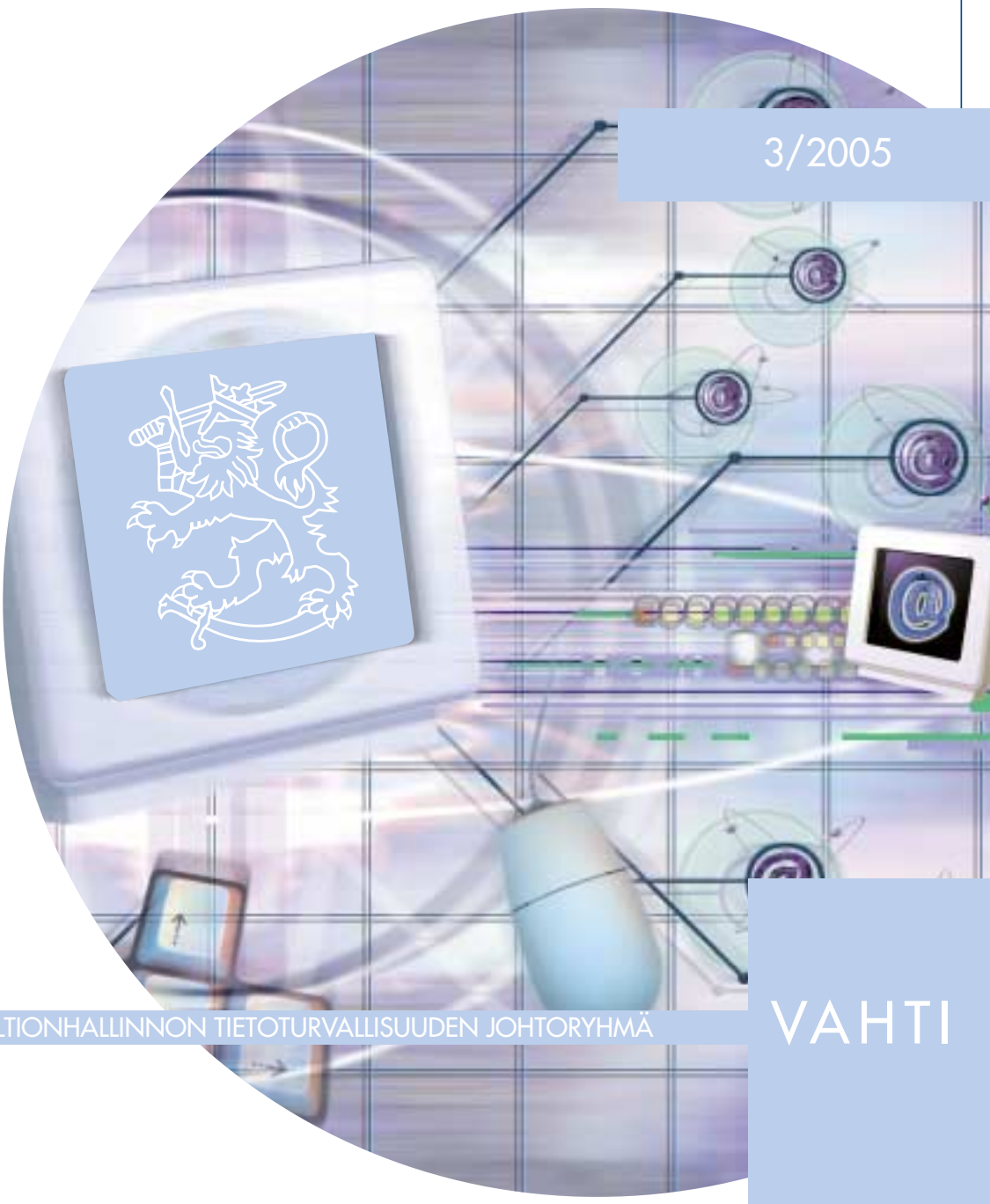
VALTIOVARAINMINISTERIÖ

TIETOTURVAPOIKKEAMATILANTEIDEN HALLINTA



3/2005

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

TIETOTURVAPOIKKEAMATILANTEIDEN HALLINTA

3/2005

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A, Helsinki
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
Vahtijulkaisut@vm.fi

ISSN1455-2566
ISBN 951-804-521-6 (nid)
ISBN 951-804-522-4 (pdf)

Edita Prima Oy
HELSINKI 2005

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 11/01/2005

OHJE
15.6.2005

Ministeriöille, virastoille ja laitoksille

OHJE TIETOTURVAPOIKKEAMATILANTEIDEN HALLINNASTA

Valtiovarainministeriö antaa oheisen tietoturvaohjeen (jäljempänä ohje), joka on laadittu valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta.

Ohje korvaa ohjeen Toimet tietoturvaloukkaustilanteissa. VAHTI 7/2001. Tietoturvapoikkeamien laajan käsitteen vuoksi ohjeen käyttöalue on selvästi kattavampi kuin aikaisemman ohjeen. Erityisesti sisäisen tarkastuksen, yleisen kriisinhallinnan, tietoturvallisuuden ja tietohallinnon johdun sekä tietojärjestelmien ylläpitohenkilöstön ja ark-tuen tulee perehtyä koko ohjeeseen. Muiden kohderyhmien perehtyminen on kuvattu ohjeessa.

Ohjeessa käsitellään tietoturvapoikkeamien havaitseminen, niihin reagoiminen ja niistä toipuminen sekä ennaltaehkäiseviä toimenpiteitä ja lainsäädäntöä. Havaitseminen ja reagoinnin kannalta keskeistä on ymmärtää eri-laiden mahdolliset syyt ja miten erilaiset poikkeamat ilmenevät. Poikkeaman vakavuudesta riippuu, miten ja millaisella organisaatiolla on syytä reagoida.

Päätöksentekovastuut, reagointiorganisaatio ja –menettelyt on määriteltävä etukäteen erilaisille poikkeamatilanteille. Reagoinnin ja toipumisen harjoittelu sekä tiedottamisen, viestinnän ja mahdollisesti tarvittavan ulkoisen yhteistyön suunnittelu ovat tärkeä osa poikkeamatilanteisiin varautumista. Jo poikkeaman epäilyn tulee käynnistää selvitystoimet, joiden osana koko poikkeamatilanteen ajan kirjataan havainnot, päätökset ja toimenpiteet.

Asiakirja tulee VAHTIn Internet-sivuille (www.vm.fi/vahti). Ohjetta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi).

Lisätietoja antavat tietoturvallisuusasiantuntija Juhani Sillanpää (etunimi.sukunimi@vm.fi) ja neuvotteleva virkamies, VAHTIn puheenjohtaja Mikael Kivisiemi (etunimi.sukunimi@vm.fi)

Toimen valtiovarainministeri Ulla-Maj Widemos

Ylijohtaja Jorma Kuusjalainen

Liite Tietoturvapoikkeamatilanteiden hallinta (VAHTI 3/2005)

TIIVISTELMÄ JA OHJEEN RAKENNE

Luvussa on johdatus tämän ohjeen aihepiiriin. Tietoturvallisuudesta huolehtiminen on osa organisaation koko toiminnan laatua ja siten siihen panostamisen aste on ylimmän johdon strateginen valinta.

Luvussa 1.1 käydään läpi keskeistä tietoturvapoikkeamatilanteissa ja niihin varautumisessa sovellettavaa, organisaatioita sitovaa lainsäädäntöä.

Luku 2 käsittelee tietoturvapoikkeamiin varautumista. Normaalitoiminnan tietoturvallisuuden hyvä taso ja poikkeamareagoinnin suunnittelu ehkäisevät tietoturvapoikkeamien toteutumista, vähentävät poikkeamissa syntyviä vaurioita sekä edistävät niistä toipumista.

Ohjeen luvussa 2.1 käsitellään ennaltaehkäiseviä toimenpiteitä.

Ennaltaehkäisy on olennainen osa organisaation tietoturvallisuuden toteuttamista. Huomiota kiinnitetään tietoturvan strategisen ja käytännön tason määrittelyyn ja ohjeistukseen. Tähän liittyy olennaisesti myös henkilökunnan jatkuva tietoturvakoulutus ja organisaation tietoturvakulttuurin luominen. Tietoturvallisuuteen liittyvät vastuut niin normaalitilanteissa kuin tietoturvapoikkeamatilanteiden aikana tulee määritellä ennakolta, kirjata toimenkuviin ja tiedottaa organisaation sisällä. Vastuu tietoturvasta on aina organisaatiolla itsellään riippumatta tietohallinnon ja tietoturvallisuuden toimintojen käytännön toteutuksesta (mahdollinen ulkoistus tai alihankinta). Tämä edellyttää organisaatiolta riittävästi omaa tietoturvaosaamista.

Tietoturvallisuuden jatkuva kehittäminen ja sen tason seuranta varmistavat organisaation kannalta tarkoituksenmukaisen tietoturvatason. Tarkoituksenmukaisen tietoturvatason määritteleminen on osa organisaation yleistä riskienhallintaa. Olennainen merkitys tietoturvapoikkeamien ehkäisyssä on osaavalla ja vastuuntuntoisella tietojärjestelmien ylläpidolla. Verkostoituminen omien sidosryhmien kanssa on tietoturvankin osalta hyödyllistä ja osin myös välttämätöntä.

Luvussa 2.2 esitellään keinoja varautua ennalta sekä tietoturvapoikkeamien havaitsemiseen että mahdollisiin poikkeamatilanteisiin reagoimiseen.

Tarkoituksenmukainen reagointi edellyttää, että ymmärretään, millä tavoin erilaiset tietoturvapoikkeamat ilmenevät ja mitä syitä näkyvien oireiden taustalla voi olla. Kyseessä

saattaa olla tahaton poikkeamatilanne tai tahallinen tietoturvaloukkaus. Tahattomia poikkeamia ovat yhtälailla laiterikot, vasta tuotantoympäristössä ilmenevät päivityksen sivuoireet, tuottamukselliset ylläpidon laiminlyönnit tai sähkönjakeluun vaikuttavat luonnonkatastrofit. Tahalliset tietoturvaloukkaukset jaetaan satunnaisesti kohteensa valitseviin sekä kohdistettuihin hyökkäyksiin. Kohdistetussa hyökkäyksessä tietoturvaloukkauksen tekijä valitsee kohteen sen sisältämän tiedon tai esimerkiksi kohdetta kohtaan tuntemansa kaunan perusteella.

Luvussa käydään esimerkinomaisesti läpi varautumista muutamaan erilaiseen poikkeamatilanteeseen sekä tuodaan esiin tietoturvapoikkeamien taustalla olevia rikoksia.

Poikkeaman vaikuttavuudesta sekä tyypistä riippuu, millä tavoin ja millaisella organisaatiolla poikkeamaan on syytä reagoida. Sekä päätöksentekovastuut, reagointiryhmät että reagointimekanismit on määriteltävä etukäteen erilaisia poikkeamatilanteita varten. Ennakolta on myös varattava resurssit ja luotava rakenteet, joilla voidaan taata tilannetta selvittävän ja korjaavan ylläpidon mahdollisuus keskittyä poikkeaman hallitsemiseen. Merkittäviin poikkeamiin reagoinnissa tehdään yhteistyötä organisaation mahdollisen kriisinhallintaryhmän kanssa.

Reagoinnin ja toipumisen harjoittelu on tärkeä osa poikkeamatilanteisiin varautumista. Harjoittelu on hyvä suunnitella pitkäjänteisesti, jotta kaikkia eri toimintoja tulee testattua myös harjoitustilanteissa. Harjoitus palvelee operatiivisten toimijoiden kykyä reagoida poikkeamiin ja sen avulla saadaan tietoa reagointi- ja toipumissuunnitelmien toimivuudesta ja muista tietoturvallisuuden kehittämistarpeista.

Tiedottamisella ja viestinnällä on poikkeamatilanteissa keskeinen merkitys mm. lisävahinkojen estämisessä sekä organisaation julkisuuskuvan kannalta. Tiedotuksen ja viestinnän tulee olla suunnitelmallista. Erityisesti organisaatiosta ulospäin suuntautuva viestintä tapahtuu yhteistyössä viestintäyksikön kanssa. Sidosryhmien välinen verkosto poikkeamatilanteita varten on syytä rakentaa jo normaalioloissa.

Myös poikkeamatilanteesta toipuminen on syytä suunnitella mahdollisimman tarkasti etukäteen, jottei harkitsemattomilla toimenpiteillä siinä vaiheessa aiheuteta lisää vahinkoa. Keskeistä ovat ajantasaiset toipumissuunnitelmat sekä niihin liittyvät varajärjestelyt ja huoltosopimukset. Näitä käsitellään lyhyesti luvussa 2.3.

Ohjeen luku 3 keskittyy varsinaiseen reagointiin tietoturvapoikkeaman tapahduttua.

Riippumatta siitä, kuka organisaation käyttämät tietotekniikkapalvelut toteuttaa, vastuu tietoturvapoikkeamiin reagoinnista ja kyvystä reagoida on organisaatiolla itsellään. Reagointi pohjautuu onnistuneeseen tapahtuma-analyysiin ja poikkeaman vakavuuden määrittelyyn. Poikkeamia ei useinkaan havaita heti koko laajuudessaan, vaan ensin huomataan jokin normaalitilasta poikkeava yksityiskohta, indikaatio mahdollisesta poikkeamasta. Havaittuihin indikaatioihin ja poikkeamiin on suhtauduttava vakavasti. Jo poikkeaman epäilyn tulee käynnistää selvitystoimet.

Koko poikkeamatilanteen ajan kirjataan tehdyt havainnot, päätökset ja toimenpiteet. Toimenpiteet, mukaan lukien poikkeaman kohteen eristäminen, riippuvat poikkeaman

tyypistä: esimerkiksi palvelunestohyökkäys edellyttää erilaisia toimenpiteitä kuin tietomurto. Erityisen ryhmänsä muodostavat organisaation oman henkilökunnan tekemät tietoturvaloukkaukset. Luvussa otetaan kantaa, mitä niiden tutkimiseksi on lainsäädännön puitteissa mahdollista tehdä sekä millaisia seuraamuksia organisaatio voi niistä tekijälle työnantajan roolissa määrätä.

Todisteaineistolla on tärkeä merkitys niin tapahtumien selvittämisessä kuin mahdollisessa oikeusprosessissakin. Käyttötarkoitus vaikuttaa todisteaineiston keräämiseen ja käsittelyyn, jotka eivät saa olla ristiriidassa asianosaisten oikeusturvan kanssa.

Poikkeamaan liittyvän viestinnän ja tiedottamisen tulee käynnistyä poikkeaman havaitsemisen myötä. Kohderyhmiä organisaatio sisällä ovat kaikki, joiden toimintaan poikkeama vaikuttaa, poikkeaman selvittämiseen osallistuvat sekä poikkeaman aikaista toimintaa ohjeistavat tahot. Merkittävistä poikkeamista tulee informoida myös organisaation johtoa ja viestintäyksikköä sekä mahdollista kriisinhallintaryhmää.

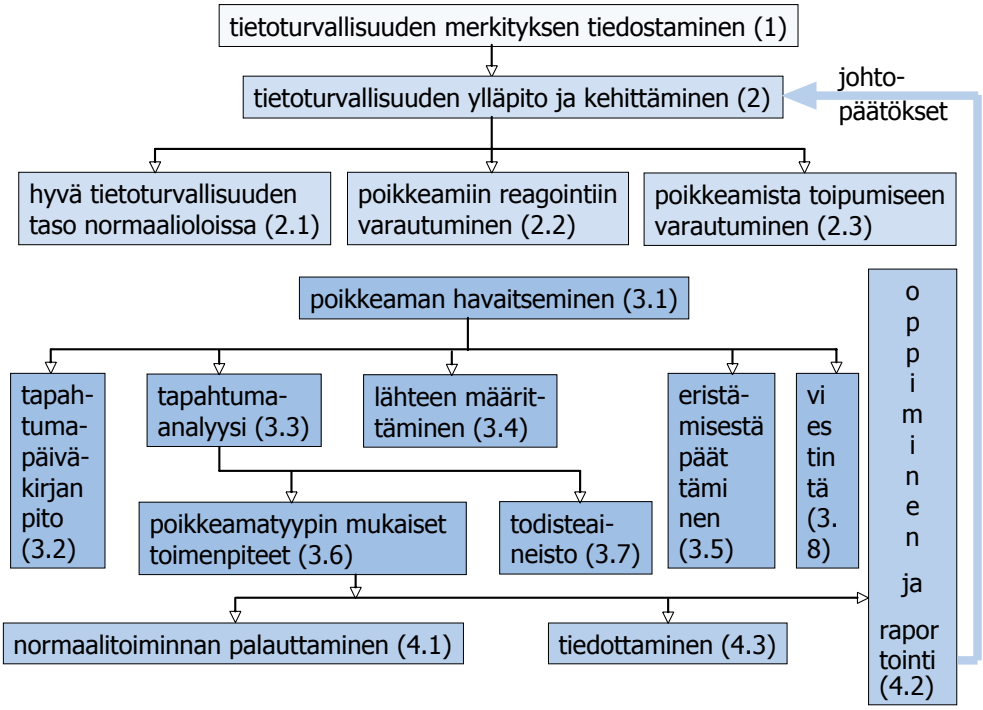
Poikkeamatilanteessa on usein syytä kommunikoida myös ulkopuolisten sidosryhmien ja asiantuntijoiden kanssa. Tilanteen ratkaisemiseen voi saada tukea CERT-toimijoilta (Computer Emergency Response Team) sekä tietotekniikkarikostutkijoilta ja muilta poliisiviranomaisilta. He ottavat mielellään vastaan tilastointimielessä oman toimialansa liittyvää tietoa, vaikka organisaatio ei tarvitsisikaan apua tai halua tehdä rikosilmoitusta.

Valtiovarainministeriö (VM) ohjaa ja koordinoi valtionhallinnon tietoturvallisuutta ja sen kehittämistä. Valtionhallinnon organisaatioiden on hyvä tiedottaa merkittävistä tietoturvapoikkeamista valtiovarainministeriön hallinnon kehittämisosastoa. Valtiontalouden tarkastusvirastosta annetun lain perusteella tehdään tarvittavat ilmoituksen myös sinne.

Luvussa 4 annetaan ohjeita tietoturvapoikkeamatilanteesta toipumiseen.

Tuotantokäytön aloittaminen poikkeamatilanteen jälkeen edellyttää, että tarvittavat akuutit korjaukset on toteutettu ja tiedot ja tietojärjestelmät palautettu niin hyvään kuntoon kuin mahdollista. Olennainen osa toipumista on poikkeamatilanteen aikana saatujen oppien kokoaminen ja tietoturvallisuuden kehitys- ja toipumissuunnitelmien tarkentaminen ja täydentäminen niiden perusteella. Myös poikkeamatilanteen jälkeen tulee huolehtia tiedottamisesta: asianosaosaisille kerrotaan tilanteen normalisoituneen. Jos poikkeamasta on aiemmin tiedotettu julkisuudelle, voidaan lehdistötiedotetta harkita myös tässä vaiheessa.

Onnistunut toipuminen tietoturvapoikkeamatilanteesta edellyttää hyvää varautumista ja antaa siten aiheen palata kehittämään luvussa 2 esille tuotuja asioita.


tietoturvallisuuden merkityksen tiedostaminen (1)
tietoturvallisuuden ylläpito ja kehittäminen (2)
johto-
päätökset
hyvä tietoturvallisuuden taso normaalioloissa (2.1)
poikkeamiin reagointiin varautuminen (2.2)
poikkeamista toipumiseen varautuminen (2.3)
poikkeaman havaitseminen (3.1)
tapah-
tuma-
päivä-
kirjan
pito
(3.2)
tapahtuma-
analyysi (3.3)
lähteen määrit-
täminen (3.4)
eristä-
misestä
päät
tämi
nen
(3.5)
vi
es
tin
tä
(3.
8)
poikkeamatyypin mukaiset toimenpiteet (3.6)
todisteai-
neisto (3.7)
normaalitoiminnan palauttaminen (4.1)
tiedottaminen (4.3)
o
p
p
i
m
i
n
e
n
ja
rapor
tointi
(4.2)

Lukuohje kohderyhmittäin

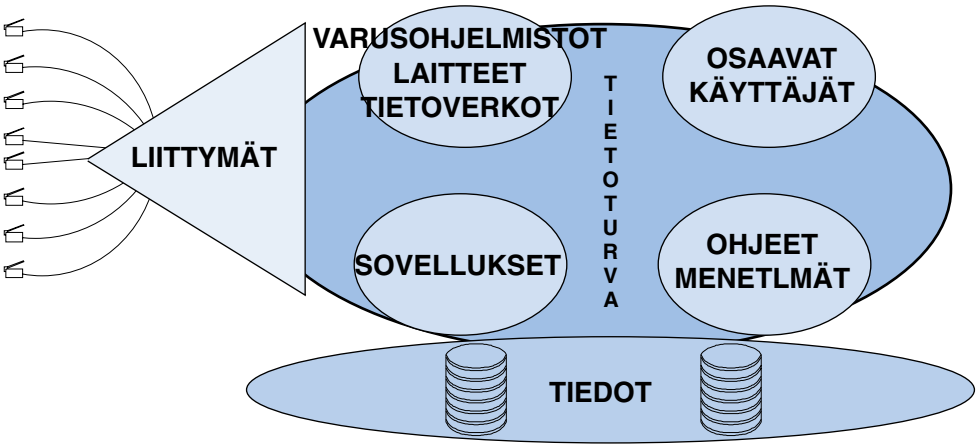
Sisäisen tarkastuksen, yleisen kriisienhallinnan, tietoturvallisuuden ja tietohallinnon johdon sekä tietojärjestelmien ylläpitohenkilöstön ja atk-tuen on syytä perehtyä koko ohjeeseen. Muiden kohderyhmien osalta oheisessa taulukossa on kerrottu, mihin lukuihin heidän tulisi ainakin perehtyä. Kohderyhmät on nimetty toiminnoittain, ei niinkään nimikkeittäin, koska eri organisaatioissa roolit voivat olla jakautuneet eri tavoin:

Kuka Luku	Ylin johto	Henkilöstö-hallinto	Viestintä-yksikkö	Oikeudellinen yksikkö
1	x	x	x	x
2.1	x	2.1.3, 2.1.4, 2.1.6, 2.1.9		2.1.1, 2.1.2, 2.1.4, 2.1.6, 2.1.7, 2.1.9
2.2	2.2.3-6	2.2.4, 2.2.5	2.2.6, 2.2.7	2.2.3, 2.2.6, 2.2.7
2.3	x			
3.6		3.6.4		3.6.2, 3.6.4
3.7				x
3.8			x	3.8.2, 3.8.3, 3.8.4
4.3			x	
4.4	x			
Liite 3			x	
Liite 6 ja 7	x	x		x
Liite 9	x	x		

Sisällysluettelo

Tietoturvapoikkeama

on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut.



Tietojärjestelmä on kokonaisuus, joka koostuu tiedoista, niitä käsittelevistä sovelluksista ja laitteista sekä tietoverkoista, käyttöä määrittävistä ja ohjaavista ohjeista, tehtäviensä tasalla olevista käyttäjistä sekä liittymistä toisiin tietojärjestelmiin. Tietojärjestelmään kuuluu myös siinä käsiteltävien tietojen turvallisuus sekä yleinen tietoturvallisuuden hallinta ja valvonta.

Poikkeama missä tahansa kokonaisuuden osassa merkitsee häiriötä järjestelmän toiminnassa.

1 JOHDANTO

Kansallisen tietoturvallisuusstrategian mukaisesti yhteiskunnan tehokkuus, toimivuus, kehitys ja kilpailukyky ovat riippuvaisia myös tietoturvallisuuden toteutuksesta. Organisaatiot eivät voi toimia ilman oikeaa ja ajantasaista tietoa. Yhteiskunnan palvelut riippuvat tietotekniikasta siinä määrin, että tietotekniikkapalveluiden keskeytyksetön käytettävyys on monissa tilanteissa välttämätöntä. Samalla organisaation tietoihin, tietotekniikan toimivuuteen ja tietoturvallisuuteen kohdistuvat uhat lisääntyvät jatkuvasti. Tämän ohjeen tavoitteena on auttaa organisaatioita

- valmistautumaan etukäteen tietoturvapoikkeamatilanteisiin mahdollisimman huolellisesti
- havaitsemaan tietoturvapoikkeamat
- reagoimaan poikkeamatilanteisiin nopeasti ja tarkoituksenmukaisesti
- toipumaan poikkeamatilanteista suunnitelmallisesti.

Ohje on osa valtionhallinnon laajaa tietoturvaohjeistusta. Liite 2:ssa on luettelo keskeisistä VAHTI-ohjeista ja muusta soveltuvasta materiaalista. Ohjeessa käsitellään tietoturvapoikkeamatilanteiden hallintaa laajasti, jolloin organisaatiot voivat poimia sieltä omaan toimintaansa soveltuvat osat toteutettaviksi.

Tietoturvallisuuteen panostaminen sekä yleisellä että tietotekniikan tasolla ovat johdon strategisia päätöksiä, joilla organisaation toimintakykyyn vaikutetaan merkittävällä tavalla. Vaikka tietoturvallisuuteen panostaminen näkyy välittömästi kuluna, tietoturvallisuuden kiistattomat edut tulevat kuitenkin näkyviin esimerkiksi häiriöttömänä toimintana, toiminnan laadukkuutena ja positiivisen julkisuuskuvan säilymisenä. Lisäksi lainsäädäntö edellyttää tietoturvallisuudesta huolehtimista. Tietoturvallisuuden ja tietotekniikan ammattilaisilla on tässä kokonaisuudessa keskeinen merkitys johdon neuvonantajina.

Tietoturvallisuuteen kohdistuva uhka on jatkuvaa. Satunnaisesti kohdistuvat haittaohjelmahyökkäykset, laitteiden ja ohjelmistojen turva-aukkojen systemaattinen etsiminen sekä valtava määrä roskapostia ovat verkossa lähes normaalia taustaliikennettä, johon tie-

toliikenneverkkoa hyödyntävän organisaation on varauduttava. Verkossa ilmenee myös tietoisesti kohdistettuja hyökkäyksiä, joilla hyökkääjä voi pyrkiä estämään organisaation tarjoaman palvelun toiminnan tai pääsemään käsiksi kohdeorganisaation tietopääomaan. Tietopääoman oikeudettoman käsittelyn voivat mahdollistaa myös oman henkilökunnan laiminlyönnit tai vahingot, kuten asiakirjojen huolimaton säilytys tai tuhoaminen ja käyttöoikeuksien lainailu. Toisaalta käsittelyn estymisessä ei välttämättä ole taustalla tahallista toimintaa. Syynä voivat olla myös erilaiset olosuhdeongelmat, kuten luonnonilmiöistä johtuvat sähkökatkot tai vesivahingot, laitteistojen vikatilanteet tai laiminlyönnit tietoturvaohjeiden noudattamisessa.

Tietoturvapoikkeamatilanteisiin varautumisen ensisijainen vastuu on organisaation ylimmällä johdolla. Johdon on varmistettava tietoturvallisuustyön riittävä resursointi ja seuranta.

1.1 Huomioitavia säädöksiä

Organisaation omien tarpeiden lisäksi lainsäädäntö velvoittaa tietojen suojaamiseen. Valtion viranomaisia säätelee laki viranomaisten toiminnan julkisuudesta (JulkL, 621/1999). Sen 18§:n määrittelemä hyvä tiedonhallintatapa velvoittaa huolehtimaan asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä. Sitä tarkentaa asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999). Myös muiden kuin valtionhallinnon organisaatioiden kannattaa hyödyntää hyvää tiedonhallintatapaa omien tietohallinnon ja tietoturvallisuuden toimintatapojensa määrittelyssä, sillä se antaa erinomaisen tarkistuslistan tietojen turvaamisen toteuttamiseen. Tätä kirjoitettaessa on meneillään julkisuuslain osa-uudistus, joka vaikuttanee myös lain soveltamisalaan.

Henkilötietojen osalta kaikkia koskee henkilötietolaki (HetiL, 523/1999), joka edellyttää huolellisuuden ja hyvän tiedonkäsittelytavan noudattamista henkilötietojen käsittelyssä. Sen 6§ velvoittaa suunnittelemaan henkilötietojen käsittelyn. Henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään. 7§ toteaa käytön sallituksi vain suunniteltuihin tarkoituksiin. Näin ollen myös tietojärjestelmien turvaaminen ja poikkeamien selvittäminen tulee huomioida tietojen käsittelyn tarkoituksina. Tämän ohjeen luvussa 3.6.4 *Oman henkilökunnan tekemät tietoturvaloukkaukset* palataan tähän kysymykseen. Lain luvussa 7 säädellään vielä erikseen tietoturvallisuutta ja tietojen säilytystä. Lain soveltamista valvoo tietosuojavaltuutettu.

Laki yksityisyyden suojasta työelämässä (TETSL, 759/2004) säätelee mm. teknistä valvontaa työpaikoilla. Sen 21§ mukaan työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö kuuluvat yhteistoimintamenettelyn piiriin. YT-käsittelyn

jälkeen työnantajan on ne määriteltävä ja tiedotettava työntekijöille. Monet tietojärjestelmien käytöstä kerättävät lokitiedot ovat osa teknistä valvontaa ja siten TETSL:n piirissä.

Sähköisen viestinnän tietosuojalain (SVTSL, 516/2004) tarkoituksena on mm. turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa. Sen luvun 2 *Yksityisyyden ja luottamuksellisen viestin suoja* pykälät 4 ja 5 velvoittavat kaikkia toimijoita. Suuri osa julkishallinnon yksiköistä ja yrityksistä on lain tarkoittamia yhteisötilaajia, joille on asetettu laissa useita velvoitteita. Luku 3 *Viestien ja tunnistamistietojen käsittely*, keskeisenä 8§, ja luku 5 *Viestinnän tietoturva*, keskeisenä 20§, tulee huomioida sekä tietoturvapoikkeamiin varautumisessa että poikkeamatilanteiden käsittelyssä. Viestintävirasto ja tietosuojavaltuutetun toimisto valvovat ja ohjeistavat lain soveltamista.

Tietojenkäsittelyrauhaa[1] suojataan rikoslaissa (RL, 39/1889). Esimerkiksi 38 luvussa *Tieto- ja viestintärikoksista* määritellään monia tietoturvapoikkeamissakin takana olevia rikoksia ja niistä langetettavia rangaistuksia. Niiden lisäksi tietotekniikka voi olla väline moniin muihin rikoksiin. Tämän ohjeen luvussa 2.2.3.1 *Rikosnimikkeistä* on käsitelty näitä tarkemmin.

[1] tietojärjestelmiin kohdistuvien rikosten loukkaama suojeluobjekti, joka koostuu eheydestä, luottamuksellisuudesta ja käytettävyydestä

2 TIETOTURVAPOIKKEAMIIN VARAUTUMINEN

Nykytilanteessa tiedot ja tietojärjestelmät ovat jatkuvasti uhattuina ja organisaatioiden toiminnan varmistaminen edellyttää hyvää tietoturvapoikkeamiin varautumista jo ennalta. Normaalitoiminnan tietoturvallisuuden hyvä taso ehkäisee tietoturvapoikkeamien toteutumista, vähentää poikkeamissa syntyviä vaurioita sekä edesauttaa niistä toipumista. Organisaatiota velvoittavaa säädösperustaa on käsitelty edellä luvussa 1.1 *Huomioitavia säädöksiä*.

Tietoturvapoikkeamiin varautuminen on osa organisaation laajempaa riskienhallintaa, jossa on huomioitava samat seikat kuin muussakin riskienhallinnassa (mm. taloudelliset, julkisuus-, ympäristö- ym. arvot). Normaalioloissa tulee hakea tarkoituksenmukainen tasapaino organisaation toiminnan ja siihen kohdistuviin riskeihin varautumisen välille ja toteuttaa tietoturvallisuutta sen mukaisesti. Tietoturvallisuustason määrittelyissä ja resursoinnissa on syytä tunnistaa ja huomioida myös tilanteet, joissa tarvitaan kohotettua varautumista tietoturvapoikkeamien varalta. Tällaisia ovat esimerkiksi vaalien tuloslaskenta, tulopoliittiset neuvottelut, konesalin muutto tai muut kunkin organisaation kannalta merkittävät tapahtumat, jolloin tietoturvallisuuden pettäminen voi aiheuttaa organisaatiolle poikkeuksellisen paljon esimerkiksi taloudellista tai julkisuuskuvaan liittyvää vahinkoa. Näissä tilanteissa voi olla tarpeen mm. tehostaa järjestelmien seurantaa, lisätä varalla olevan henkilöstön määrää ja sopia erityisjärjestelyistä laitteistotoimittajien kanssa.

Organisaation ylin johto on vastuussa tietoturvapoikkeamiin varautumisesta ja tietoturvastyön riittävästä resursoinnista. Vastuu on riippumatonta siitä, onko joitakin organisaation toimintoja ulkoistettu vai ei.

2.1 Ennaltaehkäisevät toimenpiteet

2.1.1 Tietoturvapolitiikka

Organisaatioiden riippuvuus oikeasta ja ajantasaisesta tiedosta tekee tietoturvallisuuteen panostamisesta johdon strategisen valinnan. Tietoturvapolitiikka on välttämätön lähtökohta organisaation tietoturvallisuuden kehittämiselle. Sen avulla ylin johto määrittelee organisaation tietoturvallisuuden päämäärät, periaatteet ja toimintatavat sekä ohjaa tietoturvallisuuden huomioimista, suunnittelua ja toimeenpanoa organisaation eri tasoilla. Tietoturvapolitiikkaan sisältyvät periaatteet ovat toiminnasta lähteviä vaatimuksia ja järjestelmistä ja teknisistä toteutustavoista riippumattomia.

Tietoturvapolitiikka on julkinen asiakirja, joka tulee olla koko henkilöstön tiedossa. Sillä on olennainen merkitys organisaation positiivisen tietoturvakulttuurin luomisessa. Malli tietoturvapolitiikan laatimiseksi löytyy esimerkiksi julkaisusta *Tietotekniikan turvallisuus ja toiminnan varmistaminen* [1, erityisesti luku 3.2].

2.1.2 Tietoturvasuunnitelmat ja –ohjeet

Tietoturvallisuuteen liittyvät kehitys- ja toimintasuunnitelmat sekä ohjeet perustuvat tietoturvapolitiikassa asetetuille tavoitteille. Koko organisaatiota koskeva tietoturvasuunnitelma pohjaa tietoturvapolitiikkaan ja riskikartoituksiin. Se koskee perusturvallisuuden toteutusta ja ylläpitoa normaalioloissa ja tulee tarkistaa vuoden kahden välein. Sen avulla laaditaan tietoturvallisuuden kehittämisohjelma suunnitelman päivitysjaksolle. Tietoturvasuunnitelmia on koko organisaation lisäksi syytä laatia myös pienemmille kokonaisuuksille, kuten yksittäisille tietojärjestelmille.

Samankin tiedon tai tietojärjestelmän kriittisyysaste voi vaihdella tilanteesta ja ajankohdasta riippuen. Esimerkiksi palkanlaskentajärjestelmä ja sen tietoliikenneyhteys pankkiin ovat kriittisiä palkanmaksun aikaan, muulloin se voi kestää useankin päivän katkoksia. Tavoiteltavaa turvallisuustasoa ja sen edellyttämää resursointia harkittaessa tulee tällaiset vaihtelevat tarpeet huomioida. Ohjeita tietoturvallisuuden suunnitteluun löytyy mm. julkaisusta [1].

Oppaassa julkishallinnon tietoturvakoulutuksen järjestämisestä [2] luvussa 6 on esimerkki organisaation tietoturvaohjeistuksesta. Kussakin organisaatiossa tarvittavat ohjeet on johdettava organisaation toiminnasta. Ohjeistuksessa on syytä huomioida myös eri kohderyhmät ja heidän tarpeensa.

Tietoturvasuunnitelmat ja ainakin osa tietoturvallisuuteen liittyvästä ohjeistuksesta eivät ole julkisia (viranomaisia koskien esim. JulkL 24§ 1 mom 7 kohta) ja niiden jakelu voi olla rajoitettua myös organisaation sisällä.

2.1.3 Koulutus

Pelkkä ohjeistus ei riitä. Tärkeää on kouluttaa ja valmentaa henkilökunta ohjeistuksen mukaiseen toimintaan ja muutoinkin edistää henkilökunnan tietoturvatietoisuutta. Koulutus ja tiedotus ovat jatkuvaa toimintaa. Erityisesti sitä tarvitaan uusien järjestelmien, ohjeiden ja lainsäädännön yhteydessä.

Kuten ohjeistuksessa myös koulutuksessa tulee huomioida eri kohderyhmien tarpeet. Tietoturvallisuuden kehittäminen koko organisaation tasolla edellyttää myös johdon koulutusta ja heille suunnattua riittävää tiedotusta ajankohtaisista tietoturvakysymyksistä. Tietojärjestelmien tietoturvallisuuden suhteen erityisesti teknisen ja tukihenkilöstön tietojen ajantasaisuus on ensiarvoisen tärkeää. Peruskäyttäjän koulutuksesta löytyy lisätietoa [2] sekä siihen liittyvistä *Käyttäjän tietoturvaohjeesta* [3] ja VAHTIn koulutus-CD:ltä. CD:n materiaali on muokattavissa organisaation omiin tarpeisiin. *Valtionhallinnon tietoturvallisuuden kehitysohjelman* 2004-2006 [4] pohjalta käynnistetty Peruskäyttäjien tietoturvatyö -jaosto tulee myös tuottamaan materiaalia tähän tarkoitukseen ja päivittämään CD:n sisällön.

2.1.4 Vastuut

Tietoturvallisuudesta on omalta osaltaan vastuussa jokainen tietoja käsittelevä henkilö. Keskeisellä sijalla on ylimmän johdon sitoutuminen tietoturvallisuuden kehittämiseen ja siten myös sen resursoimiseen. Erityiset vastuut (ylin johto, hallinto, tietohallinto, turvallisuus- ja tietoturvallisuusjohto, tekninen henkilöstö, tietojärjestelmien omistajat jne.) tulee selkeästi määritellä ja saattaa henkilöstön tietoon. Samoin lakisääteiset vastuut tulee tuoda esiin (ks. esim. SVTSL, erityisesti luku 3).

Tietoturvallisuusvastuut on hyvä kirjata osaksi henkilöiden toimenkuvia. Kuten kaikessa toiminnassa vastuiden ja toimivaltuuksien tulee olla oikeassa suhteessa toisiinsa. Tietoturvallisuuden vastuullinen ylläpito ja kehittäminen ovat mahdollisia vain, jos käytössä on riittävät taloudelliset ja henkilöresurssit sekä valtuudet puuttua tietoturvallisuutta vaarantaviin toimintoihin ja toimintatapoihin koko organisaatiossa.

Vastuiden määrittelyssä tulee huomioida niiden jakautuminen vastuuseen normaalitilanteissa ja tietoturvapoikkeamatilanteiden aikana. Poikkeamatilanteissa joudutaan tekemään koko organisaation tietojenkäsittelyyn vaikuttavia päätöksiä usein nopeasti ja puutteellisin tiedoin: esimerkiksi milloin katkaistaan koko organisaation verkkoyhteydet järjestelmien suojaamiseksi tai voidaanko tuhoutunutta tietoa turvallisesti palauttaa varmuuskopioilta. Poikkeaman ilmenemisajankohdasta riippuen käytettävissä ei välttämättä ole koko organisaation asiantuntemus. Toimenpidepäätösten vastuutuksen poikkeamatilanteissa (kenellä, missä tilanteessa, minkä asioiden suhteen) on oltava selkeä ja niiden tekijällä tulee olla johdon tuki. Myös muu henkilökunta on koulutettava ymmärtämään poikkeamatilanteiden erityisvaatimukset. Esimerkkejä tietoturvallisuuteen liittyvistä vas-

tuujaoista löytyy mm. *Valtion viranomaisen tietoturvallisuustyön yleisohjeesta* [5, luku 2.4] ja [1, Liite 4a]. Poikkeamatilanteiden toimivaltuuksia ja vastuita käsitellään tämän ohjeen luvussa 2.2.4 *Reagoinnin organisointi ja toimivaltuudet*.

2.1.5 Tietoturvallisuuden seuranta, valvonta ja raportointi

Tietoturvallisuuden kehittäminen ja ylläpito edellyttävät jatkuvaa seurantaa, johon kuuluvat tietoturvallisuuden valvonta sekä tietoturvallisuuden tason ja poikkeamien tilastointi ja raportointi. Seurannan tulee kohdistua koko tietoturvallisuuteen, ei vain tietotekniikan turvallisuuteen. Säännölliset ja systemaattiset tietoturva-auditoinnit tarjoavat tietoa tietoturvallisuuden tilasta.

Tietoturvallisuus on osa yksiköiden tulosohjausta. Tietoturvallisuuden tulostavoitteiden asettamisen yhteydessä määritellään myös seurannassa käytettävät mittarit, joita voivat olla esimerkiksi vakavien häiriötilanteiden lukumäärä sekä imagomenetyksistä johtuvien ongelmien välttäminen. Tietoturvallisuuden tulosohjauksesta tarkemmin *Tietoturvallisuus ja tulosohjaus* [6]. Myös *Valtionhallinnon tietoturvallisuuden kehitysohjelman 2004-2006* [4] Tietoturvallisuus ja tulosohjaus –työryhmä tulee tuottamaan aineistoa tähän tarkoitukseen.

Suunnitellusti toteutettu ja henkilökunnalle tiedotettu seuranta vaikuttaa sekä ennaltaehkäisevästi että auttaa havaitsemaan poikkeamatilanteet mahdollisimman nopeasti. Seurantaa toteutetaan sekä automaattisesti teknisin keinoin että henkilöiden toimesta esimerkiksi osana esimiesvastuuta. Tietoturvallisuuden teknisen valvonnan operatiivisesta toteutuksesta vastaavalle ylläpidolle tulee antaa selkeät ohjeet, joissa on huomioitu myös asiaa koskeva lainsäädäntö, keskeisimpinä henkilötietolaki, sähköisen viestinnän tietosuojalaki ja laki yksityisyyden suojasta työelämässä. Tietoturvapoikkeamien teknistä havainnointia käsitellään tarkemmin luvussa 3.1 *Tietoturvapoikkeaman havaitseminen*.

Toimenkuviin sisällytetään tietoturvavastuiden osana tietoturvallisuuteen liittyvät valvonta- ja raportointivelvoitteet. Ylimmällä johdolla on valvontavastuu tietoturvan asianmukaisuudesta. Organisaation tietoturvavastaavan tehtävänä on koordinoida tietoturvallisuuden seuranta ja tuottaa saadun aineiston perusteella johdon tarvitsemat raportit. Raportointi toimii omalta osaltaan pohjana organisaation tietoturvan kehityssuunnitelmien laadinnalle ja resursoinnille sekä tuottaa tietoa myös organisaation yleiseen riskienhallintaan. Lisätietoa tietoturvallisuuden seurannasta löytyy mm. [6, luku 5] ja [1, esim. luku 6.2].

2.1.6 Ulkoistaminen tai alihankinta

Tietojärjestelmiin tai tietoturvallisuuteen liittyvien toimintojen ulkoistusta tai alihankintaa harkittaessa tulee tietoturvariskit arvioida perusteellisesti. Jos siitä huolimatta hankintaan päädytään, on muistettava, että tietoturvallisuuteen liittyvät vastuut pysyvät aina

organisaatiolla itsellään. Tämä edellyttää riittävää tietoturvaosaamista organisaation sisällä. Ulkopuolisen toimittajan tietoturvallisuuteen liittyvät vastuut ja oikeudet tulee kirjata selkeästi sopimuksiin sekä varmistua toimittajan oman tietoturvallisuuden ja tietoturvallisuuteen liittyvän osaamisen riittävästä tasosta. Erityisesti kriittisten järjestelmien osalta on suhtauduttava varauksellisesti Force Majeure -pykäliin, koska kriittisten järjestelmien on toimittava myös tilanteissa, joissa palveluntarjoaja pyrkii vähentämään vastuutaan sopimusteknisin keinoin.

Toimittajan velvollisuuksiin tulee sisällyttää määriteltyjen tietoturvallisuuden kriteereiden jatkuva seuranta ja niistä raportointi. Sopimuksissa on kiinnitettävä erityistä huomiota tietoturvapoikkeamatilanteiden käsittelyyn: toimittajan on ryhdyttävä poikkeaman havaittuaan välittömästi korjaaviin toimenpiteisiin. Tämä edellyttää toimittajalta riittäviä resursseja useankin asiakkaan yhtäaikaiseen poikkeamatilanteiden käsittelyyn (esim. maailmanlaajuinen virusepidemia lamauttaa useamman asiakkaan toiminnan). Ulkoistetuille tietojärjestelmille on toimittajan puolelta nimettävä vastuulliset yhteyshenkilöt, joihin ollaan yhteydessä poikkeamatilanteissa.

Poikkeamatilanteiden päätöksentekovastuut on määriteltävä vastaavasti kuin organisaation sisälläkin. Lisäksi sopimuksiin tulee määritellä, että tilaajalla on oikeus saada tarvittaessa käsiteltäväksi toimittajalle kertyneet tilaajaa koskevat loki- tai muut tiedot poikkeamatilanteiden selvittämiseksi (ellei laki toisin määrää). Lisätietoa ulkoa ostetun toiminnan tai palvelun tietoturvakysymyksistä löytyy mm. *Valtionhallinnon tietohallintotoimintojen ulkoistamisen tietoturvasuosituksesta* [7].

2.1.7 Riskien hallinta

Tietoturvariskien hallinta on osa organisaation yleistä riskienhallintaa. Se edellyttää aktiivista yhteistyötä tietoturvallisuuden ja muiden riskien hallinnan asiantuntijoiden välillä. Palvelun tai toiminnon hyöty on kyseenalainen, jos sen riskejä ei aktiivisesti hallita. Riskikartoituksen tulee olla mukana palveluiden ja toimintojen suunnittelusta lähtien. Sisäisen tarkastuksen tulee valvoa kriittisten järjestelmien riskienhallintaa.

Riskikartoitusten avulla organisaatio muodostaa kuvan tietoturvallisuutensa nykytasosta. Tavoitteena on löytää uhkatekijät sekä arvioida uhkien todennäköisyys ja niiden seurausten vakavuus. Kartoituksia on tarpeen tehdä säännöllisesti ja monella tasolla: koko organisaatio, osastot tai muut yksiköt, toimintaprosessit, erilaiset tietojärjestelmät, palvelimet tai muut laitteistokokonaisuudet jne.

Riskikartoitusten ja tietoturvapolitiikassa asetettujen tasovaatimusten perusteella valmistellaan tietoturvasuunnitelma(t). Suunnitelmassa otetaan kantaa, kuinka riskeihin suhtaudutaan. Riskiä ja sen suuruutta voidaan hallita eri menetelmin vaikuttaen riskin todennäköisyyteen, siihen liittyvään haavoittuvuuteen tai seuraukseen. Riskiä voidaan pyrkiä pienentämään hyvällä tietohallinnolla tai se voidaan hyväksyä. Riskin poistaminen kokonaan ei useinkaan ole mahdollista.

Hyvänä lähtökohtana riskikartoituksessa toimii tietoturvallisuuden jako kahdeksaan osa-alueeseen. Riskien arvioinnista lisää tietoa löytyy mm. *Ohjeesta riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa* [8]. Myös *Valtionhallinnon tietoturvallisuuden kehitysohjelman 2004-2006* [4] Tietoturva-arvioinnit –työryhmä tulee tuottamaan aineistoa tähän tarkoitukseen.

2.1.8 Tietojärjestelmien turvallinen ylläpito

Edellä olevien hallinnollisten toimenpiteiden lisäksi tiedon turvaamiseen tarvitaan niihin liittyvien tietojärjestelmien suunnitelmallista ja turvallista ylläpitoprosessia, jonka tavoitteena on ennaltaehkäistä tietoturvapoikkeamia ja minimoida niiden vaikutusta. Se edellyttää tietoturvallisuuden ennakoivaa huomioimista järjestelmien kehittämisessä ja ylläpidossa koko järjestelmän elinkaaren ajan, sekä varsinaisten ylläpitotoimenpiteiden turvallista toteutusta.

Turvallisessa ylläpidossa ylläpitotoimenpiteiden suunnittelun merkitys korostuu. Tietojärjestelmien ylläpidosta laadittu organisaatio- ja järjestelmäkohtainen ohjeistus helpottavat ylläpitotoimenpiteiden tietoturvallista toteutusta. Ohjeistuksen tulee rajata sallittuja ja kiellettyjä ylläpitotoimenpiteitä eri käyttötilanteissa sekä määritellä vastuurajat käyttöhenkilöstölle. Yleisten ”hyvien käytäntöjen” soveltuvuus omaan organisaatioon tulee aina arvioida.

Turvallinen ylläpito edellyttää omien järjestelmien ja niiden normaalitilan tuntemista, aktiivista tietoturvahaavoittuvuuksien seurantaa ja järjestelmien tietoturvatason testaamista. Erilaiset tietoturvallisuutta käsittelevät www-sivut ja postituslistat tarjoavat ajankohtaista tietoa uhkatilanteesta.

Käyttöjärjestelmät ja ohjelmistot on pyrittävä pitämään ajan tasalla päivittämällä ja paikkaamalla tunnetut tietoturva-aukot, kun se on mahdollista. Päivitystarve harkitaan oma ympäristö huomioiden. Varsinkin laajojen korjausten toiminta ja integroituminen omaan ympäristöön on testattava ennen tuotantokäyttöön ottamista.

Riskejä tulee hallita myös muutoin. Esimerkiksi haavoittuvien järjestelmien verkkotekninen eristäminen pyritään suunnittelemaan siten, että järjestelmän käyttö on yhä mahdollista, mutta haavoittuvuuden väärinkäyttö on hankalaa ja siitä jää todisteet. Nämä tehtävät kuuluvat kaikkien käyttöjärjestelmistä ja ohjelmistoista vastaavien työhön, mikä on huomioitava myös henkilöiden toimenkuvassa.

Turvallisessa ylläpidossa keskeisiä huomioitavia seikkoja ovat esimerkiksi

- tietoturvallisuuden kerroksellisuus ja mahdollisimman suurien kokonaisuuksien tehokas suojaaminen: esimerkiksi virustarkistus postipalvelimella ja tehokkaasti suojatut harvat liityntäpisteet julkiseen verkkoon asettavat vähemmän paineita työasematasolle
- järjestelmien ylläpidossa käytettyjen tietoliikenneyhteyksien tietoturvallisuus
- verkon ositus siten, että verkon seurantaa ja pääsynvalvontaa voidaan toteuttaa tarkoituksenmukaisesti

- jatkuvuussuunnittelu, erityisesti ohjelmistopäivitysten osalta
  - käytettävillä käyttöjärjestelmäversioilla tulee olla toimittajan tuki
  - ohjelmistoista ja palveluista on syytä käyttää vain luotettuja versioita
  - järjestelmiin tehtävät konfiguraatio- ja ohjelmistopäivitykset sekä muutokset tulee suunnitella ja testata erillisessä testiympäristössä ennen toteutusta itse tuotantojärjestelmässä
  - toimenpidesuunnitteluun kuuluu varasuunnitelman laatiminen epäonnistuneesta päivityksestä tai järjestelmämuutoksesta palautumiseksi
- haittaohjelmilta on syytä suojautua paitsi käyttöjärjestelmäpäivitysten myös ajan tasalla olevan virustorjuntaohjelmiston avulla, erityisesti Windows-järjestelmissä ja enenevässä määrin erilaisissa mobiililaitteissa
- käytössä on riittävät menettelyt suunnittelemattomien järjestelmämuutosten havaitsemiseksi (esim. IDS-järjestelmät, tarkistussummat)
- pääkäyttäjän oikeudet on vain nimetyillä ylläpitäjillä ja niiden käyttö on suunnitelmallista (käytetään vain tarvittaessa, oikeudet kasvatetaan pääkäyttäjäksi henkilökohtaisilla ylläpitosalasanoilla eikä pääkäyttäjän salasanalla)
- laitteistojen ajantasaisuudesta ja riittävästä kapasiteetista sekä varalaitejärjestelyistä huolehditaan
- huolto- ja ylläpitosopimusten tarve niin laitteistoille kuin ohjelmistoillekin tulee miettiä ja sopimukset pitää ajan tasalla
- kriittisille järjestelmille voidaan harkita myös sopimuksia varajärjestelyistä
- huoltosopimusten lisäksi laiterikkoihin varaudutaan tarvittaessa laitteistojen tarkoituksenmukaisella kahdennuksella tai laajemmalla monennuksella.

Lähes jokaisella verkkoon kytketyllä tai kytkettävällä laitteella, esimerkiksi monitoimikirjoittimet ja mobiililaitteet, on ominaisuuksia, jotka voivat vaarantaa tietoturvallisuutta (esim. sisäiset muistit, verkkoyhteydet). Kuten kaikilla järjestelmillä, myös niillä on oltava vastuullinen ylläpitäjä, sillä vakavaa vahinkoa aiheuttavissa tahallisissa tietoturvaloukkauksissa käytetään usein välineenä laitetta, jonka tietoturvallisuudesta huolehtimista ei ole suoranaisesti vastuutettu.

2.1.9 Yhteistyö organisaatioiden välillä

Tietoturvallisuuden tasoon vaikuttavat sen kehittämiseen panostettujen henkilöiden määrä ja heidän osaamistasonsa niin tietotekniikan kuin tietoturvallisuuden suhteen. Pienillä organisaatioilla ei välttämättä ole erityisesti tietoturvallisuuteen perehtynyttä henkilöstöä ja tietotekninen osaaminenkin saattaa olla muutaman henkilön varassa. Organisaatioiden välisellä verkostoitumisella ja aktiivisella tietojen vaihdolla voidaan huomattavasti parantaa tietoturvallisuuden tasoa. Erityisen hyödyllistä jatkuva yhteistyö on samantyyppisten organisaatioiden välillä, jolloin ongelmat ovat yhteneviä ja hyväksi havaitut ratkaisut ovat helposti sovellettavissa. Myös päivystyksen osalta voidaan tehdä yhteistyötä.

Jatkuva tietoturvayhteistyö on välttämätöntä esimerkiksi yhteisessä tuotanto- tai toimintaverkossa toimivien organisaatioiden välillä, sillä koko toimintaketjun tietoturvallisuus riippuu siitä, kuinka hyvin kukin organisaatio huolehtii omasta osuudestaan.

Valtionhallinnon tietoturvallisuuden kehitysohjelman 2004-2006 [4] Jaetut tietoturvaresurssit –työryhmä sekä Ympärivuorokautinen tietoturvatoiminta –työryhmä tulevat tuottamaan aineistoa näistä aihepiireistä.

2.2 Reagoimiseen varautuminen

2.2.1 Tietoturvapoikkeamatyypit

Tehokkaan suojautumisen edellytyksenä on tietoturvapoikkeaman mahdollisten aiheuttajien ymmärtäminen. Tietoturvapoikkeamat voidaan jakaa seuraaviin ryhmiin:

- tahattomasti syntyvät tietoturvapoikkeamat
- tahallisesti aiheutetut tietoturvapoikkeamat.

2.2.1.1 Tahattomasti syntyvät tietoturvapoikkeamat

Tahattomasti tai vahingossa syntyviä poikkeamia aiheuttavat esimerkiksi tekniset laitteisto-ongelmat, ohjelmistovirheet, tietoliikennehäiriöt, sähkönsyöttöongelmat sekä luonnonilmiöt, kuten tulvan aiheuttama vesivahinko konesalissa. Tahaton poikkeamatilanne voi aiheutua myös käyttöjärjestelmäpäivityksen sivuvaikutuksista: vaikka päivitys poistaisikin tietoturvahaavoittuvuuden itse käyttöjärjestelmästä, se voi samalla aiheuttaa ongelman käyttöjärjestelmän päällä toimivaan sovellukseen, joka on varautunut aiemman käyttöjärjestelmäversion tapaan toimia. Päivitykset on testattava muualla kuin tuotantojärjestelmässä. Kaikkiin tuotantojärjestelmissä esiin tuleviin sivuvaikutuksiin ei kuitenkaan aina voida testeissä täysin varautua.

Tahattomia, mutta jossain määrin tuottamuksellisia tietoturvapoikkeamia ovat erilaiset käyttäjien ja ylläpidon laiminlyönnit, joissa ei kuitenkaan ole varsinaista tahallista aietta. Henkilökunta saattaa syyllistyä käyttöoikeuksiensa ylittämiseen ilman pahantahtoista aietta. Taustalla voi olla tarve päästä nopeasti käsiksi tietoon, joka sinällään kuuluu työntekijän työtehtäviin, mutta jonka oikeutettu käsittely edellyttää erillistä käyttöoikeuksien hankintaa. Järjestelmien asianmukaisella käyttöoikeushallinnalla nämä tilanteet ovat tavallisten käyttäjien osalta estettävissä.

Vastaavasti ylläpidon laiminlyöntejä voivat olla puutteet järjestelmien toiminnan seurannassa tai käyttöoikeushallinnassa: esimerkiksi ohjelmistoasennuksen onnistumista ei tarkisteta, kriittisen resurssin loppuminen aiheuttaa käytettävyysongelman tai käyttöoikeuksia ei poisteta henkilön työsuhteen loppuessa. Näissä tietoturvapoikkeamissa varsinainen syy on puutteellinen tietoturvallisuuden kokonaishallinnointi.

2.2.1.2 Tahallisesti aiheutetut tietoturvapoikkeamat

Tahallisesti aiheutetuissa poikkeamissa jokin taho on jostakin syystä halunnut käynnistää hyökkäyksen. Nykyisin taustalla on yleensä hyödyn tavoittelu, joskaan hyöty ei välttämättä ole taloudellista. ”Akateemista” hakkerointia järjestelmien toiminnan selvittämiseksi ei enää juurikaan ilmene. Tunkeutuminen tietojärjestelmien kautta mielletään rikolliseksi toiminnaksi yhtä lailla kuin reaalimaailman murrot, joten akateemisella hakkeroinnilla aiemmin tavoiteltu meriitti hankitaan nykyään turvallisuusongelmien selvittämisellä omista järjestelmistä ja haavoittuvuuksien julkaisemisella tietoturva-alan postituslistoilla.

Tahallisesti aiheutetut tietoturvapoikkeamat on hyvä jakaa edelleen kahteen erilliseen alaluokkaan:

- satunnaisesti kohteen valitseviin hyökkäyksiin
- kohdistettuihin hyökkäyksiin,

sillä näiltä suojautuminen edellyttää toisistaan poikkeavia toimenpiteitä.

2.2.1.2.1 Satunnaisesti kohteen valitsevat hyökkäykset

Satunnaisesti kohdistuvissa hyökkäyksissä kohteeksi voi valikoitua mikä tahansa tietojärjestelmä, jossa on hyökkäysohjelmistolla hyödynnettävä haavoittuvuus. Mediassa eniten esillä olevassa poikkeamailmiössä, itsekseen tai viestinnän välityksellä leviävissä haittaohjelmissa, kyse on juuri satunnaisesti kohdistuvista hyökkäyksistä. Hyökkääjä käynnistää hyökkäyksen syöttämällä verkkoon haittaohjelman, jolloin se leviää hyökkäyksen käynnistäjästä riippumatta ja kohteista välittämättä.

Satunnaisesti kohdistetuissa hyökkäyksessä tunkeutuja ei tavoittele kohteen tietosisältöä sinänsä, vaan tarkoituksena on saada hyökkäys leviämään mahdollisimman laajalle. Tunkeutujan tavoitteena voivat olla esimerkiksi:

- identiteetit
- resurssit
- verkon jonkin komponentin haavoittuvuuden osoittaminen mahdollisimman näyttävästi.

Resursseja tai identiteettejä keräävät tunkeutujat kokoavat tyypillisesti saastuttamansa koneet niin sanotuksi bot-verkoksi, jonka koneita voi etäohjata yhdellä kertaa yksittäisillä käskyillä muutaman kontrollikoneen kautta. Tällöin valtavaa määrää suojattomia koneita voidaan käyttää lukuisiin rikollisiin tarkoituksiin koneen laillisen haltijan tietämättä.

Alkuperäinen käyttö bot-verkoille oli hajautettu palvelunestohyökkäys (ks. luku 2.2.1.2.2 *Kohdistetut hyökkäykset*). Nykyisin bot-verkkoja käytetään pääasiassa erilaisiin välitystarkoituksiin, esimerkiksi roskapostin välitykseen. Tällöin tunkeutuja varastaa sekä bot-verkkoon kaapatun koneen verkkoliikenneresursseja että koneen haltijan identiteetin. Vastatoimet kohdistuvat ensinnä kaapatun koneen lailliseen haltijaan eikä roskapostituksen todelliseen tekijään. Myös laitonta materiaalia levitetään usein viattomien sivullisten

koneilta, jolloin levittäjät toisaalta pienentävät kiinnijäämisen riskiä esiintymällä muiden identiteetillä ja toisaalta säästävät verkkokuluissa. Vastaavasti kohdistetun hyökkäyksen tekijä voi peittää jälkensä kierrättämällä yhteytensä lopulliseen kohteeseen useiden botverkon koneiden kautta. Koska varsinaisen kohdeorganisaation lokeista löytyy murretun bot-verkon koneen IP-osoite, esitutkintatoimenpiteet kohdistuvat ensinnä tähän koneeseen ja sen haltijaan.

Usein bot-verkkoon liitettyihin koneisiin on syötetty myös näppäinkaappareita, jotka keräävät talteen koneelta rahanarvoista tietoa, kuten luottokorttinumeroita tai verkkokauppojen tunnus-salasana -pareja. Näitä käytetään ostotapahtumiin uhrin identiteetillä uhrin laskuun.

Haavoittuvuuksien osoittaminen näyttävästi on nykyisistä tahallisista tietoturvapoikkeamista lähimpänä vanhaa idealistista ”akateemista” hakkerointia: hyökkääjän ensisijaisena tarkoituksena ei ole hyödyn tavoittelu tai vahingon aiheuttaminen, vaan hän haluaa osoittaa jonkin komponentin haavoittuvuuden tavalla, joka ei jää huomiotta.

Satunnaisilta hyökkäyksiltä suojautumisessa keskeistä on haavoittuvuuksien korjaaminen, ajantasainen haittaohjelmatorjunta (erityisesti Windows-koneissa ja kasvavassa määrin erilaisissa mobiililaitteissa), johon kuuluu sekä virusten/matojen että vakoiluohjelmien havainnointi, sekä tarkoituksenmukainen konekohtaisten ohjelmistopalomuurien käyttö.

2.2.1.2.2 Kohdistetut hyökkäykset

Kohdistetuissa hyökkäyksissä kohde valitaan tietosisällön tai kohdetta ylläpitävän organisaation perusteella. Niinpä hyökkäyksissä ei lähtökohtaisesti käytetä tunnettuja haittaohjelmia, vaan tunkeutumiset toteutetaan ”käsin” tai tunnistamattomalla haittaohjelmalla, jollaista virustorjunta ei pysäytä.

Tunkeutujan tai muun hyökkääjän tähtäimessä voi olla esimerkiksi:

- identiteetit, joilla pääsee käsiksi johonkin tiettyyn kohteeseen
- palvelun toimintakyvyn haittaaminen
- palvelun tietosisällön muuttaminen tai varastaminen hyötymistarkoituksessa.

Kohdistetuissa identiteettivarkauksissa tunkeutuja voi pyrkiä pääsemään käsiksi sellaisiin välikohteisiin, joiden kautta voi edelleen päästä varsinaiseen kohteeseen tai joista voi kerätä varsinaiseen kohteeseen autentikoiduttaessa tarvittavaa tietoa. Tällaisia välikohteita ovat esimerkiksi kohdeorganisaation työntekijöiden kotikoneet. Pahimmillaan identiteettivarkaus on pääkäyttäjän oikeuksien päätyessä vääriin käsiin.

Tunkeutuja voi pyrkiä haittaamaan tai kokonaan estämään palvelun toiminnan palvelunestohyökkäyksillä. Taustalla voi olla taloudellisia tai myös aatteellisia tavoitteita. Katkerat irtosanotut työntekijät kuuluvat usein tähän ryhmään. Palvelunestohyökkäyksen (Denial of Service, DoS) tarkoituksena on estää tai heikentää verkkojen, järjestelmien tai sovellusten käytettävyyttä, esimerkiksi kuluttamalla järjestelmien resursseja niin paljon, että palvelun normaali käyttö estyy.

Palvelunestohyökkäyksissä voidaan joko käyttää hyväksi jotakin kohteen ohjelmistohaavoittuvuutta

- lähetetään virheellisiä TCP/IP –paketteja palvelimelle, kunnes haavoittuva palvelin kaatuu
- lähetetään virheellisiä komentoja sovellukselle, kunnes haavoittuva sovellus hyytyy

tai yksinkertaisesti ylivoimaa

- tuotetaan valtavia määriä verkkoliikennettä kohteeseen, kunnes verkkokapasiteetti täyttyy roskaliikenteestä
- avataan useita samanaikaisia sisäänkirjautumisyhteyksiä palvelimelle, jolloin muut käyttäjät eivät pääse kirjautumaan palveluun.

Ylivoimaa käytetään erityisesti hajautetuissa palvelunestohyökkäyksissä: satojen tai jopa tuhansien koneiden samanaikainen liikenne haittaa kohteen käytettävyyttä vaikka kohteessa itsessään ei olisi minkäänlaista haavoittuvuutta.

Kohdistetun hyökkäyksen lopullisena kohteena on kuitenkin useimmiten tieto: joko tiedon varastaminen tai sen muuttaminen harhaanjohtavaksi tai käyttökelvottomaksi.

Palvelunestohyökkäyksiä voidaan tehdä ylivoiman turvin hyvin suojattuunkin kohteeseen. Sen sijaan onnistunut tunkeutuminen edellyttää aina haavoittuvuutta, jota tunkeutuja voi käyttää hyväkseen. Helposti hyödynnettävä haavoittuvuus löytyy usein kohdasta, jossa järjestelmään liikkuu tietoa sisään tai ulos. Heikkous voi olla esimerkiksi ohjelmistohaavoittuvuus tietojärjestelmien palvelinohjelmistoissa tai tietojärjestelmän tietoa käsittelevän ihmisen tietoturvapolitiikan vastainen palvelualttius, jota hyödynnetään Social Engineeringin keinoin.

Kohdistetuilta hyökkäyksiltä on olennaisesti hankalampaa suojautua kuin satunnaisilta hyökkäyksiltä, sillä tunkeutuja on yleensä motivoitunut etsimään systemaattisesti haavoittuvuuksia. Suojaus edellyttää tietoturvallisuudelta syvyyttä luvussa 2.1 *Ennaltaehkäisevät toimenpiteet* esitellyllä tavalla.

2.2.2 Esimerkkejä eräisiin poikkeamatilanteisiin varautumisesta

Tässä luvussa annetaan esimerkinomaisesti ohjeita muutamiin tietoturvapoikkeamatilanteisiin varautumisesta.

Seuraavat ennakoivat toimenpiteet ovat suositeltavia palvelunestohyökkäyksen (ks. luku 2.2.1.2.2) ehkäisemiseksi:

- määrittele palomuureihin suodatussäännöstö, joka tunnistaa ja estää väärennettyjä lähdeosoitteita käyttävää liikennettä
- määrittele reunareitittimet ja/tai palomuurit sallimaan vain oman verkon lähdeosoitteilla ulos lähtevä liikenne

- valmistele runkoverkkotason suodatusjärjestelyt verkkopalvelutarjoajan kanssa
- määritä tietoturvaohjelmistot havaitsemaan palvelunestohyökkäykset
- määrittele verkon reunareitittimet ja/tai palomuurit estämään kaikki liikenne, joka ei ole erikseen sallittu
- laadi hyökkäyksen torjuntasuunnitelma, joka sisältää käytettävissä olevat torjuntatoimenpiteet.

Seuraavat ennakoivat toimenpiteet ovat suositeltavia luvaton käyttö –tilanteiden torjunnan valmistelussa:

- huolehdi järjestelmien päivityksistä
- osita verkko
- määrittele hyökkäyksenhavaitsemisjärjestelmä havaitsemaan luvattoman käytön yritykset
- määrittele kaikki työasemat ja palvelimet käyttämään keskitettyä lokipalvelinta
- määrittele toimintatapa kaikkien käyttäjien salasanojen vaihtamiseksi
- määrittele ja harjoittele toimintatapa työaseman tai palvelimen eristämiseksi verkosta
- mieti varmuuskopiojärjestelyt mahdollista todistusaineiston keräämistä varten.

Seuraavat ennakoivat toimenpiteet ovat suositeltavia valmistauduttaessa haittaohjelmien torjuntaan:

- pidä käyttöjärjestelmät ajan tasalla
- käytä ajantasaista, automaattisesti päivittyvää virustorjuntaohjelmistoa palvelimissa ja työasemissa, ainakin Windows-ympäristössä
- määrittele sähköpostipalvelimet ja –asiakasohjelmat toimimaan riittävän suojaavalla turvallisuustasolla, esimerkiksi estämään tiedostojen automaattinen suorittaminen ja liitetiedostojen automaattinen avaaminen
- ohjeista käyttäjiä sähköpostiviestien liitetiedostojen turvallisista käsittelymenettelyistä
- rajoita työtehtävien kannalta tarpeettomia tiedostonsiirto-ominaisuuksia sisältävien ohjelmien käyttöä. Esimerkkeinä vertaisverkko-ohjelmat, musiikkitiedostojen jako-ohjelmat, pikaviestintäohjelmat ja IRC-asiakasohjelmat
- poista työasemista avoimet Windows-tiedostojaot
- käytä työasema- ja palvelinkohtaisia palomuureja
- huomioi erityisesti kannettaviin työasemiin ja muihin mobiililaitteisiin liittyvät riskit (virustorjunnan ajantasaisuus, liityntä suoraan sisäverkkoon)
- määrittele www-selaimen tietoturvamäärittelyt rajoittamaan liikkuvan koodin suorittamista (esimerkkinä allekirjoittamattomat ActiveX-komponentit, javascript-koodi) ja harkitse mahdollinen surffailun tekninen rajoittaminen.

2.2.3 Tietoturvapoikkeamasta tietorikokseen

Tietoturvapoikkeaman yhteydessä on syytä varautua myös rikoksen mahdollisuuteen. Rikokseen syyllistyminen edellyttää tekijältä tahallisuutta tai selkeää tuottamuksellisuutta, joten tahattomista tietoturvapoikkeamista vain raskaat laiminlyönnit, jolla on vakavat seuraukset, voisivat tulla tarkastelluiksi epäiltyinä rikoksina. Sen sijaan tahallisten tietoturvapoikkeamien taustalla on usein rikos. Nykyisin tahallisen tietoturvapoikkeaman aiheuttajat lähtökohtaisesti myös tietävät, että tietojärjestelmät nauttivat omaisuuden suojaa siinä missä fyysinenkin omaisuus.

2.2.3.1 Rikosnimikkeistä

Oikean rikosnimikkeen punnitseminen on poliisin tehtävä, eikä asianomistajan tarvitse ottaa siihen millään tavoin kantaa. Alla on kuitenkin eritelty esimerkinomaisesti eräitä tyypillisiä kriteereitä tietotekniikkaan liittyville rikoksille. Tarkoituksena on helpottaa sen harkintaa, tulisiko tietoturvapoikkeamaa käsitellä rikoksena vai ei. Myös ”perinteisin” menetelmin tehty rikos voi toki aiheuttaa tietoturvapoikkeaman.

Palvelunestohyökkäys voi olla tietoliikenteen häirintää (Rikoslaki, RL, 38:5), mikäli se estää tai häiritsee asiallista liikennettä. Olennaista on nimenomaan liikenteen toiminnan häiritseminen, joten pelkkä käyttäjien häiriintyminen ei riitä. Niinpä postipalvelimen helposti välittämien muutaman sadan roskapostiviestin lähettäminen ei täytä tietoliikenteen häirinnän tunnusmerkistöä[2], vaikka ne vastaanottajia tavattomasti häiritsevätkin. Sen sijaan postijärjestelmän hidastuminen voi muodostaa tietoliikenteen häirinnän. Syinä voivat olla esimerkiksi roskapostin määrä tai virheilmoitukset, jotka johtuvat kohdeorganisaation nimissä väärennetyistä roskaposteista.

Erilaisissa järjestelmiin tunkeutumisissa ja käyttöoikeuksien ylittämisissä voi kyseessä olla tietomurto, joka nimikkeenä kuitenkin väistyy, jos jonkin muun seuraamuksiltaan vastaavan rikosnimikkeen tunnusmerkistö täyttyy. Yleensä kyseessä on ainakin luvaton käyttö (RL 28:7), mutta lukuisat muutkin rikokset voivat tulla kyseeseen riippuen tunkeutujan toiminnasta kohdejärjestelmässä (”vahingonteko”, jos tietojärjestelmään asennetaan jotain tai jos jotain tietoa muutetaan tai poistetaan; ”törkeä viestintäsalaisuuden loukkaus”, jos murretun järjestelmän kautta kuunnellaan viestintäliikennettä tarkoitukseen suunnitellulla ohjelmalla; petos, kiristys…).

Haittaohjelman tekeminen tai levitys täyttävät rikosnimikkeen ”vaaran aiheuttaminen tietojenkäsittelylle” (RL 34:9a) tunnusmerkistön. Rikokseen syyllistyy tällöin kuitenkin vain haittaohjelman tekijä sekä alkuperäinen levitykseen laskija, ei haittaohjelman saastuttaman työaseman haltija, jonka koneelta haittaohjelma on levinnyt edelleen - ellei tut-

[2] Mainosroskapostin lähettäminen saattaa kuitenkin loukata sähköisen viestinnän tietosuojalakia, jonka noudattamista valvoo tältä osin tietosuojavaltuutettu.

kinnassa voida osoittaa leviämisessä työaseman haltijan tahallisuutta tai merkittävää tuottamuksellisuutta.

2.2.4 Reagoinnin organisointi ja toimivaltuudet

Jokainen Internet-verkkoa tai tietojärjestelmiä hyödyntävä organisaatio törmää tietoturvapoikkeamiin lähes varmasti. Niiltä ei voi välttyä siinäkään tapauksessa, että kaikki tietohallintotoiminnot on ulkoistettu. Toimintojen mahdollisen ulkoistamisen jälkeenkin poikkeamareagoinnin hallinnollinen vastuu on organisaatiolla itsellään: organisaation on suunniteltava itse, miten se havaitsee tietoturvapoikkeamat ja reagoi niihin. Poikkeaman ja siihen reagoimisen aiheuttamien vaikutusten analysointia varten organisaatiolla tulee siten olla käytettävissään omaa henkilöstöä, jolla on sekä teknistä että tietoturva-asiantuntemusta. Ulkoistustoimittajan vastuut, palvelutaso ja menettelytavat poikkeamareagoinnin osalta on selkeästi kirjattava sopimuksiin.

Tietoturvapoikkeamien havainnointi ja niihin reagointi on osa järjestelmäylläpitoa. Organisaation yleisistä toimintaperiaatteista johdetaan myös poikkeamareagointia ohjaavat periaatteet. Johdon tulee tavoitetilan lisäksi kuvata yksilöidyt toimintavaltuudet ja poikkeamareagoinnin henkilöresursointi yleisellä tasolla. Yksityiskohtaisissa tietoturvasuunnitelmissa on kuvattava kunkin toiminnon tai tavoitetilan yhteydessä myös, kenen johdolla ja millaisella ryhmällä poikkeamiin varaudutaan ja millä valtuuksilla niihin reagoidaan. Toiminta- ja taloussuunnitelmissa tulee huomioida varautumisen ja reagoinnin kustannusvaikutukset sekä huolehtia, että poikkeamareagoinnissa välttämättömät hankintavaltuudet on annettu oikeille henkilöille.

Poikkeaman vakavuus ja tyyppi vaikuttavat siihen, keitä on kulloinkin otettava poikkeamareagointiin mukaan. Pääsäännöksi on hyvä ottaa, että teknisesti perehtyneitä ja kokeneita reagoijia on aluksi mukana mieluummin liian monta kuin liian vähän.

Toimintaohjeissa on määritettävä ne tunnusmerkit, jotka automaattisesti johtavat reagointiryhmän laajentamiseen ja mahdolliseen operatiivisen johtovastuun siirtämiseen vastuuketjussa ylöspäin. Teknisille ja operatiivisille asiantuntijoille on syytä antaa etukäteen riittävät itsenäiset toimintavaltuudet. Jos toimenpiteet vaikuttavat oleellisesti koko organisaatioon, operatiivisten toimijoiden tulee lisäksi saada toimenpiteilleen organisaation johdon hyväksyntä (parhaimmillaan jo etukäteen yksilöidysti, mutta ainakin erittäin lyhyellä varoitusajalla suullisesti).

Poikkeaman vaikuttavuuden arvioinnissa on oleellista verrata seuraavia asioita poikkeaman itsensä aiheuttamaan uhkaan:

- kyseisen järjestelmän tärkeys yksikön tai sen sidosryhmän toiminnalle ja sen tietosisällön tietoturvavaatimukset
- poikkeaman mahdolliset seurannaisvaikutukset organisaation toimintaan
- poikkeaman ja siihen reagoimisen taloudelliset seuraukset
- poikkeaman vaikutus yksikön julkisuuskuvaan ja sidosryhmiin / yhteistyökumppaneihin.

Järjestelmän vastuuhenkilöiden ja muiden tarvittavien asiantuntijoiden kanssa sovitaan etukäteen, onko, ja millä ehdoin, heihin mahdollista saada yhteys heidän työaikansa ulkopuolella, ja miten yhteydenotot organisoidaan. Poikkeamatilanteeseen reagoiminen onnistuu parhaiten ryhmätyöskentelynä ja siksi epäselvässä tilanteessa kannattaa kaikille järjestelmän ylläpitoon osallistuville saada ainakin tieto epäillystä poikkeamasta ja antaa heille näin mahdollisuus käyttää ja tarjota asiantuntemustaan poikkeaman analysoinnissa. Etukäteen on määritettävä, missä tilanteissa ja kenellä on oikeus kutsua ylläpitäjät ja muut tarvittavat henkilöt hätätöihin, ottaa heidät pois hoitamasta normaaleja arkirutiineja tai teettää heillä tarvittaessa yli- tai lisätöitä.

On muistettava varautua myös siihen, että reagointiryhmän toiminnan käynnistäminen voi itsessään synnyttää poikkeamatilanteen muussa toiminnassa, kun henkilöt siirtyvät käsittelemään poikkeamatilannetta.

Järjestelmästä vastuussa olevan henkilön täytyy olla tavoitettavissa sen mukaan, mitä kyseisen järjestelmän kriittisyys organisaation toiminnan kannalta määrää järjestelmän käytettävyydestä, suojaamisesta ja toipumisesta. Tämä voi edellyttää myös varahenkilöja päivystysjärjestelyjä.

On huomattava myös, että vaikka järjestelmää itseään käytettäisiin vain virka-aikana, se tai siihen vuorovaikutuksessa olevat muut järjestelmät saattavat luonteensa vuoksi vaatia valvontaa muinakin aikoina. Tämä voi aiheuttaa päivystysjärjestelyistä johtuvia lisäkustannuksia.

Päivystyskäytäntö on järkevää toteuttaa, vaikka tuntuisikin siltä, ettei organisaation henkilömäärä anna siihen mahdollisuutta. Päivystysvuorossa olevan henkilön on koko ajan varauduttava jättämään tehtävä, jota juuri hoitaa, ja siirryttävä toiseen. Päivystysjärjestelyn avulla päivystysvuorossa oleva henkilö voi ennakoida, ettei hänen kannata varata päivystysajalle tehtäviä, joissa häntä ei saa häiritä. Kun päivystysvuoro vaihtelee, voidaan aikaa vieviä ja keskittymistä vaativia työtehtäviä hoitaa paremmin. Virka-ajan ulkopuolisen varallaolon korvauksesta tulee sopia etukäteen.

Monilla, varsinkin isoilla organisaatioilla on käytössä erityinen kriisijohtamisen malli, jolla huolehditaan organisaation kriisitilanteissa mm. asiakassuhteista, tuotanto- ja toimitusketjun viivästysten käsittelystä, organisaation imagosta, tarvittavista lisärahoitusjärjestelyistä jne. Merkittävät tietoturvapoikkeamat laajenevat helposti koko organisaation toimintaan vaikuttavaksi kriisiksi, jolloin yleinen kriisinhallinta tulee tietoturvapoikkeamatilanteen hallintaan mukaan.

Työnjako tässä luvussa kuvatun tietoturvapoikkeamien reagointiryhmän ja kriisinhallintaryhmän välillä tulee sopia etukäteen. Reagointiryhmälle kuuluu tällöinkin tietoturvan ja tietotekniikan ammattitaitoa edellyttävä tietoturvapoikkeamaan reagointi eri vaiheineen (ks. tarkemmin luku 3 *Reagoiminen poikkeaman ilmettyä*), tietoteknisen struktuurin kuntoon saattaminen sekä oikean informaation tuottaminen poikkeamatilanteesta. Reagointiryhmän tehtävänä on myös pyrkiä mahdollisuuksien mukaan estämään tietoturvapoikkeaman laajeneminen yleiseksi kriisiksi organisaatiossa. Jos tämä ei ole mahdollista,

yleinen kriisinhallintaryhmä huolehtii poikkeamatilanteen organisaatiolle aiheuttamien vaikutusten hallitsemisesta.

2.2.5 Poikkeamatilanneharjoitukset

Harjoitusten tarkoituksena on kehittää organisaation valmiuksia selviytyä siihen kohdistuvista poikkeamatilanteista mahdollisimman vähin vaurioin ja pienin kustannuksin. Mielekäs harjoitus edellyttää, että organisaatiolla on toipumissuunnitelmia ja ohjeita menetelmistä, joita käytetään poikkeamiin reagoinnissa ja niistä toipumisessa, sekä tarvittavien toimenpiteiden organisoinnista.

Harjoitusten laajuus ja monipuolisuus riippuu olennaisesti organisaation koosta, haavoittuvuudesta, sen käsittelemien tietojen merkityksestä ja luottamuksellisuuden asteesta sekä julkishallinnossa organisaation tärkeysluokituksesta ja velvollisuuksista keskeytymättömien palveluiden tuottamiseen. Harjoitukset skaalautuvat yksittäisestä järjestelmästä tai prosessista useiden organisaatioiden yhteisharjoituksiin

2.2.5.1 Harjoitusten tarkoitus

Tietoturvapoikkeamien reagointi- ja toipumisharjoituksilla pyritään sekä arvioimaan ja kehittämään tehtyjä toipumissuunnitelmia että harjoittamaan reagointiryhmien toimintaa ja johtamista. Harjoitukset tulee suunnitella niin, että eri harjoituksissa tulee testattua reagoinnin ja toipumisen sekä toipumissuunnitelman eri toimintoja.

Toipumissuunnitelman testaamisen tarkoituksena on selvittää, onko varauduttu oikeisiin asioihin, kestävätkö, ja missä määrin, tehdyt suunnitelmat yllätyksiä sekä onko esimerkiksi järjestelmien toipumisjärjestyksessä huomioitu niiden keskinäiset riippuvuudet riittävästi. Yhtenä tavoitteena voi olla selvittää, toimivatko sopimukset yhteistyökumppaneiden kanssa: saadaanko esimerkiksi apua tai varalaitteita sovitussa ajassa ilman esivaroituksia. Sopimuksissa kannattaa mainita myös niiden testaaminen, jolloin testaus esimerkiksi kerran vuodessa ei aiheuta ylimääräisiä kustannuksia. Osin sopimusten testaaminen jää puolitiehen, koska palvelujen priorisointia (kuka saa useita organisaatioita koskevissa poikkeamatilanteissa ensimmäiseksi toimittajan resurssit käyttöönsä) tai muita ulkopuolisia syitä ei voida yleensä testata.

Reagointiryhmän ja sen sidosryhmien harjoitusten tarkoitus on taata saumaton ja tehokas työskentely tilanteen niin vaatiessa. Siihen kuuluu mm.

- tilanteen johtamisen testaaminen, esimerkiksi kyetäänkö tekemään oikeita päätöksiä oikeaan aikaan ja riittävätkö olemassa olevat valtuudet tarkoituksenmukaiseen poikkeamareagointiin
- kuinka hyvin poikkeaman etenemisen havaitseminen ja seuranta edistyy ja tilannekuva kyetään tämän perusteella muodostamaan sekä kuinka vallitsevaa tilannetta kyetään analysoimaan

– kartoitus puutteista ja kehittymistarpeista osaamisessa ja tehtävien hallinnassa
– reagointiryhmän kokoonpanon määrittelyn ja sen tarkoituksenmukaisuuden sekä yhteistoiminnan testaus. Lisäksi testataan esimerkiksi ryhmän reagointikykyä, tiedottamista ja toimivaltuuksien riittävyyttä.

Hyvään ylläpitotapaan kuuluu koko ajan aktiivisesti seurata uhkia ja haavoittuvuuksia sekä uusia teknisiä ratkaisuja. Näiden tietojen hyödyntäminen on tärkeä testauksen kohde. Harjoituksia varten voidaan analysoida erilaisia tietoturvauhkia, jotta tietämys ja ymmärrys niistä kasvaisi.

2.2.5.2 Harjoitustoiminnan suunnittelu

Harjoituksen huolellisella suunnittelulla varmistetaan, että harjoitus kohdistuu niihin asioihin, joita halutaan testata, harjoitus ei luo ennakoimattomia ongelmia ja todellinen poikkeamatilanne harjoituksen aikana voidaan erottaa oikeaksi poikkeamaksi eikä harjoitukseen kuuluvaksi häiriöksi. Tuotantojärjestelmät eivät saa vaarantua harjoituksen tai sen mahdollisten sivuvaikutusten seurauksena.

Harjoitusten on hyvä olla säännöllisiä ja niitä tulisi toteuttaa tarpeeksi usein, jotta harjoitetut asiat ja opit pysyvät toimijoiden mielessä. Harjoitustoimintaa kannattaa suunnitella riittävän pitkäjänteisesti. Harjoittaa voidaan sekä laajojen kokonaisuuksien hallintaa (esimerkiksi lämpötilan nousu laitetilassa on rikkonut useita keskeisiä tuotantopalvelimia) että tehdä yksittäisiä testejä, joissa keskitytään vain yhteen asiaan (esimerkiksi yksittäinen palvelin on murrettu).

Harjoituksissa kannattaa muistaa, että moni ulkoinen tekijä voi todellisessa poikkeamatilanteessa häiritä tilanteen hallintaa. Esimerkkinä häiriöstä voi olla tilanne, jossa yhden reagointiorganisaatioon kuuluvan avainhenkilön on lähdettävä kesken toiminnan hakemaan lapsi tarhasta.

Kaikkien, joiden tulee todellisessa tilanteessa toimia yhteistyössä, on myös harjoiteltava yhteistoimintaa keskenään. Mikäli tarvitaan yhteistyötä ulkopuolisten asiantuntijoiden tai laite-/ohjelmistotoimittajien kanssa, on myös yhteistyötä heidän kanssaan (esimerkiksi sopimusten toimintaa) hyvä testata.

2.2.5.2.1 Harjoituksen perusasioiden määritys

Harjoituksen suunnittelevat ja sen etenemistä seuraavat eri henkilöt kuin ne, jotka toimivat operatiivisesti harjoitukseen osallistuvissa reagointiryhmissä. Harjoitusten suunnittelu aloitetaan harjoituksen perusasioiden määrittelystä. Näitä ovat:

– Harjoituksen ajankohta
  Harjoitus voidaan järjestää siten, että sen ajankohta on etukäteen kaikkien tiedossa tai harjoitus voidaan myös käynnistää operatiivisille toimijoille yllätyksenä. Ongelmallisimpia aikoja poikkeamien kannalta ovat esimerkiksi loma-ajat. Har-

joitusta ei kuitenkaan ole suotavaa järjestää tällaiseen aikaan. Muuna aikana voidaan lomia simuloida siten, ettei koko reagointiryhmä osallistu aktiivisesti toimintaan.
Päätökseen harjoitusajankohdasta ja sen yllätyksellisyydestä vaikuttaa, mitä halutaan harjoitella. Yllätyksellisellä harjoituksella voidaan harjoitella valvontaprosessien sekä hälytys- ja eskalointimenettelyjen toimintaa. Suunniteltu ja etukäteen tiedotettu harjoitus taas voi motivoida reagointiryhmien jäseniä omien tietojen päivittämiseen ja järjestelmien kehittämiseen jo ennakolta.

– Harjoituksen resursointi
Harjoituksen suunnittelu, toteutus ja jälkityöt vaativat sekä aikaa että henkilötyötä. Ilman niihin panostamista harjoitukseen uhrattu aika on kuitenkin turhaa.
– Harjoituksen teema
Mitä halutaan harjoitella ja miten se parhaimmin toteutuu. Harjoituksen teeman myötä tulee valittua myös toiminteet ja henkilöt, joita harjoitetaan.

2.2.5.2.2 Harjoituksen edellytysten varmistaminen

Hyvän harjoituksen edellytyksenä on hyvän suunnittelun lisäksi oikea asenne: harjoituksen tarkoituksena ei ole etsiä virheitä yksittäisten henkilöiden toiminnasta, vaan kyseessä on toimintatapojen ja menetelmien testaaminen. Niistä on tarkoituskin löytää mahdolliset virheet, jotta harjoitus palvelisi myös kohteen poikkeamatilanteissa toimimisen kehittämistä.

Harjoitukseen osallistuvan reagointiryhmän henkilöillä tulee olla ohjeistus ja/tai koulutus siihen tehtävään, johon heidät poikkeamatilanteessa asetetaan. Harjoituksen tulee sisältää yllättäviäkin asioita, esimerkiksi jokin asia tai henkilö ei olekaan tarvittaessa käytettävissä tai saavutettavissa. Tällainen yllätystilanne voi sisältää pikakoulutuksen antamisen esimerkiksi puhelimen kautta jollekin asiaan täysin perehtymättömälle. Ex tempore -asiantuntija olisi todellisessa poikkeamatilanteessa merkittävä riskitekijä, joskin esimerkiksi ajan voittamiseksi se saattaa olla välttämätöntä.

2.2.5.3 Harjoituksen toteutus

Harjoitukset toteutetaan noudattaen suunnitelmaa mahdollisimman tarkasti. Harjoituksen toteutumista seuraavan ohjaajan on joskus puututtava reagointiryhmän toimintaan. Jos todellisessa poikkeamatilanteessa välttämättömiä toimenpiteitä ei jostakin syystä ole mielekästä harjoituksessa toteuttaa, (esimerkiksi jonkin järjestelmän käyttö häiriytyisi liikaa), kuvataan toimenpiteet harjoituksen ohjaajalle, joka hyväksyy ne. Tilannetta jatketaan kuin toimenpiteet olisi tehty. Harjoituksissa toimiva ryhmä saattaa myös lähteä syventymään omasta mielestään oleelliseen asiaan, jota ei harjoituksen suunnittelussa tai edes toiminnan kannalta voida pitää mielekkäänä. Tällöinkin harjoituksen ohjaaja voi puuttua tilanteeseen.

2.2.5.4 Harjoituskertomuksen laadinta ja kokemuksista oppiminen

Harjoituksen jälkityö on tärkeää, jotta harjoituksesta saataisiin kaikki mahdollinen hyöty. Harjoituksen kaikkia osallistujia on kuunneltava ja kaikkien tulee myös osaltaan raportoida, mikä heidän toiminnassaan onnistui ja mikä ei.

Harjoituksen analysointi on hyvä tehdä kahdessa vaiheessa. Heti harjoituksen päätyttyä kerätään ensimmäiset kokemukset ja ajatukset, jotka jo voivat käynnistää kehitystoimenpiteitä. Tämän lisäksi harjoitus käydään siihen osallistuneiden kanssa läpi sen jälkeen, kun harjoituksen suunnittelijat ja ohjaaja ovat perusteellisesti läpikäyneet kaiken harjoituksen yhteydessä tehdyn materiaalin ja dokumentoinnin. Läpikäynnissä on muistettava, että vaikka asiat voivat henkilöityä, on tärkeää, että kaikki kritisoitavat tai kehitettävät asiat tuodaan esiin. Tämä voi yksittäisen henkilön kohdalla tarkoittaa koulutusta tai toimintatavan muutosta. Jälkityöskentelyn ammattitaitoa on tarjota osallistujille rakentavaa palautetta ja kiitosta.

Harjoituskokemusten on tarkoitus kehittää myös itse harjoituksia. Harjoitusten laatukysymyksiin liittyy

- kuinka hyvin harjoitus vastasi tavoitteita
- saatiinko halutut asiat testattua
- toimiko harjoitus suunnitellulla tavalla
- kuinka reagointiryhmä toimi
- aiheuttiko harjoitus ennalta suunnittelemattomia riskejä.

Harjoituksen esille tuomista tietoturvallisuuden kehityskohteista tulee laatia toimenpideluettelo aikatauluineen.

2.2.6 Tietoturvapoikkeamatilanteiden viestintäsuunnitelman luonti

Viestintäsuunnitelmassa määritellään viestintä- ja tiedotusvastuut ja muut viestinnässä huomioitavat asiat. Tässä tiedottamisella tarkoitetaan viestinnän yksisuuntaista osaa, missä organisaatio antaa tietoa toiminnastaan esimerkiksi tiedottein. Tiedottamisen ja viestinnän ero on hyvä pitää mielessä: tiedottaminen luo pohjan vuorovaikutteiselle viestinnälle esimerkiksi ohjaamalla tilanteeseen liittyviä kysymyksiä jo ennalta tiettyyn suuntaan. Poikkeamatilanteissa tiedottaminen on tärkeä osa viestintää. Sen avulla organisaatio voi paremmin huolehtia siitä, että sen antama tieto, ja julkisuuskuva, on linjakas ja johdonmukainen. Tiedottamista täydennetään muilla viestintätavoilla ja vastavuoroisuudella. Jos organisaatiolla on erillinen kriisiviestintäsuunnitelma, tulee tietoturvapoikkeamatilanteiden tiedotus ja viestintä liittää siihen omaksi osakseen.

Tiedottamisen sisäisiä kohderyhmiä ovat mm. organisaation johto, tietohallinto, ylläpitohenkilöstö, helpdesk, mikrotuki, käyttäjät, puhelinkeskus ja viestintäyksikkö sekä mahdollinen kriisinhallintaryhmä. Ulkoisia kohderyhmiä ovat mm. kumppaniorganisaa-

tiot, yleisö, tiedotusvälineet, alihankkijat, asiakkaat ja verkko-operaattorit (ks. myös 2.2.7 *Verkoston ja yhteistyöpolitiikan luominen sidosryhmien kanssa*).

Tietoturva-asioissa tiedottamista ja erityisesti raflaavia ilmaisuja on käytettävä harkiten, etteivät vastaanottajat väsy tai turru. Oikealla tiedottamisella on mahdollista rajata poikkeamasta aiheutuvia ongelmia. Ajantasaisella tiedottamisella vältytään myös helpdeskin ja reagointiryhmän kuormittumiselta asiakkaiden kyselyistä.

Seuraavista asioista tulee olla konkreettiset toimintaohjeet:

– Kuka
  Tiedottamisvastuun on oltava yksissä käsissä ennalta määrätyllä henkilöllä eli poikkeamatilanteen viestintävastaavalla, jolla mielellään on jo kokemusta poikkeamatiedottamisesta. Tilanteen, poikkeaman vakavuuden ja sen aiheuttamien seurannaisvaikutusten muuttuessa saattaa olla tarpeen vaihtaa viestinnästä vastaavaa. Erityisesti organisaation ulkopuolelle kohdistuvan tiedottamisen pitää olla ennalta määrätyllä taholla (ks. 2.2.6.1 *Viestintävastuut*).
– Tiedotetaanko
  Etukäteen on määritettävä se kynnys, joka laukaisee aktiivisen tiedottamisen. Jos organisaatio on paraikaa rikoksen kohteena, voi olla tarpeellista välttää varsinkin julkista tiedottamista asiasta. Kuitenkin, jos käynnissä oleva poikkeama vaikuttaa organisaation ulkopuolelle näkyvään toimintaan (asiakaspalvelu, www-sivut tms.), on ensisijaisesti oltava valmiina aktiiviseen tiedottamiseen ja jätettävä tiedottamatta vain sellaiset asiat, joiden paljastaminen vaikeuttaisi poikkeamasta palautumista tai rikoksen selvittämistä.
– Mille kohderyhmille
  "Tarpeen mukaan": Poikkeamista tiedotetaan pääsääntöisesti vain niille, joiden toimintaan, oikeuksiin tai tietosuojaan poikkeama vaikuttaa. Erityiseen salailuun ei tule ryhtyä, koska julkinen epäilys on haitallisempi kuin faktat todellisesta ongelmasta. Samalla valmistaudutaan julkiseen tiedottamiseen siltä varalta, että asia tulee muuta kautta julkisuuteen.
– Mitä
  "Tarpeen mukaan": Poikkeamatilanteen viestintävastaava päättää viime kädessä myös tiedotettavista asioista. Tämä ei siis ole organisaation viestintäyksikön asia; se päättää vain miten tiedotetaan. Tiedottamisessa on huomioitava turvajärjestelyjen salassapitovaatimukset eli on pidättäydyttävä kertomasta asioita, jotka voivat vaarantaa turvajärjestelyjen varsinaisen toteuttamisen.
– Missä vaiheessa
  Tavoitteena on, että virallinen tiedottaminen pystytään toteuttamaan ennen kuin väärät tiedot lähtevät leviämään epävirallisia reittejä pitkin.
– Oletettavien kysymysten lista
  On mietittävä ja harjoiteltava ennakkoon todennäköisiä poikkeamaan liittyviä kysymyksiä. Tällaisia ovat esimerkiksi poikkeaman mahdolliset vaikutuk-

set organisaation normaaliin toimintaan, kansalaisten tietosuojan mahdollinen vaarantuminen, arvioitu toipumisaikataulu, arvio taloudellisista vahingoista, jo tehdyt ja suunnitellut toimenpiteet viranomaisten kanssa (esitutkinta, korvausvaatimuksiin valmistautuminen jne.). (Ks. Liite 3 *Esimerkkejä tiedotteiden sisällön perusrungosta*, kohta 4)

2.2.6.1 Viestintävastuut

Tietoturvapoikkeamatilanteeseen liittyen viestintä- ja tiedottamisvastuun tilanteen aikana ja sen jälkeen tulee pysyä yhdessä henkilöllä. Kaikki poikkeamaa koskeva tietojen antaminen ja kysymyksiin vastaaminen on tiedottamista, mikä kaikkien asianosaisten on syytä tiedostaa.

Poikkeamatilanteen tiedotuksessa ja viestinnässä voidaan erottaa seuraavat toimijat, joilla kullakin on oma roolinsa:

- poikkeamaviestinnästä ja sen sisällöstä kokonaisvastuun kantava viestintävastaava. Hänellä on hyvä olla jo ennalta kokemusta poikkeamatilanteissa tiedottamisesta, ja tilanteeseen liittyvän tekniikan ja termistön on hyvä olla ennestään tuttua. Viestintävastaava huolehtii, ainakin sisällöllisesti, kaikesta viestinnästä organisaation ulkopuolelle sekä organisaation johdolle.
- organisaation viestintäyksikkö toimii viestinnän ammattilaisena yhteistyössä poikkeamatilanteen viestintävastaavan kanssa.
- reagointiryhmän kontaktihenkilö (voi olla sama kuin viestintävastaava). Reagointiryhmän sisältä määritellään kontaktihenkilö, jonka välityksellä reagointiryhmä tiedottaa poikkeaman vaikutuksista ja saa informaatiota (virheilmoituksia jne.) käyttäjien kanssa suorassa vuorovaikutuksessa olevilta tahoilta. Hän kommunikoi myös tilanteen viestintävastaavan kanssa. Kaikkien reagointiryhmään tulevien sisäisten yhteydenottojen tulee ohjautua kontaktihenkilölle, jotta muulle reagointiryhmälle taataan työrauha (ks. Liite 3, kohta 1).
- vikapäivystys / neuvonta / helpdesk tms. kommunikoi reagointiryhmän kontaktihenkilön kanssa. Se huolehtii loppukäyttäjien neuvonnasta ja toisaalta kerää heiltä poikkeamaan liittyviä havaintoja (ks. Liite 3, kohdat 2 ja 3).

Tietoturvapoikkeamasta tiedottavilta tahoilta edellytetään nopeaa reagointikykyä ja tavanomaista tehostetumpaa viestintää. Viestinnän työnjaon ja vastuiden on oltava selkeitä, ja vastuuhenkilöiden on hallittava tilanteen kokonaisuus. Viestinnän tulee poikkeamatilanteissa olla kaksisuuntaista. Tilanteiden onnistunut hoito vaatii atk-henkilöstön ja viestintäyksikön yhteistä varautumista.

Tässä kuvattua rakennetta kannattaa soveltaa myös pienemmissä organisaatioissa. Niissä sama henkilö todennäköisesti hoitaa kaikkia yllämainittuja tehtäviä, mutta eri roolit kannattaa pitää tällöinkin mielessä.

2.2.6.2 Viestintäkanavat

Poikkeamatilanteissa käytetään kulloinkin parhaiten soveltuvia viestintäkanavia. On huomattava, että osa viestintäkanavista voi olla mahdollisen murtautujan hallussa (salakuuntelu, viestinnän estäminen), tai poikkeaman (www- tai sähköpostipalvelin kaatunut) tai sen mahdollisten sivuvaikutusten (ylikuormitustilanne sähköpostissa) vuoksi viestintä ei saavuta haluttuja kohderyhmiä myöskään organisaation sisällä.

Poikkeamatiedottamisessa on ensiarvoisen tärkeää olla selvillä kaikista organisaatiossa käytössä olevista viestintäkanavista. Selvitystyö tehdään viestintäsuunnitelman käyttöönoton yhteydessä erillisenä helposti päivitettävänä liitteenä. Liitteen tulee sisältää tärkeät puhelinnumerot ja muut yhteystiedot sekä olla saatavilla myös ei-sähköisessä muodossa. Mikäli selvityksessä havaitaan puutteita viestintäkanavissa, ryhdytään toimenpiteisiin uusien kanavien luomiseksi. Viestintäkanavat eritellään sähköisiin ja perinteisiin kanaviin. Esimerkiksi:

Perinteiset viestintäkanavat

- puhelin (neuvonta, vikapäivystys, helpdesk, soittoringit, puhelinkeskus)
- puheposti / vastausautomaatti
- kirjalliset tiedotteet (viikkotiedote, organisaation oma lehti)
- faksi
- ilmoitustaulut
- tiedotteet ovissa yms.
- suullinen informaatio (mikrotuki ym.)
- tiedotusvälineet.

Sähköiset viestintäkanavat

- sähköposti / sähköpostilistat
- tekstiviestit (SMS yhdyskäytävä)
- sähköiset ilmoitustaulut (esim. Intranetissä)
- sisäänkirjautumisviestit
- informatiiviset näytönsäästäjät
- www-sivut (ajankohtaista, tapahtumakalenterit, jne.)
- pikaviestit (netSend, wall)
- uutisryhmät
- info-TV.

Käytettävät kanavat määräytyvät poikkeaman laajuuden, sen aiheuttamien vaikutusten, sähköisten palveluiden sen hetkisen käytettävyyden sekä kohderyhmän perusteella. Tiedottamisen asiasisällöstä päättää aina viestintävastaava tarvittaessa yhteistyössä reagointiryhmän kanssa.

2.2.6.3 Muuta viestinnässä huomioitavaa

Poikkeaman vaikutusten ollessa selkeästi pitkäkestoisia, tulee niiden kohteena oleville henkilöille ja yksiköille antaa välittömästi vaikutusten kiertämistä tai lieventämistä koskevia ohjeita. Muutoksista poikkeamatilanteessa tai tilanteeseen liittyvistä uusista tiedoista tai ohjeista tulee myös tiedottaa käyttäjille. Ohjeiden olemassaolosta tiedottamiseen käytetään samoja tiedotuskanavia kuin poikkeamatiedottamiseen.

Käyttäjien kanssa suorassa vuorovaikutuksessa toimiva taho (helpdesk, vikapäivystys, neuvonta) on pidettävä koko ajan tilanteen tasalla.

Verkoston ja yhteistyöpolitiikan luominen sidosryhmien välille jo ennakkoon edesauttaa huomattavasti poikkeamasta toipumista. Siksi myös nämä on syytä ottaa huomioon viestintäsuunnitelmaa luotaessa ja jokaiselle sidosryhmälle on etukäteen hahmotettava oma roolinsa sekä tiedotuksen kohteena että poikkeaman osapuolena.

2.2.7 Verkoston ja yhteistyöpolitiikan luominen sidosryhmien kanssa

Tietoturvapoikkeamatilanteissa tarvitaan toimivaa yhteistyötä organisaation tietojenkäsittely- ja turvallisuustoimintojen sidosryhmien kanssa. Yhteistyösuhteiden luominen on toteutettava jo normaalitilanteessa. Organisaation kannattaa ylläpitää luetteloa sidosryhmien yhteystiedoista. Omien yhteystietojen muutoksista on aktiivisesti tiedotettava sidosryhmille.

Toipumissuunnittelun yhteydessä on arvioitava tietojärjestelmiltä edellytettävä palvelutaso. Arvioinnissa voidaan käyttää hyväksi myös kriittisiä sidosryhmiä. Tarkastelun tulokset voivat edellyttää mahdollisesti ulkoistettujen palveluiden palvelutasosopimusten tarkastamista ja päivittämistä.

Tietoturvapoikkeamatilanteiden hallinnan kannalta tärkeitä ulkoisia yhteistyökumppaneita ovat:

- kumppaniorganisaatiot, joiden kanssa jaetaan esimerkiksi yhteisiä tietovarastoja tai tietoliikenneverkkoa (esimerkiksi päämiehet, alihankkijat ja asiakkaat)
- organisaation tietoliikennepalvelujen toimittajat
- organisaation ulkoistettujen käyttö- ja huoltopalvelujen toimittajat
- organisaation laitteisto-, käyttöjärjestelmä- ja ohjelmistotoimittajat
- tietotekniikkarikostutkijat ja muut poliisiviranomaiset
- CERT-toimijat
- tila- ja kiinteistöhuoltopalvelut.

Yhteistyökumppaneiden kanssa tulisi vaihtaa seuraavia tietoja:

- yhteystiedot työaikana ja päivystystilanteissa
- toimintavalmius ja palvelutaso työaikana ja päivystystilanteissa

– palvelut ja toimintamenettelyt tietoturvapoikkeamatilanteissa
– mahdolliset salausavaimet (esim. PGP) suojattua yhteydenpitoa varten.

2.3 Toipumiseen varautuminen

Toipumiseen varautumisessa keskeisiä osatekijöitä ovat ajantasaiset jatkuvuus- ja toipumissuunnitelmat sekä niihin liittyvät varajärjestelyt ja huoltosopimukset. Toipumissuunnitelmista lisätietoa löytyy esimerkiksi julkaisusta *Tietotekniikan turvallisuus ja toiminnan varmistaminen* [1, erityisesti luku 6.3] sekä *Valtion viranomaisen tietoturvallisuuden yleisohje* [5, erityisesti luku 4.4]. Tärkeysluokitelluilla organisaatioilla tulee olla myös valmiussuunnitelmat.

Toipumissuunnitelmien pitää olla tarvittaessa saatavilla ja ajan tasalla, jotta niistä olisi hyötyä toipumistilanteessa. Suunnitelmien pohjana on toimintojen ja niihin liittyvien tietojen ja tietojärjestelmien luokitus. Järjestelmille tulee tehdä sekä tärkeys- että turvallisuusluokittelu. Luokittelussa tulee erottaa toisaalta tiedon suojaaminen (luottamuksellisuus ja eheys) ja toisaalta käytettävyydestä johdettavat vaatimukset. Elintärkeä tieto saattaa kestää pitkähköjä katkoja käytettävyydessä ja toisaalta vähemmän kriittisen tiedon käytettävyysongelmat voivat aiheuttaa suurta ylimääräistä työtä ja vaurioita organisaation julkisuuskuvaan. Organisaation toiminnan kannalta elintärkeät toiminnot tulee ylläpitää keskeytyksistä huolimatta mahdollisimman korkeatasoisesti. Yhdessä tietojärjestelmän osassa sattuneen tuhon vaikutusten leviäminen muualle tietojärjestelmään tulee voida välttää.

Järjestelmillä ja prosesseilla tulee olla omat toipumis- ja jatkuvuussuunnitelmansa, joihin sisällytetään ne toimenpiteet, joita tarvitaan toiminnan jatkamiseen poikkeamatilanteissa siihen asti, kunnes toiminta voidaan palauttaa alkuperäiselle käyttötasolle. Kantaa otetaan mm.

– hyväksyttävien käyttökatkosten kestoon
– käyttöoikeuksien rajoittamiseen poikkeamatilanteen aikana
– varajärjestelyiden ja –laitteistojen tarpeeseen ja toteutukseen
– varajärjestelyihin siirtymiseen ja sen ajankohtaan sekä varajärjestelyistä takaisin palaamiseen
– tiedon ja ohjelmistojen korruptoitumisesta toipumiseen.

Suunnitelmissa tulee huomioida myös henkilöriskien toteutuminen (esimerkiksi oikea henkilö ei ole käytettävissä ja varamiesjärjestely on puutteellinen, sama henkilö on suunniteltu useampaan samanaikaiseen tehtävään, avainhenkilöryhmä saa samanaikaisesti ruokamyrkytyksen).

Järjestelmäkohtaisten ja henkilöstöä koskevien toipumissuunnitelmien lisäksi tarvitaan dokumentointi tietojärjestelmien riippuvuuksista ja niiden käyttökatkosten sivuvaikutuksista.

Varajärjestelyt voivat olla manuaalisia ja teknisiä. Esimerkiksi käsikirjanpito tapahtumista tai lomakkeiden kerääminen mahdollistavat tietojen ajantasaistuksen tietojärjestelmiin viiveellä poikkeaman selvittyä. On syytä myös harkita, onko osa tietojärjestelmissä olevasta tiedosta tarpeen määräajoin tulostaa tai replikoida muussa muodossa poikkeamatilanteissakin käytettävään muotoon. Erityisesti toipumissuunnitelmien on oltava myös muussa kuin sähköisessä muodossa.

Tekniset varajärjestelyt pitävät sisällään tiedon varmuus- ja suojakopioiden sekä ohjelmistojen jakelumedioiden hallinnan, omat varaosat ja muut varalla olevat laitteet sekä tietojärjestelmäympäristön ja tietoliikenneverkon eritasoiset replikoinnit. Varajärjestelmän käyttöönotto voi tapahtua automaattisesti tai edellyttää ylläpidon toimenpiteitä. Varajärjestelmään siirtymä ja paluu tulee olla huolellisesti ohjeistettu.

Asianmukaisilla huolto- ja ylläpitosopimuksilla lyhennetään merkittävästi palvelujen käyttökatkoksia ja vältetään budjettitekniset ongelmat esimerkiksi kalliin laitteiston rikkoutuessa. Varalaitteistot ja -tietojärjestelmäympäristöt voivat olla myös oman organisaation ulkopuolella. Esimerkiksi valtionhallinnon yksiköillä on mahdollisuus tehdä sopimus Huoltovarmuuskeskuksen kanssa.

3 REAGOIMINEN POIKKEAMAN ILMETTYÄ

3.1 Tietoturvapoikkeaman havaitseminen

Ensimmäisen havainnon tietoturvapoikkeamasta voi tehdä kuka tahansa, esimerkiksi organisaation työntekijä, tietojärjestelmän ylläpito tai jopa joku ulkopuolinen. Organisaation henkilöstöllä tulee olla ohjeet, kehen tai mihin ottaa yhteyttä eri poikkeamatilanteissa. Tietojärjestelmiin liittyvissä poikkeamissa on otettava heti yhteyttä organisaation tietoturvavastaavaan tai tilanteen mukaan ylläpitoon, lähitukeen tai palvelupisteeseen (helpdesk, vikapäivystäjä). Muille poikkeamatyypeille on oma ohjeistuksensa.

Jos poikkeaman kohteena tai lähteenä on ulkoistettu tietojärjestelmä, huolehditaan reagoinnista tiiviissä yhteistyössä ulkoistustoimittajan vastuuhenkilöiden kanssa sopimusten mukaisesti.

Alustava arvio tietoturvapoikkeamasta tehdään, kun tieto siitä tulee mainituille henkilöille. Ylläpito voi poikkeaman havaitessaan tehdä alustavan arvion itsekin. Arvioita tekemään ryhtyvän henkilön on syytä jo ennen varsinaisia toimenpiteitä miettiä

- mitä tämä voisi olla?
- onko asialle ns. hyvää selitystä vai voiko kyse olla tietoturvapoikkeamasta?
- mitä tämä pahimmillaan voisi olla?
- kuinka laajaksi poikkeama on levinnyt: missä sitä on ja missä sitä ei ole (vielä)?

Alustavan arvio voi edellyttää joitain tarkistussoittoja tai selvityksiä, mutta siinä vaiheessa, kun tilanne ei näytä rutiininomaiselta, tulee reagointivastuu siirtää kyseisen järjestelmän ennalta määrätylle reagointiryhmälle (ks. luku 2.2.4 *Reagoinnin organisointi ja toimivaltuudet*). Arvion tekijän on myös päätettävä, kuinka nopeasti hän kutsuu reagointiryhmän koolle. Kutsuminen työajan ulkopuolella merkitsee hätätyöhön kutsumista, josta seuraa aina myös kustannuksia.

3.1.1 Indikaatiot ja ennusmerkit

Mahdollista tietoturvapoikkeamaa voidaan epäillä indikaatioiden ja ennusmerkkien perusteella. Indikaatiot ilmaisevat tietoturvapoikkeaman tapahtuneen tai olevan tapahtumassa parasta aikaa. Esimerkkejä indikaatioista:

- verkkotason hyökkäyksenhavaitsemisjärjestelmä hälyttää postipalvelimeen kohdistuvasta puskuriylivuotohyökkäyksestä
- virustorjuntaohjelmisto hälyttää tietojärjestelmästä löytyneestä haittaohjelmakoodista
- internet-palveluntarjoaja, CERT-toimija tai kolmas osapuoli ilmoittaa epäilyttävistä liikennehavainnoista koskien organisaation omaa osoiteavaruutta
- www-palvelin kaatuu
- käyttäjät valittavat Internet-yhteyden huomattavasta hitaudesta
- järjestelmäylläpitäjä havaitsee tiedostonimen, joka sisältää outoja merkkejä
- käyttäjä soittaa helpdeskiin raportoidakseen uhkaavasta sähköpostiviestistä
- palvelinjärjestelmän eheydenvalvontaohjelmisto ilmoittaa konfiguraatiomuutoksesta huoltoikkunan ulkopuolella
- sovellus ilmoittaa useista epäonnistuneista kirjautumisyrityksistä tuntemattomasta organisaation ulkopuolisesta järjestelmästä
- sähköpostijärjestelmän ylläpitäjä havaitsee huomattavan määrän käyttäjille palautuvia viestejä
- verkkoylläpitäjä havaitsee epätavallisen poikkeaman verkon liikenneprofiilissa
- organisaation kirjanpidon luvut poikkeavat odotetusta
- helpdeskiin tulee outoja puheluita
- IRC- ja keskustelukanavilla näkyy organisaation tietojärjestelmiin liittyviä tietoja tai kommentteja
- konesalin olosuhdehälytin hälyttää.

Joissain tilanteissa organisaatio voi havaita tietoturvapoikkeamatilanteen ennusmerkkejä. Esimerkkejä ennusmerkeistä:

- www-palvelimen lokitiedostossa on merkintöjä, jotka viittaavat www-haavoittuvuusskannerin käyttöön palvelinta kohtaan
- ilmoitus uudesta hyödyntämismenetelmästä organisaation postipalvelimen haavoittuvuudelle
- hakkerointia harjoittavan aktivistiorganisaation uhkaus hyökkäyksestä organisaatiota kohtaan
- levypalvelimesta kuuluu ääntä, joka viittaa fyysiseen vikaan levyjärjestelmässä
- organisaatio on normaalia runsaammin hakkereiden mielenkiintoa herättävällä tavalla esillä mediassa.

Indikaatioita tai ennusmerkkejä tietoturvapoikkeamatilanteista voidaan saada esimerkiksi seuraavista lähteistä:

- tietoturvaohjelmistojen hälytykset
  - verkko- ja tietojärjestelmäkohtaiset hyökkäyksen havaitsemisjärjestelmät (NIDS, HIDS)
  - antivirus-ohjelmistot
  - tiedostojen eheyden tarkistusohjelmistot
  - palveluiden käytettävyyden mittausohjelmistot
- lokitiedostot
  - käyttöjärjestelmän, palveluiden ja sovellusten lokitiedostot
  - verkkoelementtien (esimerkiksi reitittimet, kytkimet, kuormanjakolaitteet) lokitiedostot
  - honeypot-järjestelmien lokit
- julkisesti saatavilla olevat tietolähteet
  - haavoittuvuusinformaatio
  - tiedot muihin organisaatioihin kohdistuvista /muista organisaatioista lähtevistä hyökkäyksistä
- erilaiset keskusteluryhmät/kanavat
  - IRC-kanavat
  - NEWS-ryhmät
  - postituslistat
- olosuhdehälytykset
  - lämpötila
  - kosteus
  - liiketunnistin
  - palo
- käyttäjät
  - käyttäjien yhteydenotot asiakaspalveluun/ylläpitoon tietojärjestelmien tai muiden käyttäjien poikkeavan toiminnan johdosta.

Indikaatiot ja ennusmerkit voivat aiheuttaa tarpeen organisaation operatiivisen valmiustason nostamiseen. Esimerkiksi verkon aktiivilaitteiden seurantaa tehostetaan, ohjelmistojen päivitystasot tarkistetaan sekä varallaolo- ja päivystysrutiineja tehostetaan.

3.2 Reaaliaikaisen tapahtumapäiväkirjan pitäminen

Tietoturvapoikkeamien käsittelyssä tehtävät havainnot, päätökset ja toimenpiteet kirjataan. Tapahtumapäiväkirjaa aletaan pitää poikkeaman havaitsemisesta lähtien ja siihen kir-

jataan ajankohta, mitä on tehty, kuka on tehnyt, mikä on toimenpiteiden vaikutus ja mahdolliset lisätiedot. Päiväkirjasta on hyvä käydä ilmi ainakin seuraavat asiat (ks. tarkemmin Liite 4 *Poikkeaman dokumentaatioon kirjattavia asioita*):

- tietoturvapoikkeamatilanteen nykystatus
- tiivistelmä tilanteesta
- kaikkien tilannetta hoitaneiden henkilöiden toimenpiteet poikkeaman johdosta
- kaikkien tilanteeseen osallisten tahojen yhteystiedot (esimerkiksi järjestelmien omistajat, järjestelmäylläpitäjät)
- lista tilanteen aikana kerätystä todisteaineistosta
- tilannetta hoitaneiden henkilöiden kommentit
- seuraavat toimenpiteet tilanteen johdosta.

Jokainen kirjaa kaikki asiaan liittyvät toimenpiteensä. Reagointiryhmän johtaja vastaa tietoturvapoikkeaman selvitystyön dokumentoinnista kokonaisuutena. On hyvä, että jokainen kirjoittaa itse omat muistiinpanonsa, koska siten tapahtumat on tarvittaessa helpompi palauttaa mieleen. Apuna voidaan käyttää myös sanelukonetta, jolloin tieto voidaan purkaa kirjalliseen muotoon myöhemmin. (Ks. Liite 5 *Esimerkki poikkeaman dokumentoinnista*)

3.3 Tapahtuma-analyysi

Poikkeamaan reagoinnin alkuvaiheessa päätökset joudutaan usein tekemään puutteellisten tietojen nojalla, mikä on tiedostettava ennen korjaustoimiin ryhtymistä. Tässä vaiheessa on aktiivisesti varmistettava myös tietoja ja toimintoja, joissa ei vielä ole huomattu ongelmia. Poikkeaman rajoittamisen ja onnistuneiden ensitoimenpiteiden tähden on tärkeää, että poikkeaman analysointi aloitetaan mahdollisimman nopeasti ja siten saadaan selvyys, mitä todella on tapahtunut ja mitkä seikat ovat vain oireita. Syiden ja oireiden erottaminen on tärkeimpiä selvityksen kohteita, koska korjausten on kohdistuttava (ainakin ensin) syihin: jos maitoa valuu pöydälle, ei kannata aloittaa kuivaamalla lattiaa sitä mukaa kun maito valuu sinne.

Tapahtuma-analyysissä arvioidaan poikkeaman tyyppi, laajuus ja vakavuus. Seuraavissa taulukoissa on esimerkkejä tyyppi- ja vakavuusluokituksista.

Taulukko 1. Tietoturvapoikkeamatyyppejä

Poikkeamatyyppi	Kuvaus
Palvelunesto	Hyökkäys, joka estää verkkojen, järjestelmien tai palvelujen luvallisen käytön kuluttamalla resursseja
Haittaohjelma	Virus, mato, ”troijalainen hevonen” tai muu haitallinen ohjelmakoodi, joka saastuttaa kohdetietojärjestelmän
Järjestelmän luvaton käyttö	Henkilö saa luvatta fyysisen tai loogisen pääsyn järjestelmään
Asiaton käyttö	Henkilö rikkoo tietojärjestelmien, -verkkojen tai -palvelujen sallitun käytön ehtoja
Olosuhdehäiriö, fyysinen tietoturvahäiriö	Palvelin kaatuu konesalitilan liian korkeaan lämpötilaan. Asiaton henkilö pääsee organisaation toimitiloissa rajoitetulle alueelle.
Tiedon korruptoituminen/tuhoutuminen	Pyöristysvirhe kirjanpito-ohjelmassa. Arkistotilan tulipalo. Varmuuskopioinnin havaitsematon epäonnistuminen. Tiedon tahallinen tuhoaminen.
Tiedon varastaminen	Asiakirjasalkku varastetaan autosta. Tietoa kopioidaan luvatta tietokannasta.
Yhdistelmäpoikkeama	Yksittäinen tietoturvapoikkeama, joka kuuluu useampaan edellä kuvattuun luokkaan

Taulukko 2: Tietoturvapoikkeamien vakavuusasteet

Vakavuusaste	Kuvaus
Ei tietoturvapoikkeamaa	Havaittu ilmiö on tietojärjestelmän tai –verkon normaalia toimintaa, joka ei sisällä tietoturvaa vaarantavia ominaisuuksia.
Lievä	Tietoturvapoikkeama vaikuttaa lähinnä yksittäiseen käyttäjään. Vaikutus ei estä normaalia työntekoa. Tietojen eheys ja luottamuksellisuus eivät ole vaarassa. Hyökkääjä ei ole päässyt ohi verkon turvajärjestelmistä. Esimerkkejä: – selainkaappain asentuu yksittäisen käyttäjän työasemalle – verkon hyökkäyksenhavaitsemisjärjestelmä tai palomuurijärjestelmä havaitsee porttiskannausliikennettä – työaseman levy vahingoittuu
Kohtalainen	Tietoturvapoikkeama uhkaa yksittäisen palvelun tai käyttäjän toimintakykyä. Tietojen eheys tai luottamuksellisuus on vaarassa. Esimerkkejä: – virustartunta yksittäisen käyttäjän työasemassa – roskapostihyökkäys organisaation sähköpostipalvelimelle
Vakava	Tietoturvapoikkeama on rikkonut organisaation tietojenkäsittelyrauhaa. Poikkeamatilanne saattaa laajeta ilman käyttöhenkilöstön toimenpiteitä. Esimerkkejä: – hyökkääjä saa yksittäisen käyttäjän ja tai pääkäyttäjän oikeudet tietojärjestelmään ja etsii murrettua järjestelmää hyväksikäyttäen haavoittuvia järjestelmiä organisaation tietoverkossa / muissa organisaatioihin – palkanmaksujärjestelmän käyttämä henkilöstötietokanta korruptoituu
Kriittinen	Poikkeamalla on organisaation toimintakyvyn lamaannuttava vaikutus. Poikkeaman hallinta ei onnistu ilman radikaaleja palveluiden käytettävyyteen vaikuttavia toimenpiteitä Esimerkkejä: – organisaation ulkoiseen verkkoliitäntään kohdistuva palvelunestohyökkäys lamaannuttaa kaiken ulos suuntautuvan tietoliikenteen. Hyökkäys vaikuttaa myös yhteydet toimittaneen palveluntarjoajan verkkoon. – haittaohjelmaepidemia saastuttaa valtaosan organisaation työasema- ja palvelinkannasta – konesalin tulipalo tai muu tuhoutuminen – lähistöllä tapahtunut kemikaalivuoto estää työskentelyn

Vakavuusasteen määrittelyssä tärkeimpiä tekijöitä ovat
- poikkeaman nykyinen ja potentiaalinen tekninen vaikutus järjestelmiin ja verkkoihin
- poikkeaman kohteena olevien resurssien kriittisyys organisaation toiminnalle
- uhattuna olevien tietojen merkitys organisaatiolle.

Seuraavaksi selvitetään poikkeaman vaikutus toimintaan. Onko poikkeama uhka
- käytettävyydelle, esim. palvelunestohyökkäys, varmuuskopioiden tuhoutuminen
- eheydelle, esim. haittaohjelmat, havaittu ohjelmistovirhe
- luottamuksellisuudelle, esim. hakkerointi, liian avulias helpdesk?

Tutkitaan, onko poikkeama rajoitettavissa, laajeneeko se ja jos, niin kuinka nopeasti, organisaation sisällä vai myös ulkopuolelle. Tärkeä tekijä on poikkeaman vaikutus organisaation toimintaan (taloudellinen vaikutus, julkisuuskuva, kriittinen palvelu). Reagointi riippuu poikkeaman vakavuusluokasta ja siitä, mitä toipumissuunnitelmassa on määritelty (ks. luku 2.3 *Toipumiseen varautuminen*).

Tässä vaiheessa myös arvioidaan alustavasti, millä edellytyksillä toimintaa voidaan jatkaa (esim. tiedon korruptoitumisen aste, varmuuskopioiden tilanne). Lievistä tietoturvapoikkeamista riittää ilmoitus tietoturvavastaavalle. Järjestelmän ylläpitäjä varmistaa, että uhka on torjuttu (mahdollista turva-aukkoa ei ole käytetty hyväksi ja se paikataan; kone puhdistetaan viruksesta; viallinen komponentti vaihdetaan). Tilannetta seurataan jonkin aikaa.

Havaitun vakavan tai kriittisen tietoturvapoikkeaman selvitys keskitetään reagointiryhmälle (ks. luku 2.2.4 *Reagoinnin organisointi ja toimivaltuudet*). Reagointiryhmän kokoonpano on etukäteen määrätty ainakin tietyllä tarkkuudella. Ryhmä tekee tarvittavat päätökset ja kantaa vastuun toimenpiteistä. Jälkikäteen arvioidaan, miten on toimittu, mutta kriisin aikana ryhmän toimintaan ei pääsääntöisesti puututa eikä sen yksittäisiltä jäseniltä odoteta jatkuvaa raportointia. Ryhmä huolehtii tapahtumien kirjaamisesta ja ryhmän kontaktihenkilö hoitaa viestinnän viestintäsuunnitelman mukaisesti (ks. luku 2.2.6 *Tietoturvapoikkeamatilanteiden viestintäsuunnitelman luonti*).

3.4 Poikkeaman lähteen määrittäminen

Tärkeä osa tietoturvapoikkeaman käsittelyä on ongelman lähteen määrittäminen. Oireiden korjaaminen ei auta, jos syihin ei puututa. Poikkeaman tyyppi määrittää sen, miltä alueelta syytä etsitään.

Olosuhdeongelmat ovat useimmiten aistein havaittavissa ja niiden poistaminen kuuluu muille kuin tietotekniikan ammattilaisille. Sivuvaikutukset voivat tosin työllistää heitä runsaastikin, esimerkiksi jäähdytyksen pettämisen hajottamat laitteet, sähkökatkoista aiheutuvat käyttökatkot ja sprinklerien kastelemat varmuuskopionauhat.

Yksittäinen rikkoontunut laite on useimmiten helppo paikantaa. Ohjelmistovirheen löytäminen varsinkin laajassa monikomponenttisessa tietojärjestelmässä saattaa olla hyvinkin vaikeaa. Tällöin korostuvat ajantasaisen tietojärjestelmädokumentaation ja ympäristönsä hyvin tuntevien tietotekniikan ammattilaisten tärkeys. Huoltosopimukset mahdollistavat järjestelmätoimittajien asiantuntemuksen käytön ongelmissa.

Inhimilliset virheet, tietämättömyys ja laiminlyönnit edellyttävät ohjeistuksen ja koulutuksen kehittämistä.

Verkon kautta tulevista uhista haittaohjelmilla on omat leviämistapansa, hyökkäykset tehdään tiettyjä liikennöintiprotokollia käyttäen ja niin edelleen. Leviämistavan avulla voidaan rajata etsimisaluetta. Näihin poikkeamiin liittyy usein lähdeosoite, joka pyritään

selvittämään. Haittaohjelmissa ja erityisesti roskapostin lähetyksessä sähköpostin lähettäjän osoite (esimerkiksi etunimi.sukunimi@organisaatio.fi) on yleensä väärennetty ja siksi on tarpeen tutkia viestin muita otsikkotietoja todellisen lähettäjän selvittämiseksi. Aina ei sieltäkään löydetä IP-osoitetta, josta saastunut viesti tai roskaposti on lähtöisin.

Myös palvelunestohyökkäyksissä käytetään usein väärennettyjä osoitteita. Parhaimmin hyökkäyksen aiheuttavan tahon jäljille pääsee tutkimalla liikennettä. Liikenteen määriä osoittavista tiedoista voidaan löytää normaalista poikkeavat liikennepiikit. Reitittimien lokitiedoista voidaan etsiä viitteitä poikkeaman aiheuttajasta. Jos liikenne näyttää tulevan tietystä suunnasta, mutta itsellä ei ole tietoa osoitteesta, voidaan kysyä, onko liikenteen välittäneellä organisaatiolla saatavissa tietoa tapahtuneesta.

Kun todennäköinen tietoturvapoikkeaman lähteen IP-osoite onnistutaan selvittämään, etsitään seuraavaksi osoitteen omistajaa. IP-osoitteita hallinnoivat tahot tarjoavat ns. whois-palvelua, jolla verkko-osoitealueiden haltijoiden yhteystiedot ovat saatavissa. Tällaista palvelua löytyy osoitteista

- http://www.ripe.net/ Eurooppa
- http://www.afrinic.net/ Afrikka
- http://www.arin.net/ Amerikka
- http://www.apnic.net/ Aasia
- http://lacnic.net/en/index.html Latinalainen Amerikka

Yksittäistä IP-osoitteen omistajaa ei näin saada välttämättä selville, mutta verkko-osoitealueen haltija pystyy sen tarvittaessa selvittämään. Tilanteen niin vaatiessa hyökkäyksen kohteena oleva organisaatio voi rajoittaa liikennettä hyökkäyksen lähteeksi havaitusta osoiteavaruudesta enempien vahinkojen välttämiseksi

Suoraa yhteydenottoa hyökkääjän lähdeosoiteavaruuden haltijaan tulee käyttää harkiten. Lähdeosoite voi olla väärennetty tai lähdeosoiteavaruuden haltija voi itse olla hyökkäyksessä osallisena. Kun lähteen määrityksessä ollaan näin pitkällä, on viimeistään hyvä ottaa yhteyttä CERT-toimijaan, jolta mahdollisesti löytyy kontakteja tarvittaviin tahoihin, tai antaa tapaus poliisin tutkittavaksi (ks. luvut 3.8.1 *Yhteydenpito omaan verkkopalvelujen tarjoajaan ja CERT-toimijoihin* ja 3.8.2 *Yhteydenpito poliisiin*).

3.5 Eristämistaktiikasta päättäminen

Vakavissa tietoturvapoikkeamissa esimerkiksi järjestelmän eheys tai tiedon luottamuksellisuus on jo kärsinyt vahinkoa. Todisteaineiston turvaaminen on huomioitava eristämistaktiikasta päätettäessä (ks. keruutavasta myös luku 3.7.3 *Todisteaineiston kerääminen ja käsittely*). Järjestelmää ei saa käynnistää uudelleen eikä siinä käynnissä olevia prosesseja/ohjelmia lopettaa ennen kuin todisteaineisto on saatu varmuudella talteen. Enempien muutosten tai tietojen vaarantumisen estämiseksi palvelu voidaan kuitenkin irrottaa verkosta tai muutoin keskeyttää. Keskeyttäminen ja/tai uudelleenkäynnistäminen mietitään

tapauskohtaisesti huomioiden sekä palvelun että uhan kriittisyys. On huomattava, että palvelun keskeytyminen saattaa olla hyökkäyksen varsinainen tarkoitus.

Poikkeaman leviäminen oman organisaation ulkopuolelle on estettävä.

Tietojärjestelmiä tai –verkkoja voidaan tilanteen niin vaatiessa eristää muusta ympäristöstä myös ennaltaehkäisevänä suojaustoimenpiteenä. Esimerkiksi normaalisti luvallista liikennettä tietyillä IP-protokollilla voidaan rajoittaa haittaohjelmaepidemian aikana organisaation reunapalomuurien asetusmuutoksilla.

Eristämistaktiikkaan vaikuttavia kriteereitä ovat:

- mahdollinen resursseihin tai tietoon kohdistunut vahinko ja varkaus
- omiin tietoihin/tietojärjestelmiin kohdistuvat akuutit uhat
- poikkeaman kohteena olevien järjestelmien käytettävyystarve
- poikkeaman leviämisuhka muihin organisaatioihin
- tarve säilyttää todisteaineistoa
- tarvittavien eristämistoimenpiteiden laajuus
- eristämistoimenpiteiden toteuttamiseksi tarvittava aika ja resurssit
- eristämistoimenpiteiden tehokkuus
- eristämisratkaisun vaikutuksen kesto, esimerkiksi
  - toimenpide, joka poistetaan / muutetaan muutaman tunnin kuluttua
  - väliaikainen järjestelmämuutos muutamaksi viikoksi
  - lopullinen ratkaisu tilanteeseen.

3.6 Tekniset toimenpiteet erilaisissa poikkeamatilanteissa

Eristämisen jälkeen poikkeamatilanteen korjauksen ensimmäiset tehtävät liittyvät tilanteen rauhoittamiseen ja lisävahinkojen estämiseen. Tämä tarkoittaa poikkeaman laajuuden hallintaa ja sen leviämisen hidastamista ja ehkäisemistä. Rajoittaminen voi merkitä joidenkin asioiden uhraamista tärkeämpien edestä. Esimerkiksi järjestelmien tärkeysluokituksen mukaan voidaan vähemmän tärkeään järjestelmään liittyvä pienikin työ lykätä, kun henkilöitä tarvitaan tärkeämmissä töissä.

Harkitsemattomat korjaustoimenpiteet voivat pahentaa tilannetta ja aiheuttaa uusia ongelmia. Tietoturvapoikkeamien käsittelyssä riskien hallinta merkitsee kaikkien vasta- ja korjaustoimien toteutusta suunnitelmallisesti sekä mahdolliset haitat ja kustannukset huomioiden. Siten haittavaikutukset voidaan välttää tai ainakin ennakoida.

Toimenpidesuunnitelmien yhteydessä esitetään seuraavat kysymykset

- mitä on ajateltu tehtäväksi?
- mikä on toimenpiteiden suunniteltu hyöty?
- mikä on toimenpiteiden kustannus?
  - mikä on toimenpiteisiin tarvittava työmäärä?

  - missä ajassa toimenpiteet voidaan toteuttaa?
  - kuinka paljon henkilötyötä tarvitaan, tarvitaanko hätätyötä?
  - mitkä ovat toimenpiteiden sivuvaikutukset?
    - vähimmäisvaikutukset?
    - enimmäisvaikutukset?
  - tarvitaanko erityisosaamista, työkaluja tms.?
  - tarvitaanko jotain, mitä ei aiemmin ole testattu tai mihin ei ole annettu koulutusta?
- mitä tarkoittaa, ellei toimenpiteitä suoriteta esitellyllä tavalla?
- suunnitelman toteutuksen riskitaso (esim. matala, siedettävä, korkea, erittäin korkea)?

Yllä olevien kohtien perusteella verrataan eri suunnitelmia keskenään toimenpiteiden hyödyn maksimoimiseksi. Näin voidaan myös ennakoida mahdolliset sivuvaikutukset ja varautua niihin jo ennen kuin ne ilmenevät.

Valitut toimenpiteet toteutetaan suunnitelman mukaisesti. Tässä luvussa käsitellään muutamissa poikkeamatyypeissä tarvittavia toimenpiteitä.

3.6.1 Verkkoa vastaan on käynnistetty palvelunestohyökkäys

Aluksi on selvitettävä hyökkäyksen laajuus (kuinka monesta lähteestä ulkoverkosta, kuinka monta kohdetta sisäverkossa) ja millä tietoliikenneprotokollalla hyökkäys tapahtuu. Tiedot selviävät verkon rajalaitteiden tai sisäisten aktiivilaitteiden lokeista tai yhteydentarjoajan verkkolokeista. Tietojen luovutusoikeuksista on sovittava jo etukäteen yhteydentarjoajan kanssa. Sähköisen viestinnän tietosuojalaki sallii tietojen keräämisen tietoturvallisuudesta huolehtimiseksi ja niiden luovuttamisen tietoturvapoikkeamissa niille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa.

Jos näyttää siltä, että organisaation omassa verkossa olevia koneita käytetään palvelunestohyökkäykseen, ne tulee ensimmäiseksi paikallistaa ja eristää:

- hyökkäys tehdään todennäköisesti väärennetyillä ja vaihtelevilla lähdeosoitteilla, mutta MAC-osoitteen perusteella voidaan häiritsijän kone yleensä löytää
- häirintään valjastettu kone on irrotettava fyysisesti/loogisesti verkosta. Lisäksi on varauduttava tutkimaan se perusteellisesti, sillä todennäköisesti se on joko murrettu (ks. 3.6.2 *Järjestelmässä on tunkeutuja*) tai haittaohjelman saastuttama (ks. 3.6.5 *Haittaohjelmatilanteet*). Myös koneen omistaja voi olla tarkoituksellisesti tai vahingossa saanut aikaan palvelunestohyökkäyksen.

Yleisiä toimenpiteitä palvelunestohyökkäyksen torjumiseksi ovat esimerkiksi

- korjaa mahdollinen haavoittuvuus tai heikkous, jota hyökkäys hyödyntää
- ota käyttöön hyökkäyksen liikenneprofiiliin pohjautuva pakettisuodatus

– ota käyttöön verkkopalvelun tarjoajan kanssa ennalta sovitut suodatusmenetelmät
– siirrä hyökkäyksen alainen kohdejärjestelmä toiseen verkko-osoitteeseen.

3.6.2 Järjestelmässä on tunkeutuja

Kyseessä voi olla paitsi tarkoituksellinen tai vahingossa tapahtuva luvaton toiminta, myös erilaiset haittaohjelmat ja niiden käyttö.

Yksittäisen käyttöoikeuden tai käyttäjätunnuksen väärinkäyttöön rajoittuvan rikkeen tutkinnasta ei välttämättä aiheudu käyttökatkoja palveluihin, ja tapaus voidaan yleensä tutkia tietojärjestelmän omin työkaluin. (SVTSL 9§)

Toimenpiteet luvaton käyttö -tilanteessa:

– ensisijainen toimintamalli on, että tietojärjestelmän käyttö estetään tarvittavilta osin ainakin aktiivisen tutkinnan ajaksi. Konetta ei sammuteta eikä prosesseja keskeytetä ilman harkintaa.
– vaihtoehtoinen toimintamalli on, että käyttöoikeuden oikeudetonta käyttöä seurataan ja tallennetaan lokiin todisteaineistoksi. Käyttöoikeus jätetään auki siksi aikaa, kun se on aktiivisesti seurattuna. Tällöin on myös varmistuttava, ettei väärinkäyttö vaaranna muun järjestelmän tietoturvallisuutta. Seuraaminen on poikkeuksellinen toimintamalli, jota on käytettävä äärimmäisen harkiten ja yleensä tiiviissä yhteistyössä esitutkintaviranomaisen ja/tai CERT-toimijan kanssa. Toimenpide vaatii ylläpitohenkilöstöltä korkeaa ammattitaitoa ja resursseja kohdejärjestelmän jatkuvaan seurantaan.

Pääkäyttäjämurron jälkeen mihinkään koneessa olevaan tietoon ei voi varmuudella luottaa, ei myöskään varusohjelmistoihin.

Toimenpiteet pääkäyttäjämurtotilanteessa:

– kohdekone irrotetaan fyysisesti tietoliikenneverkosta (verkkokaapeli irti), jotta tunkeutuja ei pääse koneeseen käsiksi.
– ei sammuteta konetta. Sammutettaessa kone menetetään tietoa (esimerkiksi tunkeutujan prosessien varaamista resursseista).
– tiedostojärjestelmästä otetaan kopio. Järjestelmän tutkiminen muuttaa järjestelmän tilaa ja saattaa siten vähentää todisteaineiston luotettavuutta rikosprosessissa. Paras vaihtoehto on raakakopio levyjärjestelmätasolla. Jos tämä ei ole mahdollista, otetaan mahdollisimman täydellinen tiedostojärjestelmätason varmistus talteen. Jo toipumissuunnitelmassa on huomioitava, miten varmuuskopiointi on mahdollista tehdä: konetta ei voi ottaa verkosta ennen varmuuskopiointia, jos kopiointiohjelmat toimivat vain verkon kautta eikä varajärjestelyä ole. Vähintään tutkinnan kohteeksi tulevat osat tiedostojärjestelmää on otettava talteen, jos koko järjestelmän tietosisällön varmuuskopiointi on tietomäärästä johtuen kohtuuttoman hidasta.

- pidetään mielessä, että varmuuskopioidut tiedot eivät välttämättä ole käyttökelpoisia. Palautettaessa tietoja varmuuskopioilta tai käsiteltäessä varmuuskopiotietoja todisteaineistona, tulee varmistaa, että tunkeutuja ei ole muuttanut tietoja jo ennen niiden varmuuskopiointia.
- selvitetään järjestelmän lokitietojen, verkkoliikenteen tai verkkoelementtien tietojen perusteella muut hyökkääjän kohteet kohdeorganisaatiossa tai kolmansilla osapuolilla. Käynnistetään torjuntatoimenpiteet löydettyjen muiden kohdejärjestelmien osalta ja tiedotetaan mahdollisimman nopeasti kolmansia osapuolia joko suoraan tai CERT-toimijan kautta tilanteesta.
- poistetaan mahdollisuuksien mukaan tunkeutumiseen käytetty palvelu käytöstä. Jos hyökkääjä käyttää jotain tiettyä palvelua ja sen haavoittuvuutta sisäänpääsyyn, estetään kyseisen palvelun käyttö väliaikaisesti muissa järjestelmissä uusien tunkeutumisien estämiseksi.
- estetään tunkeutujan käyttämän hyökkäysreitin hyväksikäyttö. Jos tunkeutuja on käyttänyt esimerkiksi tiettyä verkkopalvelua tai –protokollaa toiminnassaan, estetään verkon ulkorajoilla liikenne käyttäen kyseistä verkkopalvelua tai protokollaa mahdollisuuksien mukaan.
- todisteiden käsittely ks. luku 3.7 *Todisteaineiston turvaaminen*.

3.6.3 Palvelimia on käytetty muuhun laittomaan tarkoitukseen

Tarve toimenpiteisiin voi tulla esiin organisaatiosta itsestään tai pyynnöstä muilta organisaatioilta tai henkilöiltä. Ennen toimenpiteisiin ryhtymistä väärinkäyttöilmoituksen asianmukaisuus on syytä arvioida. Kyseessä saattaa olla myös ilkivaltainen ilmoitus, jolla pyritään haittaamaan syylliseksi ilmoitetun toimintaa. Kun ilmoituksen asiallisuudesta on varmistuttu, väärinkäytöksistä epäillyn käyttöoikeuden käyttö on estettävä viivytyksettä ja pidettävä estettynä vähintään poikkeaman tutkimisen ajan. Kaikista tiedoista, joihin väärinkäytöksistä epäilty käyttöoikeus pääsee käsiksi, tulee mahdollisuuksien mukaan ottaa varmuuskopio ennen mahdollisten muutosten tutkimista (ks. 3.6.2 *Järjestelmässä on tunkeutuja*).

3.6.4 Oman henkilökunnan tekemät tietoturvaloukkaukset

Jos omaan henkilökuntaan kuuluvaa epäillään tietoturvaloukkauksesta, voidaan organisaatiossa soveltaa tilanteen tutkintaan henkilötietolakia, lakia yksityisyyden suojasta työelämässä sekä sähköisen viestinnän tietosuojalakia ennen kuin otetaan yhteyttä poliisiin. Jos kyse on organisaation omien sääntöjen, mutta ei suoranaisesti säädösten vastaisesta toiminnasta, voi kyseeseen tulla ”luvaton käyttö”. Henkilötietolain mukaan (12§ 1 mom 4 kohta) arkaluontoisia henkilötietoja saadaan käsitellä, jos se on tarpeen oikeusvaateen laa-

timiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi. Kohta ei oikeuta keräämään tietoa tietoturvaloukkauksen selvittämiseksi, mutta jos tiedot jo muutoin ovat laillisesti työnantajan hallussa, saadaan niitä käyttää mainittuun tarkoitukseen. Kohta ei myöskään velvoita tekemään tutkintapyyntöä, jos se osoittautuu aiheettomaksi tai sitä ei muutoin katsota tarpeelliseksi. Sähköisen viestinnän tietosuojalain luku 3 säätelee viestien ja tunnistamistietojen käsittelyä esimerkiksi tietoturvasta huolehtimiseksi (9§) ja väärinkäytöstapauksissa (13§). Tietojen käsittely väärinkäytösten selvittämiseksi tulee jo etukäteen käsitellä YT-menettelyssä. Tietoturvaloukkauksen selvittämisen aikana tulee tarkoin harkita, ettei eri osapuolten oikeusturvaa vaaranneta.

Kun tietoturvapoikkeaman aiheuttaja kuuluu omaan henkilökuntaan, seuraamukset ovat organisaation omien sääntöjen ja asiaa koskevien lakien mukaiset. Omissa säännöissä teot on hyvä luokitella rikkomuksen vakavuuden ja teon tahallisuuden mukaan. Lievimmissä tapauksissa riittää huomautus asiattomasta toiminnasta. Vakavimmat tapaukset voivat johtaa irtisanomiseen tai palvelusuhteen purkuun. Korvausvastuut koskevat sekä väärinkäytettyjä resursseja että väärinkäytön selvitystyöstä aiheutuneita kustannuksia.

Liite 6 on esimerkki ohjeesta, kuinka organisaatiossa voidaan reagoida henkilökunnan tekemiin tietoturvarikkomuksiin ja Liite 7:ssä on esimerkkitaulukko erityyppisten rikkomusten seuraamusvaihtoehdoista. Näiden liitteiden tyyppiset ohjeet on käsiteltävä YT-menettelyssä tai muutoin vastaavalla tavalla henkilöstön kanssa ennen niiden käyttöönottamista.

3.6.5 Haittaohjelmatilanteet

Haittaohjelmia on käsitelty kattavasti *Haittaohjelmilta suojautumisen yleisohjeessa* [9].

3.6.5.1 Haittaohjelmien havaitseminen

Haittaohjelmat havaitaan käytettyjen virustorjuntaohjelmien antaman tiedon perusteella. Ilmoituksia saadaan myös organisaation ulkopuolelta silloin, kun haittaohjelman saastuttama kone lähettää jollekin haittaohjelmalle tyypillistä liikennettä verkkoon. Käyttäjä ottaa yleensä yhteyttä tietohallintoon silloin, kun työskentely koneella syystä tai toisesta hidastuu tai häiriintyy. Syyksi saattaa paljastua haittaohjelma.

3.6.5.2 Haittaohjelmatilanteen hallinta

Tietojärjestelmien hallinnasta ja valvonnasta tulee sopia kirjallisesti järjestelmien omistajien ja järjestelmiä valvovan ja hallinnoivan organisaation kesken. Haittaohjelmien torjunnassa toimitaan sovitun toimintatavan mukaisesti.

Ensimmäinen tehtävä on rajoittaa vahinkojen vakavuutta. Menettelyt kohdistuvat tietoverkkoon ja palvelimiin. Reagointiaika on lyhyt ja moni toiminta pitää käynnistää ilman, että paikalla on vielä päätöksiä tekemässä muita kuin mikrotuen päivystäjä. Haittaohjel-

man siivoamisessa hän onkin useimmiten paras asiantuntija. Jos yksi laite havaitaan saastuneeksi, on muidenkin koneiden mahdollinen saastuminen tutkittava. Laitteen tai ohjelmiston omistajan / ylläpitäjän on kartoitettava, miten laajalle vaikuttavasta järjestelmästä on kyse. Vahingot pyritään rajaamaan mahdollisimman suppeiksi. Helpoin tilanne on silloin, jos laite ei ole kytketty organisaation verkkoon ja tartunta on saatu esimerkiksi siirrettävän tiedontallennusvälineen kautta.

Jos haittaohjelma aiheuttaa runsaasti liikennettä esimerkiksi joihinkin portteihin, voidaan vahinkoa pyrkiä rajaamaan rajoittamalla liikennettä kyseisiin portteihin (tai osoitteisiin). Myös sähköpostiliikennettä voidaan viivästyttää (esimerkiksi muutamalla tunnilla), jotta saadaan aikaa sähköpostin kautta leviävältä haittaohjelmalta suojautumiseen.

Kun on selvillä, mistä haittaohjelmasta on kyse, voidaan käyttää sitä vastaan tehtyjä työkaluja. Virustorjuntaohjelmistojen valmistajilla on erilaisia haittaohjelman poistotyökaluja, jotka ovat ladattavissa heidän sivuiltaan. CERT-FIn sivuilla on ohjeita yleisimpien haittaohjelmien poistamisesta tietojärjestelmistä.

Kun laite on puhdistettu, on päivitettävä ohjelmistot (käyttöjärjestelmä, virustorjuntaohjelmisto) tai ainakin paikattava tiedossa olevat haavoittuvuudet. Kun järjestelmän uskotaan olevan kunnossa, voi koneen liittää takaisin verkkoon.

3.7 Todisteaineiston turvaaminen

3.7.1 Todisteaineisto

Tietoturvapoikkeaman todisteaineistoa on kaikki informaatio, josta on apua selvitettäessä mitä ja missä on tapahtunut. Todisteaineistoa ovat siten yhtä lailla yhteyksiä dokumentoivat lokitiedot ja käyttäjien kuvaukset poikkeaman ilmenemisoireista kuin poikkeaman kohteeksi joutuneen tietojärjestelmän tallennusmedioilta löytyvä tekninen todisteaineistokin.

3.7.2 Todisteaineiston käyttö

Todisteaineistolla on kaksi eri merkitystä. Toisaalta tietoturvapoikkeaman kohdeorganisaatio saa todisteaineistosta olennaisen tärkeää informaatiota poikkeamasta, toisaalta aineistoa voidaan käyttää todisteena mahdollisessa rikosprosessissa.

Kohdeorganisaatiossa tietoa tarvitaan selvittämään poikkeaman laajuus ja sen merkitys organisaation toiminnalle: missä poikkeama esiintyy ja millaisia vaikutuksia uhka aiheuttaa. Todisteaineiston avulla selvitetään myös, millaisista olosuhteista, esimerkiksi haavoittuvuutta hyväksikäyttäen, poikkeamatilanne syntyi. Tämän perusteella on edelleen selvitettävä, mistä syystä järjestelmässä oli hyväksikäytettävissä oleva haavoittuvuus ja miten ylläpitoprosesseja voidaan parantaa vastaavien poikkeamien estämiseksi jatkossa.

3.7.3 Todisteaineiston kerääminen ja käsittely

Todisteaineiston keruutapa on riippuvainen aineiston keruun tarkoituksesta. Jos tietoturvapoikkeamasta voi heti havaittaessa päätellä, ettei taustalla ole rikosta, todisteaineiston voi kerätä uhriorganisaation itsensä kannalta järkevällä tarkkuudella. Jos kysymys on selkeästi rikoksesta, organisaation on syytä ottaa yhteyttä poliisiin ja keskustella heidän kanssaan todisteaineiston keräämisestä. Rikostutkinnan käynnistyttyä poliisi joko kerää aineiston itse tai ohjeistaa asianomistajaorganisaation tapauksesta ja kohdejärjestelmistä riippuen.

Jos poikkeaman syystä ei ole selvyyttä, organisaation tulee varautua keräämään aineisto tavalla, joka tekee siitä mahdollisimman käyttökelpoisen oikeusprosessissa.

Todisteaineiston käsittelyssä rikosprosessin yhteydessä on olennaista:

1. aineiston mahdollisimman suuri muuttumattomuus
2. mahdollisimman täydellisen aineiston kerääminen
3. aineiston keruun dokumentointi.

Aineiston muuttumattomuutta edesauttaa, että tutkinta kohdistuu kopioon eikä alkuperäiseen mediaan. Tällöin tutkinta ei muuta tutkittavaa järjestelmää lukuaikaleimojenkaan osalta. Kopion muuttumattomuus osoitetaan joko käyttämällä vain kerran kirjoitettavissa olevaa mediaa tai laskemalla tarkistussummat sekä alkuperäisestä mediasta että kopiosta (esimerkiksi md5sum-ohjelmalla). Tutkittaessa tunkeutujan jälkiä tulisi tietojärjestelmän kopiota käsitellä vain lukemisen sallivassa muodossa.

Mahdollisimman täydellisen aineiston keruun kriteeri merkitsee sitä, että tunkeutujan käsittelemistä kohdejärjestelmistä otetaan mieluummin levyjärjestelmän image kuin vain kopio tiedostojärjestelmien sisällöstä. Kohdejärjestelmän käyttöjärjestelmästä riippumatta levy-image saadaan dd-ohjelmalla käynnistämällä kohdekone Linux-käynnistysmedialla. Imagen ottaminen ei sen sijaan ole tarpeen silloin, kun tunkeutuja ei ole ollut kohdejärjestelmässä, vaan järjestelmästä löytyy vain todisteaineistoa. Tyypillinen esimerkki tästä ovat lokipalvelimet, joissa tapaukseen liittyvät lokirivit muodostavat riittävän todisteaineiston.

Muuttumattomuuden ja mahdollisimman täydellisen aineiston kriteerit eivät aina ole tavoitettavissa, esimerkiksi jos ulkoistussopimus estää järjestelmän pysäyttämisen imagen ottamisen ajaksi. Dokumentointi on korostetun tärkeää erityisesti silloin, kun kriteerit 1 ja 2 eivät ole saavutettavissa. Muulloin dokumentoinnin tarkoituksena on helpottaa aineiston luotettavuuden osoittamista sekä auttaa muistamaan toimenpiteet koko pitkän oikeusprosessin ajan.

Jos todisteaineistoa käytetään rikosprosessissa, se tulee lähtökohtaisesti säilyttää koko rikosprosessin ajan huolehtien samalla, etteivät asiattomat pääse aineistoon käsiksi: sen enempää muuttamaan sitä kuin tutustumaan sen sisältöön. Säilyttämistavasta voidaan sopia poliisin kanssa. Omaan käyttöön tarkoitettu aineisto säilytetään sen ajan kuin aineisto

on tarpeellinen ja sitä käytetään vain poikkeaman tutkimiseen. Todisteaineistoa tulee käsitellä ja myös hävittää sillä huolellisuudella, mitä sen sisältämät tiedot edellyttävät.

3.8 Sisäinen ja ulkoinen viestintä reagoinnin aikana

Poikkeamatilanteissa korostuu jatkuvasti saatavilla olevan, luotettavan ja ajantasaisen tiedon tarve. Tiedottamisen ja viestinnän tulee olla informoivaa, ohjaavaa, ohjeistavaa ja rauhoittavaa ja sen perustarkoituksena on ylläpitää tietoisuutta tosiasioista ja toimenpiteistä. Sen tulee ehtiä väärien tietojen edelle.

Poikkeamatilanteeseen liittyvä tiedottaminen tulee käynnistää heti poikkeaman ilmettyä viestintäsuunnitelman mukaisesti (ks. 2.2.6 *Tietoturvapoikkeamatilanteiden viestintäsuunnitelman luonti*). Poikkeaman laajuuden ja vakavuuden mukaan valitaan viestintävastaava ja reagointiryhmän kontaktihenkilö. Viestintävastaava ja reagointiryhmä arvioivat, keille poikkeamatilanne näkyy ja keiden toimintaan se vaikuttaa. Samoin arvioidaan käytettävissä olevat viestintäkanavat: onko poikkeama lamaannuttanut joidenkin viestintäkanavien käytön (esimerkiksi www-palvelin on rikki) tai ovatko jotkin viestintäkanavat poikkeaman luonteen vuoksi turvattomia (esimerkiksi murtautuja kuuntelee verkkoliikennettä).

Usein tärkeä osa poikkeaman rajoitusta on tiedottaminen käyttäjille. Esimerkiksi henkilöstölle annettu ohje olla avaamatta tietyn nimistä liitetiedostoa estää uudet haittaohjelmatartunnat ja ylikuormittuneen järjestelmän käytöstä pidättäytymisellä saadaan ongelmatilanne purettua.

Poikkeaman laajuuden mukaisesti tiedotetaan vaikutuksen kohteena oleville henkilöille ja muille tahoille toimenpiteistä, vaikutuksista ja palautumisen tilanteesta, sekä mahdollisista jatkotoimenpiteistä. Vakavissa poikkeamatilanteissa toimitaan yhteistyössä viestintäyksikön ja mahdollisen kriisienhallintaryhmän kanssa. Samoin aina, kun poikkeama näkyy toiminnassa organisaatiosta ulospäin.

3.8.1 Yhteydenpito omaan verkkopalvelujen tarjoajaan ja CERT-toimijoihin

Kun havainnot osoittavat poikkeamatilanteen vaativan yhteistyötä oman verkkopalvelun tarjoajan tai kolmansien osapuolien kanssa, on päätettävä soveltuvasta yhteydenpitotavasta. Omaa verkkopalveluntarjoajaa on syytä informoida etenkin palvelunestohyökkäyksistä. Yhteyttä otetaan tekniseen asiakaspalveluun tai erityisen kriittisissä tapauksissa mahdollisesti suoraan palveluntarjoajan verkonvalvomoon.

CERT-toimijat (Computer Emergency Response Team) ovat tietoturvaloukkaus- ja ohjelmistohaavoittuvuustilanteiden koordinointiin erikoistuneita organisaatioita. Viestin-

täviraston alainen CERT-FI on kansallinen koordinoiva CERT-toimija, jonka tehtävänä on tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu / ratkaisussa avustaminen sekä tietoturvauhkista tiedottaminen. Se palvelee julkishallintoa, yrityksiä ja yksityisiä kansalaisia sekä kerää tietoa tietoturvallisuuden tilasta. CERT-FI toimii teknisten tekotapojen tutkimuksessa tiiviissä yhteistyössä poliisin kanssa, mutta päätökset rikosilmoituksista ja tapausten jatkokäsittelystä tekevät yksin asianomistajat. Funetilla (Suomen korkeakoulujen ja tutkimuksen tietoverkko) on omia asiakkaitaan palveleva CERT. Useilla teleyrityksillä ja IT-palvelutaloilla on myös tietoturvapoikkeama- ja väärinkäytöstilanteiden hallintaan erikoistuneita ryhmiä.

CERT-toimijaan kannattaa erityisesti olla yhteydessä, kun

- tietoturvapoikkeama vaikuttaa Internet-verkon runkopalveluihin (nimipalvelu, IP-reititys)
- organisaation merkittävä palvelu on uhattuna
- poikkeamatilanne vaikuttaa laajalle levinneeltä
- poikkeamatilanteessa on mukana useita osapuolia, joihin ei ole suoraa luontevaa kontaktia ja organisaatio tarvitsee tilanteessa koordinointiapua
- poikkeamatilanteessa havaitut menetelmät ovat uusia tai niitä käytetään uudella tavalla.

CERT-toimijoilla on yhteyksiä muihin tietoturvatoimijoihin, myös kansainvälisesti. Yhteyksien avulla CERT-toimijat voivat huolehtia muiden tietoturvapoikkeaman kohteeksi joutuneiden tahojen varoittamisesta ja siten vähentää oman organisaation resurssikuormitusta poikkeamatilanteen ollessa aktiivisimmillaan. CERT-toimijat hoitavat tarvittaessa myös tiedonvälitystä eri osapuolten välillä ja auttavat tilanteen hallinnassa tarvittavien tietojen hankkimisessa.

3.8.2 Yhteydenpito poliisiin

Jos havainnot viittaavat siihen, että teon taustalla saattaa olla rikos (ks. luku 2.2.3 *Tietoturvapoikkeamasta tietorikokseen*), tulee lähtökohtaisesti aina olla yhteydessä poliisiin. Tietotekniikan avulla tehtyjä rikoksia tutkivat poliisissa tietotekniikkarikosyksiköt tai –tutkijat, joita on keskusrikospoliisin lisäksi paikallispoliisissa ympäri Suomea. Pääsääntöisesti otetaan yhteyttä lähimpään paikalliseen rikospoliisiyksikköön, joka saa virka-apua lähimmästä tietotekniikkarikosyksiköstä, ellei paikkakunnalla sellaista ole. Tietotekniikkarikostutkijoita voi konsultoida myös epävirallisesti, jos ollaan epävarmoja siitä, onko tietoturvapoikkeamassa kyse rikoksesta, sekä pohdittaessa, tehdäänkö rikosilmoitus. Poliisin tehtävänä on tällöin arvioida, täyttääkö tapahtuma jonkin rikoksen tunnusmerkistön. Rikosilmoitus on tehtävä aina, kun halutaan selvittää omaan työntekijään kohdistuva rikosepäily, koska lainsäädännön työnantajalle suomat oikeudet selvittää työntekijän epäiltyjä väärinkäytöksiä ovat hyvin rajalliset (ks. luku 3.6.4 *Oman henkilökunnan tekemät tietoturvaloukkaukset*).

Rikosilmoituksen tekemisen yhteydessä sovitaan poliisin kanssa, millä tavoin todisteaineisto turvataan juuri käsillä olevassa tapauksessa.

3.8.2.1 Rikosilmoitus ja esitutkinta

Poliisin on suoritettava rikoksen esitutkinta silloin, kun on syytä epäillä rikoksen tapahtuneen. Tietoon kohdistuvista rikoksista suurin osa on kuitenkin asianomistajarikoksia, joissa poliisi voi pääsääntöisesti tutkia rikosta vain, mikäli asianomistaja (rikoksen uhri) vaatii rangaistusta. Tutkinta voidaan käynnistää ennen kuin asianomistaja on tietoinen rikoksesta. Se on kuitenkin keskeytettävä, jos asianomistaja ei vaadi rangaistusta tai peruuttaa aiemman rangaistusvaatimuksen. Poikkeuksen perusperiaatteeseen muodostavat tapaukset, joissa yleisen edun voidaan katsoa vaativan tutkintaa. Poliisi voi tällöin syyttäjän pyynnöstä suorittaa tutkinnan asianomistajan rangaistusvaatimuksesta riippumatta.

Rikosilmoitus tehdään joko paikallispoliisiin tai KRP:n tietotekniikkarikosyksikköön. Yrityksen, julkishallinnon yksikön tai oikeustoimikelpoisen yhteisön tehdessä asianomistajana rikosilmoituksen, ilmoituksen allekirjoittaa nimenkirjoitusoikeuden haltija, eli käytännössä ylin johto, tai sen valtuuttama henkilö. Ylläpitäjät ja muut asiantuntijat esiintyvät tällöin esitutkinnassa todistajan asemassa. Tietoturvavastaava voi kuitenkin tehdä kiireellisessä tapauksessa rikosilmoituksen ”rikoksen silminnäkijän roolissa”. Tällöin poliisi voi aloittaa rikoksen tutkinnan nopeasti. Esitutkinnan jatkaminen edellyttää yhä kuitenkin rangaistusvaatimusta asianomistajalta.

Rikosilmoituksen muoto on vapaa, mutta siinä tulisi huomioida esitutkinnan merkitys ja sen käynnistämisen edellytykset. Esitutkinnan tarkoituksena on selvittää tapauksen tosiasiat: osapuolet, teko sekä näyttö yhtälailla epäiltyä vastaan kuin epäillyn eduksikin. Tapahtuman lisäksi esitutkinnassa selvitetään rikoksella aiheutettu vahinko ja vastaavasti epäillyn hankkima hyöty, sekä mahdollisesti myös asianomistajan vahingonkorvausvaatimukset. Niinpä rikosilmoituksessa tulee olla vähintään lyhyt kuvaus tapahtumasta, asianomistajan yhteystiedot, sekä tieto siitä, että asianomistaja vaatii rangaistusta. Itse rikosilmoitukseen ei tarvitse liittää teknistä todisteaineistoa, vaan poliisi hankkii sen esitutkinnan yhteydessä. Asiantunteva ylläpito voi kerätä todisteaineistoa poliisia varten itsekin, huomioiden kuitenkin se, mitä todisteaineiston keruusta sanotaan luvussa 3.7.3 *Todisteaineiston kerääminen ja käsittely*.

Teknisen todisteaineiston lisäksi rikosprosessissa on paljon hyötyä organisaation omasta tietoturvapoikkeaman selvittämisen dokumentoinnista. Dokumentointi toisaalta helpottaa aineiston oikeusvarmuuden arviointia oikeudessa, toisaalta suoritettujen toimenpiteiden määrän ja keston kirjaus auttaa tuomioistuinta mahdollisten vahingonkorvausten suuruusluokan arvioinnissa.

3.8.3 Ilmoittaminen valtiovarainministeriölle

Valtiovarainministeriö (VM) ohjaa ja koordinoi valtionhallinnon tietoturvallisuutta ja sen kehittämistä. VM:n asettama valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) tavoitteena on parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta tietoturvallisuutta kehittämällä sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa. Valtionhallinnon organisaatioiden on hyvä tiedottaa merkittävistä tietoturvapoikkeamista valtiovarainministeriön hallinnon kehittämisosastolle tietoturvan kehittämisestä vastaaville virkamiehille.

3.8.4 Ilmoittaminen valtiontalouden tarkastusvirastolle

Valtiontalouden tarkastusvirastosta (VTV) annetun lain (676/2000) 16 §:n mukaan valtion viranomaisen, laitoksen, liikelaitoksen ja valtion rahaston on salassapitosäännösten estämättä ilmoitettava viipymättä toiminnassaan tehdystä, sen hoitamiin tai vastattavina oleviin varoihin tai omaisuuteen kohdistuneesta väärinkäytöksestä tarkastusvirastolle. Ilmoitus tehdään VTV:n 15.10.2003 antaman ohjeen mukaisesti. Ohje löytyy VTV:n www-sivuilta (http://www.vtv.fi).

4 TOIPUMINEN TIETOTURVA-POIKKEAMATILANTEISTA

4.1 Normaalitoiminnan palauttaminen

Normaaliin toimintaan palataan suunnitelmien ja hyväksytyn riskitason mukaisesti. Tilannetta palautettaessa tehdään pysyviä toimenpiteitä, joilla toivutaan poikkeamasta ja estetään samalla vastaavien poikkeamien uusiutuminen. Palauttamisessa hyödynnetään toipumissuunnitelmia niin paljon kuin mahdollista.

Kaikki suunnitellut toimenpiteet eivät välttämättä ole niin helppoja toteuttaa kuin on ajateltu ja palautumisvaiheessa voi tulla vastaan yllättäviä ongelmia. Esimerkiksi:

- palvelin ei ole käytettävissä, vaan poliisin takavarikossa tai tuhoutunut palossa
- avainhenkilöt eivät ole käytettävissä
- rakennusta, jossa pitäisi työskennellä, ei enää ole
- varavoimakoneisiin ei ole toimitettu polttoainetta.

Usein tuudittaudutaan uskoon, että varmuuskopiot, etenkin jos ne ovat testattu, olisivat pelastus. On kuitenkin tilanteita, joissa varmuuskopioiden palauttaminen voi olla mahdotonta. Esimerkiksi joissakin reaaliaikajärjestelmissä ei varmuuskopioita välttämättä kannata palauttaa tai palautuksen jälkityö muodostuu hyvin työlääksi. Muutoinkin ennen tietojen palautusta varmuuskopioilta on tarkistettava, mitä versiota palautuksessa voidaan käyttää: esimerkiksi milloin tiedon korruptoituminen on alkanut ja onko sitä edeltävä varmuuskopioversio muutoin vielä käyttökelpoinen.

4.2 Raportointi ja tapauksesta oppiminen

Kun tilanne on saatu normalisoitua, ei tapaus vielä ole ohi. Toimintatapoja ja toipumissuunnitelmia ei voida kehittää ilman harjoituksia. Tositilanteet ovat valitettavia, mutta silti parhaimpia harjoitustilanteita. Tästä syystä on tärkeää, että kaikki tapaukseen liittyvät dokumentaatiot ja tiedot kootaan yhteen ja materiaali analysoidaan huolellisesti. Mikäli tapauksen analysointi osoittaa, ettei mitään toimintatapaa tai menettelyä ole tarpeen kehittää, on todennäköistä, että jokin asia on jäänyt huomiotta.

Jälkianalysoinnin tarkoitus ei ole etsiä syyllisiä mahdollisiin väärin toimenpiteisiin, vaan etsiä menetelmiä, joilla voidaan minimoida virheitä tulevissa poikkeamatilanteissa. Tavoitteena on saada materiaalia, jolla tapahtuma-analyysiä voidaan tulevaisuudessa tarkentaa. Analysointi antaa myös työkaluja suunnittelun ja riskienarvioinnin tarkentamiseen esimerkiksi siten, että saadaan arvioita eri toimenpiteiden kestoista. Analyysin tarkoituksena on oppia tulevaisuutta varten. Jos poikkeaman käsittelyn aikana tuli esiin puutteita organisaation toiminnassa tai toiminnan ohjeistuksessa, tulee ohjeet päivittää ja kouluttaa asianosaiset niiden mukaiseen toimintaan. Toipumissuunnitelmia tulee parantaa ja tarkentaa havaittujen puutteiden perusteella sekä laatia puutteiden korjaamisesta aikataulutetut suunnitelmat (ks. myös luku 2.2.5.4 *Harjoituskertomuksen laadinta ja kokemuksista oppiminen*). Myös mahdolliset ulkoistussopimusten toimivuudessa havaitut puutteet tulee käsitellä ja sopimukset tarvittaessa tarkistaa.

Yksityiskohtainen raportti palvelee parhaimmin tietohallintoa sen toimintojen kehittämisessä. Yhtä tärkeää on kuitenkin raportoida sopivalla tarkkuustasolla myös organisaation johdolle tapahtuneista tietoturvapoikkeamista. Johdolle suunnattu raportointi edistää tietoturvallisuuden kokonaiskehitystä organisaatiossa ja tietoturvatyön resursoinnin varmistamista. Merkittävistä tapauksista raportoidaan myös organisaation mahdolliseen riskienhallintayksikköön.

4.3 Tiedottaminen ja muu viestintä

Tietoturvapoikkeama ja siihen reagointi vaikuttavat monien tahojen toimintaan (oma henkilökunta, organisaation sidosryhmät, muut tapausta tutkineet tahot ja mahdolliset muut uhrit). Kun tilanne on korjattu, on vielä kerran tiedotuksen aika.

Tietojen ja palveluiden käyttäjille tulee kertoa, milloin he voivat palata omalta osaltaan normaaliin toimintaan. Organisaation julkisuuskuvan kannalta on tärkeää huolehtia tiedotuksesta sidosryhmille. Jos poikkeama on ollut esillä mediassa, voidaan harkita lehdistötiedotetta. Jos CERT-FI:hin ei olla oltu aiemmin yhteydessä, kannattaa merkittävistä tapauksista tilastollisessa mielessä raportoida myös sinne.

4.4 Onnistuneen toipumisen edellytykset

Poikkeamaan reagointi ja siitä toipuminen voidaan katsoa onnistuneeksi, kun poikkeamasta ei aiheudu suuria haittoja organisaation toiminnalle, häiriön syy saadaan nopeasti selvitettyä ja hoidettua ja oireet nopeasti korjattua. Toipumisen onnistumisen mittarina on myös se, kuinka riskien ja kustannusten hallinnassa onnistuttiin.

Korjaustoimenpiteistä voidaan arvioida kustannusten osalta esimerkiksi seuraavasti:

$$\text{Korjauksen onnistuminen} = \frac{\text{(toipumisen + menetetyn mahdollisuuden kustannus)}}{\text{(häiriön aiheuttama kustannus organisaatiolle)}}$$

Yllä olevassa kustannus ei välttämättä ole tarkka luku, eikä siten vertailukelpoinen eri organisaatioiden välillä. Organisaation sisällä tällaisella tunnusluvulla on merkitystä vertailtaessa eri poikkeamia ja niiden ratkaisuja keskenään.

Edellytyksiä onnistuneelle toipumiselle ovat:

- ajan tasalla oleva järjestelmädokumentointi, joka sisältää "kaiken" tietoverkoista ja yhteyksistä lähtien. On oleellista, että dokumentaatio (esimerkiksi asennetuista ohjelmista ja niiden versioista) ja todellisuus vastaavat toisiaan. Dokumentaatiota on syytä testata säännöllisesti organisaation eri osiin kohdistuvilla tarkastuksilla. Tässäkään ei tarkoituksena ole etsitä syyllisiä, vaan kehittää toipumiskykyä.
- ajan tasalla olevat sekä erillisten järjestelmien että myös kokonaisuuden toipumissuunnitelmat prioriteetteineen ja mahdollisine erityisvaatimuksineen. Toipumissuunnitelmat vaativat säännöllistä päivittämistä.
- korjaukseen motivoitunut koulutettu ja harjoitettu henkilöstö. Koulutuksen tulee kattaa koko henkilöstö. Harjoittelua tarvitsee suunniteltu korjaushenkilöstö ja etenkin organisaation runko.
- ajan tasalla olevat sopimukset toipumisessa tarvittavien sidosryhmien sitouttamiseksi. Yleensä toimittaja on liittänyt tarjoamiinsa sopimuksiin Force Majeure -pykälät, joissa sopimuksien toteutusvastuuta esimerkiksi luonnonkatastrofeissa, terrori-iskussa ja aseellisissa konflikteissa rajoitetaan. Organisaation tulee arvioida, ovatko juuri nämä tapahtumat sellaisia, joissa kyseistä sidosryhmää tarvitaan (valmiussuunnittelu).
- korjaus- ja vianselvitystyössä tarvittavat työvälineet tulee olla valmiina jo ennakolta. Liite 10:ssä on lista reagointiryhmän tarvitsemista työvälineistä.

Onnistunut toipuminen edellyttää etukäteistä varautumista ja valmistautumista.

LIITTEET

Liite 1 Käytetyt lähteet

Valtiovarainministeriön julkaisemat VAHTI-ohjeet löytyvät osoitteesta http://www.vm.fi/vahti

1. Tietotekniikan turvallisuus ja toiminnan varmistaminen
   © Puolustustaloudellinen suunnittelukunta
   ISBN 951-53-2406-8
   http://www.nesa.fi/julk/VALMO_4=Kooste_web.pdf

2. Opas julkishallinnon tietoturvakoulutuksen järjestämisestä, VAHTI 6/2003
   ISSN 1455-2566
   ISBN 951-804-407-4

3. Käyttäjän tietoturvaohje, VAHTI 5/2003
   ISSN 1455-2566
   ISBN 951-804-405-8

4. Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006, VAHTI 1/2004
   ISSN 1455-2566
   ISBN 951-804-425-2

5. Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
   ISSN 1455-2566
   ISBN 951-804-211-X

6. Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004
   ISSN 1455-2566
   ISBN 951-804-432-5

7. Valtionhallinnon tietohallintotoimintojen ulkoistamisen tietoturvasuositus, VAHTI 2/1999

8. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
ISSN 1455-2566
ISBN 951-804-408-2

9. Haittaohjelmilta suojautumisen yleisohje, VAHTI 3/2004
ISSN 1455-2566
ISBN 951-804-443-0

10. NIST: Computer Security Incident Handling Guide,
Special Publication 800-61 (Tim Grance, Karen Kent, Brian Kim)
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

Liite 2 VM:n ja VAHTIn tietoturvaohjeet ja -määräykset

VAHTI 2/2005: Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005: Information Security and Management by Results
VAHTI 5/2004: Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004: Datasäkerhet och resultatstyrning
VAHTI 3/2004: Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004: Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004: Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 6/2003: Opas julkishallinnon tietoturvakoulutuksen järjestämisestä
VAHTI 5/2003: Käyttäjän tietoturvaohje
Datasäkerhetsanvisning för användaren
User´s Information Security Instruction
VAHTI 4/2003: Valtionhallinnon tietoturvakäsitteistö
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointi
VAHTI 2/2003: Turvallisen etäkäytön arkkitehtuuri
VAHTI 1/2003: Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 4/2002: Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002: Etätyön tietoturvaohje
VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
VM ja PTS, 2002: Tietotekniikan turvallisuus ja toiminnan varmistaminen
VAHTI 6/2001: Tietotekniikkahankintojen tietoturvallisuustarkistuslista
VAHTI 4/2001: Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 3/2001: Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 2/2001: Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 3/2000: Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000: Valtion tietoaineistojen käsittelyn tietoturvaohje
VM 17.2.2000: Tietojärjestelmäselosteen laadintasuositus
VM 5/01/2000: Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje (ohje on uudistumassa ja yhdistymässä tietoaineistojen käsittelyohjeeseen)
VAHTI 2/1999: Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus (uudistuu 2005)

Liite 3 Esimerkkejä tiedotteiden sisällön perusrungosta

Vikapäivystyksestä, neuvonnasta tai helpdeskistä käyttäjille jaetun informaation tulee olla poikkeamaan liittyvästä viestinnästä vastaavalta henkilöltä saatua informaatiota. Ainoastaan vikapäivystys, neuvonta tai helpdesk saa tiedottaa poikkeamasta organisaation sisällä, ellei tiedottamisesta ole annettu erillisohjetta poikkeamaan liittyvästä viestinnästä vastaavalta henkilöltä. Kaikki käyttäjiltä tulevat kyselyt tulee ohjata vikapäivystykseen, neuvontaan tai helpdeskiin.

ÄLÄ ARVAILE, JOS ET TIEDÄ!

1. **Mitä reagointiryhmä kertoo vikapäivystykselle, neuvonnalle tai helpdeskille**
   - millaisesta poikkeamasta on kyse
   - miten poikkeama vaikuttaa; laitteistot, palvelut
   - keitä vaikutukset koskettavat
   - kuinka pitkä on poikkeamasta aiheutuvan häiriön arvioitu kestoaika
   - kuka on yhteyshenkilö / vastuuhenkilö tapauksessa
   - miten poikkeamasta aiheutuneita haittoja voidaan vähentää tai kiertää
   - mitkä ovat neuvonnalta / päivystykseltä vaaditut toimenpiteet
   - mitkä ovat loppukäyttäjiltä vaadittavat toimenpiteet

2. **Mitä vikapäivystyksestä, neuvonnasta, helpdeskistä kerrotaan reagointiryhmän kontaktihenkilölle**
   - missä järjestelmissä tai palveluissa poikkeama ilmenee
   - missä ja milloin poikkeama ilmeni ensimmäisen kerran
   - mitä tapahtui ennen poikkeaman ilmaantumista
   - miten poikkeama ilmenee
     - tarkka virheilmoitus
     - miten toistettavissa
     - koskeeko kaikkia järjestelmän käyttäjiä
     - mitä on tehty tai kokeiltu poikkeamasta aiheutuneen vian poistamiseksi
   - poikkeaman laatu, jos tunnistettavissa
   - kenelle ilmoitetaan
   - kenelle ilmoitettu
   - kuka ilmoittaa, ilmoittajan yhteystiedot

3. **Mitä vikapäivystyksestä, neuvonnasta, helpdeskistä kerrotaan käyttäjille**
   - mikä on vialla
   - miten häiriö vaikuttaa loppukäyttäjän käyttämiin palveluihin

- keihin poikkeama vaikuttaa
- kuinka pitkä on poikkeamasta aiheutuneen häiriön arvioitu kestoaika
- mistä saa lisätietoja poikkeamasta aiheutuneen vian korjauksen edistymisestä
- miten poikkeaman haittoja voidaan vähentää tai kiertää
- mitkä ovat mahdolliset loppukäyttäjältä vaadittavat toimenpiteet

4. Mitä viestintävastaava kertoo tiedotusvälineille

Yleisperiaatteita:

1. viestintäsuunnitelman mukaisesti vain viestintävastaava hoitaa tiedottamisen tiedotusvälineille
2. vain poikkeustilanteissa lähdetään aktiivisesti tiedottamaan ongelmista
3. poikkeamatilanteissa(kaan) ei kerrota sellaisia teknisiä tai toiminnallisia yksityiskohtia, mitä ei muutenkaan kerrota julkisuuteen.

- mikä on vialla (”yleisesti”)
- miten häiriö vaikuttaa loppukäyttäjien palveluihin
- voiko loppukäyttäjä saada palvelua jollain vaihtoehtoisella tavalla
- miten poikkeama on syntynyt (sillä tarkkuudella, kun voidaan kertoa (3))
- arvioitu kestoaika
- milloin asiasta kerrotaan ensimmäisen kerran / seuraavan kerran

Reagointiryhmän on syytä miettiä ennakkoon, mitä kysymyksiä tiedotusvälineet voivat tehdä ja mitä niihin voidaan ja pitää vastata.

Mallikysymyksiä ja vastauksia:

- Ovatko toimintaprosessit vaarassa?
- Ovatko kansalaisten tiedot vaarassa?
- Onko ihmisten yksityisyys vaarassa?
- Tuliko tämä yllätyksenä?
- Vahingon suuruus (euroja)/ laajuus?

Liite 4 Poikkeaman dokumentaatioon kirjattavia asioita

- Päiväys ja kellonaika
- Kuka tai mikä ilmoitti tapahtumasta ja kuinka
- Tapahtuman luonne
  - Koska on tapahtunut
  - Koska tapahtuma havaittiin
  - Kuinka tapahtuma havaittiin
- Mitkä ovat ensimmäiset arviot tapahtuman vaikutuksesta heti ja jatkossa
- Asiasta tietävien kontaktitietojen saaminen
- Mitä laitteita ja ohjelmistoja poikkeamaan liittyy
  - Laitteet/Käyttöjärjestelmät/Ohjelmat
  - Altistuneiden koneiden IP-osoitteet
  - Tietoverkon tyyppi
  - Modeemit: numero
  - Koskeeko poikkeama kriittisiä toimintoja?
  - Sisältääkö kriittistä tietoa?
  - Fyysinen sijainti
  - Fyysinen suojaus/turvallisuustoteutus
  - Kuka on ensisijainen järjestelmävastaava? Yhteystiedot?
  - Laitteen tila juuri nyt
- Mahdollisen hyökkääjän tekemiset
  - Jatkuuko toiminta?
  - Lähde- ja kohdeosoite?
  - Onko oikeudetonta tunkeutumista havaittavissa?
  - Onko palveluksenestoa käytetty?
  - Onko jotain vandalisoitu?
  - Havaintoja siitä, onko hyökkääjä ulko- vai sisäpuolinen?
- Tehdyt toimenpiteet
  - Onko verkko irrotettu?
  - Onko lokeja tutkittu?
  - Onko altistuneisiin laitteisiin etäkäyttö/etäyhteys mahdollinen
  - Muutoksia verkossa, ACL:ssä jne?
  - Kenelle on ilmoitettu?
  - Mitä aiotaan tehdä?
- Mitä työkaluja on olemassa paikallisesti?
  - Onko olemassa järjestelmän valvontatyökaluja?
  - Onko verkonvalvontatyökaluja?
  - Onko sniffaus mahdollista?

- Keneen voidaan olla yhteydessä lisäkysymyksiä varten?
  - Järjestelmän käyttäjät
  - Järjestelmän pääkäyttäjät
  - Verkkovastaavat
- Erityistoiveita ja -ohjeita
  - Onko olemassa joku, jonka kanssa ei tule asiasta keskustella?
  - Muuta?

Tapahtumapaikan tietoja
- Toimistoa käyttävät henkilöt
- Niiden työtekijöiden nimet, joilla on pääsy toimistoon
- Tietokoneiden ja -järjestelmien sijainti huoneessa
- Järjestelmän tila (oliko virrat päällä, ja jos oli, mitä näytössä oli auki ja jos näytönsäästäjä, niin mitä sen takana)
- Verkkoyhteydet sekä mahdolliset muut tietoliikenneyhteydet
- Kohdejärjestelmän kopioinnin yhteydessä paikalla olleet henkilöt
- Kiintolevyjen sekä muiden järjestelmäkomponenttien tiedot: sarjanumerot, valmistajan tiedot, jne.
- Järjestelmän oheis- ja verkkolaitteet.

Liite 5 Esimerkki poikkeaman dokumentoinnista

Liite 4: esimerkki tietoturvapoikkeaman dokumentoinnista pöytäkirjan muodossa

X-Virasto Helsingin toimipiste Tietohallinto	TIETOTURVALOUKKAUKSEN SELVITYS

Tietoturvaloukkaustapaus	1/2005
Status	SELVITETTY
Tapahtuma-aika	9.3.2005 klo 23:10
Selvitetty	10.3.2005 klo 15:45
Tiivistelmä:	Tietomurto X-Viraston WWW-palvelimelle sivustot sotkettu

Tapahtumakuvaus

9.3 klo 23:11	päivystäjä: SMS-viesti päivystäjälle: eheystarkistus: www.x-virasto.fi sivusto muuttunut virka-ajan ulkopuolella
9.3.klo 23:13	päivystäjä: www.x-virasto.fi pääsivu muutettu, sivulla teksti ”This box 0wn3d by B-Crew”.
9.3 klo 23:18	päivystäjä: Soitto X-Viraston tietohallintopäällikölle ja turvallisuuspäällikölle: – käynnistetään tietoturvapoikkeamansuunnitelman mukainen toimintaryhmän toiminta, ryhmän vetovastuu päivystäjällä – hälytetään www-palvelimen ylläpito hätätöihin ja verkkoylläpidon varallaolo työpaikalle – päivystäjä siirtyy virastoon
9.3 klo 23:30	Hälytetty verkkoylläpito: arvio varallaolija työpaikalla n. klo 00:00 Hälytetty WWW-palvelin ylläpito: arvio paikalla n. 00:30 Päivystäjä siirtyy työpaikalle
10.3 klo 00:15	Päivystäjä työpaikalla. Verkkoylläpito eristänyt www-palvelimen kytkimen L3-tason pääsylistalla. Kaikki liikenneyritykset lokiin lokipalvelimelle.
10.3. klo 00:22	verkkoylläpito: www-palvelin yrittää avata yhteyttä ip-osoitteeseen a.b.c.d porttiin 6667. EPÄILY: botnet-asiakasohjelma koneessa. Soitto CERT-FI –päivystäjälle – tarkistaa onko kyseessä tunnettu botnet-komentopalvelimen osoite. www-palvelimen ylläpitäjä saapuu

10.3. klo 00:31 www-ylläpito: lsof –i –listaus liitteenä 1 – yhteyttä osoitteeseen a.b.c.d yrittää /tmp/xx1 –ohjelma. Päätetään ottaa palvelimesta kuuma dumppi ulkoiselle levylle.

10.3 klo 00:40 CERT-FI –päivystäjä soittaa: a.b.c.d on tunnettu botnet-komentopalvelin. Erikoista, että sekä sivut on sotkettu ja botnet-client asentunut koneelle. Keskustellaan, mitä tulee ottaa talteen.

10.3. klo 00:52 www-ylläpito: Varmuuskopio otettu ulkoiselle USB2-levylle VARA1. Lokipalvelimen tietoja tutkitaan: 9.3 klo 23:10 php-haavoittuvuusskannauksen merkkejä, osoiteesta e.f.g.h. Soitto CERT-FI -päivystäjälle: osoite on Ranskassa – ovat yhteydessä osoitteen verkko-operaattoriin.

10.3 klo 01:10 päivystäjä: Lokipalvelin: extranet-webipalvelimen lokista (samassa verkkosegmentissä www-palvelimen kanssa) löytyy palvelimen omasta palomuurista merkkejä 135-137 –portteihin sekä php-haavoittuvuuteen liittyvästä skannauksesta. Eheystarkistus täsmää – ei ole ilmeisesti päässyt sisälle. Sisäverkon puolella ei merkkejä ylimääräisestä liikenteestä. Päätetään rakentaa uusi www-palvelin vararunkoon ja pitää murretussa koneessa virrat päällä mahdollista poliisitutkintaa varten. Verkkoylläpito vaihtaa www-palvelimen ip-osoitteen nimipalveluun, vanhaan osoitteeseen tulevasta liikenteestä pakettidumppi lokipalvelimelle.

10.3 klo 01:15 www-ylläpito: Varmuuskopioajot menossa – palautus uudelle palvelimelle kestää aamuun. Todetaan että www-palvelu ei ole yöllä kriittinen – ohjelmistopäivitys ja tietoturvatarkastus palvelimelle tehtävä ennen käyttöönottoa.

10.3 klo 01:55 päivystys: Uusi www-palvelin asentumassa yön aikana varmuuskopionauhoilta. Yhteydenotto tietohallintopäällikköön: hyväksyntä toimenpiteille

10.3 klo 07:50 www-ylläpito: yhteydenotto viestintään: www-palvelu pois käytöstä klo 10:00 asti. WWW-palvelimen tiedot palautettu varapalvelimelle 9.3 klo 03:00 varmistuksen mukaiseksi. Aloitetaan ohjelmistojen päivitykset.

10.3 klo 08:30 päivystäjä: Toimintaryhmän palaveri, paikalla myös tietohallintopäällikkö, turvallisuuspäällikkö ja viestintä

- sisäinen tiedote jakeluun sähköpostilla ennen 09:00
- rikosilmoitus on paikallaan – tietohallintopäällikkö esittelee asian viraston pääjohtajalle välittömästi
- tarvittavat lokitiedot talteen (lokipalvelin, extranet-www-palvelin): vastuutaho palvelinylläpito, poltetaan CD-ROM –sarja lokitiedoista
- tavoitteena www-palvelun palautus klo 10 mennessä

10.3.klo 09:15 päivystäjä: viraston pääjohtaja allekirjoittanut rikosilmoituksen. Toimitettu faksilla Helsingin rikospoliisiin. Soitettu rikospoliisiin: sovittu lokiaineiston noutamisesta klo 12.

10.3 klo 09:40	www-ylläpito: varapalvelin päivitetty. PHP-haavoittuvuuksien osalta varmistettu viimeisimmät ohjelmistoversiot. Lisätty lokitoimintoja. Viestintä päivittää sivuille ajankohtaista-osuuteen lyhyen neutraalin tiedotteen tilanteesta.
10.3 klo 09:55	www-ylläpito: Uusi www-palvelin tuotantoon. Verkkoylläpito seuraa tiiviisti mahdollisia liikennehäiriöitä.
10.3 klo 12:05	Rikosylikonstaapeli X kuittasi tapaukseen liittyvän aineiston sisältävän CD-ROM –levyn tunnisteella ttl-1/2005-todisteet1. Luettelo tiedostoista ja sisällöstä liitteenä 2. Kopio CD-ROM –liitteenä 3.
10.3. klo 12:30	verkkoylläpito: CERT-FI soitti, keskusteltiin tapauksen tilanteesta. Ilmeisesti yksittäinen botnet-tartunta. Syytä tiukentaa www-palvelimen päivitysmenettelyjä. Yöllä löytynyt osoite e.f.g.h oli myös mukana samassa bot-verkossa. Operaattorilta tuli kiitoksia tiedosta, saivat sielläkin suhteellisen tuoreeltaan koneen kiinni
10.3. klo 14:00	www-ylläpito: Vanhaa www-palvelinta tutkittu. Bot-ohjelman binääri on levykopiolla. Kaikki prosessilistaukset, avoimet tiedostot dumpattu listauksina talteen. Sovittu rikostutkinnan kanssa, että palvelin voidaan sammuttaa.
10.3. klo 15:45	Toimintaryhmän loppupalaveri: Syynä murtoon oli päivittämätön php-ohjelmisto. Palvelinylläpitoon tehostusta varusohjelmien ohjelmistohaavoittuvuuksien seurannan osalta. Verkkoylläpito jatkaa vanhan www-palvelimen IP-osoitteeseen kohdistuvan liikenteen seurantaa. Vanhan palvelimen levyt ja ”kuuma” varmuuskopio tietohallinnon kassakaapissa jatkotoimenpiteitä varten. Vanha www-palvelinrunko voidaan uudelleenkäyttää uusilla levyillä. Tapaukseen reagoitiin rivakasti, kiitos automatisoidun muutosten seurantajärjestelmän. Käytetyt henkilöstöresurssit: hätätyö 4 tuntia, ylityö 5 tuntia. Normaalia työaikaa 10 tuntia.

Vakuudeksi	N.N	P.P
	päivystäjä	tietohallintopäällikkö

Liite 6 Esimerkki ohjeesta henkilökunnan tekemien tietotekniikkarikkomusten käsittelemiseksi

Tämän kaltainen ohje tulee käsitellä YT-menettelyssä ennen käyttöönottoa!

TIETOTEKNIIKKARIKKOMUSTEN SEURAAMUSKÄYTÄNTÖ

Tietotekniikkarikkomuksina pidetään organisaation tietojärjestelmien käytöstä annettujen sääntöjen tai määräysten vastaista toimintaa tai tietojärjestelmien käyttöä Suomen lakien vastaisesti.

Tässä dokumentissa on kuvattu toimenpiteitä, joita henkilöön kohdistetaan, kun tietotekniikkarikkomus on havaittu tai sitä on perusteltua syytä epäillä. Toimenpiteet on jaettu käyttöoikeuksien rajoituksiin rikkomuksen *selvitystyön ajaksi* sekä mahdollisiin rikkomuksesta määrättyihin *seuraamuksiin*.

Dokumentti keskittyy ensisijaisesti organisaation henkilökuntaan. Mahdolliset muut tunnuksen haltijat (esim. yhteistyökumppanien työntekijät) tulee käsitellä tapauskohtaisesti

Kaikki havaitut tietotekniikkarikkomukset ja niistä aiheutuneet toimenpiteet on ilmoitettava organisaation tietoturvapäällikölle.

1. Käyttöoikeuksien rajoittaminen selvitystyön ajaksi

Käyttöoikeuksia voidaan rajoittaa joko sulkemalla kaikki tai osa käyttäjän käyttäjätunnuksista tai muutoin estämällä jonkin tietojärjestelmän käyttö (esim. poistamalla tiedon muutosoikeus)

Selvitystyön ajaksi käyttöoikeuksia rajoitetaan tarvittavassa määrin. Rajoituksena verkkohäiriötilanteissa voi olla myös työaseman kytkeminen irti verkosta.

Käyttöoikeuksia on rajoitettava aina, kun on perusteltua syytä epäillä, että käyttäjä on syyllistynyt väärinkäytökseen, ja on mahdollista, että käyttöoikeudesta on haittaa rikkomuksen selvittämiselle tai vahinkojen minimoimiselle.

Käyttöoikeuksien rajoittamisesta selvitystyön ajaksi päättää tietojärjestelmän omistaja, yksikön johtaja tai muu tehtävään nimetty henkilö. Rajoittamisen toteuttaa ylläpitäjä. Kiireellisissä tapauksissa ylläpitäjä voi omalla päätöksellään rajoittaa käyttöoikeuksia enintään kolmeksi päiväksi, mistä tulee välittömästi ilmoittaa rajoituksista vastaavalle henkilölle.

2. Seuraamukset

Tapahtuneiden tietotekniikkarikkomusten vaihtoehtoisia seuraamuksia arvioitaessa on aina kuultava rikkomuksesta epäiltyä käyttäjää ennen kuin lopullisista seuraamuksista päätetään.

Lievimmissä tapauksissa käyttäjälle huomautetaan asiattomasta toiminnasta.

Muissa tilanteissa seuraamuksia voivat olla työ- ja virkamiesoikeudelliset toimet (kirjallinen varoitus, irtisanominen, palvelussuhteen purku) [3] sekä rikosilmoituksen tekeminen (laissa rangaistaviksi määritellyt teot). Varoituksen antaa yksikön johtaja tai hallintojohtaja. Käyttöoikeudet yksittäisiin järjestelmiin voidaan väärinkäytöksestä johtuvan luottamuspulan synnyttyä evätä määräajaksi tai pysyvästi.

Tietotekniikkarikkomuksen seurauksena käyttäjä on korvausvastuussa sekä väärinkäyttämistään resursseista (esim. koneaika) että väärinkäytön selvitystyöstä aiheutuneista kustannuksista.

3. Seuraamustaulukko

Liitteen taulukossa annetaan suositukset tietotekniikkarikkomusten seuraamuksista. Taulukossa on esimerkkejä tyypillisistä tietojärjestelmien käytön yhteydessä esiintyvistä rikkomuksista luokiteltuina rikkomuksen vakavuusasteen mukaan. Seuraamuksiin vaikuttaa rikkomuksen vakavuuden lisäksi teon tahallisuuden aste.

Taulukon seuraamusruuduissa ylin rivi on varattu mahdolliselle rikosilmoitukselle, seuraavalla rivillä ovat hallinnolliset toimenpiteet ja alimmalla tietohallinnon / atk-yksikön toteuttamat toimet.

4. Käsitteitä

Rikoslain alaisen materiaalin oikeudeton käsittely

- *rikoslain alaista materiaalia* ovat esimerkiksi lapsiporno, eläimiin sekaantuminen, raaka väkivalta, rasistinen aineisto ja kansankiihottamismateriaali
- *käsittelyä* ovat mm. materiaalin levittäminen ja hallussapito

Tekijänoikeuslain alaista materiaalia on esimerkiksi musiikki, videot, sarjakuvat, elokuvat, pelit ja ohjelmistot.

Palvelu on toiminto, jota voidaan käyttää koneen ulkopuolelta. Esimerkiksi

- sähköpostipalvelu (smtp, imaps, …)
- tiedostonsiirtopalvelu (ftp, http, scp, ...)
- vertaisverkko- palvelu (Kazaa, eDonkey,...)

Tunnuksen luovuttamista on esim. salasanan kertominen toiselle käyttäjälle tai istunnon auki jättäminen niin, että joku toinen pääsee valvomattomasti käyttämään toisen käyttöoikeutta.

Tiedon luottamuksellisuuden vaarantamista ovat esim.

- ei-julkiseksi luokitellun tiedon luovuttaminen henkilölle, jolla ei ole oikeutta saada sitä, esim. palvelinten käyttäjätietojen luovutus

[3] Virkamieslaki 24§, 33-34§, 40§ ja Työsopimuslaki 7 luku,2§ 8luku,1§

– ei-julkiseksi luokitellun tiedon tietoturvan laiminlyönti, esim. puutteelliset suojaukset järjestelmässä, jossa tietoa käsitellään
– salassapitorikokset
– henkilötietolain rikkominen

Henkilökohtaisen tietoturvan laiminlyöntiä on esimerkiksi salasanan jättäminen näkyviin.

Liite 7 Esimerkki henkilökunnan tekemien tietotekniikkarikkomusten seuraamuskäytännöstä

Tämän kaltainen ohje tulee käsitellä YT-menettelyssä ennen käyttöönottoa!
Taulukkoa tulee soveltaa Liite 6:n hengessä tapaukseen liittyvät olosuhteet huomioiden.

Rikkomus = pienehkö rikos, paheksuttava, tuomittava teko, virhe, synti (Nykysuomen sanakirja)

	SEURAAMUSASTEIKKO		
TEON TAHALLISUUDEN ASTE ▶	Tietämättömyys Osaamattomuus Huolimattomuus Vahinko Tahattomuus	Piittaamattomuus Törkeä huolimattomuus Välinpitämättömyys Näyttämisen halu Tahallisuus Toistuvuus	Rikoksentekotarkoitus (vahingonteko, luvaton käyttö, vakoilu, salassapitorikos, virka-aseman väärinkäyttö yms.) Hyötymistarkoitus
▲ RIKKOMUKSEN VAKAVUUS			
Vakava rikkomus (Lain mukaan rikkomuksena tai rikoksena tuomittava teko), esim. * Hakkerointi, tunkeutuminen * Rikoslain alaisen materiaalin oikeudeton käsittely * Tekijänoikeuslain alaisen materiaalin laiton levittäminen * Tarkoituksellinen luvaton porttiskannaus * Virusten tahallinen levittäminen * Palvelunestohyökkäys	Rikosilmoitusta harkitaan Huomautus / Kirjallinen varoitus	Rikosilmoitus Kirjallinen varoitus / Irtisanominen / Palvelussuhteen purku	Rikosilmoitus Palvelussuhteen purku
Rikkomus (Vakava väärinkäyttö tai turvallisuuden vaarantaminen), esim. * Ohjelmien ja pelien luvaton kopiointi * Luvattomien ohjelmien asentaminen * Hakkerointi-/ylläpitäjän työkalujen luvaton hallussapito * Palvelun luvaton pystytys * Tunnuksen luovuttaminen * Tiedon luottamuksellisuuden vaarantaminen	Huomautus / Kirjallinen varoitus	Kirjallinen varoitus / Irtisanominen / Palvelussuhteen purku	Rikosilmoitus Irtisanominen / Palvelussuhteen purku
Lievä rikkomus (Väärinkäytös), esim. * Henkilökohtaisen tietoturvan laiminlyönti * Epäasiallinen käytös * Haitan aiheuttaminen * Resurssien tuhlaus * Virustorjunnan tai tietoturvapäivitysten laiminlyönti * Luvaton kaupallinen tai poliittinen toiminta * Kulunvalvontasääntöjen rikkominen	Huomautus	Huomautus / Kirjallinen varoitus	Rikosilmoitusta harkitaan Kirjallinen varoitus / Irtisanominen / Palvelussuhteen purku
▲ RIKKOMUKSEN VAKAVUUS			

Liite 8 Tarkistuslista tietoturvapoikkeaman käsittelyyn

Toimenpiteet

- Tutkitaan, onko kyse tietoturvapoikkeamasta:
  - Miten asia on ilmennyt?
  - Onko vastaavaa tapahtunut aiemmin, ja jos on, mikä sen on aiheuttanut?
  - Onko vastaavanlaisesta poikkeamasta tietoa jossain muualla (haku www-sivuilta, tietokannoista yms.)
  - Heti, kun todetaan, että on kyse tietoturvapoikkeamasta, aletaan dokumentointi, tarkemmat tutkimukset ja todisteaineiston kerääminen.
- Millaisesta poikkeamasta on kyse? (Palvelunestohyökkäys, haittaohjelma, murto yms.)
- Pysähdy ja mieti rauhassa
  - Missä ongelma esiintyy ja missä ei?
  - Mikä on syy ja mikä on vain oire?
  - Onko kyseessä aktiivinen hyökkäys ja mikä on sen motiivi?
  - Kuinka vakavasta poikkeamasta on kyse?
    - Miten poikkeama vaikuttaa; laitteistot, palvelut?
    - Keitä vaikutukset koskettavat?
    - Kuinka pitkä on poikkeamasta aiheutuvan häiriön arvioitu kestoaika?
- Tiedotetaan asianosaisille
- Kerätään, talletetaan, suojataan ja dokumentoidaan todisteaineisto
- Eristetään tietoturvapoikkeaman kohde käsittelyä ja puhdistusta varten.
  - Selvitetään haavoittuvuudet, joita käytettiin hyväksi, ja paikataan ne.
  - Poistetaan vahingollinen koodi, asiaankuulumaton aineisto ja muu vastaava.
- Toipuminen tietoturvapoikkeamatilanteesta:
  - Palautetaan järjestelmät puhdistamisen jälkeen toimintakuntoon.
  - Varmistetaan, että vahingoittuneet systeemit toimivat normaalisti.
  - Jos katsotaan tarpeelliseksi ja on mahdollista, lisätään valvontaa vastaisen varalle.
- Lopuksi:
  - Viimeistellään loppuraportti tietoturvapoikkeamasta.
  - Pidetään kokous, jossa käydään läpi, mitä opittiin.

Enemmän aiheesta *NIST: Computer Security Incident Handling Guide* [10].

Liite 9 Ohjeen *Tietoturvapoikkeamatilanteiden hallinta* toteutusohje

Toteutusohjeessa kerrotaan ne toimenpiteet, joilla luodaan valmius tämän ohjeen mukaiseen toimintaan tietoturvapoikkeamatilanteessa. Toimenpiteet voidaan kiteyttää sanoihin

suunnittele - kouluta - harjoittele

1. Suunnittele

- tietoturvapolitiikkaan sisällytetään lausuma, minkälaisiin poikkeamiin ja millä vakavuudella varaudutaan ja reagoidaan
- tietoturvasuunnitelmaan kirjataan, miten politiikassa asetettuun tavoitteeseen päästään ja koska
- määritellään erilaisiin poikkeamatilanteisiin osallistuvat tahot
- nimetään henkilöt
- budjetoidaan vuosisuunnitelmiin työaikaa ja rahaa
- laaditaan organisaatiokohtainen toimintasuunnitelma
- laaditaan toiminto- ja toimijakohtainen toimintaohje eri tilanteisiin
- kootaan tarvittavat tiedot: järjestelmäkuvaukset, verkkokuvat, yhteystiedot (organisaatiot, nimet, sposti, puhno, faksi, ...)
- hankitaan tarvittavat laitteistot ja ohjelmat

2. Kouluta

- perehdytetään toimijat tehtäviinsä
- perehdytetään toimijat välineiden ja ohjelmistojen käyttöön

3. Harjoittele

- 1-2 kertaa vuodessa
- tietoturvavastaava suunnittelee ja toteuttaa poikkeamatilanteen (niin aidon kuin mahdollista, ilman että (kohtuuttomasti) vaarannetaan normaalia toimintaa)
- käydään läpi poikkeamatilanteeseen reagoiminen ja toipuminen olemassa olevien ohjeiden mukaan
- tehdään koko ajan ohjeen mukaiset muistiinpanot
- harjoituksen jälkeen analysoidaan toiminta
- pidetään palautustilaisuus
- suunnitellaan parannus/korjaustoimenpiteet toimintaan ja ohjeisiin
- edellä mainitut toimenpiteet toteutetaan tai viedään toimintasuunnitelmiin myöhemmin toteutettavaksi

Liite 10 Reagointi- ja toipumisorganisaation tarvitsemia työkaluja ja varusteita

- Tietokone
  - tyhjää tallennustilaa
  - tutkinta- ja varmuuskopiointiohjelmia (esimerkiksi dd ja md5sum)
  - ohjeita ja manuaaleja
  - nopea CD-RW/DVD-RW-asema
  - nauhavarmistuslaite
  - ohjelmistot
    - useita käyttöjärjestelmiä
    - tiedostojen katseluohjelmia
    - kopiointiohjelmia
- Digitaalikamera
- Sanelukone
- Erilaisia kaapeleita
  - tietokonekaapeleita
    - erilaiset emot, levyt sekä muut laitteet
  - verkkokaapelit
    - kääntäviä ja suoria kaapeleita
  - jatkojohtoja

- Työkaluja
  - "Leatherman”
  - taskulamppu
- Lähiverkkotarvikkeita
  - hubi
- Tyhjiä tallennuslevyjä
  - IDE-levyjä
  - SCSI-levyjä
  - CD/DVD-aihioita
- Muistiinpanovälineitä
  - mm. CD-levytussi

TYÖKALUPAKISTA EI SAA LAINATA TAVAROITA!!!

Liite 11 Ohjeen *Tietoturvapoikkeamatilanteiden hallinta* laatiminen

Ohje *Tietoturvapoikkeamatilanteiden hallinta* laadittiin Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) alaisuudessa ja ohjauksessa. Se korvaa ohjeen *Toimet tietoturvaloukkaustilanteissa (VAHTI 7/2001)*. Työryhmän kokoonpano oli seuraava:

Puheenjohtaja:
Minna Manninen, Tampereen yliopisto
Jäsenet:
Kimmo Helaskoski, puolustusvoimat
Kauto Huopio, Viestintävirasto
Sari Kajantie, KRP
Mats Kommonen, Turun yliopisto
Leila Pohjolainen, CSC Tieteellinen laskenta
Juha Rautava, puolustusvoimat
Juhani Sillanpää, Valtiovarainministeriö

Työ suoritettiin virkatyönä.

Esitys VAHTI 7/2001:n uudistamisesta käsiteltiin VAHTIn kokouksessa 5/2004 (25.5.2004). VAHTI ohjasi työryhmää kokouksissaan 9/2004 (28.10.2004) sekä 3/2005 (3.3.2005), minkä jälkeen ohjeluonnos lähetettiin lausuntokierrokselle. Luonnoksesta tiedotettiin laajasti hallinnossa ja yrityksille ja se oli nähtävissä myös VAHTI:n kotisivuilla. Lausuntoja saatiin 23 kappaletta. VAHTI hyväksyi lausuntojen perusteella muokatun ohjeen kokouksessaan 5/2005 (12.5.2005).

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin: (09) 160 01
Telefaksi: (09) 160 33123
www.vm.fi

3/2005
TIETOTURVAPOIKKEAMATILANTEIDEN HALLINTA

ISBN 951-804-521-6 (nid)
ISBN 951-804-522-4 (PDF)
ISSN 1455-2566