin vaihtoehtoihin. Jos esimerkiksi yrityksessä tehdään varmuuskopiointi pilveen tai halutaan suojata kopiot salauksella ja salasanalla, yksikin unohtunut varmuuskopiointi voi tulla kalliiksi, kun lasketaan yhteen menetetty työaika ja menetettyjen tietojen mahdollinen arvo. Muutaman kymmenen euron lisenssimaksu kaupallisesta omiin taitoihin riittävän helppokäyttöisestä tuotteesta on useimmiten kannattava sijoitus.

3.4 Yhteystiedot

Valmistautumisen yhteydessä tulee selvittää liiketoiminnalle kriittisten toimintojen ylläpidon kannalta oleelliset henkilöt ja organisaatiot. Näiden yhteystiedot tulee säilyttää siten, kuin tärkeiden tietojen varmuuskopioita tulee yleensäkin säilyttää. Yhteystiedoissa tulee olla päivitetyt tiedot vähintään seuraavista tahoista:

- laitteiden ylläpidosta vastaavat henkilöt tai organisaatiot
- asiakkaiden tiedot
- yrityksen käytössä olevan Internet-yhteyden ylläpidosta vastaava organisaatio
- tarvittavat viranomaistiedot esimerkiksi kotikunnan poliisi
- maksuliikenteen ylläpitoon tarvittavat yhteystiedot pankkeihin ja luottokorttiyhtiöihin.

Lisäksi yrityksen kannattaa selvittää, mikä taho voisi auttaa mahdollisessa tietoturvan häiriön selvityksessä. Tukea ei välttämättä saa tavanomaisilta yhteystahoilta, mutta useampikin kotimainen yritys, kuten F-Secure tai Nixu, voivat auttaa omien palveluidensa kautta.

3.5 Liiketoiminnan kannalta kriittinen omaisuus

Yrityksen käytössä olevalle liiketoiminnalle kriittinen omaisuus voi olla esimerkiksi laitteita, sovelluksia, henkilöitä, toiminnan kuvauksia ja hinnoittelumalleja. Jos omaisuus on laite tai se on sähköisessä muodossa, tulee se kirjata muistiin ja listausta säilyttää kuten varmuuskopioita. Samoin ainoastaan paperilla olevat tiedot tulee kopioida ja tallentaa siten kuin muutkin varmuuskopiot. Jos yrityksessä on töissä useampia kuin yksi henkilö, tulee liiketoiminnalle kriittisen tiedon olla tarvittaessa muidenkin käytettävissä.

Omaisuuden luettelointiin voi käyttää haluamaansa tapaa, kunhan tapa on sellainen, että se on helposti ylläpidettävissä ja käytettävissä myöhemmin. Sähköisen luettelon lisäksi kannattaa pitää saatavilla myös paperista versiota, josta käyvät ilmi vähintään ne tiedot, joita tarvitaan sähköjen ja muiden yrityksen toiminnalle erityisen kriittisten palveluiden palauttamiseksi, esimerkiksi sähkölaitoksen yhteystiedot ja muiden kriittisten henkilöiden kattavat yhteystiedot.

Pienessä yrityksessä riittää, että kriittiset tiedot ovat listattuna tekstitiedostoon tai taulukkoon, josta on olemassa tarvittaessa paperikopio. Tietoturvallisuuden häiriönhallinnan kannalta dokumentin tärkeimpinä tietoina ovat listalle merkittyjen asioiden alla olevan luettelon mukaiset tiedot:

- haltija
- omistaja
- sijainti
- käyttötarkoitus
- käyttötarkoitukseen käytetyt ohjelmat
- laitteiden tunnisteet (esimerkiksi ip-osoite, mac, malli, nimi ja sarjanumero)

- sovellusversiot (vähintään sillä tasolla, että ympäristö saadaan niiden perusteella pystytettyä).

Suuremmissa yrityksissä tietojen hakuun ja ylläpitoon voi ja kannattaa käyttää erillisiä sovelluksia.

Listauksen omassa verkossa olevista laitteista ja niissä suoraan näkyvistä sovelluksista saa esimerkiksi NMAP-ohjelman [NMAP 2016] seuraavalla pääkäyttäjän oikeuksilla suoritettavalla komennolla:

```
nmap -v -O --osscan-guess -T5 xxx.xxx.xxx.xxx/xx >> nmap-ppkkvv.txt
```

jossa xxx.xxx.xxx.xxx/xx on yrityksen sisäverkon osoiteavaruus esimerkiksi 192.168.1.0/24 (IP-osoitteet ovat tällöin väliltä 192.168.1.0-192.168.1.255) ja nmap-ppkkvv.txt on tiedosto, johon tulokset halutaan. Tiedoston ppkkvv osa korvataan komennon suoritushetken päivämäärällä.

Liitteessä 1 on esimerkki tällaisesta omaisuuslistasta. Omaisuuslista kuvaa muutaman hengen yrityksen sisäisten verkkojen IT-laitteita. Yrityksen varsinaiset tuotantokoneet on hankittu ulkopuolisen toimittajan pilvestä, mutta nekin kannattaa luetteloida. Listaan kannattaa myös lisätä puhelimet ja muut vastaavat laitteet, joilla käsitellään yrityksen viestejä tai kalenterimerkintöjä tai jotka muuten liittyvät oleellisesti yrityksen toimintaan. Vaikka laite olisi työntekijän oma, se kannattaa merkitä luetteloon, jos laitteella käsitellään työpaikan tietoja. Vaikka omaisuuslistaa ei saisikaan täysin kattavaksi, on osittainenkin ajantasainen lista parempi lähtökohta tietoturvallisuuden häiriönhallinnan selvityksessä kuin ei listaa ollenkaan. Listalle kannattaa mahdollisuuksien mukaan kirjata kaikki ne asiat, joilla on vaikutusta yrityksen toimintaan, esimerkiksi mahdolliset varalaitteet, jotka voidaan ottaa käyttöön, ja tieto siitä, kuka vastaa kunkin laitteen hallinnasta. Jos laitteita on enemmän, kannattaa luettelointiin käyttää siihen tarkoitettua sovellusta. Listasta olisi hyvä käydä myös ilmi se, mitä yrityksen tietoja laitteella käsitellään. Tämä auttaa esimerkiksi mahdollisessa varkaustilanteessa arvioimaan, mitä tietoja on voinut kadota.

3.6 Ympäristön ylläpito ja koventaminen

Kun ympäristö on saatu kuvattua, sitä tulee ylläpitää ja tietoturvallisuutta parantaa tavallisten rutiinien yhteydessä. Esimerkiksi työntekijän työkäytössä olevaan Windows-kannettavaan tietokoneeseen pitää asentaa palomuuri ja virustentorjuntaohjelma. Nämä eivät kuitenkaan poista sitä mahdollisuutta, että koneelle jokin haittaohjelma pääsee. Nämä toiminnot kuitenkin helpottavat ylläpitoa ja mahdollistavat tunnettujen ongelmien pitämisen poissa koneelta. Yhtä tärkeää on huolehtia, että kaikki koneessa olevat ohjelmat, kuten käyttöjärjestelmä ja sovellukset lisäosineen, on päivitetty viimeisimpään versioonsa ja tarvittaessa käyttää sellaisia ohjelmia, joissa turvallisuudesta on huolehdittu paremmin.

Jos kyseessä on yrityksen omistama laite, kannattaa sille lisäksi tehdä kovennus (engl. hardening) eli poistaa koneelta kaikki ylimääräiset ohjelmat ja ajurit, joita ei tarvita työntekijän päivittäisissä työtehtävissä. Tarvittavia kokeiluja varten kannattaa olla erillinen kone, jolle ei anneta suoraa pääsyä kriittisimpiin tietoihin. Jos laite on työntekijän oma, tulee tietoturvapolitiikan huomioida omien laitteiden käyttö ja siihen liittyvät velvollisuudet ja rajoitukset. Työntekijältä voidaan esimerkiksi edellyttää koneen tietoturvallista ylläpitoa ja työantajalle mahdollisesti haitallisten sovellusten käyttökiellon noudattamista. Työntekijän oman koneen mahdollisessa vikatilanteessa konetta ei välttämättä voi käyttää työnantajan ympäristössä.

Esimerkkinä koneen vikatilanteesta on tilanne, jossa koneeseen on päässyt jokin haittaohjelma ja sen saastuttama laite aiheuttaa haittaa työantajan ympäristölle. Häiriö voidaan hoitaa siten, että työntekijä ei käytä konettaan ympäristössä ennen haittaohjelman yrityksen tietoturvapolitiikan mukaista poistamista. Tämä voi johtaa myös tilanteeseen, jossa työntekijä joutuu asentamaan koneen käyttöjärjestelmän ja tarvittavat sovellukset uudestaan ennen koneen päästämistä työnantajan ympäristöön. Turhien ohjelmien poistamisella pienennetään ohjelmistohaavoittuvuuksien aiheuttamaa riskiä. Samalla parannetaan vianselvityksen mahdollisuuksia, kun verkossa näkyvä normaalitilanteen liikenne vähenee. Yrityksen on mahdollista hankkia verkkolaitteisiinsa tunnistus, jossa tarkistetaan, voidaanko työntekijän käyttämälle laitteelle sallia pääsy yrityksen verkkoon, ovatko sen ohjelmat ja virustunnisteet ajan tasalla ja mihin verkkoihin laitteelle sallitaan pääsy. Verkon pääsynhallinnan järjestelmät (engl. Network Admission Control NAC) voivat helpottaa verkon hallittavuutta. Kunnolliset ratkaisut maksavat

ja vähemmän kunnolliset myös vievät aikaa, kun laitteiden verkkoyhteydet eivät toimi oletetuilla tavoilla.

Tarkempaa tietoa koventamisesta PK-yrityksen näkökulmasta on saatavilla esimerkiksi Joensuun [2012] opinnäytetyöstä.

Yhtenä osana ympäristön ylläpitoa on sen toiminnan ja turvallisuuden testaaminen. Jos ympäristön palvelut kestävät hyvin niihin kohdistuvan kuorman myös kiireisimpinä aikoina, se riittää yleensä tavallisiin tilanteisiin. Tietoturvatestaamisella kartoitetaan ne epätavallisimmat tilanteet, joissa palvelut eivät enää kestä muuten tavallista kuormaa tai niiden toiminnasta tulee muuten epäluotettavaa. Tietoturvatestaamisella voidaan kartoittaa myös ympäristön haavoittuvuuksia ja muita tietoturvaa vaarantavia heikkouksia, kuten sovellusten huonoja asetuksia. Sovellusten haavoittuvuuksiin ja tietoturvan kannalta huonoihin asetuksiin tutustumisen voi aloittaa OWASP Suomen ylläpitämältä Top 10 2007 Finnish -sivustolta [OWASP 2016] listatuista tyypillisimmistä sovellushaavoittuvuuksista.

3.7 Normaalitilanne

Pienellä yrityksellä voi olla vaikeuksia seurata aktiivisesti ympäristönsä normaalitilannetta. Tunnistamalla ympäristössä käytössä olevat tekniikat ja seuraamalla kriittisimpiä toimintoja voidaan normaalitilanteesta kuitenkin muodostaa kuva. Normaalitilanne voi vaihdella vuorokaudenajasta ja päivästä riippuen, mutta yleisesti ympäristön liikennemäärän pitäisi olla tietyissä rajoissa ja koneiden yhteydet vain tunnistettuihin kohteisiin. Esimerkiksi jos yrityksen henkilökunnasta kukaan ei opiskele tietyssä yliopistossa, sinne ei välttämättä kuuluisi suuntautua liikennettä yrityksen ympäristöstä. Toki erilaiset p2p-yhteyksiä käyttävät ohjelmat esimerkiksi Skype, voivat olla yhteyksissä tuntemattomiin kohteisiin. Jos yrityksessä on tunnistettu yrityksen koneissa työtehtävien hoitoon käytetyt ohjelmat, voidaan niistä johtuva liikenne katsoa normaalitilanteen liikenteeksi. Työntekijän muiden ohjelmien osalta voidaan niiden käytön tarpeellisuudesta työpäivän aikana sopia työntekijän kanssa ja sen perusteella määrittää ne tavanomaiseksi tai muuksi liikenteeksi.

Yrityksellä kannattaa lisäksi olla valmius lokittaa eli tallentaa liikennetiedot omasta verkkoliikenteestä julkisen verkon rajalla ja muissa merkittävissä pisteissä varsinkin

tuotantolaitteiden osalta. Työntekijöiden liikenteen lokittaminen on rajattu Tietoyhteiskuntakaaressa [2014] siten, että yrityksen tulee tehdä ilmoitus tietosuojavaltuutetun toimistolle, jos työntekijöiden yksityisyyden suojaamaa liikennettä lokitetaan ilman häiriötilannetta. Häiriötilanteen selvittämiseksi lokeja saa kerätä ja käyttää häiriönselvityksessä tai poliisille esitutkintaan saattamiseksi. Häiriötilanteen varalta työntekijöiden liikennettä saa siis lokittaa, mutta sitä saa käyttää vain häiriöiden selvittämiseksi.

4 Tietoturvallisuuden häiriöiden havaitseminen

Pienessä yrityksessä ilmoitukset häiriöistä tulevat yleensä ulkopuoliselta taholta. Asiakas voi esimerkiksi kertoa oudosti käyttäytyvästä palvelusta, operaattori voi ilmoittaa haittaohjelmasta yrityksen verkossa tai palveluntoimittaja havaitsee ylläpidon yhteydessä ongelman. Tästä syystä on erityisen tärkeää, että yrityksen yhteystiedoista on olemassa julkisesti saatavilla oleva osoite ja puhelinnumero, joihin tulleisiin yhteydenottoihin reagoidaan kohtuullisessa ajassa.

Jos yrityksellä on omaa osaamista ja resursseja, se voi järjestää teknistä valvontaa omaan ympäristöönsä tai näiden puuttuessa ostaa valvontaa palveluna. Pienellä yrityksellä on harvoin kykyä toteuttaa täysin kattavaa tietoturvatietojen ja tapahtumien hallintajärjestelmää (engl. Security Information and Event Management SIEM). Jos resursseja sen sijaan on, järjestelmiä on saatavilla myös Open Source -toteutuksina, kuten Alienvaultin OSSIM [Alienvault 2016]. Yksi mahdollisuus parantaa omaa kyvykkyyttä häiriöiden havaitsemiseen ja reagointiin on ostaa esimerkiksi tietoturvan tilannekuvaa tarjoava palvelu.

Jos haluaa olla itse aktiivinen osapuoli, kannattaa vähintään eri järjestelmien tuottamia lokeja tallentaa keskitetylle koneelle ja katselmoida niitä säännöllisesti. Lisäksi kannattaa pyrkiä seuraamaan oman verkon kriittisten pisteiden verkkoliikennettä, jotta pystyy arvioimaan, millainen liikenne on tavallista. Laajempaa lokitietojen analysointia kannattaa tehdä automaattisesti SIEM-järjestelmällä. Kun lokitus on kattavaa, tallentuu tapahtumia enemmän, kuin on järkevää käsitellä manuaalisesti. Automaattisella käsittelyllä voidaan myös käynnistää käyttäjien varoittaminen poikkeavasta tilanteesta ja mahdollistaa nopeampi reagoiminen häiriötilanteisiin.

4.1 Ulkopuolelta tulevat ilmoitukset

Pienen yrityksen parhaat mahdollisuudet havaita tietoturvallisuuden häiriöt ympäristössään tulevat ulkopuolisten tahojen kautta. Jos yritys pitää yhteystietonsa saatavilla teleoperaattoreille, muille palveluntarjoajille ja muille tahoille, voidaan pienetkin ilmoitukset kohdentaa paremmin yritykselle. Esimerkiksi CERT-FI toimittaa Autoreporter-järjestelmän [Autoreporter ilmoitukset 2011] kautta tiedon tietoturvallisuuden häiriöstä yrityksen Internet-yhteyttä ylläpitävälle taholle, joka toimittaa ilmoituksen yritykselle. Tiedon saaminen edellyttää, että yhteystiedot ovat kunnossa ja niissä olevia sähköpostiosoitteita seurataan säännöllisesti.

Yksi yleisimmistä ilmoitustyypeistä on ilmoitus yrityksen ympäristöstä tulleesta roskapostista. Ilmoitus voi johtua myös yrityksen oman viestinnän puutteista Todennäköisesti kyseessä on kuitenkin haittaohjelman saastuttama kone, jota käytetään roskapostin välittämiseen. Koska suomalaisilla teleyrityksillä on velvollisuus estää häiriötä aiheuttavan liikenteen pääsy julkiseen verkkoon, pitää näihinkin ilmoituksiin reagoida mahdollisimman pian.

Teleyritysten tarjoamilta sähköpostipalveluilta tulee myös löytyä yhteystiedot häiriöiden raportointia varten. Yleensä nämä yhteystiedot ovat muotoa abuse@teleyritys.xxx. Suurimpien suomalaisten teleyritysten tietoturvallisuuden häiriönhallinnasta vastaavat erilliset asiantuntijat. Pienemmillä toimijoilla työt hoidetaan yleensä muiden töiden ohessa. Suurimmassa osassa muita yrityksiä tietoturvan häiriöistä huolehditaan muiden tehtävien ohella. Näistä syistä yritys ei välttämättä saa heti lisätietoa häiriön selvittämiseksi. Jotain omaa seurantaakin yrityksen kannattaa pitää yllä.

Kannattaa huolehtia, että eri tahoilla on yritykseen toimivat yhteystiedot, esimerkiksi huolehtimalla laskutustietojen ajantasaisuudesta. Lisäksi voi olla hyvä antaa yrityksen sivuilla jokin yhteystieto, jota seurataan säännöllisesti myös tietoturvan häiriöilmoitusten näkökulmasta.

4.2 Oma seuranta

Yrityksen oma seuranta voi olla hyvin pienimuotoista tai hyvinkin laajaa ja käsittää yrityksen ylläpitämiä tietoturvallisuuden tapahtumia ja tilannekuvaa näyttävää järjestel-

mää. Riippuen yrityksen koosta pienimuotoinen seuranta voi tärkeimpien kohteiden tapahtumatietoja ja hälytyksiä. Vähintään haittaohjelmatapahtumien seuraamista, päivitysten tilan seuraamista ja järjestelmien tuottamien lokien seurantaa kannattaa tehdä. Haittaohjelmien tapahtumien seuraaminen voi käsittää keskitetyn automatisoidun järjestelmän käyttämistä samalta toimittajalta kuin käytössä olevat virustorjunnan sovellukset. Vaihtoehtoisesti käyttäjät ohjeistetaan ilmoittamaan tietyn kriittisyyden ylittävistä havainnoista keskitettyyn pisteeseen. Päivitysten tilan seurannan osalta eri toimittajilla on saatavilla erilaisia ratkaisuja päivitysten seurantaan ja automaattiseen asennukseen. Toisaalta käyttäjät voidaan velvoittaa ylläpitämään käyttämiään laitteita ja seuraamaan niihin saatavia päivityksiä.

Lokien seurantaa on hyvä tehdä vähintään tietyin väliajoin, jotta omasta ympäristöstä syntyy oletetusta normaalitilanteesta kuva. Normaalitilannetta voi sitten verrata tilanteeseen, jossa tiedetään olevan häiriöitä. Sama pätee verkkoliikenteen seurantaan, jotta saadaan kuva oletetusta normaalitilanteesta mahdollisia häiriötilanteita varten. Tilannetta, jossa ei ole tiedossa olevaa häiriötä, voidaan pitää normaalitilanteena. Ympäristössä voi kuitenkin olla häiriö, mutta sen liikenne ei erotu riittävästi normaalista tilanteesta. Haittaohjelmien torjunta ei välttämättä ole saanut tarvittavia tietoja uusimman haittaohjelman tunnistamiseksi, häiriö on luonteeltaan sellainen, että haittaohjelmien torjunta ei siihen reagoi tai jostain muusta syystä käynnissä olevaa häiriötilannetta ei pystytä havaitsemaan. Lokien hallintaan on erilaisia sovelluksia, kuten esimerkiksi LOGalyze, Graylog tai Fluentd riippuen omasta ympäristöstä [LOGalyze 2016; Graylog 2016; Fluent 2016].

4.3 Ilmoituksen ja seurannan yhdistäminen

Paras tapa tietoturvallisuuden häiriöiden havaitsemiseksi on yhdistää omat havainnot ulkopuolelta tulevaan tietoon. Esimerkkinä voidaan mainita tilanne, jossa työntekijä ilmoittaa, että hänen koneeltaan on haittaohjelman torjunta poistanut tietyn haittaohjelman, mutta koneen käyttämä ip-osoite ei vastaa teleoperaattorilta tulleen ilmoituksen tunnisteita. Tällöin voidaan verrata ilmoitusten haittaohjelman kuvausta, jos toisessa koneessa olisi sama haittaohjelma. Tässä tapauksessa kummatkin ilmoitukset koskevat samaa häiriötä, jonka vakavuutta voidaan pitää yksittäiseen tapaukseen nähden korkeampana. Ilmoittaneen työntekijän laitteessa oleva haittaohjelma on voinut tulla toiselta työntekijältä esimerkiksi muistitikun välityksellä, koska tikun antaneen työnteki-

jän koneen virustunnisteet eivät ole olleet päivitettyjä. Helpointa seurannan yhdistäminen on, jos saapuvien ilmoitusten käsittelyyn käytetään jotain yrityksen muutenkin työnohjauksessaan käyttämää järjestelmää. Periaatteessa tietoturvan häiriöidenhallintaan varatut sähköpostiosoitteet riittävät, mutta erilaiset tikettien ja tapahtumien hallintaan käytettävät järjestelmät helpottavat varsinkin asioiden yhdistelyä ja aiempien tapahtumien selaamista.

5 Tietoturvallisuuden häiriöihin reagointi

Tietoturvallisuuden häiriöihin reagoidaan lähtökohtaisesti samalla tavalla kuin mihin tahansa tietotekniikan tai ympäristön häiriöön. Tapahtumat (engl. event) ja hälytykset (engl. alert) käsitellään esimerkiksi ITIL v3 -mallin mukaisesti ja häiriönhallinnan prosessista tulevat häiriöt (engl. incident) hoidetaan ohjeiden mukaisesti.

Käytännössä esimerkiksi yritykseen sähköpostiin tullut ilmoitus teleoperaattorilta yrityksen verkosta lähtevästä roskapostista tarkoittaa todennäköisesti, että joko yrityksen käyttämä tietokone on haittaohjelman saastuttama tai yrityksen markkinointia tehdään lähettämällä roskapostiksi tulkittavia viestejä niille, jotka eivät ole kyseisiä viestejä halunneet. Kummassakin tapauksessa teleoperaattori voi esimerkiksi rajoittaa yrityksen Internet-yhteyttä, mikä sitten estää yrityksen operatiivisen toiminnan.

5.1 Häiriön tunnistaminen

Teleoperaattorilta tai muualta tulleen viestin mukana on yleensä lähettävän koneen tunnistamisen aloittamiseen tarvittavat tiedot. Joko niistä näkee suoraan lähettävän koneen tai ne kertovat yrityksen palomuurin tai vastaavan verkkolaitteen julkisen osoitteen. Jos tarjolla on vain verkkolaitteen osoite ja viestistä ei muuten käy ilmi lähettävää konetta, pitää koneen selvittämiseksi tehdä jatkotoimia. Mahdollisesti tarvittavista jatkotoimien vuoksi olisi hyvä, että myös palomuurista ulospäin suuntautuvaa liikennettä lokitettaisiin. Jos tähän ei ole mahdollisuutta kaikissa tilanteissa, tulisi ainakin lokitus valmistella siten, että sen saa tarpeen vaatiessa viipymättä päälle. Käytettävissä olevien mahdollisuuksien mukaan omaa havainnointikykyä ympäristön tapahtumiin kannattaa kehittää seuraamalla verkkonsa tapahtumia toisaalta Internetiin päin ja toisaalta verkon sisällä.

5.2 Häiriötä aiheuttavan laitteen tunnistaminen

Jos häiriö aiheuttaa verkkoon liikaa kuormaa, on häiriö yleensä pienessä ympäristössä helpoimmin poistamalla yksittäisiä koneita verkosta ja testaamalla tämän jälkeen verkon toimivuutta. Jos ympäristö on hyvin pieni, ei erilliselle lokitukselle välttämättä ole tarvetta. Sellaiseen verkkoliikennetietoon, jota saadaan katsomalla suoraan yksittäisen tietokoneen verkkoliikennettä, ei voi täysin luottaa. Esimerkiksi haittaohjelma voi muuttaa käyttäjän näkemää tietoa piilottamalla yhteyksiä tai uudelleen nimeämällä verkkoliikenteen tunnisteita vähemmän epäilyä herättävään muotoon.

Jos häiriön takia useampi kone kuormittaa verkkoa, ei yksittäisen koneen poistaminen verkosta ratkaise ongelmaa. Tällöin organisaatioissa voidaan yrittää seurata verkon liikennettä kopioimalla liikenne joko suoraan reitittimestä tai kytkemällä verkkoon porttitoistin. Seuraavaksi kopioitu liikenne ohjataan seurantaa tekevälle työasemalle. Tämä työasema kannattaa asentaa valmiiksi, ja sitä ei kannata käyttää Internetissä sivujen selailuun tai muuhun toimintaan. Tietokone kannattaa myös koventaa [Valtionarainministeriö 2008: 160] mahdollisuuksien mukaan, ja se kannattaa pitää päivitettynä. Koska haittaohjelman saastuttaman koneen kertomaan verkkoliikenteeseen ei pysty luottamaan, tulee koneen näyttämään verkkoliikenteeseen suhtautua varauksella. Se voi kertoa häiriön aiheuttaman ohjelman, mutta joskus haittaohjelma on voinut piilottaa liikenteen myös pääkäyttäjän näkyviltä. Tällöin ainoa mahdollisuus on tallentaa koneen verkkoliikenne aiemmin kuvatun mukaisesti.

Jos kuorma ei ole poikkeuksellisen suurta, voi häiriön aiheuttavaa konetta selvittää verkkoliikennettä tarkkailemalla. Esimerkiksi mikäli aiempi tiedonkeruu on tehty ja nykytilanteessa esiintyy siihen verrattuna poikkeamia, ne voivat liittyä haittaohjelman aiheuttamaan liikenteeseen command & control -palvelimille. Jos ei ole mahdollisuutta seurata verkkoliikennettä epäillyn koneen ja internet-yhteyttä tarjoavan reitittimen väliltä, voi koneen verkkoliikenteestä saada jotain selville komentorivin `netstat`-komennolla tai vastaavilla työkaluilla. Microsoftin työkalupaketti Sysinternals Suiten [Technet 2011] sisältämä TCPview on visuaalisempi versio `netstat`-komennolla saatavista tiedoista. Komentojen ajamisessa kannattaa jättää IP-osoitteiden nimipalvelutiedot hakematta ainakin yhdellä kertaa. Tämä siitä syystä, että nimipalvelutiedot voivat muuttua lyhyessäkin ajassa ja haitata myöhempää tutkimista, mutta ip-osoitteesta on yleensä tarjolla historiatietoja.

Käyttäjä saa komentorivin esille Windowsin ”etsi tiedosto” -kohdasta kirjoittamalla ”cmd”. Cmd käynnistetään klikkaamalla hiiren oikeaa näppäintä ja valitsemalla komennon suorittaminen pääkäyttäjätunnuksin (run as administrator). Komento ”netstat –nab” näyttää kaikki verkkoyhteydet, osoitteet numeerisessa muodossa ja yhteyttä käyttävät prosessit. Koska komennon suorittaminen antaa vain otoksen tietyn hetken liikenteestä, ei sen avulla saada selville otoksen ulkopuolelle ajoittuvia yhteyksiä tai sellaisia yhteyksiä, joiden liikenne on hyvin vähäistä.

Jos tietoturvahäiriöstä aiotaan tehdä tutkintapyyntö poliisille, tulee selvityksen vaiheet kirjata muistiin ja tallentaa myös suoritetut komennot, niillä kerätyt tulosteet ja havaittu verkkoliikenne. Selvityksen vaiheet kannattaa muutenkin kirjata muistiin, jotta toiminnasta jää jotain kirjanpitoa, jota voi myöhemmin käyttää toiminnan kehittämisen lähtökohtana. Jos koneesta katkaisee virran ennen tietojen keräämistä, todennäköisesti ainakin osa mahdollisista todisteista tuhoutuu. Tämä johtuu siitä, että haittaohjelmat ovat yhä useammin vain koneen muistissa. Ne eivät siten kirjoita mitään itsestään kiintolevylle, joten sähkön katkaisu kadottaa haittaohjelman, mutta ei kerro, mitä tietoja yritykseltä on mahdollisesti viety tai miten koneeseen on tultu sisään.

5.3 Häiriön rajaaminen

Kun häiriötä aiheuttava kone tai koneet on saatu rajattua tiettyyn ympäristöön tai varmuudella selville, voidaan häiriön aiheuttamaa riskiä tietoturvallisuudelle ruveta pienentämään. Jos kyseessä on yksittäinen työasema, jolla ei ole yksinään suurta merkitystä päivittäiseen tuotantoon, on helpointa asentaa se puhtaaksi tiedetyistä varmuuskopioista kokonaan uudelleen. Jos kyseessä on tuotannon kannalta kriittinen laite, on häiriön rajaaminen hankalampaa. Jos on käytettävissä edes pääosin samantasoinen varakone, kannattaa häiriön saanut kone poistaa tuotannosta, tarkistaa varakoneen mahdolliset päivitykset ja korvata sillä häiriön saanut kone. Tämän jälkeen voidaan tarkemmin tutkia, mikä häiriön on aiheuttanut. Jos häiriön juurisyytä eli varsinaista aiheuttajaa tai aiheuttajia ei saada selville, on riskinä, että tapaus uudistuu tai sitä ei oikeasti edes saada korjattua.

5.4 Häiriön korjaus

Tietoturvallisuuden häiriön korjauksessa on käytännössä kaksi tapaa. Ensimmäisessä voidaan vain poistaa ongelma miettimättä juurisyytä. Toisessa häiriön juurisyy selvitetään ja korjataan. Aina juurisyyn selvittäminen ei ole tarpeellista tai taloudellisesti järkevää tai Suomen lainsäädäntö rajoittaa sitä. Tällöin häiriön aiheuttanut kone joudutaan vain asentamaan uudelleen ja päivittämän mahdollisuuksien mukaan tietoturvallisemmaksi.

Suositeltavaa on, mikäli mahdollista, että häiriön juurisyy selvitetään palvelimilta ja muilta tuotannon kannalta kriittisiltä laitteilta, jotta häiriötä ei joutuisi korjaamaan uudestaan. Suomen lakien [Tietoyhteiskuntakaari 2014] mukaan vikatilanteen ja tietoturvan häiriön saa selvittää, mutta esimerkiksi selvityksessä paljastuneita henkilön yksityisyyttä työelämässä vaarantavia tietoja ei saa käsitellä tarpeettomasti. Esimerkiksi jos yksittäinen henkilö on käynyt työkoneellaan sivustolla, joka sisälsi haittaohjelman, tulee ongelmasta kertoa kaikille työntekijöille yleisellä tasolla ilman tarkkoja yksityiskohtia ja työntekijöiden pääsyä eri verkkosivuille rajoittaa jatkossa kaikkien käyttäjien osalta ilma, että rajaus kohdistettaisiin yksittäisiin henkilöihin. Jos herää epävarmuutta siitä, miten pitkälle asiaa saa itse tutkia, kannattaa tutkinta keskeyttää ja pyytää päätökseen tukea sopivalta taholta. Näitä tahoja voivat olla esimerkiksi tietoturvapalveluita myyvät konsulttitalot tai tietoturvallisuutta työelämässä ymmärtävät lakitoimistot.

Ensin pitää varmistaa, että häiriön juurisyyn selvitystä voi Suomen lakeja rikkomatta jatkaa. Sen jälkeiset käytännön toimet, joilla häiriö voidaan selvittää, riippuvat tapauksen ominaispiirteistä ja käytettävissä olevista resursseista. Jos kyseessä on jonkin haittaohjelman tartuttama yksittäinen kone, kannattaa siitä selvittää vain se, mikä on voinut olla syynä haittaohjelman saamiselle. Jos syyksi selviää koneen päivittämättömyys, kannattaa kaikki oman ympäristön koneet tarkistaa päivitystarpeiden osalta ja päivittää ne hallitusti.

Jos puuttuvat päivitykset eivät olleet syynä häiriöön tai päivityksiä ei ole mahdollista asentaa, tulee konetta suojata jatkossa paremmin. Tällöin tulee vähintään miettiä käytössä olevien palomuurien asetuksien tiukentamista tai korvaamista sellaisella, jossa asetuksia voi paremmin säätää. Esimerkiksi yrityksen levypalvelimelle ei kannata avata suoraa pääsyä julkisesta verkosta. Jos pääsyn salliminen on välttämätöntä, tulee yhteys toteuttaa jonkin hyppykoneen kautta. Samoin oman verkon turhat palvelut kannattaa

ottaa pois käytöstä, kuten laitteiden ja ohjelmien hallintayhteydet julkisen verkon puolelta, jos niihin ei ole käytännössä tarvetta tai niitä ei ole kukaan käyttänyt pitkään aikaan.

Jos haittaohjelma on päässyt pääkäyttäjän oikeuksia vaativiin tiedostoihin, voi olla varmempaa asentaa koko kone uudestaan kuin yrittää korjata tilannetta eri virustorjuntaohjelmilla. Virustorjuntaohjelmat eivät aina tunnista varsinkaan uudempia haittaohjelmien versioita. Tällöin on riskinä, että koneeseen jää vielä joitain haittaohjelmia, jotka jatkavat toimintaansa koneen palattua tuotantoon.

6 Tietoturvallisuuden häiriönhallinnan kehittäminen

Tietoturvallisuuden häiriönhallinnan kehittämiseen tarvittavat tiedot tulevat häiriönhallinnan aiemmista vaiheista, joista oppimalla voidaan reagointia vanhoihin ja uusiin uhkiin parantaa. Kehittämiseen on useampiakin eri tapoja, ja niihin perehdytään seuraavaksi.

6.1 SANS-malli

Sansin [Kral 2012: 9] mallin mukaan alkuun pääsee löytämällä vastaukset seuraaviin kuuteen kohtaan ja parantamalla niiden kautta toimintaa:

- Milloin ongelma havaittiin ensimmäisen kerran ja kuka sen havaitsi?
- Mikä on häiriön kohde?
- Miten häiriö rajattiin ja poistettiin?
- Miten palautuminen tilanteesta hoidettiin?
- Missä onnistuttiin?
- Mitkä alueet tarvitsevat parantamista?

Sansin malli toimii hyvänä pohjana tapauksissa, joissa häiriön rajaus ja poisto tehtiin viiveellä eli tilanteissa, joissa häiriö oli ollut ympäristössä jo kauan ja kyseessä oli lähinnä jälkien siivoaminen ja siivoamista oppiminen. Malli toimii myös seuraavan mallin kohdalla, kun käsitellään useampaa kyseisen mallin käyttökertaa.

6.2 OODA-silmukka

Jos yrityksen toiminta on ketterää ja häiriönhallintaan pystyään panostamaan, kannattaa kehityksessäkin noudattaa HTPT-silmukkaa (engl. OODA-loop). Tässä mallissa siis

- havainnoidaan
- tilanne arvioidaan
- päätetään
- toimitaan päätöksen mukaan.

Kierros aloitetaan alusta korjaten toimintaa havaitun vaikutuksen mukaan. OODA on John Boydin [Mindtools 2016] Korean sodassa keksimä malli. Kuten Frode Hommedal [2015] kuvaa esityksessään, mallista on hyötyä myös tietoturvan häiriönhallinnassa. Malli mahdollistaa nopeampien ja parempien päätösten tekemisen ja kehittämisen tarkemman kohdentamisen. Vaikka pääsääntönä onkin, että silmukka pitää läpäistä nopeasti, varsinkaan pienellä yrityksellä ei ole varaa tehdä monia perättäisiä huonoja päätöksiä käytettävissä olevien resurssien vähyyden vuoksi. Toiminnan kehittämisen kannalta eri vaiheista pidetään kirjaa ja pohditaan kehittämisessä päätösten hyvyyttä suhteessa saatavilla olleeseen tietoon uhasta ja oman ympäristön riskeistä. Käytännössä silmukan käyttö ohjaa välittömään kehittämiseen ja kirjanpidon kautta mahdollistaa paremman tapahtumien läpikäynnin.

Karuimmillaan kaikkia kierroksen vaiheita tehdään puutteellisista lähtökohdista esimerkiksi arvioimalla väärin hyökkäyksen varsinainen kohde. Silmukan useammalla kierrolla pyritään saatuja tietoja ja oppeja hyödyntämällä saamaan yksittäiseen häiriöön kuitenkin kunnollinen ratkaisu.

6.3 Kehittämisen kohteet

Pienellä yrityksellä, joilla ei ole aiempaa kokemusta laajemmasta tietoturvan häiriönhallinnasta, on rajallinen määrä kehityskohteita. Esimerkiksi hyökkääjän tarkka tunnistaminen on isoillekin toimijoille hankalaa. Toisaalta omien tietolähteiden parempi tunnistaminen on pitkälti vain itsestä kiinni. Kun tuntee ne kauttaaltaan, pystyy paremmin kehittämään niihin kohdistuvien hyökkäysten ennakointia ja havaitsemista. Kehittämi-

sen kohteina voidaan karkeasti pitää seuraavia: vastustajan tunnistaminen, tunkeutumisyritysten tunnistaminen, hyökkäysrajapinnan tunnistaminen, oma kyvykkyys havaita ja kerätä talteen ympäristössä tapahtuneita muutoksia, oma kyvykkyys havaita hyökkäys ja oma kyvykkyys vastata hyökkäykseen.

Vastustajan tunnistaminen

Vaikka varsinaisen vastustajan tunnistaminen on hankalaa, voi sitäkin kehittää miettimällä, kuka voisi haluta vahingoittaa yritystä tahallaan, ansaintamielessä tai vain käyttääkseen yrityksen resursseja omiin tarkoituksiinsa. Tällöin pystyy paremmin arvioimaan, mihin kohteisiin hyökkäys voisi kohdistua tai mitä sillä yritetään saavuttaa.

Tunkeutumisyritysten tunnistaminen

Jotta pystyisi tunnistamaan hyökkäyksen tunkeutumistapoja, pitäisi pystyä arvioimaan, mitä hyökkääjä haluaa saavuttaa ja mitä kautta hän aikoo sen saavuttaa. Näin pystyttäisiin arvioimaan ne omien palveluiden kohdat, joihin hyökkääjä saattaa kohdistaa toimensa, tai ainakin, mitkä tiedot tai resurssit olisivat hyökkäyksen varsinaisena tavoitteena. Kehittämisen kannalta on oleellista miettiä, miten noihin kohteisiin voisi päästä käsiksi ja miten saatavilla olevan tiedon perusteella se voisi onnistua. Jos yritys pystyy kehittämään näiden kohteiden valvontaa, voidaan hyökkäykset havaita nopeammin ja pystytään keskittymään varsinaisen kohteen suojaamiseen.

Hyökkäysrajapinnan tunnistaminen

Kun tuntee omat ympäristönsä, pystyy paremmin kehittämään sitä, miten niitä voisi suojella ja hyökkäysrajapintaa siten pienentää. On hyökkäysrajapintana sitten yrityksen verkkosivusto, jotta sen takana oleviin asiakastietoihin päästäisiin käsiksi, tai sähköpostin mukanaan tuomat haittaohjelmat, jotta käyttäjän kone saadaan kaapattua hyökkääjän käyttöön. Kummassakin tapauksessa on yleensä kyseessä joku haavoittuvuus, jota hyödyntämällä kohteena olevaan koneeseen pystyy hyökkäämään. Verkkosivusto voi olla tehty Wordpress -julkaisujärjestelmällä ja viimeisiä päivityksiä ei ole vielä asennettu. Työaseman osalta voi riittää, että käyttäjä saadaan klikkaamaan viestissä olevaa linkkiä, josta käyttäjän koneelle asentuu haittaohjelma vain käymällä kyseisellä verkkosivulla.

Oma kyvykkyys havaita ja kerätä talteen ympäristössä tapahtuneita muutoksia

Jos pystyy kehittämään omaa kyvykkyyttään havaita ympäristön muutoksia ja tunnistaa, mitkä niistä ovat normaaleja, pystyy paremmin tunnistamaan myös hyökkäykset. Jos tavallisesta toiminnasta jää jotain lokeja ja muita tunnisteita, pystytään paremmin arvioimaan, miten niitä voisi hyödyntää myös hyökkäyksen tunnistamisessa. Kyvykkyyttä voi parantaa kehittämällä palveluiden seurantaa joko yrityksen omilla voimilla tai ostamalla se palveluna. Esimerkiksi oman verkkosivun säännöllinen tarkistus auttaa havaitsemaan siihen kohdistuneet ulkopuoliset muutokset ja mahdolliset päivitystarpeet.

Oma kyvykkyys havaita hyökkäys

Jos yritys ei jostain syystä käytä virustorjuntaa koneissaan ja sähköposteissaan, sen kyvykkyys havaita mitään hyökkäyksiä jää hyvin pieneksi. Mikäli yrityksen tärkeät tiedot ovat ylläpidettyjen palomuurien takana, auttavat nekin hyökkäyksen torjunnassa. Näiden perusosien jälkeen voi sitten miettiä, miten muuten omaa kyvykkyyttä voi parantaa eri hyökkäystapojen osalta. Esimerkiksi olivatko omat yhteystiedot helposti muiden saatavilla ja seurataanko niihin tulevia viestejä riittävän säännöllisesti? Kannattaa myös arvioida, olisiko henkilökunnan koulutuksella voinut saavuttaa parannusta hyökkäyksen havaitsemiseen.

Oma kyvykkyys vastata hyökkäykseen

Vaikka vastustajan tunnistaminen jää usein saavuttamatta, jossain vaiheessa hyökkäys kuitenkin havaitaan ja voidaan aloittaa vastatoimet. Jos oma kyvykkyys jää koneiden uudelleenasennuksen asteelle, on seuraava hyökkäys vain ajan kysymys. Yrityksen pitää päästä tilanteeseen, jossa se pystyy löytämään hyökkääjän jäljet ja varsinaisen kohteen. Aina tämä ei ole mahdollista. Kehittämistoimina voi olla esimerkiksi eri laitteiden parempi eriyttäminen varsinkin mahdollisen hyökkäyksen rajaamiseksi.

Viime kädessä omaa kyvykkyyttä vastata tietoturvan häiriöön parhaiten kuvaava mittari on se nopeus, jolla liiketoiminta saadaan jatkumaan tavanomaisena. Kehitystoimet kannattaa kohdentaa myös varmuuskopioiden käsittelyyn, varalaitteisiin ja mahdolliseen verkkosivustoon, jotta liiketoiminnan häiriö pysyy mahdollisimman lyhytaikaisena.

7 Tietoturvallisuuden häiriönhallinnan ylläpitäminen

Käytännössä häiriönhallinnan ylläpitäminen on sitä, että toimitaan luotujen ohjeiden mukaisesti ja tapahtumista otetaan opiksi, kehitetään kykyä varautua ja reagoida uusiin uhkiin ja niistä syntyviin riskeihin. Lisäksi ylläpidetään tietoa tärkeiden tietojen sijainnista ja niiden tietovuoista sekä huolehditaan niiden riittävän tiheästä varmuuskopioinnista.

7.1 Ylläpidon aikataulu

Ylläpidon aikataulutuksessa voidaan hyödyntää esimerkiksi yrityksen mahdollisesti muutenkin säännönmukaisiin toimiin hyödyntämää vuosikelloa tai muuta säännönmukaista määrittelyä. Mitä enemmän näitä tekemisiä saa automatisoitua (esim. varmuuskopioiden säännöllinen tekeminen vähintään joka viikko), sen parempi. Jos yritykseen kohdistuu paljon tietoturvallisuuden häiriöitä, ei yleisimpiä häiriötyyppejä tarvitse erikseen harjoitella – edellyttäen, että häiriöistä opitaan ja tehdään tarvittavat kehitystoimet esimerkiksi OODA-silmukan kautta. Laajempia ja vakavampia tapauksia kannattaa silti harjoitella, jotta mahdolliset ongelmakohdat esimerkiksi ylläpidon rutiineissa saadaan tunnistettua.

7.2 Päivitysten hallinta

Toisaalta voidaan puhua haavoittuvuuksien hallinnasta ja toisaalta päivitysten hallinnasta. Jälkimmäisen voi yleensä automatisoida. Ensimmäisen osalta voi joutua tekemään merkittäviäkin muutoksia omaan ympäristöönsä, jotta haavoittuvuudet, joihin ei ole korjaavaa päivitystä saatavilla, saadaan hallintaan. Kun PK-yrityksissä mietitään, miten päivitysten hallintaa tulisi ylläpitää, kannattaa tutustua saatavilla oleviin kypsyysmalleihin, kuten esimerkiksi Core Securityn Threat & Vulnerabilityh Management Maturity Model TVM [Core Security 2014]. Jos yritys skannaa omia palveluitaan haavoittuvuuksien havaitsemiseksi ja päivittää puuttuvat päivitykset, saavutetaan mallin taso 1. Mitä enemmän hallintaa tehdään riskien arvioinnin kautta ja hyödynnetään uhka-arviointeja, sitä kypsemmälle tasolle mallissa päästään. Vaikka alussa työmäärä kasvaakin, kypsempi toimintatapa helpottaa toimintaa jatkossa, kun pystytään tekemään parempia päätöksiä.

Toisin sanoen ylläpidossa pitää seurata omaa ympäristöä koskevia haavoittuvuusilmoituksia ja jollain keinolla tarkistaa, koskevatko ilmoitukset oikeasti omia laitteita ja sovelluksia myös versioiden ja ilmoitettujen asetusten osalta. Tämän perusteella tulee arvioida haavoittuvuudesta syntyvä uhka, sen tuomat mahdolliset hyökkäykset ja näiden perusteella omiin palveluihin kohdistuva riski. Jos riskiarvion perusteella päivitys ei ole välttämätön tai mahdollinen juuri nyt, niin päivityksen voi jättää asentamatta. Muussa tapauksessa tai jos ei ole varma omasta riskiarviostaan, tulee päivitykset asentaa.

Jos yrityksen työasemissa ei ole mitään erityisiä asennuksia, on hyvä laittaa suurin osa työasemien päivityksistä automaattisiksi. Tähän on useita eri työkaluja esimerkiksi Secunialla, jonka Flexera osti syksyllä 2015, ja sen ilmaisella PSI [Flexera PSI 2016] tuotteella, joilla voi tarkistaa, onko jotain jäänyt päivittämättä. Muilla kaupallisilla tuotteilla voi huolehtia laajemminkin haavoittuvuuksien hallinnasta ja siihen liittyvien riskien arvioinnista. Osa haittaohjelmien torjuntaa tekevien sovellustoimittajien ohjelmistoista tarjoaa tähän myös tukea, joko omien sovellustensa lisäosana tai omina sovelluksinaan. Jos yrityksen käyttämissä ohjelmissa on erityisiä ominaisuuksia tai halutaan olla varma päivitysten toimivuudesta, kannattaa vähintään yksi kone jättää manuaalisesti päivitettäväksi tai viivästyttää sen päivitystä muihin verrattuna. Tällä varmistutaan siitä, että toimintakyky säilyy, vaikka koneen päivitys ei onnistuisikaan. Toki tällöin pitää myös huomioida, että kyseisessä koneessa ei ole niitä viimeisimpiä päivityksiä asennettuna.

7.3 Varmuuskopiointi

Varmuuskopioinnissa kannattaa miettiä levypalvelimen käyttämistä varmuuskopioitujen tietojen tallentamiseen erityisesti silloin, kun varmistettavia laitteita on enemmän. Myös levypalvelimesta tulee ottaa säännölliset varmuuskopiot ja säilyttää niitä mielellään eri fyysisessä paikassa kuin tietoja, joita siihen on varmuuskopioitu. Yksittäisten työasemien tärkeiden tietojen varmuuskopiointiin riittää mikä tahansa tallennusväline, johon tiedot mahtuvat. Automatisoitu varmuuskopiointi levypalvelimelle poistaa unohtamisen tuomat ongelmat.

Vuodesta 2014 alkaen ja erityisesti vuoden 2015 alusta lähtien eräs haittaohjelmaperhe on kasvattanut toimivan varmuuskopioinnin merkitystä. Erilaiset versiot Ransomware-haittaohjelmista salaavat käyttäjän tiedostot ja vaativat niistä lunnaita. Jos tämän tyylinen haittaohjelma saa koneen tiedot haltuunsa, ainoa suositeltava toimenpide on

koneen uudelleenasennus ja palautus varmuuskopioilta. Ennen koneen ottamista takaisin käyttöön pitää varmistaa, että sen päivitysten puutteellisuus ei ollut tartunnan syynä. Tästä haittaohjelmaperheestä vuoksi varmuuskopioita kannattaa tallentaa myös muualle kuin yrityksen verkkoon. Jos haittaohjelma salaa kaikki tiedostot, joihin se pääsee käyttäjän oikeuksilla käsiksi, salataan myös ne varmuuskopiot, jotka ovat koneeseen kytketyssä usb-asemassa tai verkossa saatavilla.

7.4 Haittaohjelmien torjunta

Koska haittaohjelmatartunta on tyypillisin pienen yrityksen kokema tietotuvan häiriö, kannattaa sen hoitamista harjoitella ja samalla varmistaa varmuuskopioiden toimivuus ja muiden tarvittavien ohjelmistojen saatavuus. Kannattaa esimerkiksi harjoitella, mitä tapahtuu, kun työntekijän työasemalle tulee virustartunta eikä olla enää varmoja siitä, toimiiko virustorjunta. Sama harjoitus kannattaa toistaa myös palvelimen ja mahdollisen yrityksen verkkosivuston osalta. Jos yrityksen oma kotisivu on kaapattu haittaohjelmien välittämiseen tai haittaohjelmat tarttuvat yrityksen sivujen näyttämien mainosten kautta, sivuilla vierailevat käyttäjät saastuttavat omat koneensa ja yrityksen maine kärsii. Tämän harjoituksen yhtenä pääkohtana on, miten tapahtumasta viestitään ja miten sillä saadaan palautettua yrityksen maine.

7.5 Henkilöstön kouluttaminen

Varsinkin EU:n tulevan tietosuoja-asetuksen takia yrityksen oman henkilöstön ja esimerkiksi yrityksen alihankkijoiden henkilöstön kouluttamisen tärkeys korostuu. Henkilöstön pitää tunnistaa esimerkiksi se, mitkä tiedot ovat yritykselle tärkeitä, mihin henkilötiedot on tallennettu ja miten suhtautua erilaisiin huijausyrityksiin.

Jos yritys tekee itse sovelluksia tai ylläpitää omia kotisivujaan, tulee sillä olla osaamista myös näiden alueiden turvallisesta kehityksestä. Jos koulutukseen ei ole omaa osaamista, kannattaa osaamista kehittää kursseilla, oppilaitoksissa tehtävänä opiskeluna tai alan seminaareissa. Useampikin suomalainen tietoturvallisuuden parissa työskentelevä yritys myös kouluttaa tarvittaessa.

Henkilökunnan kanssa tulee vähintäänkin käydä läpi havaitut poikkeamat ja niistä opitut asiat. Miten tilanne olisi voitu välttää ja miten siitä toipumista voitaisiin nopeuttaa? Varsinkin mahdollisten phishing-viestien osalta kannattaa painottaa, miten niihin tulee suhtautua ja miten sellaiset voi erottaa oikeista viesteistä.

Perustietoa suomeksi saa Viestintäviraston NCSA:n [2016] sivuilta. Lisäksi on tarjolla tietoturvayritysten blogeja, kuten Nixun [2016] ja KPMG:n [2016]. Näistä saa pohjan, jonka perusteella voi sitten miettiä, millaista koulutusta yrityksen työntekijät tarvitsevat ja mistä sitä voisi saada. Lisäksi kannattaa seurata Tietoturva ry:n [2016] sivuja, joista saadakseen tietoa esimerkiksi tapahtumista, kursseista ja seminaareista.

8 Johtopäätökset

Tietoturvan häiriönhallinnassa tärkeintä on säilyttää maltti ja tuntea oman ympäristönsä kriittiset järjestelmät ja toiminnan kannalta kriittinen tieto. Kunhan tilanteeseen on valmistautunut esimerkiksi harjoittelemalla mahdollisia tilanteita omien kykyjensä ja käytettävissä olevien resurssien mukaisesti, on niistä yleensä mahdollista selvitä ilman merkittävää pitkäaikaista vahinkoa yritykselle. Ensimmäisessä vaiheessa on hyvä harjoitella jälkien siivoamista eli sitä miten tietoturvan häiriöstä, kuten haittaohjelmatartunnasta, toivutaan esimerkiksi palauttamalla kone varmuuskopioista ja tarkistamalla sen päivitysten ajantasaisuus. Jatkossa harjoittelua voi sitten kohdentaa myös hyökkäysten havainnointiin ja oman torjuntakyvyn parantamiseen. Tärkeää on huolehtia ihmistä, varmuuskopioiden toimivuudesta ja suojella omalle liiketoiminnalle tärkeää tietoa. Kaikki muu, kuten palvelimet, sovellukset ja verkkolaitteet, pystytään vielä rakentamaan uudestaan jälkikäteen.

Kehittämällä oman toimintansa kypsyyttä ja muokkaamalla esimerkiksi OODA-silmukasta omaan käyttöön sopiva tapa reagoida häiriöihin saadaan yritykselle toimivat käytännöt hallita tietoturvan häiriöitä. Kun yrityksen käytännöt toimivat, voidaan paremmin huolehtia henkilöstön jaksamisesta ja heidän reagointikykynsä pidetään kunnossa. Oman organisaation kykyä seurata sen ympäristön palveluihin kohdistuneita uhkia ja muutoksia tulee kehittää ja varautua myös toimimaan poikkeavissa oloissa, kuten matkapuhelinverkon ongelmien aikana. Kannattaa myös varautua siirtämään verkkosivut toiseen paikkaan.

Pienellä organisaatiolla on rajalliset mahdollisuudet toimia, mutta toisaalta kaikki tuntevat toisensa ja toistensa vahvuudet. Miettimällä etukäteen, miten nämä vahvuudet tukevat häiriönhallintaan valmistautumista, sen tekemistä ja siitä toipumista, voi pieni organisaatio joustavuudellaan kompensoida isompien resursseja. Pienellä organisaatiolla on yleensä rajallinen määrä laitteita ja verkkoja hallittavanaan. Tämä auttaa ympäristön toimintojen tunnistamisessa, rajaamisessa ja suojaamisessa. Mikäli häiriönhallintaan ei ole riittävästi valmistauduttu, sitä on huomattavasti vaikeampi tehdä, kun häiriötilanne on käynnissä.

Yrityksen toimialaan vaikuttavaan lainsäädäntöön tulee tutustua ja miettiä sen vaikutusta omien tietojen suojaamistarpeisiin. Jos on epävarma, miten tietoturvan häiriötä saa missäkin tapauksessa selvittää, kannattaa oman toiminnan kannalta merkittävimmät vaihtoehdot varmistaa toimialan ja tietoturvan lainsäädännön tuntevalta lakimieheltä. Varsinkin työntekijän yksityisyyden loukkaamista kannattaa välttää tai pyytää viranomaisia jatkamaan tutkintaa, jos esitutkinnan kynnys ylittyy. Jos esitutkinnan kynnys yrityksen mielestä ylittyy, sen tulee tehdä tapahtumasta tutkintapyyntö tai rikosilmoitus poliisille. Tämän jälkeen yritys noudattaa poliisin antamia ohjeita, suosituksia ja käskyjä myös oman tutkintansa osalta, jotta se ei vaaranna poliisitutkintaa. Kun yritys noudattaa poliisin ohjeita, varmistetaan myös se, että yrityksen työntekijät eivät syyllisty rikoksiin tutkiessaan tapahtumaa. Jos ollaan varmoja, että esitutkintaa ei tarvita, tietoturvallisuuden häiriö käsitellään tavallisena häiriönä ja havaittujen puutteiden korjausten jälkeen yrityksen liiketoiminta voi jatkua. Häiriön perustiedot ja tehdyt ratkaisut kannattaa kuitenkin kirjata muistiin, jos myöhempien muiden tapahtumien vuoksi esitutkintakynnys ylittyykin. Häiriönhallinnan kirjauksia voidaan käyttää myös pohjana harjoituksille ja kehityshankkeille.

Lähteet

Alienvault. 2016. Verkkodokumentti. Alienvault Inc. <http://communities.alienvault.com>. Luettu 3.4 2016.

Autoreporter-ilmoitukset. 2011. Verkkodokumentti. CERT-FI. <http://www.cert.fi/katsaukset/tilastot/autoreporter.html>. Luettu 20.5.2013.

Autoreporter-ilmoitusten perusteella tehty graafi haittaohjelmahavaintojen määrästä. 2013. Verkkodokumentti. CERT-FI. <https://www.viestintavirasto.fi/tilastotjatutkimukset/tilastot/2013/haittaohjelmahavaintojenmaara-2.html>. Luettu 1.3.2016.

Core Security 2014. Verkkodokumentti. Core Security. <Vulnerability-management-maturity-model-white-paper_0.pdf>. Core Security. Luettu 4.3.2016.

Elisa YRSE. 2016. Verkkodokumentti. Elisa Oyj. <http://esco.elisa.fi/rest/esco/blob/yritysten-asiakastuki/YR-YSE-15_150618.pdf>. Luettu 3.4.2016.

EU Tietosuoja-asetus lehdistötiedote. 2015. Verkkodokumentti. Euroopan Unioni. <http://europa.eu/rapid/press-release_IP-15-6321_fi.htm>. Luettu 30.3.2016.

F-Secure. 2016. Verkkodokumentti. F-Secure Oyj. <https://business.f-secure.com/81-cyber-attacks-every-minute/>. Luettu 3.4.2016.

Flexera PSI. 2016. Verkkodokumentti. Flexera Software LLC. <http://www.flexerasoftware.com/enterprise/products/software-vulnerability-management/personal-software-inspector/>. Luettu 4.4.2016.

Fluentd. 2016. Verkkodokumentti. Fluentd Project. <http://www.fluentd.org>. Luettu 5.4.2016.

Graylog. 2016. Verkkodokumentti. Graylog Inc. <https://www.graylog.org/>. Luettu 5.4.2016.

Henkilötietolaki. 1999. 525/22.4.1999.

Hommedal, Frode. 2015. CSIRT Modeling. Verkkodokumentti. Frode Hommedal. <http://frodehommedal.no/presentations/first-tc-oslo-2015/>. Luettu 10.3.2016

Hyvönen, Timo, Kalland, Ben, Lankinen, Pirkko, Mäntynen, Jyrki. 2011. ITIL® Suomenkielinen sanasto, v1.0, 29 heinäkuuta 2011. Helsinki: Axelos Limited.

Itähelsinkiläinen kahvila. 2010. Verkkodokumentti. Secmeter Oy. <http://www.secmeter.com/maksuvalinepetokset.html> Luettu 2.4.2016.

Joensuu, Juhani. 2012. Palvelinturvallisuus PK-yrityksen näkökulmasta. Insinöörityö Rovaniemen ammattikorkeakoulu.

Jordan ym. 2006. Strateginen IT-riskienhallinta. Helsinki: Edita Publishing Oy.

KPMG blogi. 2016. Verkkodokumentti. KPMG Finland Oy. <http://www.hackingthroughcomplexity.fi/> Luettu 7.3.2016.

Kral, Patrik. 2012. The Incident Handlers Handbook. Sans Institute.

Kurittu Antti. 2015. Tikka tietoturvallisuusopas. Verkkodokumentti. Elinkeinoelämän keskusliitto. <http://ek.fi/wp-content/uploads/TIKKA_Tietoturvallisuus_opas.pdf>. Luettu 1.4.2016.

Kuusela Jari. 2014. Palvelunestohyökkäyksen kriminalisointi. Maisteritutkielma. Lapin yliopisto.

Laakso, Matti. 2010. PK-yrityksen tietoturvasuunnitelman laatiminen. Insinöörityö. Turun ammattikorkeakoulu.

Laki yksityisyyden suojasta työelämässä. 2004. 759/13.8.2004.

Logalyze 2016. Verkkodokumentti. Zuriel Ltd. <http://www.logalyze.com/index.php>. Luettu 5.4.2016.

Microsoft_Security_Intelligence_Report_Volume_19_English. 2016. Verkkodokumentti. Microsoft corporation. <http://www.microsoft.com/security/sir/default.aspx>. Luettu 11.3 2016.

Mindtools. 2016. Verkkodokumentti. Mindtools Ltd. <https://www.mindtools.com/pages/article/newTED_78.htm>. Luettu 8.3.2016.

NCSA. 2016. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/ncsa-fi.html>. Luettu 4.3.2016.

Nets korttimaksaminen. 2016. Verkkodokumentti. Nets Oy. <http://www.nets.eu/fi-fi/tuki/usein-kysyttya/turvallisuus/Pages/default.aspx#tab2>. Luettu 14.3.2016.

Nixu blogi. 2016. Verkkodokumentti. Nixu Oyj <https://www.nixu.com/fi/blogi>. Luettu 7.3.2016.

NMAP. 2016. Verkkodokumentti. Nmap.org. <https://nmap.org/>. Luettu 3.4.2016.

OWASP 2016. Verkkodokumentti. Owasp Foundation Helsinki chapter. <https://www.owasp.org/index.php/Top_10_2007_Finnish>. Luettu 10.4.2016.

Sonera toimitusehdot. 2016. Verkkodokumentti. Sonera Oyj. <https://www.sonera.fi/media/12fdf6fa94b1be5571b3c9465108e2177a38ca93/Soneran+yleiset+toimitusehdot+yritysasiakkaille+T18287-09+090801.pdf>. Luettu 3.4.2016.

Sopanen, Heikki. 2016. Verkkorosovt käyvät entistä hanakammin yritysten kimppuun. Verkkodokumentti. Etelä-Saimaa http://www.esaimaa.fi/Online/2016/02/27/Verkkorosvot%20k%C3%A4yv%C3%A4t%20entist%C3%A4%20hanakammin%20yritysten%20kimppuun/2016120379436/4. Luettu 2.3.2016.

Sähköisen viestinnän tietosuojalaki. 2004. 516/16.6.2004.

Technet 2011. Verkkodokumentti. Microsoft corporation. <http://blogs.technet.com/b/security/archive/2011/11/02/cyber-threats-in-the-european-union.aspx>. Luettu 20.10.2012.

Tietoturva ry. 2016. Verkkodokumentti. Tietoturva ry. <https://www.tietoturva.fi/>. Luettu 10.3.2016.

Tietoyhteiskuntakaari. 2014. 917/7.11.2014.

Turpeinen Juha. 2010. Vikasietoinen virtuaalipalvelinjärjestelmä. Opinnäytetyö. Oulun seudun ammattikorkeakoulu.

Valtiovarainministeriö Vahti-ohje 8/2008. 2008. Verkkodokumentti. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10128&groupId=10229>. s. 160. Luettu 1.4.2016

Windows 7 varmuuskopiointi. 2013. Verkkodokumentti. Microsoft corporation. <http://windows.microsoft.com/fi-fi/windows7/back-up-your-files>. Luettu 30.5.2013.

Esimerkki omaisuuslistasta

Omaisuuden nimi	Luokka	Kuvaus	Sijainti	Sijainnin tarkenne	Tunniste	Sarjanumero	Arvo	Kriittisyys	Versio	Tunnistettu päivitystarve
tt-palvelin-1	palvelimet	Tietoturvapalvelin	Yrityskatu 1:Tuotantoverkko: Toimistoverkko	192.168.139.12:192.168.138.9	mac	234234wewer	5	4	Ossim 4.1	kyllä
tt-palvelin-2	palvelimet	Uusi tietoturvapalvelin	Yrityskatu 1:Tuotantoverkko: Testiverkko	192.168.139.11:192.168.130.11	mac	234234wewxc	3	2	Ossim 4.2	ei
h-ta-1	hallintakoneet	hallintapalvelin-1	Yrityskatu 1:Tuotantoverkko	192.168.139.10	mac	3211312xzwe1	3	4	Esxi	ei
reititin	verkkolaitteet	Reititin ja palomuuri	Yrityskatu 1:Tuotantoverkko	192.168.139.1:192.168.138.122:192.168.138.1	mac	3211312xzwe2	5	5	ZyXEL ZyWALL USG	
kytkin-1	verkkolaitteet	Tuotannon kytkin	Yrityskatu 1:Tuotantoverkko			3211312xzwe3	4	5	HP 1910	
kytkin-2	verkkolaitteet	Testiverkon kytkin	Yrityskatu 1:Testiverkko			3211312xzwe4	2	2	HP 1910	
kytkin-3	verkkolaitteet	Toimistoverkon kytkin	Yrityskatu 1:Toimistoverkko			3211312xzwe5	3	3	HP 1910	
firma-ap-1	verkkolaitteet	Toimiston Wlan	Yrityskatu 1:Toimistoverkko	192.168.138.2	mac	3211312xzwe6	2	3	Cisco WAP4410N	
ta-myynti-1	työasemat	Myynnin työasema	Yrityskatu 1:Toimistoverkko	DHCP 192.168.138.16 - 192.168.138.29	mac	3211312xzwe7	2	2	7	ei
ta-myynti-2	työasemat	Myynnin työasema	Yrityskatu 1:Toimistoverkko	DHCP 192.168.138.16 - 192.168.138.29	mac	3211312xzwe8	2	2	XPsp3	kyllä
ta-yllapito-1	työasemat	Ylläpidon työasema	Yrityskatu 1:Toimistoverkko	DHCP 192.168.138.16 - 192.168.138.29	mac	3211312xzwe9	2	3	7	ei
ta-johto-1	työasemat	Johdon työasema	Yrityskatu 1:Toimistoverkko	DHCP 192.168.138.16 - 192.168.138.29	mac	3211312xzwe10	2	3	7	ei
ta-tuotanto-1	työasemat	Tuotannon työasema	Yrityskatu 1:Toimistoverkko	DHCP 192.168.138.16 - 192.168.138.29	mac	3211312xzwe11	2	2	7	ei

Omaisuuden nimi	Luokka	Kuvaus	Sijainti	Sijainnin tarkenne	Tunniste	Sarjanumero	Arvo	Kriittisyys	Versio	Tunnistettu päivitystarve
ta-tuotanto-3	työasemat	Tuotannon työasema	Yrityskatu 1:Toimistoverkko	DHCP 192.168.138.16 - 192.168.138.29	mac	3211312xzwe13	2	2	7	ei
as1-testi-1	palvelimet	Asiakkaan testipalvelin 1	Yrityskatu 1:Testiverkko	192.168.130.22	mac	3211312xzwe15	2	2	Ubuntu server 12.10	
as1-testi-2	palvelimet	Asiakkaan testipalvelin 2	Yrityskatu 1:Testiverkko	192.168.130.21	mac	3211312xzwe16	2	2	Ubuntu server 12.10	
as1-testi-3	palvelimet	Asiakkaan testipalvelin 3	Yrityskatu 1:Testiverkko	192.168.130.20	mac	3211312xzwe17	2	2	Ubuntu server 12.10	
m-tulostin-1	tulostimet	Vanha mustavalkolaser	Yrityskatu 1:Toimistoverkko	192.168.138.5	mac	3211312xzwe18	1	1	HP Laserjet 4M	kyllä
v-tulostin-1	tulostimet	Uusi väritulostin/kopiokone	Yrityskatu 1:Toimistoverkko	192.168.138.6	mac	3211312xzwe19	3	3	Canon C2220L	
varasto-1	levypalvelimet	Keskitetyt verkkolevyt	Yrityskatu 1:Tuotantoverkko	192.168.139.8	mac	3211312xzwe20	4	4	QNAP TS-412	
varasto-2	levypalvelimet	Varmuuskopiot	Yrityskatu 1:Tuotantoverkko	192.168.139.9	mac	3211312xzwe21	5	5	QNAP TS-412	