Tietoturvapoikkeamatilanteiden hallinta

VAHTI 3/2016 -OHJELUONNOS – 14.9.2016

Sisällysluettelo

Kuviot ja taulukot

1. JOHDANTO

Julkishallinto elää voimakasta muutoksen aikaa. Sähköinen asiointi, digitalisaatio sekä palveluiden keskittäminen ja verkottuminen asettavat uusia haasteita tieto- ja kyberturvallisuuden hallinnalle. Viranomaisen tulee pystyä havaitsemaan tietoverkoissaan ja järjestelmissään mahdollisesti tapahtuvat poikkeavat tapahtumat sekä ryhtyä tarvittaviin toimenpiteisiin niiden selvittämiseksi.

Kehittyneet kohdistetut tietoturvahyökkäykset asettavat omat vaatimuksensa niin tekniselle tietoturvallisuudelle kuin henkilöstön osaamisellekin. Aikaisemmin paikalliset, järjestelmäkohtaiset poikkeamat voivat nykyään helposti laajentua koskemaan useita eri viranomaisia. Hyökkäyksen toteutustapa, kesto ja hyökkäyksen taustalla oleva motivaatio vaihtelevat tapauskohtaisesti. Tietoturvapoikkeama voi olla esimerkiksi palvelunestohyökkäys, tietovuoto tai matkapuhelimen salakuuntelu. Palvelunestohyökkäys voi kestää muutamia minuutteja. Sen sijaan kohdistetun hyökkäyksen avulla tehty tietovuoto voi kestää useita vuosia.

Harva organisaatio kykenee yksin havaitsemaan, analysoimaan tai estämään moderneja kohdistettuja tietoturvahyökkäyksiä. Viestintäviraston Kyberturvallisuuskeskus on keskeisessä roolissa tietoturvatietojen keräämisessä, tilannekuvan muodostamisessa ja tietoturvatiedon jakamisessa. Viranomaisten tulee ilmoittaa havaitsemistaan tietoturvapoikkeamista Viestintävirastolle. Aktiivinen tiedon jakaminen ja yhteistyö eri toimijoiden välillä tilannekuvan muodostamiseksi ovat omiaan parantamaan viranomaisen tietoturvallisuutta, toiminnan jatkuvuutta ja häiriötilanteiden hallintaa.

Tämä ohje on suunnattu viranomaisille ja julkishallinnolle palveluita tuottaville toimijoille. Ohjeen tavoitteena on yhdenmukaistaa ja kehittää viranomaisten tietoturvapoikkeamien hallintatapaa, lisätä poikkeamien hallintaan liittyvää yhteistyötä sekä parantaa yleisesti valtionhallinnon tietoturvallisuutta. Ohjeessa ei käsitellä toiminnan jatkuvuutta yleisissä ICT-häiriötilanteissa.

Tietoturvatapahtuma
Tietoturvallisuuteen liittyvä tapahtuma, jolla voi olla vahingollisia vaikutuksia organisaation toiminnalle.

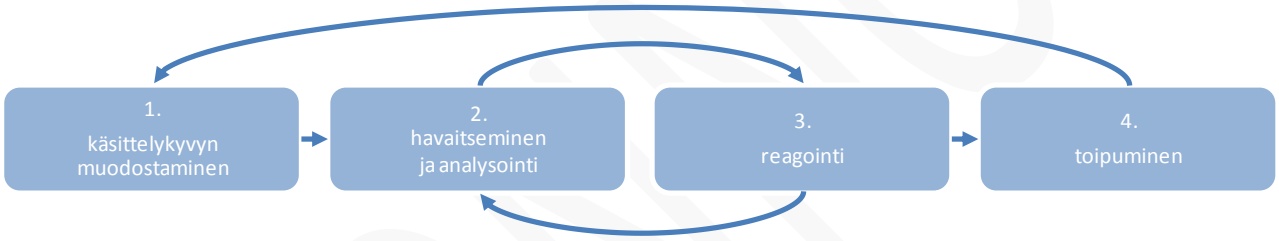
Tietoturvapoikkeama
Tahallinen tai tahaton tapahtuma, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut.

2. TIETOTURVAPOIKKEAMAN HALLINTAPROSESSI

Tietoturvapoikkeamien hallintaprosessi koostuu useista eri osista. Prosessin tarkoituksena on varautua häiriötilanteisiin, turvata toiminnan jatkuvuus ja pyrkiä estämään häiriötilanteiden muodostuminen jatkossa. Hallintaprosessi on riippuvainen riskienhallinnan avulla määritellyistä turvakontrolleista, joiden avulla poikkeamat pyritään estämään ja tarvittaessa havaitsemaan. Havainnointikyky koostuu teknisten kontrollien lisäksi myös henkilöstön ja sidosryhmien havainnoista. Tietoturvapoikkeaman hallintaprosessi jaetaan tässä ohjeessa neljään päävaiheeseen:

1. tietoturvapoikkeamien käsittelykyvyn muodostaminen
2. tietoturvatapahtuman havaitseminen ja analysointi
3. tietoturvapoikkeamaan reagointi
4. tietoturvapoikkeamasta toipuminen eli paluu normaaliin toimintaan.

Tarvittaessa prosessin vaiheita 2. ja 3. toistetaan niin kauan, että poikkeama on saatu korjattua ja voidaan aloittaa toipuminen normaalitilaan..



Kuvio 1. Tietoturvapoikkeaman hallinnan päävaiheet

Tietoturvapoikkeamien käsittelykyvyn muodostaminen (1.) käsittää erilaiset varautumistoimet, joiden avulla poikkeamatilanteessa voidaan toimia. Varautumistoimissa tulee huomioida mm. järjestelmien ja prosessien riittävä dokumentaatio, päätöksenteko, riippuvuuksien tunnistaminen, omat ja yhteistyötahojen henkilöstöresurssit, tilannekuvan muodostaminen ja tiedon jakaminen, haittaohjelmien ja poikkeavan toiminnan havainnointikyvyn kehittäminen, sopimusmenettelyt ja harjoittelu.

Tietoturvapoikkeaman havaitseminen ja analysointi (2.) käsittää normaalista poikkeavan toiminnan havaitsemisen ja analysoinnin, minkä tavoitteena on selvittää, mitä on tapahtunut ja miksi. Analysoinnin tuloksena voidaan todeta, onko kyseessä tietoturvapoikkeama tai esim. ICT-häiriötilanne.

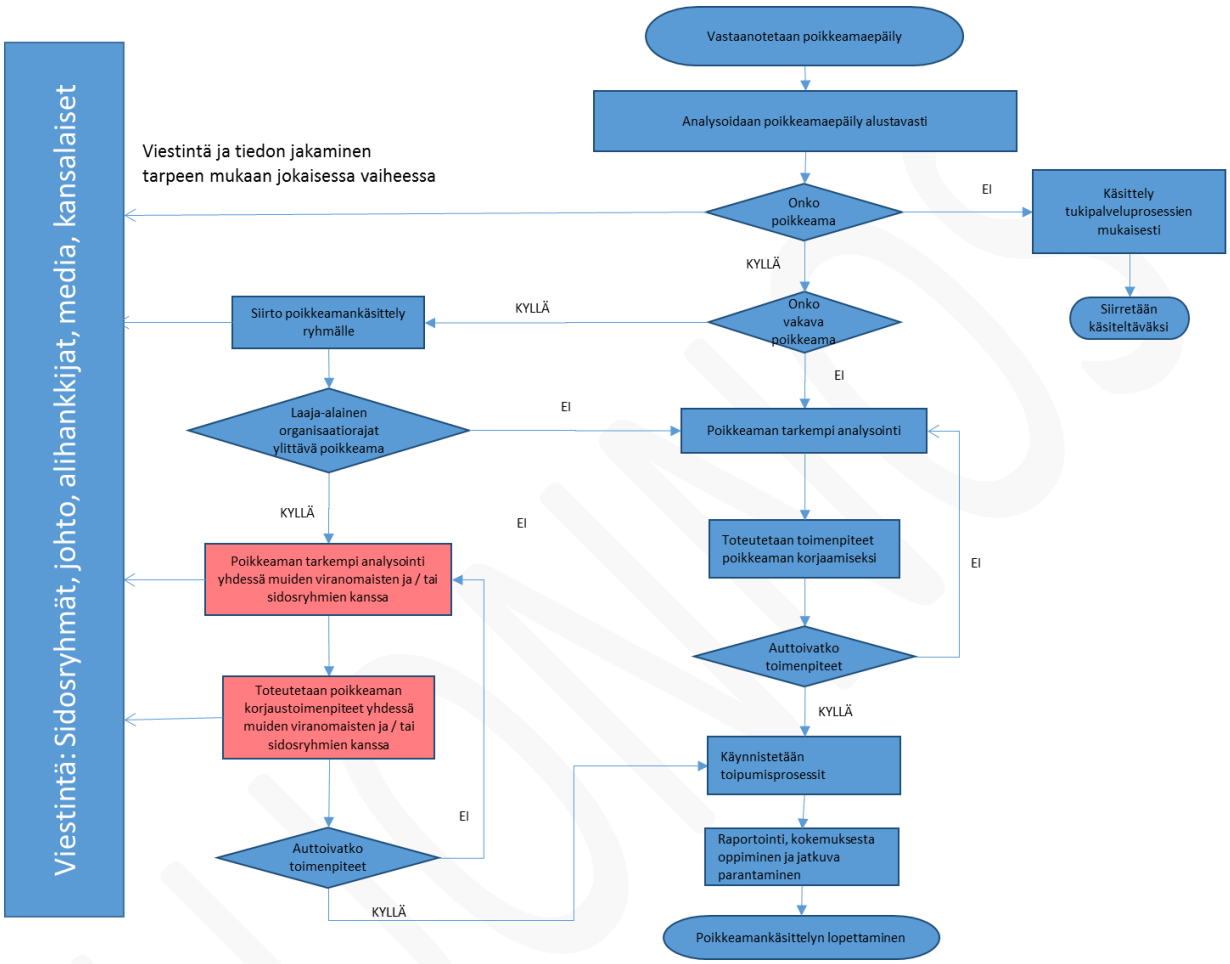
Tietoturvapoikkeamaan reagointiin (3.) liittyvät toimenpiteet, joiden avulla mahdolliset vahingot minimoidaan, poikkeamasta informoidaan muita viranomaisia ja sidosryhmiä ja käynnistetään toimenpiteet poikkeaman korjaamiseksi.

Toipumisvaiheessa (4.) organisaation ja palveluiden toiminta palautetaan normaalitilaan. Poikkeamasta laaditaan raportti, jonka havaintojen perusteella kehitetään käsittelykykyä ja varautumista, jotta poikkeaman toistuminen voitaisiin jatkossa estää.

Tämän ohjeen rakenne mukailee edellä mainittuja tietoturvapoikkeamien käsittelyn neljää päävaihetta.

2.1. Tietoturvapoikkeaman käsittelyprosessin yleiskuvaus

Tietoturvapoikkeamien käsittelyprosessiin vaikuttavat muun muassa organisaation koko, poikkeaman tyyppi ja toimintojen ulkoistaminen. Alla on kuvattu poikkeamien käsittelyprosessin malli. Poikkeamien käsittelyprosessiin voidaan kuvata lisäksi esimerkiksi vastuiden jakaminen poikkeamien selvitykseen osallistuville, todisteiden kerääminen, lisävahinkojen estäminen, lisäselvitysten tekeminen, normaalitilaan palautuminen ja poikkeamaprosessin parantaminen.



Kuvio 2. Tietoturvapoikkeamien käsittelyprosessi

3. TIETOTURVAPOIKKEAMIEN KÄSITTELYKYVYN MUODOSTAMINEN

Tietoturvapoikkeamien käsittelykyvyn tulee olla tasapainossa organisaation toiminnan sekä siihen kohdistuvien vaatimusten ja riskien kanssa. Tietoturvapoikkeamien käsittelyssä on huomioitava lakisääteiset velvoitteet. Riskeihin varautumisessa on arvioitava tietoturvapoikkeamien aiheuttamat mahdolliset / potentiaaliset haittavaikutukset suhteessa varautumisesta aiheutuviin kustannuksiin.

Tietoturvapoikkeamien tehokkaan käsittelyn varmistamiseksi on huomioitava seuraavat asiat:

- **poikkeamaryhmä** – muodostetaan tietoturvapoikkeamien käsittelyryhmä ja sovitaan ryhmän toimintakäytännöt, mukaan lukien päivystys- ja koulutusmenettelyt
- **vastuut** - asetetaan selkeät vastuut poikkeamatilanteessa toimimiseen ja päätöksentekoon
- **sidosryhmäyhteistyö -** luodaan yhteistyö- ja viestintämenettelyt eri sidosryhmien kanssa
- **tiedon jakaminen ja viestintä -** määritellään viestintäkanavat ja tiedon jakamisen vastuut
- **luokittelu** - määritellään tietoturvapoikkeamien luokitteluperiaatteet
- **oppiminen** - luodaan poikkeamatilanteista oppimisen käytännöt
- **harjoittelu** – sovitaan harjoituskäytännöt tietoturvapoikkeamien käsittelylle
- **turvakontrollit** - suunnitellaan, miten tietoturvapoikkeamien määrää ja vakavuutta vähennetään verkon, järjestelmien ja ohjelmistojen suojauksella sekä pääsynhallinnalla.

3.1. Tietoturvapoikkeamien käsittelyn organisointi

Organisaation on määritettävä tietoturvapoikkeamien käsittelyryhmä tai -toiminto, jonka tehtävänä on suunnitella tarvittavat toimenpiteet poikkeaman korjaamiseksi. Tietoturvapoikkeamien käsittelyryhmä toimii yhteistyössä ulkoisten ja sisäisten sidosryhmien kanssa. Käsittelyryhmän kokoonpano voi määräytyä tapauskohtaisesti poikkeaman perusteella. Ryhmässä voi olla myös organisaation ulkopuolisia asiantuntijoita etenkin silloin, kun toimintoja on ulkoistettu palveluntarjoajille. Ryhmän tehtävänä on varmistaa, että poikkeamiin reagoidaan suunnitelmien mukaisesti, selvitystyössä noudatetaan lakia ja että kaikissa tilanteissa on mukana riittävästi asiantuntemusta ja asianmukaiset vastuuhenkilöt. Poikkeamatilanteiden käsittelyä tulee myös harjoitella.

Tietoturvapoikkeamien hallitsemiseksi on selvitettävä, millaista osaamista tarvitaan sekä huomioitava palvelutuottajien rooli ja kyvykkyys huolehtia palveluiden tietoturvallisuudesta.

Organisaatioiden toiminnassa havaitaan jatkuvasti suuri määrä erilaisia teknisiä tietoturvatapahtumia, joiden käsittely on rutiinitoimintaa. Suurin osa tietoturvatapahtumista ei johda varsinaiseen tietoturvapoikkeamatilanteeseen. Tekniset tietoturvatapahtumat on ensisijaisesti käsiteltävä normaalien palveluhallintaprosessien mukaisesti IT-tukipalveluita tuottavassa organisaatiossa. Käyttäjille on tiedotettava, kenelle tietoturvapoikkeamista ilmoitetaan.

Tietoturvapoikkeaman käsittelyssä tarvittavia vastuita voidaan määritellä alla olevassa taulukossa kuvatulla tavalla.

Taulukko 1. Tietoturvapoikkeamien käsittelyvastuut

Rooli	Vastuualueen kuvaus
Viraston johto	Vastaa päätöksenteosta ja poikkeamanhallintaan käytettävistä resursseista.
Tietoturvapoikkeaman käsittelyryhmän vetäjä	Koordinoi käsittelyryhmän käytännön työskentelyä ja toimii yhdyshenkilönä organisaation johdolle.
Asiantuntija	Vastaa asiantuntijana omaan alueeseensa kuuluvasta poikkeamanselvitystyöstä. Ei ole välttämättä organisaation oma työntekijä.

Tietotekniikkapalvelujen vastuuhenkilö	Vastaa teknisten tietoturvatapahtumien seurannasta ja analysoinnista sekä poikkeamaepäilyjen vastaanottamisesta, alustavasta luokittelusta ja asian saattamisesta käsittelyryhmän tiedoksi.
Viestinnästä vastaava henkilö	Vastaa organisaation sisäisen viestinnän lisäksi ulkoisesta viestinnästä eri sidosryhmille.
Palvelun omistaja	Tietoturvapoikkeaman kohteena olevan palvelun omistaja vastaa toimenpiteistä ja päätöksistä, joita palvelulle on tehtävä poikkeaman korjaamiseksi.

Tietoturvapoikkeamien hallinta saattaa vaatia päivystys-, varallaolo- tai varahenkilöjärjestelyjä. Yli- tai hätätyönä tehtävän tietoturvapoikkeaman selvityksen varalle tulee määritellä, missä tilanteissa ja kenellä on oikeus kutsua tarvittavat henkilöt paikalle. Poikkeamien käsittelyyn tarvittavien henkilöiden kanssa tulee sopia etukäteen yhteydenottotavoista ja heidät tulee kouluttaa tehtävään. Tarvittaessa henkilöille on järjestettävä työtilat ja selvitystyössä tarvittavat työkalut.

Poikkeamatilanteen hoitamiseen liittyvien henkilöiden esteellisyys tulee huomioida. Jos on mahdollista, että poikkeama on aiheutettu organisaation sisäisesti, on huolehdittava, ettei aiheuttaja pysty vahingoittamaan todistusaineistoa tai hidastamaan selvitystyön tai mahdollisen poliisitutkinnan etenemistä. Todistusaineiston ja yksilön oikeuksien turvaaminen saattavat edellyttää usean henkilön osallistumista poikkeaman käsittelyyn.

Päätöksenteon turvaamiseksi johdon tulee määritellä yksilöidyt toimintavaltuudet ja tietoturvapoikkeamien käsittelyyn käytettävät resurssit. Organisaatiossa tulee määritellä, kuka päättää

- poikkeamiin varautumisesta
- poikkeamien vakavuusasteesta
- poikkeamatiedon luokittelusta
- poikkeamatilanteisiin liittyvästä viestinnästä
- organisaation toimintaa rajaavista toimenpiteistä
- sidosryhmien toimintaa rajaavista toimenpiteistä
- poikkeaman hallintaan liittyvistä ennakoimattomista kustannuksista
- toipumis- ja varamenettelyistä
- tutkintapyynnön tekemisestä.

3.2. Tietoturvatiedon luokittelu

Tietoturvapoikkeamaan tai -tapahtumaan liittyvä tieto on usein julkisuuslain 24 §:n perusteella salassa pidettävää. Tiedon luonne saattaa kuitenkin edellyttää sen nopeaa jakamista muille viranomaisille. Tällainen tieto voi liittyä mm. kohdistettuihin tietoturvahyökkäyksiin tai kiristyshaittaohjelmiin, joiden eteneminen valtionhallinnossa voidaan mm. tiedon tehokkaalla jakamisella estää.

Viranomaisen tulee arvioida etukäteen, mitä ja miten tietoturvatietoa voidaan tarvittaessa jakaa muille viranomaisille, miten tietoturvatieto tulee luokitella ja mitä riskejä tietoturvatiedon jakamiseen voi liittyä. Jos salassapitoon liittyviä menettelyitä ei ole suunniteltu, tietoturvatiedon jakaminen tarvittaville sidosryhmille voi hidastua ja näin mahdollistaa tietoturvapoikkeaman leviämisen myös muualle valtionhallintoon.

Tietoturvatiedon jakamiseen liittyvät riskit tulee huomioida ennen tiedon laajempaa jakelua. Lokitiedot saattavat sisältää henkilötietoja, joiden jakamisessa on huomioitava lain asettamat velvoitteet. Tietoturvatieto saattaa myös sisältää tietoa verkon ja tietojärjestelmien infrastruktuurista. Tällaisten tietojen päätyminen ulkopuoliselle voi vaarantaa organisaation tietoturvallisuuden.

Viestintäviraston Kyberturvallisuuskeskus jakaa yhteistyöverkostojen kautta saatuja tietoja tietoturvahyökkäyksistä. Näissä jakeluissa saattaa olla käytössä kansainvälinen Traffic Light Protocol (TLP) – luokitus, joka on kehitetty kuvaamaan, miten tietoturvatietoa voidaan jakaa eri verkostojen kesken. Kyseessä on jakelurajoite, jota ei pidä sekoittaa viranomaisen luokitusjärjestelmään. TLP-malli on kuvattu tarkemmin liitteessä 2.

Alla olevassa taulukossa on esimerkki tietoturvatiedon luokittelusta ja siitä, miten TLP-jakelurajoite ei välttämättä ole sidoksissa tiedon suojaustasoihin. Taulukon tiedot ovat suuntaa antavia, eikä niitä voi sellaisenaan soveltaa viranomaisen tietoihin.

Taulukko 2. Tietoturvatiedon luokittelu ja TLP-malli

Tietoturvatieto	Julkisuus	Salassapitoperuste	Suojaustaso	TLP
Lokitiedot	Saattaa sisältää salassa pidettävää tietoa	mm. henkilötieto, sähköisen viestinnän välitystieto	ST IV – III	TLP Amber - Red
Tilannekuvatieto	Saattaa sisältää salassa pidettävää tietoa	Julkisuuslain 24 §:n kohdat 2, 7, 8 tai 10	ST IV – II	TLP Green - Red
Käyttäjätieto	Saattaa sisältää salassa pidettävää tietoa	henkilötieto, sähköisen viestinnän välitystieto	ST IV	TLP Red
Hyökkääjän tunnistetiedot	Saattaa sisältää salassa pidettävää tietoa	henkilötieto, julkisuuslaki 24 §:n 7 k	ST IV – II	TLP Amber - Red
Kamera- ja rikosilmoitinlaitteistojen tiedot	Saattaa sisältää salassa pidettävää tietoa	henkilötieto, julkisuuslaki 24 §:n 7 k	ST IV – II	TLP Amber - Red
Haittaohjelman tunnistetiedot				TLP Green - Amber
Kohdistetun haittaohjelman tunnistetie-	Saattaa sisältää salassa pidettävää	Julkisuuslaki 24 §:n	ST IV – II	TLP Amber -

dot	tietoa	7 k		Red
Tietoturvaohjeet	Saattaa sisältää salassa pidettävää tietoa	Julkisuuslaki 24 §:n 7 k	ST IV	TLP Green - Amber
Kalasteluviestinäytteet				TLP Amber
Haittaohjelman komento- ja välityspalvelintiedot				TLP White - Red

3.3. Tietoturvatiedon jakaminen ja viestintä

Tietoturvatiedon jakamisella ja viestinnällä tarkoitetaan tässä ohjeessa eri asioita. Tietoturvatiedon jakamiselle tarkoitetaan asiantuntijoiden jakamaa teknistä tietoa, jonka avulla poikkeaman selvitystyötä pyritään nopeuttamaan, estämään poikkeaman leviäminen muihin organisaatioihin sekä ennaltaehkäisemään poikkeamien syntyminen. Viestinnällä tarkoitetaan sitä sisäistä ja ulkoista viestintää, jolla tiedotetaan tapahtuneesta poikkeamasta henkilöstölle, sidosryhmille, medialle ja kansalaisille. Viestinnän tavoitteena on mm. ehkäistä virheellisen tiedon leviäminen ja pitää tarvittavat osapuolet tietoisina poikkeaman selvitystyön etenemisestä.

3.3.1. Tietoturvatiedon jakaminen

Tiedon jakaminen on perusedellytys toimivalle yhteistyölle ja verkostotoiminnalle, joten prosessit tietojen jakamiseen tietoturvapoikkeamatilanteessa on suunniteltava huolellisesti. Tietoturvatietoa on hyödyllistä jakaa sekä viranomaisille että muille sidosryhmille. Tietoturvatietojen jakamista suunniteltaessa on otettava huomioon tietojen salassapitovelvoitteet edellisessä luvussa kuvatusti. Tietoturvatietoja ei välttämättä voi sellaisenaan toimittaa kaikille sidosryhmille, vaan tiedoista on tarvittaessa poistettava salassa pidettävät osiot tai hyödynnettävä salattuja tiedonjakoratkaisuja, kuten turvapostia. Tietoturvatiedon jakamisessa tulee huomioida sekä onnistuneet että yrityksen asteelle jääneet tietoturvatapahtumat.

Tietoturvallisuuden tilannekuva paranee, kun organisaatiot jakavat tietoturvatietoa keskenään. Kattavan tilannekuvan perusteella on mahdollista kohdistaa tietoturvatoimenpiteet niihin kohteisiin, joissa vastaavat tietoturvauhkat ovat todennäköisiä. Tiedon jakamisessa tulee kiinnittää huomiota tiedon luokitteluun. Liian korkealle luokiteltu tieto on vaikea levittää hallintoon nopeasti, mikä saattaa hidastaa mahdollisen poikkeaman selvitystyötä. Toisaalta väärin luokiteltu tieto voi myös vaarantaa organisaation tietoturvallisuuden. Tarvittaessa jaettava tieto on hyvä anonymisoida, eli poistaa sensitiivisin tieto välittäen vain välttämättömät tekniset tiedot uhkan torjumiseksi tiedon luottamuksellisuutta vaarantamatta. Kertomatta voidaan jättää, missä ongelma on aiemmin havaittu tai keneen uhka on aiemmin kohdistunut. Jos tietoturvapoikkeaman kohteiksi joutuneita on tiedotettava, ennalta harkitut tiedonjakomallit ovat hyödyksi.

Tietojen ennakoivalla jakamisella on mahdollista varmistaa tietoturvapoikkeamien tehokas koordinointi eri toimijoiden välillä ja valtionhallinnon tietoturvallisuuden tilannekuvan pysyminen ajan tasalla. Ilmoittajalla ei ole tarvetta pohtia tiedon merkityksellisyyttä, vaan edellä mainitut viranomaiset analysoivat, onko ilmoitettu tieto kokonaisuuden kannalta merkittävä. Myös toistuvista tai poikkeuksellisista

tietoturvatapahtumista on syytä jakaa tietoa, vaikka ne eivät ole välttämättä johtaneet tietoturvapoikkeamaan. Kokonaiskuvan muodostamisessa tällaisistakin tiedoista voi olla hyötyä.

Poikkeaman kohteeksi joutuneella organisaatiolla saattaa olla lakiin, määräyksiin tai sopimuksiin perustuvia ilmoitus- tai toimenpidevelvollisuuksia eri tahoille. Lakisääteiset ilmoitusvelvollisuudet on syytä selvittää etukäteen, jotta ne ovat tiedossa poikkeamatilanteessa.

Tiedonjaon suunnittelussa on varmistettava, mitä poikkeamaan liittyviä tietoja organisaatiolla on lupa jakaa.

3.3.2. Viranomaisyhteistyö ja ilmoitusvelvollisuus

Harva organisaatio kykenee yksin havaitsemaan edistyneitä kohdistettuja tietoturvahyökkäyksiä tai toipumaan niistä. Viranomaisyhteistyön tavoitteena on lisätä turvallisuustietoisuutta, parantaa tietoturvallisuutta sekä nopeuttaa poikkeamien hallintaa. Tietoturvatapahtumista tulee ilmoittaa matalalla kynnyksellä Viestintävirastoon ja valtionhallinnon VIRT-ryhmälle (*virtual incident security response team*) sekä tarvittaessa tehdä rikosilmoitus. Viestintäviraston Kyberturvallisuuskeskuksesta voi kysyä tietoja valtionhallinnon yhteistyöverkostoista ja tarvittaessa kutsua koolle viranomaisten yhteistyöverkoston (VIRT).

Viranomaisella on lakisääteinen velvoite ilmoittaa eräistä tietoturvapoikkeamista. Nämä velvoitteet on lueteltu alla olevassa taulukossa.

Taulukko 3. Tietoturvapoikkeamista ilmoittaminen

Tieto	Kenelle ilmoitetaan	Aika	Peruste
Kansainväliseen turvaluokiteltuun tietoon kohdistunut väärinkäytös	Kansallinen turvallisuusviranomainen (UM/NSA)	24 h sisällä	Neuvoston turvallisuusmääräys
Henkilötietoihin kohdistunut väärinkäytös	Kansallinen valvontaviranomainen	72 h sisällä	EU:n tietosuoja-asetus, velvoittava 25.5.2018 jälkeen
Varoihin tai omaisuuteen kohdistunut väärinkäytös	Valtiontalouden tarkastusvirasto	Viipymättä	Laki (676/2000) 16 §
Vakoilun tai törkeän vakoilun ilmoittaminen	Poliisi tai uhan kohde	Viipymättä	Rikoslaki 15 luku, 10 §

3.3.3. Viestintäviraston Kyberturvallisuuskeskus

Tietoturvapoikkeaman havaitsemisen jälkeen on ensisijaisesti otettava yhteyttä Viestintäviraston Kyberturvallisuuskeskukseen. Saatuaan yhteydenoton mahdollisesta poikkeamasta Viestintävirasto

- ohjeistaa poikkeaman vahinkojen rajoittamisessa ja lakisääteisten velvoitteiden täyttämisessä sekä mahdollisen rikosilmoituksen tekemisessä,

- auttaa tietoturvaloukkauksen analysoinnissa,
- tukee jatkotoimenpiteiden koordinointia ja
- voi kerätä kansallista tai kansainvälistä lisätietoa ongelman ratkaisemiseksi.

Lisäksi Viestintäviraston Kyberturvallisuuskeskuksen päätehtäviin kuuluu tiedonjakaminen muille viranomaisille tietoturvan kohentamiseksi ja tietoturvauhista viestiminen kansalaisille. Myös ongelman kohdanneen palveluntarjoajan tukeminen viestimisessä on luonnollinen osa yhteistyötä tilanteen ratkaisemiseksi.

Viestintävirastoon on hyvä ilmoittaa vähäisiltäkin tuntuvista poikkeamatilanteista. Pienilläkin tapahtumilla voi olla suuri merkitys kyberturvallisuuden tilannekuvan rakentamisen kannalta. Useampi merkityksettömältä vaikuttava ilmoitus eri tahoilta voi yhdessä paljastaa laajemman ongelman.

3.3.4. Poliisi

Jos havaituissa tietoturvapoikkeamissa epäillään rikosta, on aina syytä tehdä rikosilmoitus. Rikosilmoitus tehdään paikallispoliisille, josta asia tarvittaessa siirretään KRP:n tutkittavaksi. Rikosilmoituksen tekemisen yhteydessä on syytä sopia poliisin kanssa, millä tavoin todistusaineisto turvataan kyseisessä tapauksessa.

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 asianomistajan eli rikoksen uhrin vaatiessa rangaistusta.

Rikosilmoituksen muoto on vapaa, mutta ilmoituksessa on huomioitava esitutkinnan merkitys ja sen käynnistämisen edellytykset. Esitutkinnan tarkoituksena on selvittää tapauksen tosiasiat: osapuolet, teko sekä näyttö yhtä lailla epäiltyä vastaan kuin epäillyn eduksikin. Tapahtuman lisäksi esitutkinnassa selvitetään epäillyllä rikoksella aiheutettu vahinko, epäillyn tekijän hankkima hyöty sekä tarvittaessa asianomistajan vahingonkorvausvaatimukset. Tämän vuoksi rikosilmoituksessa tulee olla vähintään lyhyt kuvaus tapahtumasta, asianomistajan yhteystiedot sekä tieto siitä, että asianomistaja vaatii rangaistusta.

Rikosilmoitukseen ei tarvitse liittää teknistä todistusaineistoa, vaan poliisi hankkii sen esitutkinnan yhteydessä. Asiantunteva ylläpito voi kerätä todistusaineistoa poliisia varten itsekin huomioiden kuitenkin sen, mitä todistusaineiston keruusta sanotaan kohdassa 6.2*. Todistusaineiston turvaaminen*.

Teknisen todistusaineiston lisäksi rikosprosessissa on hyötyä organisaation omasta tietoturvapoikkeaman selvittämisen dokumentoinnista. Dokumentointi helpottaa aineiston arviointia oikeudessa. Lisäksi tehtyjen toimenpiteiden määrän ja keston kirjaaminen auttaa tuomioistuinta myös mahdollisten vahingonkorvausten suuruusluokan arvioinnissa.

3.3.5. VIRT

Valtiovarainministeriön johtama VIRT-toiminta kehittää julkisen hallinnon vakavien tieto- ja kyberhäiriöiden operatiivista kyvykkyyttä. Toiminnan painopiste on etukäteissuunnittelu, varautuminen ja harjoittelu. Toiminnassa syntyvää tietoa jaetaan jäsenten verkostojen, koulutusten ja seminaarien kautta.

Laajoissa ja vakavissa häiriötilanteissa kutsutaan koolle VIRT-koordinointikokous. Kokoukseen kutsutaan ne nimetyt yhteyshenkilöt, joiden organisaatioihin tai vastuualueeseen häiriö vaikuttaa. Kokoukseen voidaan tarvittaessa kutsua palvelutuottajia ja muita häiriön ratkaisuun osallistuvia toimijoita. Kokouksen keskeisenä tehtävänä on muodostaa yhteinen tilannekuva ja varmistaa tiedonkulku eri toimijoiden kesken. VIRT-koordinointikokouksessa voidaan tarvittaessa sovittaa yhteen poikkihallin-

nollista häiriönhallintaa. Kokouksen koollekutsujana toimii usein Kyberturvallisuuskeskus. Myös muut viranomaiset voivat esittää koordinointikokouksen järjestämistä.

3.3.6. Valtiontalouden tarkastusvirasto

Valtiontalouden tarkastusvirastosta (VTV) annetun lain (676/2000) 16 §:n mukaan valtion viranomaisen, laitoksen, liikelaitoksen ja valtion rahaston on 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 on saatavana VTV:n www-sivuilta (http://www.vtv.fi).

3.3.7. Kansallinen turvallisuusviranomainen

Jos tietoturvapoikkeaman seurauksena on vaarantunut kansainvälistä turvallisuusluokiteltua tietoa, asiasta on välittömästi ilmoitettava kansalliselle turvallisuusviranomaiselle, jotta se voi ryhtyä tarvittaviin toimenpiteisiin (Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004).

3.3.8. EU:n tietosuoja-asetuksen valvova viranomainen

EU:n tietosuoja-asetusta valvova viranomainen on Suomessa tietoturvavaltuutettu. Rekisterinpitäjien tulee ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa tietoturvaloukkauksen ilmitulosta. Jos ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys viivästykselle. Ilmoitusta ei tarvitse tehdä, jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.

Ilmoituksessa on kuvattava henkilötietojen tietoturvaloukkaus mukaan lukien arviot henkilötietotyyppien ja asianomaisten lukumäärästä. Lisäksi on ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoja. On myös kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset sekä toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta. Tarvittaessa on määriteltävä myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi. Siirtymäaika tältä osin on 25.5.2018 saakka.

3.3.9. Viestintäsuunnitelman laatiminen

Poikkeamatilanteessa vaaditaan nopeaa reagointikykyä ja tehostettua viestintää. Poikkeamatilanteen viestintä tulee suunnitella etukäteen, jotta häiriötilanteessa voidaan keskittyä sen hallintaan, eikä aikaa tarvitse käyttää ylimääräisiin toimenpiteisiin. Viestintäsuunnitelma auttaa poikkeamatilanteessa linjaamaan, mitä viestitään, kuka viestii, miksi, kenelle ja milloin.

Osana tietoturvapoikkeamien hallintamallia on laadittava viestintäsuunnitelma, jossa otetaan kantaa sisäiseen ja ulkoiseen viestintään. Viestintäsuunnitelmassa on kerrottava, minkälaisten tietojen toimittaminen eri sidosryhmille on sallittua. Jos organisaatiolla on erillinen kriisiviestintäsuunnitelma, on tietoturvapoikkeamatilanteiden viestintäsuunnitelma syytä liittää siihen.

Viestintäsuunnitelman liitteenä tulee olla sekä sisäisten että ulkoisten sidosryhmien ajantasaiset yhteystiedot, koska ne eivät välttämättä ole saatavilla poikkeamatilanteessa. Viestintäsuunnitelma on poikkeamatilanteen varalta tallennettava myös paperimuodossa siten, että se on kaikkien tarvittavien osapuolten saatavilla. Viestintäsuunnitelman sijainti on oltava viestinnästä vastaavien tiedossa.

Käytettävät viestintäkanavat määräytyvät poikkeaman laajuuden, sen aiheuttamien vaikutusten, viestintätapojen käytettävyyden sekä viestinnän kohderyhmän perusteella. Organisaation on huomioitava viestintäsuunnitelmassa julkiseen tiedottamiseen ja viestintään käytettävät viestintäkanavat, kuten sosiaalinen media, TV, radio ja muut vastaavat mediat.

Esimerkki viestintäsuunnitelman rungosta on kuvattu liitteessä 5. Lisäohjeita viestinnän suunnitteluun on ohjeessa *Valtionhallinnon viestintä häiriötilanteissa ja poikkeusoloissa* (Valtioneuvoston kanslian määräykset, ohjeet ja suositukset 1/2013).

3.3.10. Viestintävastuut

Tietoturvapoikkeamatilanteeseen liittyvän viestinnän ja tiedottamisen kokonaisvastuun tulee pysyä yhdellä henkilöllä, joka nimetään heti viestintää vaativan poikkeamaselvityksen alussa. Kaikki poikkeamaa koskeva tietojen antaminen ja kysymyksiin vastaaminen on tiedottamista. Jos vastuita ei ole etukäteen selkeästi määritelty, viestintä voi poikkeamatilanteessa olla puutteellista tai ristiriitaista.

3.3.11. Sisäinen viestintä

Poikkeamatilanteessa on tiedotettava kaikkia niitä sisäisiä tahoja, joita tietoturvapoikkeama koskee, elleivät turvallisuussyyt muuta edellytä. Tiedottaminen on kuitenkin suunniteltava siten, etteivät siihen liittyvät velvollisuudet merkittävästi hidasta tietoturvapoikkeaman selvittämistä. Tietoja on voitava vaihtaa tietoturvapoikkeamien käsittelyryhmän sisällä mahdollisimman vapaasti tietoturvallisuuden ylläpitämiseksi.

3.3.12. Ulkoinen viestintä

Tietoturvapoikkeamatilanteissa tarvitaan toimivaa yhteistyötä ulkoisten sidosryhmien kanssa. Yhteistyösuhteet on luotava jo normaalitilanteessa, mikä on syytä ottaa huomioon viestintäsuunnitelmaa luotaessa. Jokaiselle sidosryhmälle on etukäteen hahmotettava oma roolinsa sekä tiedotuksen kohteena että poikkeaman osapuolena. Luetteloa sidosryhmien yhteystiedoista on pidettävä yllä ja omien yhteystietojen muutoksista on viipymättä tiedotettava sidosryhmille.

Viestintäsuunnitelmassa tulee varmistaa, että ulkoisesta viestinnästä huolehtiva henkilö tuntee asian ja tietää mistä puhuu. Poikkeamatilanteissa tulee mm. sopia seuraavista asioista:

- mistä asioista voidaan kertoa julkisuuteen ja mitä pitää esimerkiksi tutkinnallisista syistä jättää kertomatta
- kuka edustaa tarvittaessa organisaatiota TV:ssä ja muissa keskeisissä medioissa
- kuka kertoo ja millä tavalla poikkeamista sosiaalisessa mediassa.

Poikkeamista viestiminen on mahdollisuuksien mukaan hyvä suunnitella etukäteen. Viestintää voidaan suunnitella esimerkiksi kuvaamalla, mitä tietoja eri tilanteissa kerrotaan julkisuuteen ja mitä jätetään kertomatta.

3.4. Lokienhallinnan suunnittelu

Lokilla tarkoitetaan tietoa, joka dokumentoi tapahtumia organisaation toiminnassa, järjestelmissä, verkoissa ja muussa ympäristössä (VAHTI 03/2009). Lokeja käytetään tapahtumien dokumentointiin ja häiriö- tai väärinkäyttötilanteiden selvittämiseen. Lokien käsittelyllä voidaan edesauttaa poikkeamien selvittämistä ja niistä toipumista sekä tehostaa vaatimustenmukaisuuden todentamista, tietoturvallisuuden mittaamista ja henkilöstön oikeusturvaa.

Lokien käsittelyn tulee perustua ennalta määriteltyyn tarpeeseen ja kaiken lokien käsittelyn tulee tapahtua organisaatiossa sovittujen menettelytapojen mukaisesti. Lokien käsittelyssä tulee huomioida lokien koko elinkaari.

Lokien keräämisen tavoitteena on

- helpottaa häiriöiden ja virhetilanteiden havaitsemista ja selvittelyä,
- parantaa tietoturvallisuuden ja tietosuojan valvontaa varmistamalla tietojen käytön jäljitettävyys,
- parantaa yksilön suojaa varmistamalla tapahtumien kiistämättömyys,
- mahdollistaa väärinkäytösten havaitseminen ja selvittäminen ja
- ennaltaehkäistä osaltaan väärinkäytöksiä.

Organisaation tulee tehdä lokienhallintasuunnitelma, jossa kuvataan, mitä lokitietoja organisaatiossa kerätään ja miten tallennus teknisesti tehdään. On varmistettava poikkeamien havaitsemisen ja selvittämisen kannalta tarpeellisen lokitiedon riittävä saatavuus. Kaiken lokitiedon pitkäaikainen tallentaminen ei välttämättä ole järkevää. On arvioitava, millä tarkkuudella lokitiedot otetaan talteen, jotta tietoturvapoikkeaman vaiheet voidaan mahdollisimman kiistattomasti todeta. Lokitietoja on kerättävä vähintään palvelimista, verkko-, tietoturva- ja päätelaitteista, tietokannoista sekä verkkopalveluista ja muista sovelluksista.

Järjestelmän ylläpitäjän tulee pystyä tunnistamaan järjestelmän normaaliin toimintaan kuuluvat tapahtumat. Mitä nopeammin poikkeama havaitaan, sitä paremmin kyetään reagoimaan hallituilla toimenpiteillä ja poikkeamasta aiheutuvaa haittaa voidaan vähentää. Vertaamalla mahdollista häiriötilannetta normaalitilaan on mahdollista havaita väärinkäytökset. Järjestelmien tuottamia lokitietoja voidaan hyödyntää sekä tietoturvapoikkeaman havaitsemisessa että tutkimisessa.

3.4.1. Lokitietojen keräämisessä huomioitavat vaatimukset

Lokien keräämisessä on lainsäädännöllisiä rajoitteita, jotka on otettava huomioon lokienhallinnan suunnittelussa. Erityisesti huomioitavia lakeja ja asetuksia on listattu liitteessä 9.

Lokitiedot voivat sisältää esimerkiksi henkilötietoja, jolloin on huomioitava tietosuojalainsäädännön asettamat velvoitteet. Järjestelmien lokitiedot voivat sisältää myös sähköisen viestinnän sisältöä tai välitystietoja.

Viestinnän välitystiedoilla tarkoitetaan sellaista tietoa, jonka perusteella verkko- ja viestintäpalvelun käyttäjään voidaan yhdistää tietoa tai käyttäjä voidaan tunnistaa. Välitystietoja voivat olla muun muassa:

- tiedot puhelun soittajasta ja vastaanottajasta
- tiedot sähköposti- tai tekstiviestin lähettäjästä ja vastaanottajasta
- tiedot yhteyden kestosta, reitityksestä, ajankohdasta sekä siirretyn tiedon määrästä
- lähettäjän tai vastaanottajan päätelaitteen sijaintiin liittyvä tieto
- IP-osoite.

Viestinnän osapuoli voi käsitellä omia sähköisiä viestejään ja niihin liittyviä välitystietoja, jollei laissa toisin säädetä. Seuraavissa kappaleissa käsitellään tilanteita, joissa organisaatio ei ole viestinnän osapuoli, vaan käsittelee viestintää viestinnän välittäjän ominaisuudessa.

Tietoyhteiskuntakaaren 247 §:n mukaan viestinnän välittäjän on viestejä välittäessään huolehdittava palvelujensa, viestien, välitystietojen ja sijaintitietojen tietoturvasta. Viestinnän välittäjänä toimivan yhteisötilaajan on huolehdittava kuitenkin ainoastaan käyttäjiensä viestien, välitystietojen ja sijaintitietojen käsittelyn tietoturvasta. Tietoturvatoimenpiteet on suhteutettava uhan vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Tietoyhteiskuntakaaren 138 §:ssä säädetään, että sähköisiä viestejä ja välitystietoja voi käsitellä siinä määrin kuin se on tarpeen viestinnän välittämiseksi ja sovitun palvelun toteuttamiseksi sekä 272 §:ssä säädetyllä tavalla tietoturvasta huolehtimiseksi. Viestinnän välittäjällä on oikeus ryhtyä välttämättömiin toimiin tietoturvasta huolehtimiseksi. Nämä toimenpiteet on lueteltu tietoyhteiskuntakaaren 272 §:ssä. Sellaisia tietoja, jotka on tallennettu lokiin tietoturvasta huolehtimiseksi, ei voida käyttää muihin tarkoituksiin.

Jos lokia tai sitä tuottavaa teknistä järjestelmää on tarkoitus käyttää henkilöstön valvontaan esimerkiksi yrityssalaisuuksien suojaamiseksi tai väärinkäytöstapausten selvittämiseksi, lokin käytössä sovelletaan tietoyhteiskuntakaaren 18. luvun niin sanottuja Lex Nokia -pykäliä.

Yhteisötilaajalla on tietoyhteiskuntakaaren 147 §:n mukainen huolehtimisvelvollisuus, ja menettelystä on tiedotettava myös käyttäjille ennen välitystietojen käsittelyn aloittamista. Lisäksi työnantajan on järjestettävä yhteistoimintamenettely.

Esimerkiksi lain yhteistoiminnasta valtion virastoissa (1233/2013) 13 § mukaisesti yhteistoimintamenettelyssä on käsiteltävä virkamiehiin kohdistuva teknisin menetelmin toteutettava valvonta. Jos tietoturvapoikkeamien ennaltaehkäisemisen tai selvittämisen lisäksi lokitietoja on tarkoitus käyttää henkilöstön valvontaan, on valvontamenettely käytävä läpi yhteistoimintamenettelyssä ennen sen käyttöönottoa.

Välitystietojenkin käsittely on sallittua, jos viestinnän osapuoli antaa siihen suostumuksen. Suostumuksen pyytämisessä on kuitenkin otettava huomioon EU:n tietosuoja-asetus (tulee voimaan vuonna velvoittavana 25.5.2018 siirtymäkauden jälkeen), laki yksityisyyden suojasta työelämässä (759/2004) sekä mahdolliset muut henkilötietojen käsittelyn erityislait.

Jos viestintää käsitellään yksittäisen suostumuksen perusteella, on osapuolen suostumus syytä pyytää kirjallisena ja riittävän tarkkarajaisena. Jos suostumusta ei ole, välitystietoja saa käsitellä vain laissa säädetyillä perusteilla ja käsittelyn tarkoituksen vaatimassa laajuudessa. Käsittely ei saa rajoittaa luottamuksellisen viestinnän ja yksityisyyden suojaa enempää kuin on välttämätöntä.

3.4.2. Lokien tallentaminen ja käyttö tietoturvapoikkeaman selvittämisessä

Lokitiedot on tallennettava siten, että kenelläkään ei ole mahdollisuutta käsitellä tallennettuja tietoja luvatta. Jos lokitiedot on tallennettu vain järjestelmän omille palvelimille, järjestelmään murtautuja saattaa päästä muuttamaan tai poistamaan lokitietoja. Lokitiedot on varmuuskopioitava säännöllisesti riippumatta siitä, mihin ne on tallennettu.

Lokien turvallista tallennusta varten on olemassa lokienhallintajärjestelmiä, joihin tiedot voidaan keskitetysti tallentaa. Myös laajemmasta tietoturvatiedon käsittelyyn tarkoitetusta SIEM-ratkaisusta (*Security Information and Event Management*) on usein apua tietoturvapoikkeamien hallinnassa. Jotta tällaisesta järjestelmästä ja sen tuottamista raporteista ja reaaliaikaisista näkymistä olisi selkeää hyötyä, on järjestelmän käyttöönotto ja hyödyntäminen kuitenkin suunniteltava huolellisesti.

Tietoturvapoikkeamien tutkinnassa on olennaista, että lokitiedoissa ilmeneviin tapahtuma-ajankohtiin voi tutkintatilanteessa luottaa. Tästä syystä organisaation eri järjestelmien on käytettävä samaa luotettavaa aikalähdettä.

Lokitietoja on säilytettävä riittävän kauan, koska osa poikkeamista voi pahimmillaan paljastua vasta pitkän ajan, useiden vuosien kuluttua. Lokitietoja on syytä säilyttää vähintään kaksi vuotta, ellei lainsäädäntö, sopimukset tai muut velvoitteet aseta tiukempaa vaatimusta. Esimerkiksi potilastietojen käyttölokeja on säilytettävä 12 vuoden ajan (Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 298/2009). Tällaiset erityisvaatimukset on selvitettävä lokienhallintaa suunniteltaessa.

Tietoyhteiskuntakaaren 145§ mukaan viestinnän välittäjän on tallennettava yksityiskohtaiset tapahtumatiedot välitystietojen käsittelystä luottamuksellisuuden ja yksityisyyden suojan kannalta keskeisiä välitystietoja sisältävissä tietojärjestelmissä, jos se on mahdollista teknisesti ja ilman kohtuuttomia kustannuksia. Tapahtumatiedoista on käytävä ilmi käsittelyn ajankohta, kesto ja käsittelijä. Tapahtumatiedot on säilytettävä kaksi vuotta niiden tallentamisesta.

On muistettava, että organisaatiolla voi olla myös lakisääteisiä tai sopimuksiin perustuvia velvoitteita poistaa lokitietoja tietyn ajan kuluessa. Tarkempaa tietoa on VAHTI 3/2009 lokienhallintaohjeessa.

3.5. Tietoturvapoikkeamien huomioiminen sopimusmenettelyissä

Turvallisuusnäkökohtien ja vastuiden huomioiminen palvelusopimuksissa on tärkeää. Kaikkien osapuolten tulee tietää, kuinka poikkeamatilanteissa toimitaan. Poikkeamien havaitsemiseen, analysointiin ja käsittelyyn liittyvät velvollisuudet ja oikeudet on kirjattava sopimuksiin. Lisäksi on tärkeää määritellä palveluntarjoajan vastuut tietoturvapoikkeamien ilmoittamisesta asiakasorganisaatiolle. Sopimusmenettelyssä voi olla tarpeen täsmentää ja sovittaa yhteen lainsäädännöstä tai erilaisista sitoumuksista johtuvia velvoitteita. Määriteltyjen vaatimusten noudattamista on seurattava säännöllisin väliajoin palvelunseurantakokouksissa tai muulla tarkoituksenmukaisella tavalla.

Turvallisuussopimuksessa on tietoturvapoikkeamien hallinnan kannalta otettava huomioon vähintään seuraavat seikat:

- tietojen luottamuksellisuus ja salassapito
- turvallisuusselvitykset
- tietojen pääsy- ja käsittelyoikeudet
- tietoturvapoikkeaman käsittelyyn liittyvät toimintamallit
- palvelutaso; erityisesti reagointiajat ja ajankohdat, jolloin palvelua tarjotaan
- sopimusmuutosten tekeminen
- auditointikäytännöt
- raportointi-, ilmoitus- ja viestintävastuut lakisääteiset velvoitteet huomioiden
- tietoturvapoikkeamatietojen jakamisen perusteet ja toimintamalli.

Turvallisuussopimuksessa on syytä mainita, että mahdollisten tietoturvapoikkeamien käsittelyssä noudatetaan asiakkaan määrittelemää toimintatapaa, ellei muusta erikseen sovita. Monitoimittajaympäristössä on keskeistä sopia yhteistyömenettelyistä ja vastuista. Palveluntarjoajan on vahvistettava, että se pystyy toimimaan määritellyn mallin mukaisesti. Esimerkiksi pilvipalvelujen käytön yhteydessä tällaisia vaatimuksia ei kuitenkaan välttämättä pystytä esittämään, jolloin kaikkea tietoturvapoikkeamatilanteissa tarvittavaa apua ja tietoa (esim. lokitiedot) ei ole mahdollista saada. Myös viranomaiskäytännöissä on tietoturvapoikkeamien tutkinnassa eroja eri maiden kesken. Jos turvallisuuskäytännöissä on puutteita, on harkittava, voidaanko palveluntarjoajan kanssa tehdä sopimusta lainkaan vai voidaanko tarjottu turvallisuutaso hyväksyä.

Valtionhallinnon tietoturvallisuussopimusmalli on osa VAHTI-ohjeistoa ja sitä voidaan käyttää soveltuvin osin apuna sopimusten laadinnassa. Tuorein malli löytyy www.vahtiohje.fi –sivustolta.

3.6. Harjoittelu

Poikkeamatilanneharjoituksilla testataan ja kehitetään organisaation valmiuksia selviytyä siihen kohdistuvista poikkeamatilanteista mahdollisimman vähin vaurioin ja pienin kustannuksin. Onnistuneen harjoituksen edellytyksenä on, että tietoturvapoikkeamien käsittely on organisoitu ja ohjeistettu.

Poikkeamatilanteita on tärkeää harjoitella säännöllisin väliajoin, vähintään vuosittain. Tietoturvapoikkeamien hallintamallia ja -ohjeistusta on päivitettävä harjoituksissa mahdollisesti havaittujen puutteiden pohjalta. Vaikka kaikenlaisiin poikkeamatilanteisiin on hyvä varautua, harjoittelussa on useimmiten kannattavaa keskittyä todennäköisimmiksi arvioituihin poikkeamiin.

4. TIETOTURVAPOIKKEAMAN HAVAITSEMINEN JA ANALYSOINTI

Organisaation tulee varautua poikkeamien havaitsemiseen ja poikkeamatilanteiden hallintaan. Organisaation on tiedettävä esimerkiksi salassa pidettävien tietoja hallussaan pitävät yhteistyötahot, tietojen sijainti ja käyttötavat. Organisaation on tunnettava verkkojen ja järjestelmien normaalitoiminta sekä tietojen ja tietokantojen normaali sisältö ja käyttötavat. Järjestelmien toimintaa seurataan automaattisesti ja manuaalisesti poikkeamatilanteiden havaitsemiseksi. Lisäksi käyttäjät tulee ohjeistaa ilmoittamaan epäilyttävistä tai normaalista poikkeavista tapahtumista.

4.1. Tietoturvapoikkeaman havaitseminen

Ensimmäisen havainnon tietoturvapoikkeamasta voi tehdä kuka tahansa, esimerkiksi viraston työntekijä, yhteistyökumppani, tietojärjestelmän ylläpitäjä tai täysin ulkopuolinen henkilö, kuten verkkopalvelun käyttäjä. Koska havainto voi tulla ulkopuoliseltakin taholta, on luotava menettelyt, joilla sekä sisäiset että ulkopuoliset tahot voivat ilmoittaa organisaatioon kohdistuvasta tietoturvaongelmasta. Malli tietoturvapoikkeaman ilmoituslomakkeesta on esitetty liitteessä 7.

Järjestelmissä voi ilmetä päivittäin suurikin määrä mm. tietoturvaohjelmistojen, lokitietojen ja palvelupyyntöjen perusteella havaittuja merkkejä poikkeamista. Havainnot on analysoitava, jotta poikkeamiin voidaan reagoida asianmukaisesti. Sekä automaattisen että manuaalisen analysoinnin perusteet, välineet ja toimintatavat on kirjattava tietoturvapoikkeamien hallintamalliin.

Poikkeamatiedon lähteitä voivat olla esimerkiksi

- järjestelmälokit (esim. keskitetty lokienhallintajärjestelmä tai SIEM)
- hyökkäyksen havainnointi- ja estojärjestelmät (IDS/IPS)
- tietoverkon aktiivilaitteet (mm. kytkimet, reitittimet ja palomuurit)
- haittaohjelmien ja roskapostin suodatusjärjestelmät
- päätelaitteet (työasema, mobiililaite)
- palvelutoimittajan tai tietoliikenneoperaattorin järjestelmä
- ulkopuoliselta taholta hankittavat seuranta- tai valvontapalvelut
- muiden organisaatioiden tietoturvayksiköt (esimerkiksi Viestintäviraston GovCert-palvelu)

- rikosilmoitin-, kulunvalvonta- ja kameravalvontajärjestelmät
- yleisesti saatavilla olevat tietolähteet, kuten julkiset haavoittuvuustiedotteet
- Valtorin tietoturvapoikkeamien valvomo (SSOC, Security and Service Operations Center)
- valtionhallinnon tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä GovHAVARO
- käyttäjien ja asiakkaiden palvelupyynnöt ja yhteydenotot.

Kaikki epäilyt tietoturvapoikkeamista on otettava vakavasti ja analysoitava. Tietoturvapoikkeamien / hyökkäyksen havaitsemisessa tärkeää on yhteistyö sisäisten ja ulkoisten sidosryhmien välillä. Eri lähteistä tulevien havaintojen yhdistäminen on tärkeää, koska eri tahojen havainnot samasta poikkeamasta voivat täydentää toisiaan. Esimerkiksi haittaohjelmahyökkäys saattaa näkyä käyttäjän koneen hidasteluna, kaatuiluna tai satunnaisena verkkoliikenteenä. Palveluntarjoaja tai Viestintävirasto on kuitenkin saattanut tunnistaa verkosta lähetetyn ylimääräisen liikenteen haittaohjelmaksi ennen kuin haittaohjelman kohteena olevassa organisaatiossa on havaittu minkäänlaista poikkeamaa.

Organisaatiossa tulee ohjeistaa ja kannustaa henkilöstöä ilmoittamaan havaitsemistaan tietoturvapoikkeamista.

4.2. Poikkeaman tietojen kerääminen

Organisaation tulee tunnistaa tiedot, jotka jokaisesta poikkeamasta on kerättävä. Tietoja tarvitaan poikkeaman analysointiin ja selvittämiseen tai mahdollisten raportointivaatimusten täyttämiseen. Poikkeamalle on heti havaintovaiheessa syytä antaa yksilöivä tunniste (esimerkiksi juokseva numero) helpottamaan poikkeamien käsittelyä, raportointia ja linkittämistä toisiinsa.

Poikkeamatiedon kokoamiseen ja analysointiin osallistuvat henkilöt on perehdytettävä aineiston keräämiseen ja tallettamiseen liittyviin ohjeisiin ja lainsäädäntöön. Kerättävää tietoa saatetaan tarvita selvitystyön ja raportoinnin lisäksi juridisiin tai kurinpidollisiin tarkoituksiin.

Listaus poikkeamasta kerättävistä vähimmäistiedoista on esitetty liitteessä 4 *(Tietoturvapoikkeamasta kerättävät tiedot).*

4.3. Poikkeaman analysointi

Tietoturvapoikkeama on analysoitava viipymättä. Analyysivaiheessa on tärkeää huomioida kaikki havainnot ja ongelmaraportit. Vasta kun on täysin varmaa, ettei jokin havainto liity mahdolliseen tietoturvapoikkeamaan, se voidaan jättää selvityksen ulkopuolelle.

Alustava poikkeaman vakavuuden arviointi on usein tehtävä puutteellisten tai osittain jopa virheellistenkin tietojen perusteella. Poikkeaman luokittelu voi muuttua tietojen tarkentuessa. Poikkeama on analysoinnin perusteella luokiteltava esimerkiksi alla olevassa taulukossa kuvatulla tavalla.

Taulukko 4. Poikkeaman vakavuusasteen luokittelu

Vakavuusaste	Kuvaus
Vähäinen	Poikkeaman vaikutus organisaation toimintaan on vähäinen. Vähäisten tietoturvapoikkeamien hoitaminen on osa organisaation normaalia toimintaa. Poikkeamasta voi harkinnan mukaan ilmoittaa Viestintäviraston Kyberturvallisuuskeskukseen.

Vakava	Poikkeamalla on merkittävä vaikutus organisaation toimintaan ja tietoturvapoikkeamien käsittelyryhmä kutsutaan koolle. Poikkeamasta tehdään ilmoitus Viestintäviraston Kyberturvallisuuskeskukseen.
Kriisitilanne	Kyseessä on laaja-alainen tai organisaatiorajat ylittävä poikkeama. Organisaation sisäiset kriisinhallintatoimenpiteet käynnistetään ja poikkeamasta tehdään ilmoitus Viestintäviraston Kyberturvallisuuskeskukseen. Kyberturvallisuuskeskus ja kohdeorganisaatiot arvioivat, kutsutaanko koolle VIRT-koordinointikokous. Myös toimivaltainen viranomainen voi kutsua VIRT-kokouksen koolle.

Analysoinnin alkuvaiheessa arvioidaan poikkeaman tyyppi ja syyt. Analysoinnissa tärkeimpiä tekijöitä ovat:

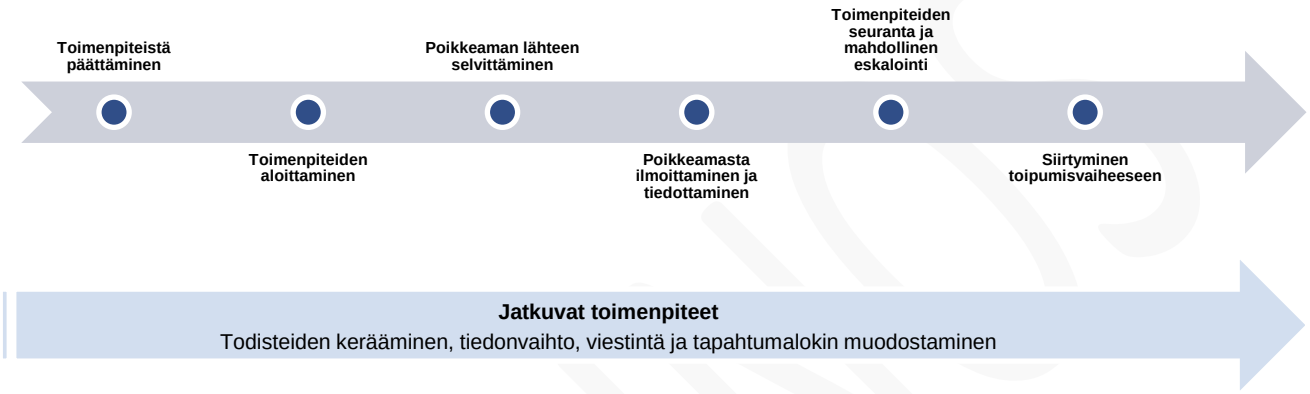
- poikkeaman nykyinen ja potentiaalinen vaikutus järjestelmiin ja muuhun tietojenkäsittelyympäristöön
- poikkeaman mahdolliset seurannaisvaikutukset organisaation toimintaan
- poikkeaman ja siihen reagoimisen taloudelliset seuraukset
- poikkeaman vaikutus organisaation julkisuuskuvaan sekä sidosryhmiin sekä
- uhattuna olevien tietojen merkitys organisaatiolle ja sidosryhmille.

Tietoturvapoikkeamaa tulee verrata muihin tapahtumiin tai poikkeamiin, joita tietoturvapoikkeamien käsittelyryhmälle tai tukipalveluille on raportoitu. Näin voidaan selvittää, onko kyseisellä poikkeamalla yhteyttä muihin poikkeamiin, vai onko se yksittäinen tapahtuma. Kaikki poikkeamatieto ei välttämättä ole käsittelyryhmän käytössä analysointivaiheessa. Nopea reagointi voi kuitenkin osoittautua jopa tärkeämmäksi kuin kattavien tietojen kerääminen ja pitkään kestävä analysointi. Useista eri lähteistä kerätyissä tiedoissa saattaa olla ristiriitoja, jolloin on päätettävä, mihin tietolähteisiin voidaan eniten luottaa. Edellä mainittujen tietojen perusteella käsittelyryhmä päättää, jatketaanko poikkeaman tutkintaa välittömästi, siirretäänkö tutkinta myöhempään ajankohtaan vai lopetetaanko tutkinta.

Poikkeamailmoituksen tekijälle on syytä kertoa, miten ilmoitukseen on reagoitu. Vaikka ilmoitus ei johtaisi tarkempiin tutkimuksiin, on yleisen tietoturvatietoisuuden lisäämiseksi hyödyllistä kertoa ilmoittajalle tehtyyn päätökseen vaikuttaneet seikat.

5. TIETOTURVAPOIKKEAMAAN REAGOINTI

Tietoturvapoikkeamiin on reagoitava nopeasti, jotta poikkeaman negatiiviset vaikutukset organisaatioon voidaan minimoida. Tietoturvapoikkeamaan reagoimisen päävaiheet on esitetty alla olevassa kuvassa.



Kuvio 3. Tietoturvapoikkeamaan reagoiminen

Reagointivaiheessa poikkeamankäsittelyryhmä laajennetaan tarvittaessa poikkeaman vakavuuden perusteella kriisinhallintaryhmäksi. Kriisinhallintaryhmän oikealla kokoonpanolla varmistetaan ryhmän päätöksentekokyky ja -valtuudet. Tämä edellyttää organisaation johdon sitouttamista ryhmän toimintaan.

Poikkeamankäsittelyryhmän pitää varmistaa, että kaikki poikkeamaan liittyvät toimenpiteet ja tapahtumat kirjataan. Tapahtumapäiväkirja on hyvä rakentaa sähköiseksi palveluksi, jolloin siihen täytetyt tiedot ovat välittömästi tarvittavien osapuolten saatavilla. Myös manuaalinen varajärjestely on suunniteltava.

Todistusaineisto on kerättävä ja säilytettävä turvallisesti ja sitä tulee valvoa siltä varalta, että aineistoa tarvitaan jälkiselvitykseen. Samalla on varmistettava, että poikkeamatietoa vaihdetaan riittävästi ulkoisten ja sisäisten sidosryhmien kanssa. On myös huolehdittava viestinnästä käyttäjille ja asiakkaille.

5.1. Tietoturvapoikkeaman käsittely

Tietoturvapoikkeamien käsittelyryhmän on päätettävä, miten todettuun poikkeamaan reagoidaan ja varmistaa, että käsittelyryhmän kokoonpano on tarkoituksenmukainen poikkeamakäsittelyn jokaisessa vaiheessa. Ryhmän on käynnistettävä toimet poikkeaman laajenemisen estämiseksi, siitä toipumiseksi ja viestimiseksi käytettävissä olevien tietojen perusteella. Reagoinnissa päätettäviä asioita ovat mm. välittömät toimenpiteet, kuten järjestelmien sulkeminen verkosta, jatkuvuussuunnitelmien käyttöönotto ja reagointiin vaadittavien resurssien käyttö.

5.1.1. Eristämiskeinoista päättäminen

Vakavissa tietoturvapoikkeamissa tiedon luottamuksellisuus tai eheys on saattanut vaarantua ennen poikkeaman havaitsemista. Todistusaineiston turvaaminen on huomioitava, kun päätetään eristämistaktiikasta (ks. keräystavasta tarkemmin kohdasta *6.2. Todistusaineiston turvaaminen*).

Toimenpiteissä pitää huomioida sekä palvelun kriittisyys, poikkeaman vakavuus että järjestelmässä käsiteltävien tietojen suojaustaso. Tilanteen niin vaatiessa tietojärjestelmiä tai -verkkoja voidaan eristää muusta ympäristöstä ennaltaehkäisevän segmentoinnin lisäksi. Esimerkiksi normaalisti luvallista liikennettä on mahdollista väliaikaisesti rajoittaa haittaohjelmaepidemian aikana.

Eristämiseen vaikuttavia kriteereitä ovat mm.:

- mahdollinen resursseihin tai tietoon kohdistunut vahinko tai varkaus
- tietoihin / tietojärjestelmiin kohdistuvat välittömät uhat
- poikkeaman kohteena olevien järjestelmien käytettävyystarve
- poikkeaman leviämisuhka muihin järjestelmiin, palveluihin ja organisaatioihin
- tarve säilyttää todistusaineistoa
- eristämistoimenpiteiden toteuttamiseksi tarvittava aika ja resurssit sekä
- eristämisratkaisun vaikutuksen kesto.

Palvelun käytön estämistä on kuitenkin harkittava esimerkiksi katkaisemalla verkkoliikenne, jos on todennäköisiä syitä epäillä, että salassa pidettäviä tietoja vaarantuu käytön jatkuessa.

5.1.2. Poikkeaman lähteen selvittäminen

Poikkeaman lähteen selvittäminen on hyödyksi, jotta korjaustoimenpiteet voidaan kohdistaa oikein ja tarvittaessa ryhtyä hallinnollisiin toimenpiteisiin esimerkiksi päivittämällä puutteellinen toimenpideohje. Mikäli selviää tai epäillään, että kyseessä on rikos, poikkeaman lähteen selvittäminen on poliisin tehtävä. Tarvittaessa lähteestä on hyvä kertoa sidosryhmille ja Viestintäviraston Kyberturvallisuuskeskukselle, jotta vastaava poikkeama voidaan ennaltaehkäistä muualla hallinnossa.

5.1.3. Tapahtumapäiväkirjan pitäminen

Tietoturvapoikkeamien käsittelyssä tehtävät havainnot, päätökset ja toimenpiteet on kirjattava tapahtumapäiväkirjaan samalla, kun niitä tehdään. Tapahtumapäiväkirjaa on pidettävä poikkeaman havaitsemisesta lähtien. Malli tapahtumapäiväkirjasta on kuvattu liitteessä 8.

Tapahtumapäiväkirjasta pitää käydä ilmi vähintään seuraavat asiat:

- kirjaaja
- kirjauksen ajankohta
- tehdyt toimenpiteet
- yhteystiedot
- lista tilanteen aikana kerätystä todistusaineistosta
- tilannetta hoitaneiden henkilöiden kommentit
- yhteydenpito eri tahoihin.

Jokainen henkilö kirjaa tai ilmoittaa kirjaajalle tekemänsä toimenpiteet. Käsittelyryhmän vetäjä vastaa tietoturvapoikkeaman selvitystyön dokumentoinnista kokonaisuutena.

Kaikki havainnot, analyysit ja niiden pohjalta tehdyt johtopäätökset on käytävä läpi koko tietoturvapoikkeaman käsittelyryhmän kesken sovituin väliajoin (esim. päivittäin tai muutaman tunnin välein) tilanteen vakavuudesta riippuen.

5.1.4. Esimerkkejä erilaisista poikkeamatilanteista

Kaikkiin tietoturvapoikkeamiin varautuminen on käytännössä vaikeaa. Tässä luvussa on kuvattu tyypillisimpiä poikkeamatilanteita sekä ohjeita niiden havaitsemiseen ja korjaamiseen. Erilaisista tietoturvapoikkeamatilanteista on syytä tehdä lyhyitä ohjeita, joiden avulla organisaation on mahdollista reagoida poikkeamaan etukäteen sovitulla tavalla. Esimerkkejä poikkeamien hallintaohjeista on esitetty tämän ohjeen liitteissä.

5.1.4.1 Epäilyttävää tiedonsiirtoa ulkopuoliseen kohteeseen

Organisaatiolla on oltava kyvykkyys havaita epäilyttävä tietoliikenne tietoverkossaan esimerkiksi tunnettuihin haitallisiin tai toiminnan kannalta epätyypillisiin kohteisiin. Havaitsemiseen on syytä käyttää automaattista tietoliikenteen seurantajärjestelmää, joka kykenee analysoimaan verkkoliikennettä ja tekemään hälytyksiä epäilyttävästä liikenteestä. Automaattisen hälytyksen vakavuus on selvitettävä ja tarvittaessa käynnistettävä poikkeaman käsittelymenettely. Automaattisen seurantajärjestelmän käyttäminen ei poista osaavan ylläpitohenkilöstön tarvetta, sillä usein automatiikka ei kykene epäselvien tilanteiden tulkitsemiseen.

Kun organisaation palvelutoimittaja tai poikkeaman käsittelyryhmä on havainnut epäilyttävää tiedonsiirtoa, sen on

- otettava kopiot selvittämisen kannalta tärkeistä tiedoista poikkeamatutkintaa varten,
- pyydettävä verkon ylläpitäjää estämään liikenne havaittuun epäilyttävään ulkopuoliseen kohteeseen (jos on tehty päätös, että ei pyritä salaamaan hyökkääjältä sen havaitsemista),
- pyrittävä selvittämään, mihin tietoihin on päästy käsiksi ja mitä tietoa on siirretty,
- tutkittava, miten hyökkääjä on päässyt tunkeutumaan verkkoon ja saanut pääsyn tietoihin,
- poistettava hyökkäyksen mahdollistavat haavoittuvuudet järjestelmästä ja
- suunniteltava kehitystoimenpiteet vastaavan tilanteen välttämiseksi.

5.1.4.2 Palvelunestohyökkäys

Palvelunestohyökkäyksen havaitsemisen jälkeen on selvitettävä, kuinka monesta lähteestä hyökkäys on peräisin ja onko organisaation sisäverkossa liikenteen lähteitä. Lisäksi on syytä kartoittaa, mitä tietoliikenneprotokollaa hyökkäyksessä hyödynnetään. Tiedot selviävät organisaation omista verkkolaitteista tai palvelutoimittajan verkkolokeista.

Tehokas tapa vähentää palvelunestohyökkäyksestä koituvia vahinkoja on suodattaa haittaliikennettä tietoliikenneoperaattorin runkoverkossa. Tähän liittyvät menettelytavat on kuitenkin sovittava etukäteen, sillä poikkeamatilanteessa suodatuksen järjestäminen on hyvin hankalaa ja hidasta. Jos tietoliikenneoperaattorin suodatuspalveluita ei ole käytettävissä, palvelunestohyökkäystä voi yrittää torjua myös organisaation omilla verkkolaitteilla. Tällöin ongelmaksi saattaa kuitenkin muodostua se, että laajamittainen hyökkäys tukkii koko verkkokaistan. Organisaation omista suodatuslaitteista ei ole merkittävää apua, koska suuri osa hyödyllisestäkään liikenteestä ei pääse suodatuslaitteistoon asti.

Jos on syytä epäillä, että palvelunestohyökkäykseen käytetään organisaation omassa verkossa olevia työasemia tai palvelimia, ne tulee paikallistaa ja eristää. Palvelunestohyökkäykseen osallistuva laite on irrotettava fyysisesti tai loogisesti verkosta. Lisäksi on varauduttava tutkimaan laite perusteellisesti,

sillä se on todennäköisesti joko murrettu tai haittaohjelman saastuttama. Myös laitteen haltija voi olla aiheuttanut tarkoituksellisesti tai vahingossa palvelunestohyökkäyksen.

5.1.4.3 Järjestelmässä on tunkeutuja

Järjestelmässä havaittu tunkeilija voi olla seurausta tietomurrosta tai haittaohjelmasta. Yksittäisen käyttöoikeuden tai käyttäjätunnuksen väärinkäyttöön rajoittuvan rikkeen tutkinnasta ei välttämättä aiheudu käyttökatkoja palveluihin, ja organisaatio voi pyrkiä selvittämään tapauksen tietojärjestelmän omin työkaluin.

Luvatonta käyttöä epäiltäessä ensisijainen toimintamalli on, että tietojärjestelmän käyttö on estettävä tarvittavilta osin vähintään aktiivisen selvitystyön ajaksi. Järjestelmää ei saa sammuttaa eikä prosesseja keskeyttää ilman erillistä päätöstä. Vaihtoehtoisesti käyttöoikeus voidaan jättää tällaisessa tapauksessa auki siksi aikaa, kun oikeudetonta käyttöä seurataan aktiivisesti. Samalla käyttö tallennetaan lokiin todistusaineistoksi. Tällöin on varmistettava, ettei väärinkäytön seuranta vaaranna muiden järjestelmien tietoturvallisuutta.

Väärinkäytön seuraaminen on poikkeuksellinen toimintamalli, jota on käytettävä äärimmäisen harkiten ja tiiviissä yhteistyössä viranomaisten kanssa. Toimenpide vaatii ylläpitohenkilöstöltä korkeaa ammattitaitoa ja riittäviä resursseja kohdejärjestelmän jatkuvaan seurantaan. Organisaation ei pidä valita tätä toimintamallia ilman viranomaisen kehotusta.

Jos järjestelmään on murtauduttu, mihinkään järjestelmässä olevaan tietoon ei voida enää varmuudella luottaa. Järjestelmä on irrotettava verkosta, mutta jätettävä se pääsääntöisesti päälle, jotta arvokasta tietoa ei menetetä esimerkiksi tunkeutujan prosessien varaamista resursseista. Lisäksi on otettava kopio järjestelmän sisältämistä tiedoista tietoturvatutkimuksiin erikoistuneiden asiantuntijoiden avulla. Muut hyökkääjän mahdolliset kohteet on pyrittävä selvittämään järjestelmien lokitietojen, verkkoliikenteen tai muiden vastaavien tietojen perusteella. Samalla on käynnistettävä torjuntatoimenpiteet ja tiedotettava nopeasti mahdollisia kolmansia osapuolia, joko suoraan tai viranomaisten välityksellä. Torjuntatoimenpiteiden yhteydessä on kerättävä todistusaineistoa ennalta määriteltyjen menettelyjen mukaisesti (ks. luku 5.2.Todistusaineiston turvaaminen).

5.1.4.4 Oman henkilökunnan tekemät tietoturvaloukkaukset

Jos organisaatio epäilee omaan henkilökuntaansa kuuluvaa henkilöä tietoturvaloukkauksesta, tilanteen selvittämiseen on sovellettava mm. kansallisia ja kansainvälisiä henkilötietojen käsittelysäännöksiä, lakia yksityisyyden suojasta työelämässä (759/2004) sekä tietoyhteiskuntakaarta (917/2014). Erityisesti huomioitavia seikkoja ovat mm. työntekijän sähköpostien esille hakemisen ja avaamisen rajoitukset sekä muiden viestinvälitystietojen käsittelyn rajoitteet.

Tietojen käsittely väärinkäytösten selvittämiseksi tulee jo etukäteen käsitellä yhteistoimintamenettelyssä. Tietoturvaloukkauksen selvittämisen aikana on tarkoin varmistettava, ettei eri osapuolten oikeusturvaa vaaranneta. Epäselvissä tilanteissa on otettava yhteyttä viranomaisiin ennen toimenpiteitä.

Kun tietoturvapoikkeaman aiheuttaja kuuluu organisaation omaan henkilökuntaan, seuraamukset ovat sisäisten sääntöjen ja asiaa koskevien lakien mukaiset. Organisaation omissa säännöissä teot on syytä luokitella rikkomuksen vakavuuden ja teon tahallisuuden mukaan. Lievimmissä tapauksissa riittää huomautus asiattomasta toiminnasta, mutta vakavimmat tapaukset voivat johtaa irtisanomiseen ja vahingonkorvauksiin. Korvausvastuut koskevat sekä väärinkäytöksen kohteena olleita resursseja että selvitystyöstä aiheutuneita kustannuksia.

Tavallinen oman henkilökunnan aiheuttama tietoturvapoikkeama on tiedon joutuminen vääriin käsiin. Esimerkiksi kannettavan tietokoneen katoaminen tai varastaminen saattaa johtaa tietojen menettämiseen, ellei organisaatio ole huomioinut tiedon käsittelyperiaatteita riittävällä tarkkuudella. Organisaation on varauduttava tällaisiin tilanteisiin mm. ohjeistamalla tiedon tallentaminen sen luottamuksellisuuden edellyttämällä tavalla, salaamalla päätelaitteissa oleva tieto ja suojaamalla laitteet vahvoilla salasanoilla tai muulla vastaavalla menetelmällä. Jos merkittävää tai arkaluonteista tietoa sisältävä laite menetetään, se on myös mahdollisuuksien mukaan hallitusti etätyhjennettävä.

Tietoa saattaa joutua vääriin käsiin myös muilla tavoin. Työntekijät saattavat esimerkiksi keskustella organisaation asioista julkisella paikalla. Tällaisia riskejä vastaan on mahdollista suojautua käytännössä vain kouluttamalla henkilöstöä noudattamaan tietoturvakäytäntöjä. Salassa pidettävän tiedon suojaaminen pitää huomioida osana tilaratkaisuja.

5.1.4.5 Haittaohjelmatilanteet

Haittaohjelmat havaitaan usein haittaohjelmien torjuntaohjelman antaman hälytyksen perusteella. Organisaation sisäinen käyttäjä ottaa yleensä yhteyttä tukipalveluun, kun työskentely koneella hidastuu tai häiriintyy haittaohjelman takia. Haittaohjelmailmoituksia saatetaan vastaanottaa myös ulkopuoliselta taholta, jos haittaohjelman saastuttama kone lähettää verkkoon haitallista liikennettä, kuten roskapostia.

Tietojärjestelmien hallinnasta ja valvonnasta tulee sopia kirjallisesti järjestelmien omistajien ja järjestelmiä valvovan ja hallinnoivan organisaation kesken. Organisaation ja palvelutuottajien on toimittava haittaohjelmien torjunnassa sovitun toimintatavan mukaisesti.

Jos yksi laite havaitaan saastuneeksi, on organisaation tutkittava muidenkin laitteiden mahdollinen saastuminen. Laitteen tai ohjelmiston omistajan tai ylläpitäjän on yhteistyössä tietoturvapoikkeaman käsittelyryhmän kanssa kartoitettava, miten laajasta tartunnasta on kyse. Jos haittaohjelma aiheuttaa runsaasti liikennettä, voidaan vahinkoa pyrkiä vähentämään esimerkiksi rajoittamalla tietoliikennettä tiettyihin portteihin tai palveluihin. Myös sähköpostiliikennettä on mahdollista suodattaa automaattisilla välineillä, jos haittaohjelman leviämistapa on tiedossa.

Kun on selvillä mistä haittaohjelmasta on kyse, IT-palvelutoimittaja voi hyödyntää haittaohjelmien torjuntaohjelmistojen valmistajien kohdennettuja työkaluja. Kun saastunut järjestelmä on puhdistettu joko apuohjelmilla tai asentamalla järjestelmä uudelleen, on tiedossa olevat haavoittuvuudet paikattava myös muualla. Vasta tämän jälkeen järjestelmän voi liittää takaisin verkkoon. Järjestelmän kriittisyys ja organisaation tietoturvapolitiikka määrittelevät, onko järjestelmä asennettava kokonaan uudelleen tai palautettava puhtaiksi todetuista varmuuskopioista.

Kiristyshaittaohjelmat (ransomware) saattavat aiheuttaa organisaatiolle vakavia seurauksia, sillä ne salaavat tietoja mm. verkkolevyiltä, palvelimilta ja työasemilta. Kiristyshaittaohjelmia vastaan voi suojautua rajaamalla käyttäjien käyttöoikeuksia, pitämällä virustorjunnan ajan tasalla sekä huolehtimalla varmuuskopioiden ajantasaisuudesta ja palautusjärjestelyjen säännöllisestä testaamisesta.

5.1.4.6 Kohdistetut hyökkäykset

Kohdistetuista hyökkäyksistä käytetään termiä APT (*Advanced Persistent Threat*). Hyökkäys pyritään tavallisesti levittämään vain rajatulle joukolle ihmisiä tai organisaatioita, jotta hyökkäys ei paljastuisi helposti. Hyökkäys kohdistuu ensisijaisesti verkkoon, johon pyritään saamaan pysyvä pääsy tiedon hankkimiseksi. Hyökkääjä valitsee kohteensa huolellisesti ja hankkii hyökkäystä varten tietoja kohteena olevasta organisaatiosta tai siellä toimivista henkilöistä.

Melko edistyneitäkin haittaohjelmia on mahdollista havaita esimerkiksi analysoimalla verkkoliikennettä. Kohdistettujen hyökkäysten haittaohjelmat ovat kuitenkin tiettyyn tarkoitukseen yksilöllisesti laadittuja ja niiden suunnittelussa on kiinnitetty erityistä huomiota siihen, että ne olisivat mahdollisimman vaikeasti havaittavissa ja tutkittavissa. Esimerkiksi verkkoliikenne pyritään naamioimaan normaaliksi verkkoliikenteeksi. Näin ollen haittaohjelmien torjuntaohjelmistot eivät yleensä tunnista niitä. APT-hyökkäystä epäiltäessä on välittömästi otettava yhteyttä Viestintäviraston kyberturvallisuuskeskukseen tarkempien ohjeiden saamiseksi.

5.1.4.7 Tietojen kalastelu (phishing)

Tärkein suojauskeino tietojenkalasteluyrityksiin on käyttäjien tietoturvakoulutus. Tiedot, joita useimmiten yritetään viedä, ovat käyttäjätunnuksia ja salasanoja, mutta hyökkääjä saattaa olla kiinnostunut myös muista tiedoista. Kun organisaation henkilöstö on tietoinen tietojenkalastelun mahdollisuudesta ja menetelmistä, kalasteluyrityksen onnistumisen todennäköisyys pysyy pienenä. Henkilöstölle on myös tiedotettava, mihin havaituista tietojenkalasteluyrityksistä pitää ilmoittaa.

Rikolliset saattavat yrittää hankkia arkaluonteisia tietoja haittaohjelmien tai väärennettyjen verkkosivujen avulla, mutta tietojenkalastelua voidaan yrittää myös muilla tavoin, kuten sähköpostitse tai puhelimitse. Yleisimpiä tietojenkalasteluyrityksiä on mahdollista torjua mm. roskapostisuodattimilla, mutta kohdennettujen viestien tapauksessa suodatinten teho on melko heikko.

On varsin yleistä, että organisaatioiden nimissä lähetetään huijaus- ja tietojenkalasteluviestejä. Tällaisia viestejä vastaan voi yrittää suojautua määrittelemällä organisaation verkkotunnukseen sallittuja sähköpostin lähettäjän IP-osoitteita. Teknisten suojauskeinojen teho on kuitenkin melko rajallinen, joten tietojenkalastelu-uhasta on tiedotettava aktiivisesti sekä sisäisille että ulkoisille käyttäjille.

5.1.4.8 Pääsynhallinnan kriittinen poikkeama

Organisaatio saa tiedon omalta henkilöstöltään, huomaa omassa valvonnassaan tai saa tiedon ulkopuolelta (esim. Viestintäviraston Kyberturvallisuuskeskus, media tai muu toimija), että sen järjestelmiin voi kirjautua oikeudetta tai päästä käsiksi tietoihin, joihin ei ole oikeutta (esim. kansalainen / yritys pääsee toisen tietoihin tai palomuuri sallii pääsyn organisaation sisäisiin palveluihin Internetistä).

5.1.4.9 Sensitiivisen tiedon laajamittainen väärä käsittely

Organisaatio saa tiedon omalta henkilöstöltään, huomaa omassa valvonnassaan tai saa tiedon ulkopuolelta (esim. Viestintäviraston Kyberturvallisuuskeskus, media tai muu toimija), että sen vastuulla olevia sensitiivisiä tietoja (kuten henkilötiedot, yritysten tiedot, turvaluokitellut tiedot) on käsitelty laajamittaisesti lainvastaisesti tai huolimattomasti niin, että niiden luottamuksellisuus on vaarantunut.

5.2. Todistusaineiston turvaaminen

Tietoturvapoikkeamien käsittelyn yksi tavoite on todistusaineiston turvaaminen mahdollisen rikoksen, väärinkäytöksen tai muun tapahtuman selvittämiseksi.

Tietoturvapoikkeaman todistusaineistoa on kaikki tieto, josta on apua tapahtuman selvittämisessä. Todistusaineistoa ovat esimerkiksi:

- tietoliikenneyhteyksiin liittyvät lokitiedot
- tietojärjestelmien ja -kantojen kirjautumis- ja tapahtumalokit
- käyttöoikeus- ja muut ylläpitolokit
- virtuaalikoneiden tilannevedokset
- levy- ja muistivedokset
- verkkoliikennetallennukset
- tietojärjestelmien tekninen todistusaineisto
- käyttäjien kuvaus poikkeamasta
- kulun- ja kameravalvonnan sekä rikosilmoitusjärjestelmien keräämät tiedot.

Todistusaineiston käsittelyssä on olennaista turvata aineiston eheys ja aikaleimat. Todistusaineisto on kerättävä ja dokumentoitava mahdollisimman täydellisesti. Dokumentointi on tärkeää erityisesti silloin kun teknisen todistusaineiston eheydestä ei voida olla varmoja. Todistusaineiston säilytysaika tulee suunnitella etukäteen tai se voi perustua organisaation lokipolitiikkaan tai tiedonohjaussuunnitelmaan.

Mahdollisen rikostutkinnan käynnistyttyä toimitaan poliisin antamien ohjeiden mukaisesti.

5.3. Tietoturvatiedon jakaminen ja viestintä

Poikkeamatilanteissa korostuu jatkuvasti saatavilla olevan, luotettavan ja ajantasaisen tiedon tarve. Tietojen lähettämisen tulee olla oikea-aikaista, täsmällistä ja ohjaavaa, sillä sen perustarkoituksena on ylläpitää tietoisuutta tosiasioista ja tehtävistä toimenpiteistä.

5.3.1. Tietoturvatiedon jakaminen reagoinnin aikana

Poikkeamasta on ilmoitettava viranomaisille luvussa 4.3.1 *Tietoturvatiedon jakaminen* kuvatulla tavalla. Tiedon jakamisessa on huomioitava, ovatko jotkin viestintäkanavat poikkeaman luonteen vuoksi turvattomia. Muille sidosryhmille jaettava tieto on muokattava kohderyhmän mukaan. Liiallisten tietojen paljastaminen voi vaarantaa poikkeaman tutkinnan tai aiheuttaa lisävahinkoja, mutta myös tietojen salailu voi aiheuttaa organisaatiolle haittaa negatiivisen julkisuuden ja tyytymättömyyden muodossa.

Tietoturvatiedon jakamisesta voi olla yhteydessä Viestintäviraston Kyberturvallisuuskeskukseen oikean tasoisen tiedon jakamiseksi tarvittaville sidosryhmille. Muut mahdolliset ilmoitusvelvollisuudet on kuvattu luvussa 2.3.

5.3.2. Viestintä reagoinnin aikana

Poikkeamasta on syytä viestiä ennen kuin virheellisiä tai puutteellisia tietoja alkaa levitä muuta kautta. Tiedonjakoa tarvitaan useassa poikkeaman käsittelyvaiheessa. Sidosryhmiä tulee informoida esimerkiksi silloin, kun tietoturvapoikkeama on todettu, poikkeaman käsittelemiseksi on jouduttu tekemään käyttäjiä koskevia toimenpiteitä, käyttäjien halutaan tekevän toimenpiteitä esim. poikkeaman leviämisen estämiseksi tai kun poikkeamatilanne on laajentunut kriisiksi.

Poikkeamatilanteeseen liittyvä viestintä tulee käynnistää viestintäsuunnitelman mukaisesti heti poikkeaman ilmettyä (ks. luku *4.3.3 Viestintäsuunnitelman laatiminen)*. Samalla on arvioitava, estääkö poikkeama teknisesti joidenkin viestintäkanavien käytön. Sisäisen viestinnän tavoitteena on pitää organisaation johto tarvittavilta osin tietoisena poikkeaman käsittelystä. Täsmällisellä viestinnällä on mahdollista myös varmistaa, että vääriä tietoja ei pääse leviämään organisaation sisällä eikä sen ulkopuolelle.

Tehdyistä tai suunnitelluista toimenpiteistä on tiedotettava tahoille, joihin ne vaikuttavat. Vakavissa poikkeamatilanteissa poikkeamankäsittelyryhmän on tehtävä yhteistyötä viestintäyksikön ja mahdollisen erillisen kriisinkäsittelyryhmän kanssa. Tietoturvapoikkeamasta on syytä kertoa poikkeaman kohteiksi varmasti joutuneiden lisäksi myös niille, joita poikkeama saattaa koskea. Tällaisia tahoja saattavat olla esimerkiksi muut organisaatiot, joiden tietoverkkoihin poikkeaman kohteella on yhteyksiä. Viestintäorganisaatio on syytä ottaa välittömästi mukaan poikkeaman käsittelyyn, kun poikkeama koskee useampia tahoja. Tällaisia tilanteita voivat olla esim. tietomurto julkiseen palveluun, henkilötietojen vuotaminen vääriin käsiin tai laaja palvelunestohyökkäys, joka estää julkisen palvelun käytön.

5.3.3. Viestintä henkilötietoihin kohdistuvissa poikkeamissa

Henkilötietojen tietosuojaloukkauksesta on ilmoitettava sen kohteiksi joutuneille viipymättä, jos tietosuojaloukkaus todennäköisesti aiheuttaa luonnollisen henkilön oikeuksia ja vapauksia koskevan suuren riskin. Ilmoituksessa on kuvattava henkilötietojen tietoturvaloukkauksen luonne ja esitettävä suosituksia siitä, miten asianomainen luonnollinen henkilö voi lieventää mahdollisia haittavaikutuksia. Ilmoitusta ei vaadita, jos henkilörekisterin pitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, kuten salausta. Ilmoitus voidaan myös jättää tekemättä, jos rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että korkea riski ei enää todennäköisesti toteudu tai jos ilmoituksen tekeminen vaatisi kohtuutonta vaivaa. Tällaisissa tapauksissa on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan tietoturvaloukkauksesta. Tässä yhteydessä on huomioitava EU-tietosuoja-asetuksen mukanaan tuomat uudet velvoitteet siirtymäkauden jälkeen 25.5.2018.

6. TOIPUMINEN TIETOTURVAPOIKKEAMATILANTEISTA

Korjaustoimenpiteiden jälkeen on seurattava, että valitut toimenpiteet ovat auttaneet ja että voidaan siirtyä toipumisvaiheeseen. Toipumisvaiheessa organisaation toiminnot palautetaan normaalitilaan. Edellytyksiä onnistuneelle toipumiselle on mm. ajan tasalla oleva järjestelmädokumentointi, joka sisältää kaiken toipumisessa tarvittavan tiedon tietoverkoista ja yhteyksistä. Lisäksi organisaatiolla on oltava päivitetyt järjestelmien toipumissuunnitelmat, riittävä määrä toipumismenettelyihin varattua henkilöstöä sekä hyvin suunnitellut sopimukset toipumisessa tarvittavien sidosryhmien sitouttamiseksi tehtäviin toimenpiteisiin. Osana toipumista tulee huomioida mahdolliset muutostyöt poikkeaman toistumisen estämiseksi. Lisätietoa löytyy muun muassa VAHTI 2/2016 Toiminnan jatkuvuuden hallinta –ohjeesta.

6.1. Tekniset toipumistoimenpiteet

Toipumisvaiheessa tehtävät toimenpiteet voivat vaihdella paljonkin riippuen siitä, minkälaisesta poikkeamasta on ollut kysymys. Poikkeaman seurauksena voidaan joutua mm.:

- palauttamaan tietoja varmuuskopioista
- korjaamaan haavoittuvuuksia
- päivittämään järjestelmiä tai asentamaan niitä kokonaan uudelleen
- vaihtamaan salasanoja tai
- tiukentamaan tietoturvavaatimuksia.

Jos tietoturvapoikkeama on johtunut haavoittuvuudesta, järjestelmien ylläpitäjien tulee korjata kyseiset haavoittuvuudet hallinnoimistaan järjestelmistä. Tietojärjestelmiin liittyvät korjaukset on toipumisvaiheessa priorisoitava muiden toimenpiteiden edelle.

6.2. Viestintä

Toipumisvaiheessa kerrotaan tilanteen palautumisesta normaaliksi. Toipumisvaiheen tiedotteeseen on syytä lisätä ainakin lyhyt kuvaus tapahtuneesta, poikkeaman syy yleisellä tasolla, poikkeaman käsittelyn lopputulos ja mahdolliset välittömät toimenpidesuositukset tai -ohjeistukset. 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, on syytä harkita myös lehdistötiedotetta.

6.3. Raportointi ja tapauksesta oppiminen

Toipumisen jälkeen kaikki poikkeamaan liittyvä dokumentaatio on koottava yhteen ja materiaali analysoitava huolellisesti erillisessä tilaisuudessa. Jälkianalysoinnin tarkoitus on etsiä menetelmiä, joilla voidaan ennaltaehkäistä poikkeamatilanteiden syntymistä ja toimia niissä tehokkaammin. Jos poikkeaman käsittelyn aikana havaittiin puutteita organisaation toiminnassa tai toiminnan ohjeistuksessa, toimintatapoja on päivitettävä ja asianosaiset koulutettava riittävällä tavalla.

Toipumissuunnitelmia tulee kehittää havaittujen puutteiden perusteella sekä laatia aikataulutetut suunnitelmat vastuuhenkilöineen puutteiden korjaamiseksi. Myös mahdollisissa ulkoistussopimusten mukaan tuotetuissa palveluissa ilmenneet puutteet on käsiteltävä palveluntarjoajien kanssa. Jos on selkeästi havaittavissa, että palveluntarjoaja toimi poikkeamatilanteessa sopimuksen tai muiden käytäntöjen vastaisesti, on tarpeen harkita reklamointia.

Yksityiskohtainen tietoturvapoikkeamasta tehty raportti palvelee koko organisaatiota sen toimintojen kehittämisessä. Tietoturvapoikkeamista on tärkeää raportoida sopivalla tarkkuustasolla myös organisaation johdolle, sillä johdolle suunnattu raportointi edistää tietoturvallisuuden kokonaiskehitystä ja tietoturvatyön resursoinnin varmistamista. Tietoturvapoikkeamaraportti on arkistoitava myöhempää käyttöä varten.

Tietoturvapoikkeamaraportti on toimitettava soveltuvilta osin myös sidosryhmille, jotta vastaavien tilanteiden toistumista muissa organisaatioissa voidaan välttää. Ilmoitusvelvollisuudesta on sovittu yleensä turvallisuussopimuksessa.

6.4. Päätöksenteko

Kun tietoturvapoikkeaman laajeneminen on saatu pysäytettyä, poikkeaman juurisyy selvitetty ja korjaukset tehty siten, että poikkeusjärjestelyjä ei enää tarvita, poikkeamankäsittelyryhmä voi tehdä päätöksen poikkeamatoiminnan lopettamisesta ja siirtymisestä normaaliin toimintaan. Tietoturvahenkilöstön ja ylläpitäjien on kuitenkin seurattava ympäristöä tehostetusti, kunnes on varmistettu, että korjaukset ovat onnistuneet eikä poikkeaman uusiutuminen ole todennäköistä.

Päätöksen normaaliin toimintaan palaamisesta tekee sama taho kuin toipumisvaiheeseen siirtymisestä. Päätös tehdään silloin, kun toipumissuunnitelmien mukaiset toimenpiteet on tehty. Jos poikkeaman käsittelyn aikana on asetettu pääsyestoja tai muita vastaavia toimenpiteitä, kyseiset toimenpiteet puretaan tässä vaiheessa.

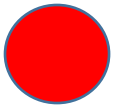
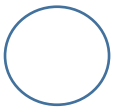
LIITE 1. Sanasto

APT	Advanced Persistent Threat, kohdistettu haittaohjelmahyökkäys. Tiettyyn kohteeseen kohdistettu pitkäaikainen ja suunniteltu hyökkäys, jossa käytetty haittaohjelma ja muut tekniikat ovat kohteen mukaan räätälöityjä.
CERT- toiminto	Viestintäviraston Kyberturvallisuuskeskuksen CERT-toiminnon tehtävänä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista.
DDoS	Distributed Denial of Service. Hajautettu palvelunestohyökkäys.
GovHAVARO	Viestintäviraston tuottaman teknisten tietoturvaloukkausten havainnointi- ja varoituspalvelun (HAVARO) valtionhallinnon tarpeisiin muokattu versio.
Haavoittuvuus	Alttius turvallisuutta uhkaaville tekijöille, puutteet ja heikkoudet turvatoimissa sekä suojauksissa.
Haittaohjelma	Ohjelma, ohjelman osa tai muu käskyjoukko, joka tarkoituksellisesti aiheuttaa ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa
Honeypot (hunajapurkki, ansa)	Tunkeilijasta tietoja keräävä järjestelmä, joka pyrkii herättämään hyökkääjän mielenkiinnon tekeytymällä huonosti suojatuksi.
IDS/IPS (Intrusion detection/intrusion prevention)	Tietomurtojen havainnointijärjestelmä / tietomurtojen estojärjestelmä.
Kiristyshaittaohjelma (ransomware)	Haittaohjelma, joka salaa kohteen tietoja ja lupaa vapauttaa ne vaadittua lunnasta vastaan.
Lokitieto	Automaattisesti kirjautuva tapahtumatieto, joka voi sisältää muun muassa erilaisia tunnistamistietoja, välitystietoja ja tietoja virhetilanteista.
SIEM	Security Incident and Event Management. Turvallisuuspoikkeamien ja -tapahtumien hallinnassa käytetty ohjelmisto tai palvelu.
SIRT	Security Incident Response Group Tietoturvatapahtumien hallinnasta vastaava ryhmä.
SSOC	Tietoturvavalvomo (Security and Service Operations Center)

Tietoturvapoikkeama	Tahallinen tai tahaton tapahtuma, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut.
Tietoturvatapahtuma	Tietoturvallisuuteen liittyvä tietojärjestelmässä tai tietoverkossa havaittu tapahtuma.
Tietoturvatieto	Tietoturvapoikkeamaan tai -tapahtumaan liittyvä tieto. Tietoturvallisuuden järjestämiseen liittyvä tieto.
Tilannekuva	Turvallisuustilanne havaintojen, arviointien, mittareiden ja analyysien perusteella.
TLP	Traffic Light Protocol. Tiedon luokittelumalli, jossa tietojen luottamuksellisuus ilmaistaan värein kuten liikennevaloissa.
Tunniste (poikkeama)	Tieto, jota käytetään tunnistamaan tiettyä tietoturvapoikkeamaa tai sen epäilyä.
Turvaluokitus	Asiakirjojen ja tietojen jakaminen luokkiin salassa pidettävyyden perusteella.
Turvamerkintä	Turvaluokituksen mukainen asiakirjaan tehtävä merkintä, josta ilmenee turvaluokitus ja sen peruste.
Uhka	Haitallinen tapahtuma, joka voi mahdollisesti toteutua, tai useampi mahdollinen häiriö, jotka toteutuessaan voivat aiheuttaa sen, että tietoon, muuhun omaisuuteen tai toimintaan kohdistuu haitallisia tapahtumia.
Varautuminen	Toiminta, jonka tarkoituksena on luoda ja ylläpitää organisaation riittävä valmius toiminnan jatkumiseen vakavissa häiriötilanteissa ja poikkeusoloissa.
Viestintäsuunnitelma (poikkeamat)	Määrittelee viestintä- ja tiedotusvastuut, sidosryhmät ja niiden yhteystiedot, joille ollaan vastuussa poikkeamien ilmoittamisesta, sekä muut poikkeamatilanteen viestintään ja tiedottamiseen liittyvät asiat.
Viestintäviraston Kyberturvallisuuskeskus	Viestintäviraston Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen, joka kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta.
VIRT	Virtual Incident Response Team. Valtiovarainministeriön johtama yhteistyöverkosto, jonka tarkoituksena on varautua vakaviin ja laajavaikutteisiin tieto- ja kyberturvapoikkeamatilantei-

	siin.
VTV	Valtiontalouden tarkastusvirasto.
KRP	Keskusrikospoliisi

LIITE 2. Traffic Light Protocol -luokittelu

Luokka	Tiedon jakelun laajuus	Kuvaus
 **RED**	Henkilökohtainen jakelu	Tieto luovutetaan henkilökohtaisesti. Vastaanottaja ei saa luovuttaa tietoa edelleen edes tiedonvaihtoryhmän tai oman organisaationsa sisällä.
 **AMBER**	Rajattu yhteisön sisäinen jakelu	Tieto voidaan jakaa muille tiedonvaihtoryhmän jäsenille ja tiedot vastaanottavan henkilön edustaman organisaation sisäisesti välttämättömille henkilöille. Tiedon luovuttaja voi tarvittaessa asettaa luokituksen yhteydessä lisärajoituksia tai -vapauksia tiedon käsittelylle.
 **GREEN**	Yhteisön sisäinen jakelu	Tieto voidaan jakaa vapaasti sen vastaanottaneen henkilön edustaman organisaation sisällä. Vastaavasti tieto voidaan luovuttaa vapaasti tiedonvaihtoryhmän muille jäsenille. Tietoa ei saa kuitenkaan julkaista esimerkiksi Internetissä eikä luovuttaa tiedonvaihtoryhmän ulkopuolisille tahoille.
 **WHITE**	Rajoittamaton	Tieto voidaan jakaa pakottavasta lainsäädännöstä johtuvat rajoitukset huomioiden vapaasti. Tyypillisesti TLP WHITE -luokiteltu tieto on jo saatavilla julkisista lähteistä.

LIITE 3. Esimerkkejä tietoturvapoikkeaman viitteistä

Mahdollista tietoturvapoikkeamaa voidaan epäillä erilaisten viitteiden perusteella. Ne ilmaisevat tietoturvapoikkeaman tapahtuneen tai olevan tapahtumassa. Tietoturvapoikkeamaa voidaan epäillä esimerkiksi silloin, kun

- verkkotason hyökkäyksenhavaitsemisjärjestelmä (IDS/IPS) hälyttää palvelimeen kohdistuvasta hyökkäyksestä
- virustorjuntaohjelmisto hälyttää tietojärjestelmästä löytyneestä haittaohjelmakoodista
- tietoliikenneoperaattori, CERT-toimija tai kolmas osapuoli ilmoittaa epäilyttävistä liikennehavainnoista organisaation omassa osoiteavaruudessa
- verkkopalvelin kaatuu selittämättömästi tai toimii muuten poikkeuksellisesti
- käyttäjät valittavat Internet-yhteyden huomattavasta hitaudesta
- järjestelmäylläpitäjä havaitsee epäilyttävän tiedoston
- palvelinjärjestelmän eheydenvalvontaohjelmisto ilmoittaa konfiguraatiomuutoksesta huoltoikkunan ulkopuolella
- sovellus ilmoittaa useista epäonnistuneista kirjautumisyrityksistä tuntemattomasta viraston ulkopuolisesta järjestelmästä
- sähköpostijärjestelmän ylläpitäjä havaitsee huomattavan määrän käyttäjille palautuvia viestejä
- verkkoylläpitäjä havaitsee epätavallisen poikkeaman verkon liikenneprofiilissa
- viraston kirjanpidon luvut poikkeavat odotetusta
- käyttäjätukeen tulee poikkeuksellisia vikailmoituksia käyttäjiltä
- keskustelukanavilla näkyy organisaation tietojärjestelmiin liittyviä tietoja tai kommentteja.

Joissain tilanteissa organisaatio voi havaita merkkejä, jotka nostavat tietoturvapoikkeamatilanteen todennäköisyyttä lähiaikoina. Esimerkkejä tällaisista tapauksista ovat mm. seuraavat:

- verkkopalvelimen lokitiedostossa on merkintöjä, jotka viittaavat organisaation ulkopuolisen tahon käyttäneen haavoittuvuusskanneria palvelinta kohtaan
- tietojärjestelmämurtoja tekevän aktivistiryhmittymän uhkaus hyökkäyksestä viranomaista kohtaan
- organisaatio on normaalia runsaammin hyökkääjien mielenkiintoa herättävällä tavalla esillä mediassa.

Havaintoja tietoturvapoikkeamatilanteista voidaan saada esimerkiksi seuraavista lähteistä:

- tietoturvaohjelmistojen hälytykset
- verkko- ja tietojärjestelmäkohtaiset hyökkäyksen havaitsemisjärjestelmät
- virustorjuntaohjelmistot
- tiedostojen eheyden tarkistusohjelmistot
- palveluiden käytettävyyden mittausohjelmistot
- käyttöjärjestelmän, palveluiden ja sovellusten lokitiedostot
- verkkolaitteiden (esimerkiksi reitittimet, kytkimet tai kuormanjakolaitteet) lokitiedostot
- julkisesti saatavilla olevat tietolähteet (esim. haavoittuvuustiedotteet)
- tiedot muihin organisaatioihin kohdistuvista tai muista organisaatioista lähtevistä hyökkäyksistä
- erilaiset keskusteluryhmät/kanavat
- postituslistat
- käyttäjien yhteydenotot asiakaspalveluun / ylläpitoon tietojärjestelmien tai muiden käyttäjien poikkeavasta toiminnasta.

LIITE 4. Muistilista tietoturvapoikkeamista kerättävistä tiedoista

Ilmoittajan tiedot

- nimi
- rooli
- organisaatioyksikkö
- sähköpostiosoite
- puhelinnumero
- fyysinen sijainti

Poikkeaman tiedot

- poikkeaman tunnistenumero
- milloin poikkeama havaittiin ja ilmoitettiin
- poikkeaman vaikutus
- poikkeaman nykytila (status)
- poikkeaman lähde ja syy, jos tiedossa
- poikkeaman kuvaus (minkälaisessa tilanteessa poikkeama havaittiin ja mitkä merkit paljastivat poikkeaman)
- kuvaus poikkeamaan liittyvistä kohteista (esim. verkot, palvelimet tai verkkopalvelut)
- muut havainnot (esim. poikkeava tietoliikenne, hälytykset tai käyttäjien ilmoitukset)
- poikkeamakäsittelyn priorisointiin vaikuttavat tekijät (mm. poikkeaman kohteena olevan järjestelmän tai tiedon tärkeys)
- vaikutusta pienentävät tekijät (esim. kovalevyn salaus varastetussa tietokoneessa)
- vaikutusta lisäävät tekijät (esim. salaiseksi luokiteltu tieto)
- tehdyt vastatoimet (esim. estetty tai suodatettu palvelun verkkoliikennettä tai irrotettu työasema verkosta)
- organisaatiot, joihin on jo otettu yhteyttä poikkeamaan liittyen

Tietoturvapoikkeaman käsittelijän tiedot

- poikkeamaan käsittelyn nykyinen tilanne (status)
- poikkeaman yhteenveto
- poikkeaman käsittelyn toimenpiteet ja tarkat ajankohdat
    - kaikkien käsittelyyn osallistuneiden yhteystiedot ja tapahtumakirjaukset
    - listaus kerätystä todistusaineistosta
- poikkeaman käsittelijän kommentit
- poikkeaman juurisyy
- poikkeaman hallintaan käytetyt kustannukset
- poikkeaman liiketoimintavaikutukset

LIITE 5. Esimerkki tietoturvapoikkeamien viestintäsuunnitelman rungosta

Aihe ja tavoitteet

Kuvaus viestinnän aiheesta ja tavoitteista: viestintäsuunnitelman tarkoituksena on varmistaa, että organisaation viestimät tiedot ovat tarkkoja, oikea-aikaisia ja johdonmukaisia.

Kohderyhmät

Määrittely viestinnän kohteista (oma organisaatio, yhteistyökumppanit, viranomaiset, kansalaiset, media). Poikkeamista tiedotetaan pääsääntöisesti vain niitä, joiden toimintaan, oikeuksiin tai tietosuojaan poikkeama vaikuttaa.

Määritelmä siitä, minkälaista tietoa eri kohderyhmälle voidaan toimittaa. Tiedottamisessa on huomioitava tietojen salassapitovaatimukset.

Viestintäsuunnitelmassa on huomioitava eri kohderyhmien tiedottamisessa

- yhteystiedot ja toimintavalmius virka-aikana ja sen ulkopuolella
- mahdollisten salausavainten luominen ja toimittaminen suojattua yhteydenpitoa varten
- päätöksenteko- ja viestintämalli tilanteissa, joissa tietoturvapoikkeama koskee useampaa tahoa.

Viestintävälineet

Kuvaus siitä, minkälaisia kanavia viestinnässä käytetään. Viestintäkanavia voivat tilanteen mukaan olla mm.

- puhelin
- kirjalliset tiedotteet
- ilmoitustaulut
- suullinen informaatio
- tiedotusvälineet (TV, radio, sanomalehdet)
- sähköposti / sähköpostilistat
- tekstiviestit
- sähköiset ilmoitustaulut (esim. intranetissä)
- käyttöjärjestelmän sisäiset tiedotteet (esim. käyttäjän tietokoneen työpöydälle ilmestyvä tiedote)
- verkkosivut
- pikaviestimet
- sosiaalinen media (Facebook, Twitter tms.)

Myös viestintävälineiden toimimattomuuteen on varauduttava ja määriteltävä viestintäkanaville varajärjestelyt.

Organisaatio, roolit ja vastuut

Kuvaus viestintäorganisaation rakenteesta sekä siitä, mitä rooleja kullakin organisaation jäsenellä on.

Määrittely siitä, kuka päättää viestinnän sisällöstä ja ajankohdasta.

Erityisvaatimukset

Poikkeamaviestinnän erityisvaatimukset esimerkiksi luottamuksellisen tiedon tai sopimusvelvoitteiden suhteen.

Viestintäsuunnitelmaan on syytä kuvata lähetettävistä tiedotteista ja muista viesteistä luonnokset, joita voidaan poikkeamatilanteessa helposti täydentää.

LIITE 6. Esimerkki poikkeamatilanneohjeistuksesta

Palvelunestohyökkäys organisaation verkkosivuille tai sähköisiin asiointipalveluihin

Kuvaus

Tahallisella ulkoisella kuormituksella tukitaan tai häiritään organisaation verkkosivuja tai sähköisiä asiointipalveluita siten, etteivät ne ole käytössä tai ne toimivat hitaasti tai virheellisesti yli neljän tunnin ajan. Kuormitus voi olla virheellistä tai oikeanlaista liikennettä ja johtaa verkko- tai alustakapasiteetin loppumiseen tai palvelun kaatumiseen virheellisen toiminnon takia.

Tietoturvapoikkeamien käsittelyryhmä

ICT-tietoturvapäällikkö
Turvallisuuspäällikkö
Tuotantopäällikkö
Verkkoarkkitehti
Käyttöpalvelutoimittajan tietoturvavastaava
Palvelutoimittajan verkkovastaava
Palvelutiimin vetäjä

Tarpeen mukaan
Viestintäasiantuntija
Tuotantoryhmän vetäjä
Palvelutoimittajan tietoturvavastaava

Sidosryhmät

Viestintäviraston Kyberturvallisuuskeskus
Poliisi
Käyttöpalvelutoimittaja
Operaattori

Viestintä

Turvallisuuspäällikkö tiedottaa viraston johtoa sähköpostilla kahdesti päivässä. Vastaavasti päivitettävä tiedote julkaistaan intranetissä ja sidosryhmille lähetetään häiriötiedote. Jos kyseessä on vakava häiriö,

viestintäasiantuntija valmistelee mediatiedotteen, joka julkaistaan lisäksi organisaation nettisivuilla ja sosiaalisen median kanavissa (Facebook, Twitter). Tilannepäivityksiä julkaistaan näissä kahdesti päivässä. Medialle ja ulkoisiin kyselyihin vastaa tietohallintojohtaja tai turvallisuuspäällikkö.

Tapahtumalokin ylläpito

Päätetään kirjuri ja kirjataan tehdyt päätökset sekä oleelliset tapahtumat ja havainnot ajankohtineen.

Toimet

1. Häiriönhallintaprosessista otetaan yhteyttä tietoturvapäällikköön ja tuotantopäällikköön.
2. Tietoturvapäällikkö ja / tai tuotantopäällikkö arvioivat, onko kyseessä todellinen palvelunesto-hyökkäys ja minkä tahojen palveluihin hyökkäys kohdistuu.
3. Tapauksesta tiedotetaan sähköpostilla / tekstiviestillä turvallisuuspäällikköä, tietohallintojohtajaa, palvelun ICT-omistajaa, palvelutiimin vetäjää sekä palvelutoimittajan tietoturvavastaavaa.
4. ICT-tietoturvapäällikkö tai tuotantopäällikkö kutsuu kriisiryhmän kokoon kriisinjohtokeskukseen
(tarkoitukseen soveltuva neuvotteluhuone tms.) sekä avaa viestintäkanavat.
5. Arvioidaan hyökkäyksen laajuus, vaikutukset ja tyyppi

- Mikä on liikenteen määrä ja lähde (kotimaa / ulkomaat) ja tyyppi
- Mitkä ovat häiriön vaikutukset? Vaikuttaako organisaation kriittisiin sovelluksiin?
- Onko kyseessä hajautettu palvelunestohyökkäys? Mihin kuormitus kohdistuu?
- Onko viitteitä kiristyksestä tai aiemmasta uhkauksesta?
- Hyödyntääkö hyökkäys haavoittuvuutta vai pelkkää resurssien ylikuormitusta?
- Voidaanko poikkeava liikenne tunnistaa?

6. Tiedotetaan tarpeen mukaan viraston johtoa, henkilöstöä ja sidosryhmiä (häiriötiedote) sekä otetaan viestintäyksikkö mukaan ulkoiseen tiedottamiseen (mediatiedote, sosiaalinen media).
7.Jos tapaukseen liittyy kiristystä, vaateisiin tai viesteihin ei vastata.
8. Otetaan yhteyttä Viestintäviraston Kyberturvallisuuskeskuksen päivystäjään (ICT-tietoturvapäällikkö) sekä poliisiin asiantuntija-avun saamiseksi. Tehdään tapauksesta rikosilmoitus.

9. Käyttöpalvelutoimittaja ottaa käyttöön teknisiä rajoituskeinoja

- Jos vihamielinen liikenne voidaan tunnistaa, tutkitaan mahdollisuutta sen torjumiseen kuormantasaajalla, konesaliverkon tai operaattorin palomuureissa
- Tutkitaan, voiko osoitteita vaihtaa tai käsitellä liikenne operaattorin DoS-torjuntapalvelussa
    - Jos hyökkäys kohdistuu DNS-nimeen, harkitaan nimen vaihtoa, ja jos kohdistuu IP-osoitteeseen, vaihdetaan IP-osoitetta
- Tutkitaan mahdollisuutta lisätä verkkokapasiteettia tai käyttää useampaa operaattoria
    - Reititysmuutokset (ohjataan palvelu toiselle operaattorille)
    - Palveluiden hajauttaminen (internet-proxy, sähköposti)

- Harkitaan mahdollisuutta estää ulkomailta tuleva liikenne
    - Harkitaan palveluiden jakoa erillisen verkon kautta (Akamai, Cloudflare jne.)
    - Sisäisen kapasiteetin kasvatus
    - Ajetaan alas toiminnallisuuksia
    - Otetaan käyttöön kevennetyt staattiset sivut hyökkäyksen kohteena olevalla sivustolla

10. Viestitään käyttöön otetuista teknisistä ratkaisuista ja uusista palvelusijainneista mediatiedotteella ja sosiaalisessa mediassa.
11.Vakavan häiriön jatkuessa yli 4 h ajan otetaan käyttöön varamenettelyt sähköisissä palveluissa sekä vaihtoehtoiset tiedotustavat organisaation nettisivujen osalta (esim. sosiaalinen media).
12. Häiriön loppuessa tiedotetaan sidosryhmiä, pidetään poikkeaman jälkeinen palaveri ja kirjataan ylös opit sekä kehitystoimet.

Lisäohjeet

Tarkemmat toimintaohjeet ja tiedotepohjat ovat täällä (viittaus tallennuspaikkaan).

LIITE 7. Tietoturvapoikkeaman ilmoituslomakkeen malli

Tällä lomakkeella ilmoitetaan organisaatiossa tapahtuneesta tietoturvapoikkeamasta tai sen uhkasta.

Ilmoittaja _____

Osasto / yksikkö / vastuualue _____

TIETOTURVAPOIKKEAMAN TAI SEN UHKAN KUVAUS

Tapahtuma-ajankohta
Tapahtumapaikka / -kohde
Poikkeaman tyyppi *Palvelunestohyökkäys* *Haittaohjelma* *Järjestelmän luvaton käyttö* *Tiedon korruptoituminen tai tuhoutuminen* *Varkaus* *Muu poikkeama*
Tapahtumakuvaus (ajankohdat, havainnot, tehdyt toimenpiteet yms.)
Tapahtumasta aiheutuneet vahingot ja / tai mahdollisesti seuraavat vahingot ja selvitys-työhön käytetyt henkilöresurssit
Sisäinen ja ulkoinen viestintä
Kokemuksesta oppiminen
Muut tiedot
Lisätietojen antaja ja yhteystiedot

LIITE 8. Tapahtumapäiväkirjan malli

Tähän päiväkirjaan kirjataan kaikki poikkeamanhallintaan liittyvät toimenpiteet ja tapahtumat

Poikkeaman kohde:

Selvitysryhmän jäsenet ja yhteystiedot:

Aika	Tapahtumakuvaus	Vastuuhenkilö	Kommentit

Lista todistusaineistosta:

LIITE 9. Tietoturvapoikkeamien hallintaan liittyvä lainsäädäntö

Tietoturvapoikkeamien hallinnassa huomioitavia lakeja ja asetuksia ovat erityisesti seuraavat:

1. EU:n tietosuoja-asetus
2. Arkistolaki (831/1994)
3. Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
4. Laki valtiontalouden tarkastusvirastosta (676/2000)
5. Laki viranomaisten toiminnan julkisuudesta (621/1999)
6. Laki yhteistoiminnasta valtion virastoissa (1233/2013)
7. Laki yksityisyyden suojasta työelämässä (759/2004)
8. Tietoyhteiskuntakaari (917/2014)
9. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)
10. EU:n tietosuoja-asetus
11. Arkistolaki (831/1994)
12. Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
13. Laki valtiontalouden tarkastusvirastosta (676/2000)
14. Laki viranomaisten toiminnan julkisuudesta (621/1999)
15. Laki yhteistoiminnasta valtion virastoissa (1233/2013)
16. Laki yksityisyyden suojasta työelämässä (759/2004)
17. Tietoyhteiskuntakaari (917/2014)
18. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)