NIS2-poikkeamailmoituksien ohjeistus

Sisällysluettelo

NIS2-poikkeamailmoituksien ohjeistus 1

1 Johdanto 2

2 NIS2-ilmoitussovellus 3

2.1 Ensi-ilmoitus 3

2.2 Jatkoilmoitus 12

2.3 Väliraportti 13

2.4 Loppuraportti 15

2.5 Vapaaehtoinen ilmoitus valvovalle viranomaiselle 18

2.5.1 Poikkeama 18

2.5.2 Kyberuhka 18

2.5.3 Läheltä piti-tilanne 19

1 Johdanto

Tämä dokumentin tarkoituksena on esimerkkitapauksen avulla neuvoa organisaatioita kyberturvallisuuslain ja julkishallinnon kohdalla tiedonhallintalain mukaisten poikkeamailmoitusten tekemisessä ja asiaan kuuluvien ilmoituslomakkeiden täyttämisessä.

Dokumentissa esiintyvät nimet, osoitteet ja muut yksilöivät tiedot on luotu esimerkinomaisina, eikä niissä kuvailtuja tilanteita ole tarkoitettu suoraan käyttökelpoisiksi NIS2-toimijalle. Tämän dokumentin kuvissa ja teksteissä esitetyt esimerkit havainnollistavat näin vain mahdollisia skenaarioita, joita kyberturvallisuuslain ja tiedonhallintalain mukaisissa poikkeamailmoituksissa voi mahdollisesti esiintyä.

NIS2-direktiivin 23 artiklan mukaisesti direktiivin soveltamisalaan kuuluvien organisaatioiden on ilmoitettava toimivaltaiselle valvovalle viranomaiselle tarjoamiinsa palveluihin kohdistuvista merkittävistä poikkeamista. Ilmoitusvelvollisuus on kolmiportainen ja koostuu ensi-ilmoituksesta, jatkoilmoituksesta ja loppuraportista. Lisäksi organisaatioiden on pitkäkestoisissa poikkeamissa tai viranomaisen pyynnöstä annettava poikkeamaa koskeva väliraportti.

Velvollisuudesta ilmoittaa merkittävästä poikkeamasta valvovalle viranomaiselle ja ilmoitusten sisällöstä säädetään kyberturvallisuuslain 11-13 §:lissä. Lisäksi vapaaehtoisesta ilmoittamisesta säädetään 15 §:ssä. Julkishallinnon organisaatioiden osalta ilmoitusvelvollisuudesta ja ilmoitusten sisällöstä säädetään tiedonhallintalain 18 d §:ssä. Lisäksi vapaaehtoisesta ilmoittamisesta säädetään tiedonhallintalain 18 f §:ssä.

Kyberturvallisuuslain 11 § 2 momentin mukaan merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön tai huomattavia taloudellisia tappioita asianomaiselle toimijalle, sekä poikkeamaa, joka on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa. Merkittävä poikkeama on määritelty viranomaisia koskien tiedonhallintalain 2 § 24 kohdassa. Lisäksi tiettyjen organisaatioiden kohdalla sovelletaan komission täytäntöönpanoasetusta 2024/2690, jolla on annettu täydentävää sääntelyä mm. merkittävän poikkeaman määrittelyyn liittyen.

Ensi-ilmoitus on toimitettava 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta, ja jatkoilmoitus 72 tunnin kuluessa merkittävän poikkeaman havaitsemista. Väliraportti on annettava valvovan viranomaisen pyynnöstä tai pitkäkestoisen poikkeaman tapauksessa viimeistään kuukauden kuluttua jatkoilmoituksen toimittamisesta. Poikkeamaa koskeva loppuraportti on annettava kuukauden kuluessa jatkoilmoituksen toimittamisesta tai pitkäkestoisen poikkeaman tapauksessa kuukauden kuluessa poikkeaman käsittelyn päättymisestä. Vapaaehtoinen ilmoitus koskee muita kuin merkittäviä poikkeamia sekä kyberuhkia ja läheltä piti -tilanteita. Vapaaehtoisen ilmoituksen kohdalla ei toimiteta erikseen jatkoilmoitusta tai loppuraporttia.

Tässä ohjeistuksessa käsitellään vain kyberturvallisuuslain mukaisten ilmoitusten tekemistä. Muu sääntely voi velvoittaa tiettyjä toimijoita ilmoittamaan poikkeamista lisäksi myös muilla tavoilla. Tämä ohjeistus ei ole oikeudellisesti sitova ja mahdollisissa epäselvissä tilanteissa lainsäädännöllä on aina etusija suhteessa tässä ohjeistuksessa todettuun.

2 NIS2-ilmoitussovellus

Tässä kappaleessa käymme läpi viisi erilaista ilmoitustyyppiä. Ensimmäiset neljä ilmoitustyyppiä kuvaillaan kronologisessa järjestyksessä ja lopuksi kuvaillaan vapaaehtoinen ilmoitus erillisenä kokonaisuutena.

Huomaathan, että lomakkeissa toistuvat kentät kuten esimerkiksi yhteystiedot, mahdolliset rikosilmoitukset tai muille viranomaisille tehtävät ilmoitukset (TSV) sekä CSIRT-lisälomakkeet kuvataan vain kertaalleen ensi-ilmoituksen ohessa. Nämä tietueet toistuvat lomakkeissa useamman kerran, joten voit tarvittaessa palata näiden toistuvien kenttien ohjeistukseen kappaleen 2.1 sisällä.

2.1 Ensi-ilmoitus

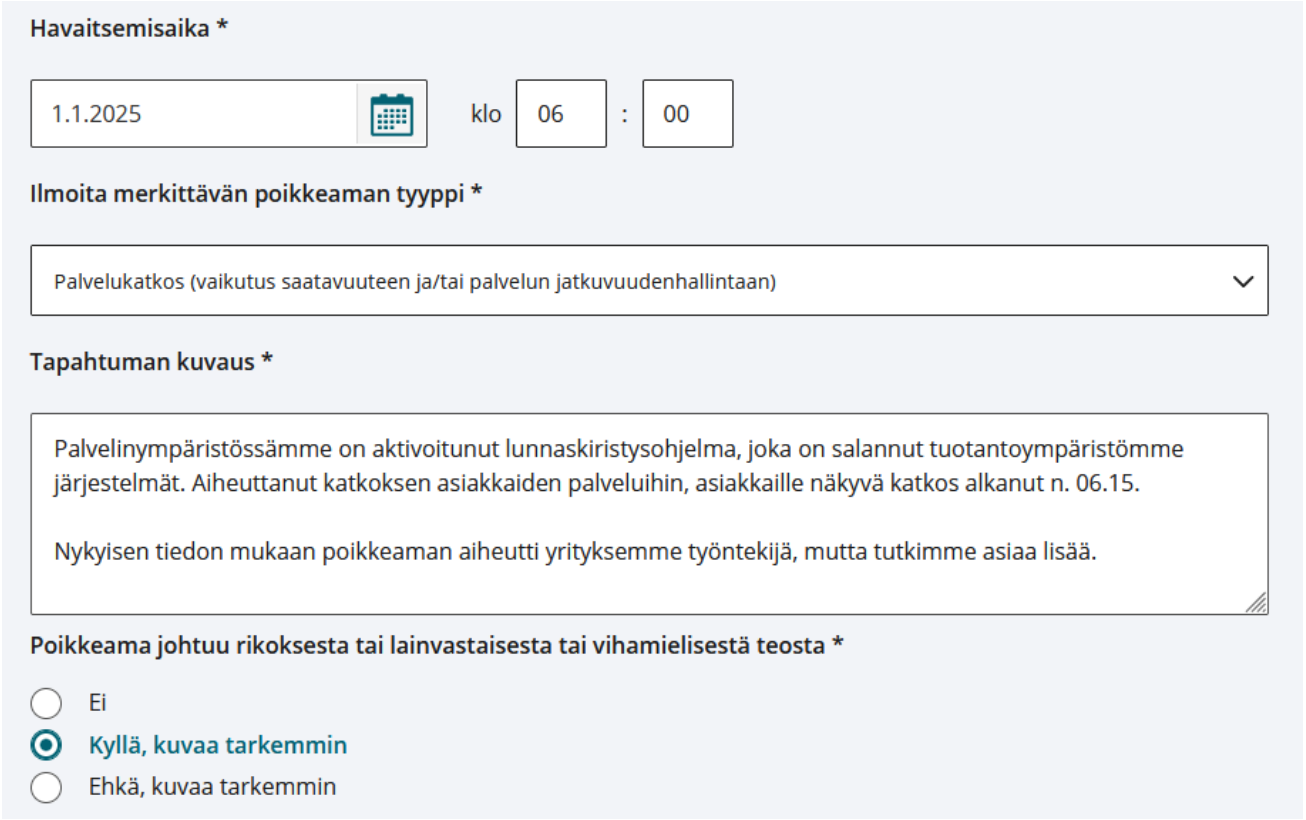
Merkittävän poikkeaman ensi-ilmoitus aloitetaan täyttämällä Kuvan 1-mukaisiin kenttiin organisaation toimialatiedot.

Kuva 1 Toimiala-tietokentät

Valittaessa organisaation toimialaa käytetään pääasiallista NIS2-sääntelyn alaista toimialaa. Tämän valinnan voi esimerkiksi tehdä vertailemalla organisaation toimialojen liikevaihtojen suuruutta, ja valitsemalla niistä suurin.

Kohtaan "muu mahdollinen toimiala" voitte lisätä ne toimialat, joilla organisaatiosi toimii yllä mainitun "päätoimialan" lisäksi. Käytännön esimerkkinä, organisaation, jonka pääasiallinen toimiala on teletoiminta voi lisätä muihin toimialoihin esimerkiksi datakeskuspalvelut, jos edellä mainittu yritys tarjoaa niitä erillisenä palveluna asiakasyrityksilleen.

Täytettyänne organisaatiosi toimialatiedot, voitte täyttää poikkeaman yleisluontoisten tietojen kentät, jotka on kuvattu Kuvassa 2.

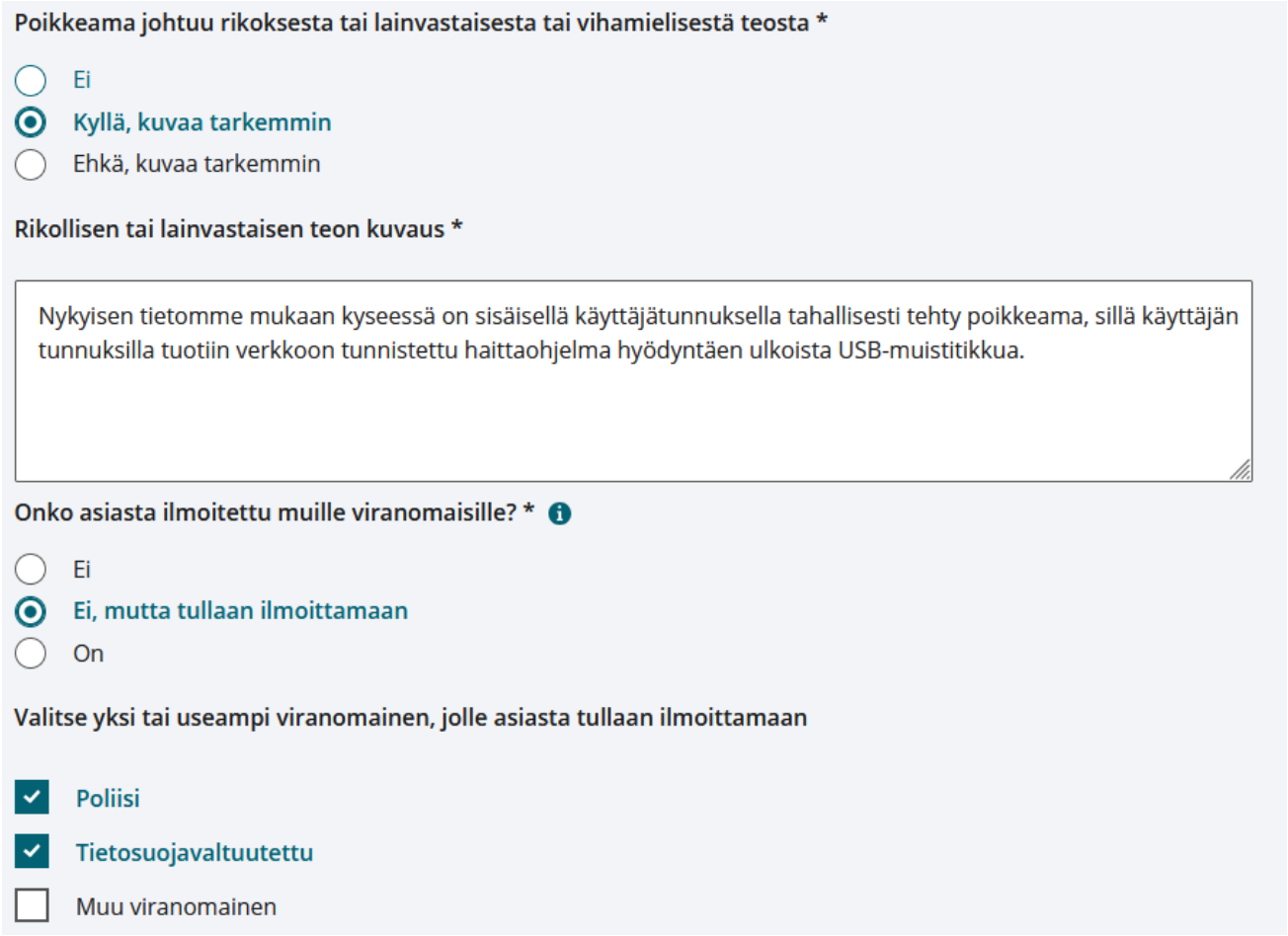


Kuva 2 Yleistiedot

Tapahtuman kuvauskenttään kirjoitetaan yleisluontoinen ja ilmoitusta tehdessä saatavilla olevan tiedon valossa tehty kuvaus tapahtumasta, arvio sen mahdollisista vaikutuksista sekä mahdollisesta poikkeaman tapahtumankulusta. Ensi-ilmoitusta tehtäessä on myös mahdollista, ettei edellä mainittuja tietoja ole vielä pystytty tarkentamaan, jolloin voitte täyttää kuvauskentän ilmoitushetken tietojen mukaisesti.

Edellä mainitussa kentässä voitte myös kuvailla vaikutuksen laajuutta organisaationne toiminnassa. Referenssitapauksen kuvauksessa on kuvattu tapaus, jossa koko organisaation palvelinympäristö on poikkeaman johdosta salattu, mutta tapauksella ei ole tunnistettu vaikutusta esimerkiksi palvelun varmistuksiin.

Näin ollen, oheista kenttää voi myös käyttää tapauksen vaikutusarvion rajaamiseen, jos olette huomanneet, ettei poikkeamalla ole vaikutuksia esimerkiksi kuin yhteen palveluun organisaatiossanne. Mainitun palvelun kohdalla voitte myös kuvailla, onko kyseessä liiketoimintakriittinen palvelu ja/tai järjestelmä vai onko kyseessä esimerkiksi sisäisen dokumentaation ylläpitoon käytetty järjestelmä.



Kuva 3 Ilmoitukset muille viranomaisille

Esimerkkitapauksen juurisyyn ollessa ns. sisäisen uhan toteutuminen on huomioitava lomakkeen tarjoamat kentät rikoksen, lainvastaisen tai vihamielisen teon mahdollisuudesta.

Johtuen ensi-ilmoituksen aikarajasta (24h) on kuitenkin huomioitava se, ettei edellä mainittujen kenttien täyttäminen välttämättä ole mahdollista. Tilanteessa, jossa organisaationne epäilee mahdollista vihamielistä tekoa, teidän on mahdollista myös valita kohta "Ehkä" ja täydentää esimerkiksi jatkoilmoituksessa tai loppuraportissa vastaustanne, kun sisäinen ja/tai ulkoinen tutkintanne on pystynyt tarkentamaan poikkeaman syntymätapaa esimerkiksi sisäisen toimijan ja teon tahallisuuden osalta.

Rikollisen tai lainvastaisen teon kuvauksen kohtaan voit kuvailla nykyisen tiedon valossa tapahtumankulkua. Ensi-ilmoituksen aikarajan johdosta on kuitenkin mahdollista, ettei tapahtumien kulusta ole vielä täyttä varmuutta, joten halutessanne voitte myös kuvailla poikkeaman syntytapaa ylätasolla ja tarkentaa kuvaustanne myöhemmin ilmoitusprosessissa, esimerkiksi jatkoilmoituksen ja/tai väliraportin muodossa.

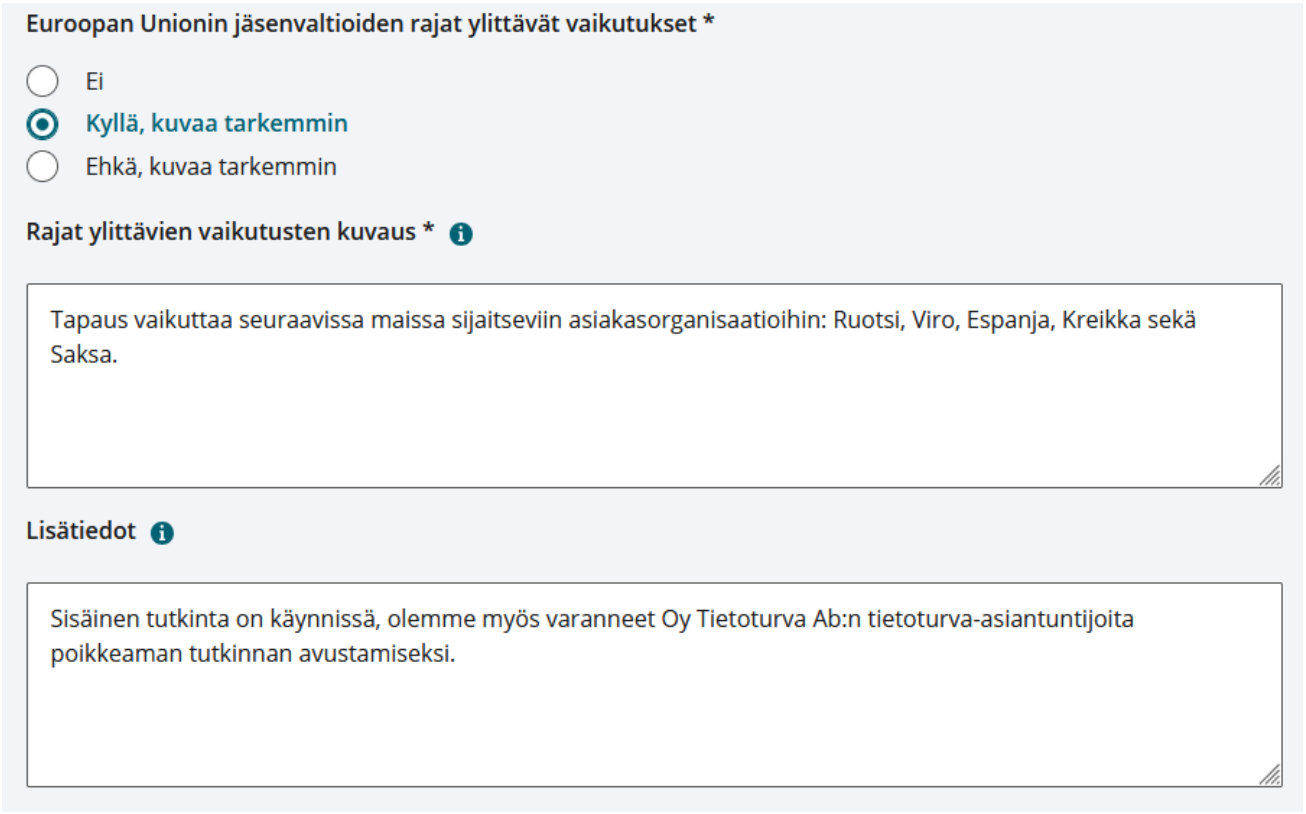
Tapauksessa, jossa myös henkilötietojen tietoturva on vaarantunut esimerkiksi tiedostovarkauden seurauksena, on huomioitava myös rekisterinpitäjän ilmoitusvelvollisuus yleisen tietosuoja-asetuksen (nk. GDPR-ilmoitus) mukaisesti tietosuojavaltuutetun toimistolle. Ilmoitusvelvollisuus koskee henkilötietojen tietoturvaloukkausta, joka tarkoittaa "tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin."

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava tietosuojavaltuutetun toimistolle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun rekisterinpitäjä on tullut tietoiseksi tietoturvaloukkauksesta.

Valittaessa viranomaisia, joille asiasta tullaan ja/tai on ilmoitettu, voit valita myös kohdan "Muu viranomainen". Tämän kohdan tarkoituksena on esimerkiksi mahdollistaa tiedonkulku eri viranomaisten väillä poikkeamissa, joiden toimijoilla on kaksi tai useampia valvovia viranomaisia toimijan laajan toimikentän johdosta. Kuvan 2 referenssitapauksessa on valittu muiksi viranomaisiksi poliisi (johtuen lainvastaisen teon mahdollisuudesta) ja tietosuojavaltuutetun toimisto mahdollisen henkilötietojen tietoturvaloukkauksen takia.

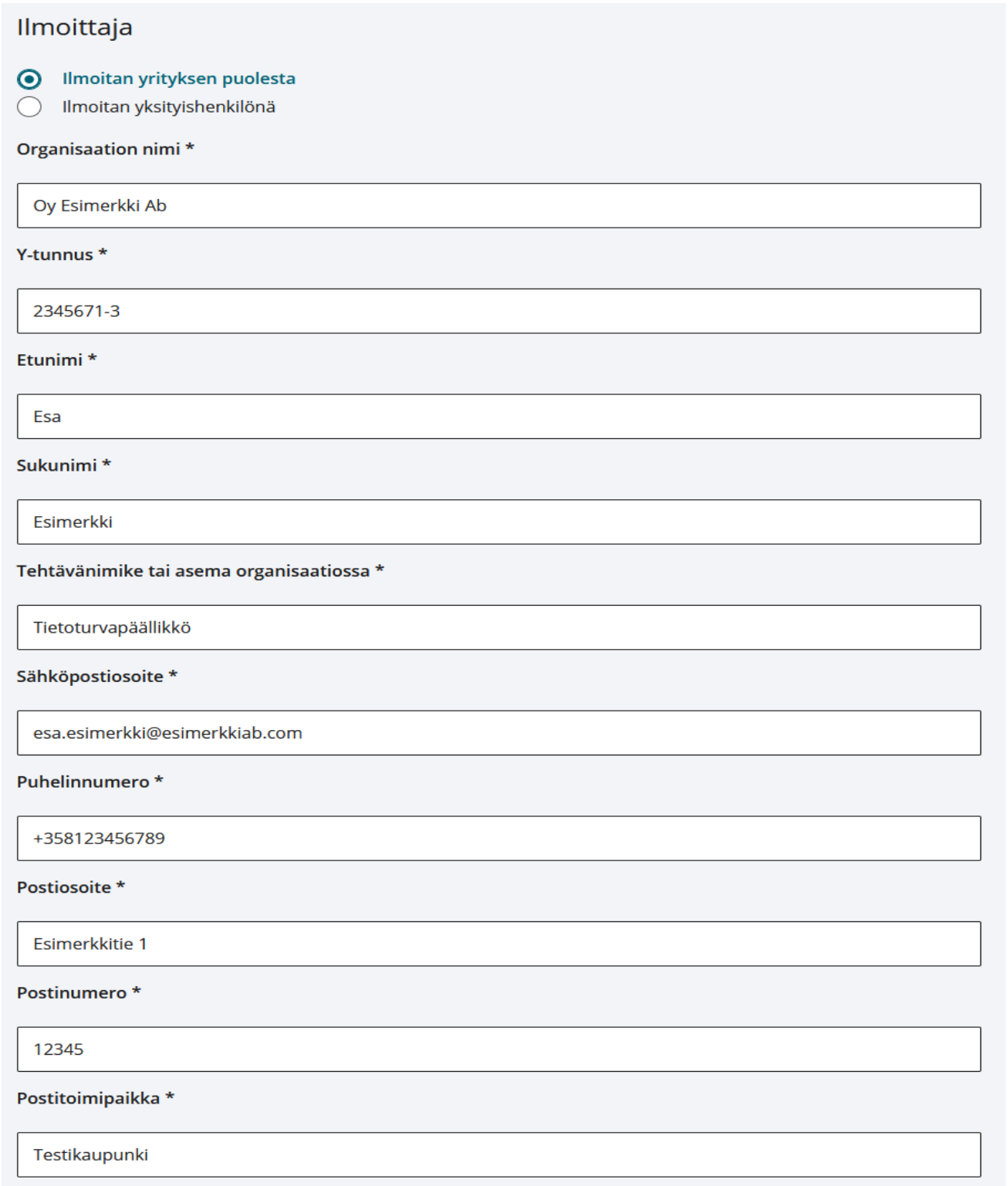
Huomioithan, että tässä yhteydessä muulla viranomaisella ei tarkoiteta Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen CSIRT-yksikköä, joka tunnetaan myös vanhalla nimellään CERT-yksikkönä. CSIRT-yksikkö saa ilmoituksessa valvovalle viranomaiselle antamanne tiedot kopiona tämän lomakkeen täyttämisen jälkeen. Yksinomaisesti CSIRT-yksikölle toimitettaville tiedoille on ensi-ilmoituslomakkeella oma erillinen alavalikkonsa, jota käsittelemme myöhemmin tässä dokumentissa.

Poikkeamatapauksissa, joiden vaikutukset ulottuvat Suomen ulkopuolelle, on täytettävä seuraavat kentät. Vaikutuksien kuvaus -kentässä voitte esimerkiksi luetella ne Euroopan unionin jäsenmaat, joihin poikkeama vaikuttaa, sekä kertoa tarkemmin poikkeaman vaikutuksista Euroopan unionin alueella. Mikäli poikkeamalla saattaa olla rajat ylittäviä vaikutuksia, mutta ensi-ilmoitusta tehdessänne varmuutta asiasta ei vielä ole, voitte myös kuvata oheiseen kenttään mahdollisia vaikutuksia ja niiden todennäköisyyttä.



Kuva 4 Rajat ylittävät vaikutukset ja lisätiedot

Seuraavaksi voitte täyttää ilmoittajan yhteystiedot, jotka voitte täyttää joko organisaation puolesta tai yksityishenkilönä, kuten Kuvan 5 esimerkissä. Muistattehan ilmoittajan yhteystietoja täyttäessä, että toimivaltainen valvova viranomainen voi olla yhteydessä ilmoitettuihin sähköpostisoitteisiin lisätietojen pyytämiseksi ja (ilmoitetun) asian/tapahtuman jatkoselvittämiseksi.



Kuva 5 Ilmoittajan yhteystiedot

Yllä olevat tiedot välittyvät organisaatiotanne valvovalle viranomaiselle, joka esimerkiksi Digitaalinen Infrastruktuuri-toimialan osalta on Liikenne- ja viestintävirasto.

Jos haluatte lähettää asian tiimoilta Kyberturvallisuuskeskuksen CSIRT-yksikölle ja/tai haluatte jakaa CSIRT-yksikölle lisätietoja, voitte valita Postitoimipaikka-tietueen alta lisälomakkeen avaavan vaihtoehdon "Tarvitsen tukea Kyberturvallisuuskeskuksen CSIRT-yksiköltä tai haluan antaa sille vapaaehtoisesti lisätietoja".

Huomaattehan, että tämän painikkeen alta esille nousseisiin kenttiin annetut tiedot välittyvät pelkästään Liikenne ja -viestintävirasto Traficomin Kyberturvallisuuskeskuksen CSIRT-yksikölle. Nämä tiedot eivät välity valvoville viranomaisille. Kyberturvallisuuslain 25 §:n mukaan CSIRT-yksikölle tämän lain mukaisten tehtävien hoitamiseksi vapaaehtoisesti luovutettua tietoa ei saa ilman tiedon luovuttaneen suostumusta käyttää tiedon luovuttajaan kohdistuvassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttajaan kohdistuvassa päätöksenteossa.

Poikkeaman tarkempi kuvaus CSIRT-yksikölle

Haittaohjelma aktivoitui tuotantoympäristössämme, nykyisen tiedon valossa päässyt verkkoomme ulkoisen USB-muistin avulla hyväksikäyttäen työntekijämme admin-tunnuksia.

Haittaohjelma on salannut tuotantoympäristömme virtualisointipalvelimet, aiheuttaen täydellisen katkon niihin kytkettyihin asiakkuuksiin ja palveluihin.

Mitä vaikutuksia poikkeamalla oli?

Poikkeama aiheutti katkoksen kaikkien asiakkaidemme palveluihin, sisältäen myös viranomaisorganisaatioita Suomessa, Ruotsissa ja Saksassa.

Toimenpiteet, joihin aiotaan ryhtyä?

- Käyttäjätunnuksien oikeuksien minimointi ja uudelleenarviointi
- Ulkoisen tietoturvapalvelun integrointi
- Ulkoisten asiantuntijoiden tuottama poikkeamaforensiikka
- Ulkoisten USB-muistien käytön estäminen yrityksen laitteissa

Poikkeamaan liittyvä tunnistetieto, esim. verkkosivun osoite, lähettäjän sähköpostiosoite tai puhelinnumero

Hash-tunniste: 1ab2ab34567c89abcd12b3a4567a8c90ab1b2c34ab567c7f8a901a234ab56789

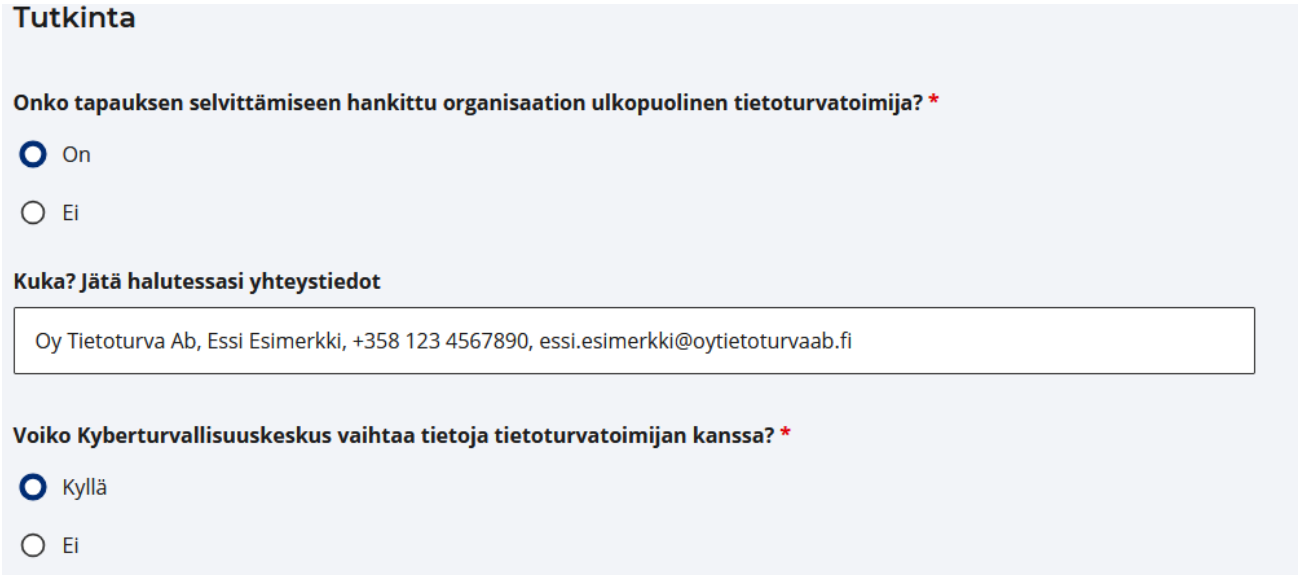
Kuva 6 CSIRT-lisälomake

Kuvassa 6 on kuvailtu referenssitapauksen mukainen lisäilmoitus CSIRT-yksikölle, johon on yleismuotoisesti kuvailtu poikkeaman tapahtumat, siitä johtuen tehdyt ensitoimenpiteet sekä poikkeamaan liittyvää tunnistetietoa. Kentän kuvauksessa lueteltujen tunnistetietojen lisäksi, voit esimerkiksi antaa ym. kentässä esimerkiksi ns. Hash-tunnisteen ja/tai ns. vaarantumisindikaattorin eli IOC-indikaattorin (engl. Indicator of

Compromise) -tunnisteen ja muuta teknistä tunnistetietoa poikkeamaan liittyen. Huomioittehan, että ensi-ilmoituksen yhteydessä CSIRT-yksikölle annettu IOC-tunniste on toimitettava myös valvovalle viranomaiselle viimeistään jatkoilmoituksen yhteydessä.

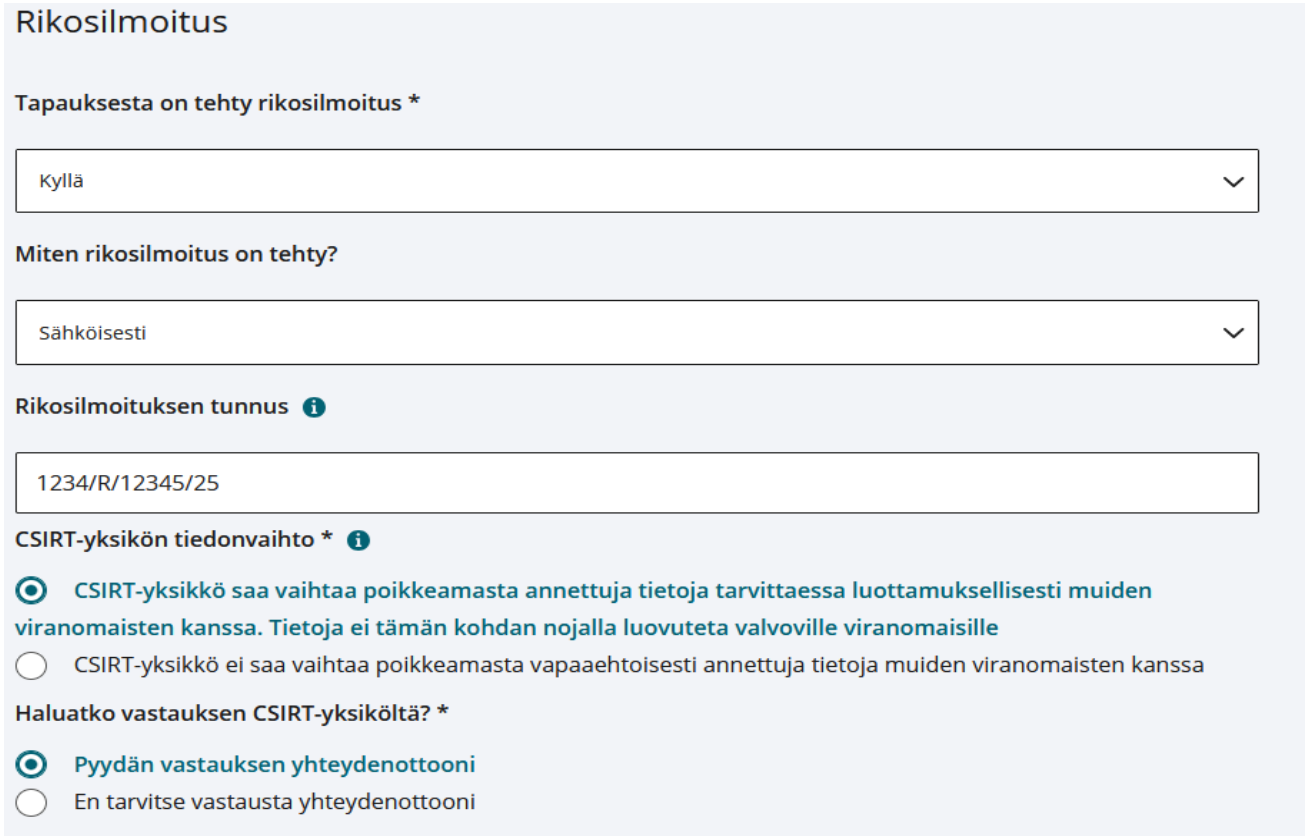
Vaarantumisindikaattorit eli IOC-indikaattorit ovat teknisiä tunnisteita tai mitattavissa olevia teknisiä havaintoja, joiden perusteella voidaan päätellä, onko kyberhyökkäys mahdollinen, parhaillaan käynnissä tai tapahtunut jo aiemmin.

Tavanomaisimmat vaarantumisindikaattorit ovat verkko-, laite-, tiedosto- ja käyttäytymispohjaisia järjestelmien tuottamia erilaisia lokitietoja. Referenssitapauksen osalta mahdolliset IOC-tietueet voisivat esimerkiksi olla lokitietoa lunnaskiristysohjelman aktivoitumisen ajankohdasta.



Kuva 7 MSSP-lisätiedot

Jos organisaatiollanne on käytössä ulkoinen tietoturvapalveluntarjoaja poikkeaman selvittämiseksi ja/tai jatkuvalla syklillä, voitte lisätä heidän yhteystietonsa Kuvan 7 mukaisiin kenttiin jos haluatte, että Kyberturvallisuuskeskuksen CSIRT-yksikkö voi olla yhteydessä mainittuun tietoturvapalveluntarjoajaan poikkeamaan liittyvissä asioissa.



Kuva 8 CSIRT-lisälomake Rikosilmoitus-osuus

Rikosilmoitus-kohdassa voitte täydentää mahdollisen rikosilmoituksen tiedot, jos olette tehneet ilmoituksen ennen ensi-ilmoituksen täyttämistä. Tarvittaessa voitte myös valita vaihtoehdon "Tullaan tekemään" ja täydentää myöhemmin tehtävissä ilmoituksissa kuten esimerkiksi jatkoilmoituksen yhteydessä myöhemmin tehtävästä rikosilmoituksesta.

Kuvan 8 alareunassa voitte myös valita haluatteko CSIRT-yksikön olevan yhteydessä teihin poikkeaman osalta, sekä antaa mahdollisen suostumuksenne luottamukselliseen viestinvaihtoon muiden viranomaisten kanssa. Haluamme tässä ohjeessa korostaa, ettei edellä mainitussa luottamuksellisessa viestinvaihdossa välitetä tietoa valvovalle viranomaiselle kyberturvallisuuslain 25 §:n mukaisesti.

Kuva 9 CSIRT-yhteystiedot

CSIRT-lisälomakkeen lopussa voitte lisätä myös yhteystiedot, johon CSIRT-yksikkö on yhteydessä poikkeaman selvittämisen tiimoilta. Nämä yhteystiedot voivat esimerkiksi olla yrityksenne SOC-tietoturvavalvomon tai teknisen asiantuntijan/asiantuntijoiden yhteystiedot.

Kun olette täyttäneet ensi-ilmoitukseen tarvittavat kentät, voitte siirtyä esikatselutilaan painamalla Jatka-painiketta. Esikatselutilassa voitte varmistaa, että olette täyttäneet poikkeamanne kannalta merkitykselliset kentät huolellisesti.

Esikatseluvaiheen jälkeen voitte täyttää sivuston alareunasta löytyvän CAPTCHA-kyselyn ja painaa lähetä painiketta, jonka jälkeen ilmoitus lähtee valitsemanne NIS2-sektorin mukaiselle valvovalle viranomaiselle. Voitte myös tulostaa poikkeamailmoituksenne tiedot lähetyksen jälkeen lomakkeen kolmannelta sivulta PDF-muodossa.

Lähettämästänne NIS2-poikkeamailmoituksesta tulee ilmoittamaanne sähköpostiosoitteeseen myös automaattinen vastaanottokuittaus, jolla voitte varmistua siitä, että ilmoitus on saapunut valvovalle viranomaiselle.

2.2 Jatkoilmoitus

Ensi-ilmoituksen jälkeen on tehtävä jatkoilmoitus 72 tunnin kuluessa merkittävän poikkeaman havaitsemista. Jatkoilmoituksen pääasiallinen tarkoitus on tarkentaa ensi-ilmoituksessa annettuja tietoja esimerkiksi tapahtuman juurisyystä, tarkemmista vaikutuksista ja vakavuudesta.

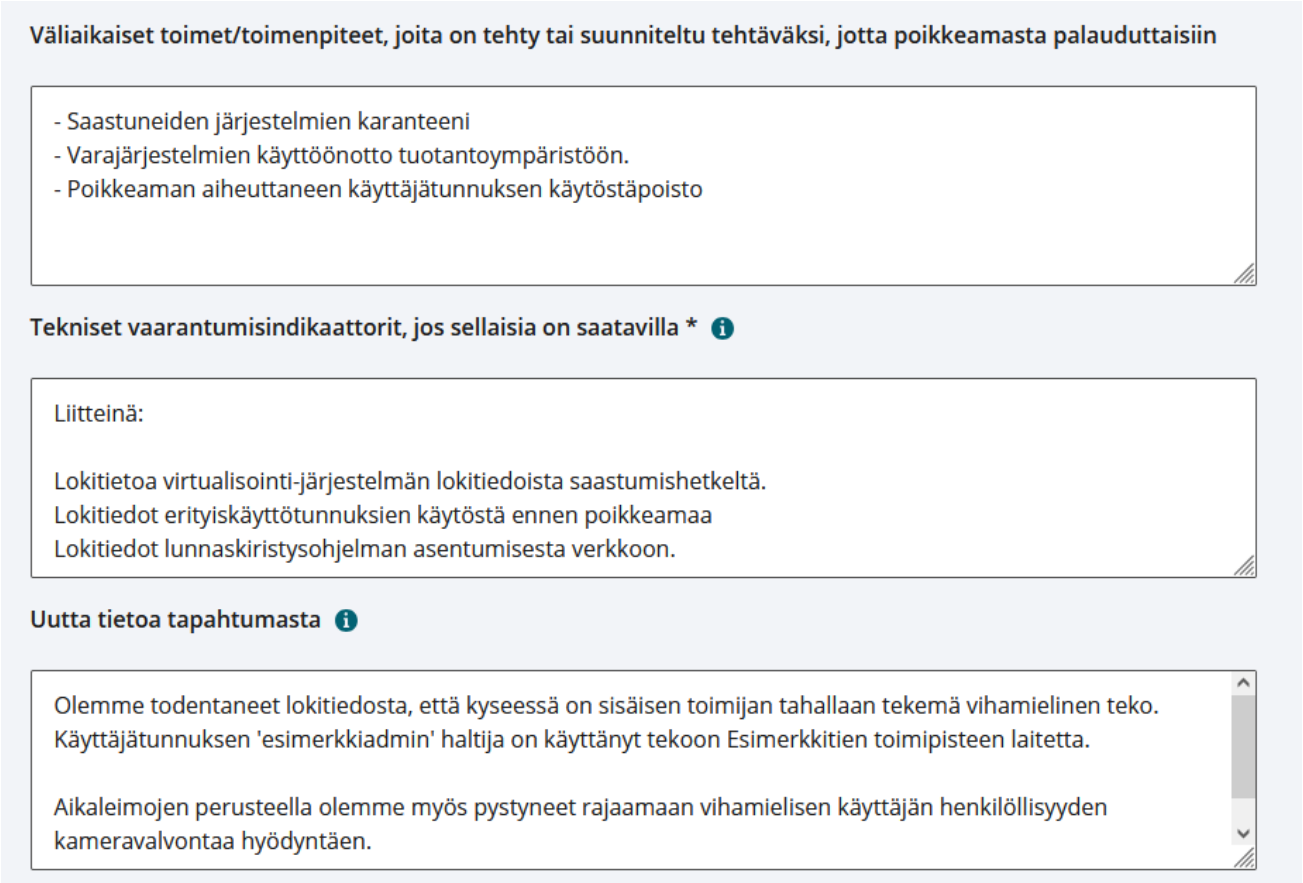
Jatkoilmoitusta täyttäessänne tarvitsette ensi-ilmoituksen vastaanottokuittausviestissä saamanne uniikin asianumeron, joka on muotoa '123456'. Löydät edellä mainitun asianumeron sähköpostiotsikolla "Vastaanottokuittaus" ensi-ilmoituksessa saamassanne sähköpostissa, joka on lähetetty ilmoittajan sähköpostiosoitteeseen.

Kuva 10 Jatko-ilmoituksen perustiedot

Valitessanne sopivaa vaihtoehtoa vaikutuksen laajuuteen on hyvä huomioida, että kyseissä kohdassa on ajateltu ns. kokonaisvaltaisen vaikutuksen periaatetta. Näin ollen, valitkaa kyseisessä kohdassa se vaihtoehto, joka kuvaa poikkeaman vaikutuksen kokonaisvaltaisesti, riippumatta siitä, että onko vaikutus täydellinen palvelukatko tai esimerkiksi viive palvelun toiminnassa esimerkiksi DDoS-palvelunestohyökkäyksen johdosta.

Esimerkkitilanteena voidaan käyttää tapausta, jossa 10% yrityksen palveluista on täydellisen katkon vaikutuksen alainen sekä 20% palveluista kärsii merkittävästä viiveestä, mutta palvelu toimii rajatulla määrällä käyttäjiä. Tässä tapauksessa tulisi valita vaihtoehto "Erittäin laaja vaikutus", sillä merkittävien vaikutuksien ylittää vaihtoehdoissa rajatun 15% rajan. Yleisellä tasolla voidaan sanoa, että jos palveluun kohdistuu merkittävä vaikutus poikkeaman johdosta, se on huomioitava tätä kohtaa täyttäessä.

Arvioidessanne poikkeaman laatua, vakavuutta sekä vaikutusta voitte täydentää ensi-ilmoituksessa antamianne ensitietoja esimerkiksi tarkentamalla vaikutuksien rajausta palvelukohtaisesti. Voitte myös kirjata alustavia arvioita vaikutuksien käyttäjämääristä sekä näiden käyttäjien palveluiden toimivuudesta (Esimerkki: täydellinen vai osittainen katko, kaikilla käyttäjillä vai osalla käyttäjistä).



Kuva 11 Toimenpiteet, IOC-tietueet ja uudet tiedot

Yllä olevassa Kuvassa 11 kuvattujen väliaikaisten toimien laatikossa voitte kuvailla esimerkiksi väliaikaistoimenpiteitä, joita on tehty poikkeaman vaikutuksien rajaamiseksi. Tämänkaltaisia toimenpiteitä voivat olla esimerkiksi varmuuskopioiden käyttöönotto, käyttöoikeuksien rajaaminen, varajärjestelmien hyödyntäminen sekä muut luonteeltaan väliaikaiset sekä nopeasti toteuttavat ensitoimenpiteet.

Tietoturvapoikkeamaan liittyvät tekniset tunnistetiedot (IOC, engl. Indicators of Compromise) voi ilmoittaa teknisten vaarantumisindikaattorien kentässä, jos IOC-tietueita on saatavilla.

Jatkoilmoitusta tehdessä on yleistä, että poikkeaman tapahtumankulku on tarkentunut ensi-ilmoituksen jälkeen. Uuden tiedon kentässä voitte tarkentaa ensi-ilmoituksessa antamianne tietoja sekä antaa lisää tietoa. Referenssitapauksen osalta uusi tieto voi olla esimerkiksi varmentunut hyökkäysvektori tai sisäisen toimijan varmentuminen.

Voitte myös mainita tässä kentässä toimenpiteitä, joilla olette pyrkineet varmistamaan, ettei nykyistä poikkeamaa voisi tapahtua uudelleen tulevaisuudessa. Referenssitapauksen osalta hyvänä esimerkkinä toimisi esimerkiksi toimenpide, jossa ulkoisten USB-muistien hyödyntäminen estettäisiin täysin yrityksen laitteilta ilman erillistä hyväksyntää.

2.3 Väliraportti

Väliraportin tarkoituksena on antaa väliaikatietoa poikkeaman selvittämisen etenemisestä poikkeaman jatkoilmoituksen jälkeen. Väliraportissa voitte kuvailla, miten poikkeaman käsittely on organisaationne osalta edennyt ensi-ilmoituksen ja

jatkoilmoituksen jälkeen ja mikä on asian tila tällä hetkellä. Ilmoita myös poikkeaman käsittelyyn osallistuneet toimijat (viranomaiset, tietoturvapalveluita tarjoavat yritykset yms.).

Väliraporttia voi hyödyntää esimerkiksi pitkäaikaisissa tapauksissa, joissa poikkeamasta palautuminen vie merkittävästi pidempään kuin kyberturvallisuuslain ilmoitusrajat spesifioivat. Referenssitapauksessa olisi mahdollista, että yritys antaisi väliraportin valvovalle viranomaiselle, kun poikkeamasta palautumisen aikataulu olisi tarkentunut.

Väliraporttia voi myös hyödyntää tapauksissa, jossa poikkeaman selvittämisessä on noussut esille asioita, joilla on huomattava merkitys tapauksen selvittämisen kannalta. Referenssitapauksessa merkitykselliseksi on noussut se, että organisaation asiakkuuksiin kohdistuvat vaikutukset saatiin minimoitua odotettua nopeammin, kun organisaation varajärjestelmät pystyivät palauttamaan organisaation palvelut täysmääräisesti toimintaan ennen tuotantoympäristön palautumista.

Asianumero *

123456

Poikkeaman käsittelyn edistyminen ja tilannepäivitys *

Poikkeaman tutkinta päättynyt, rikosoikeudellinen prosessi etenee asianmukaisesti. Asiasta on tehty sähköinen rikosilmoitus ja Helsingin poliisilaitos on aloittanut esitutkinnan epäillystä törkeästä tietomurrosta numerolla 1234/R/5678/25.

Poikkeamasta palautuminen on hyvällä mallilla, arvioitu täydellinen palautumisaika n. 1 vko, varajärjestelmät toteuttavat tuotantoympäristön ylläpidon poikkeaman ajan. Poikkeaman vaikutus asiakkaisiin loppunut n. klo 04.30, kun varajärjestelmät aktivoitiin tuotantoon.

Tutkintaan osallistuneet Oy Tietoturva Ab, Poliisi sekä Kyberturvallisuuskeskus.

Lisätiedot

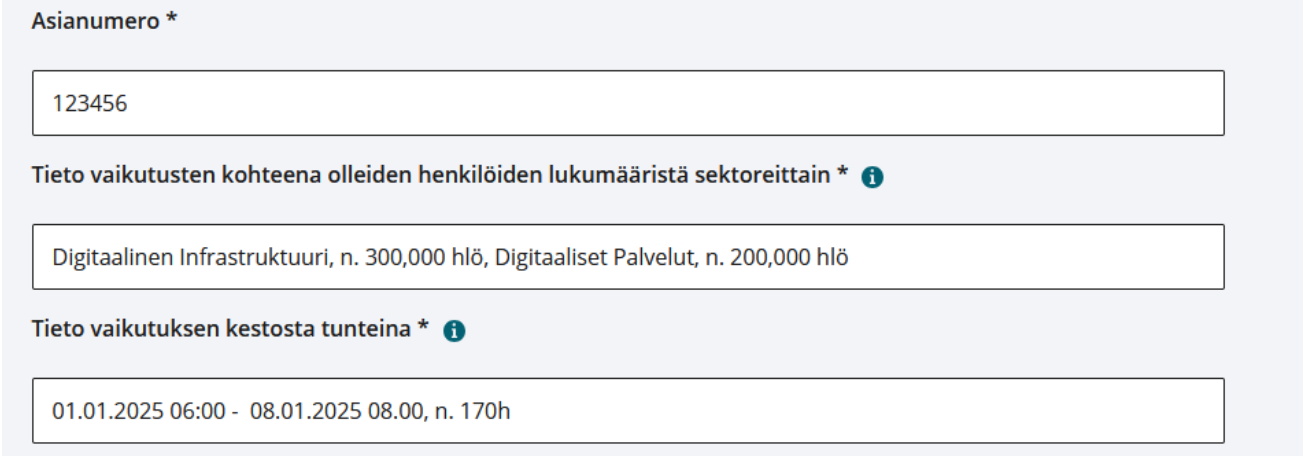
Olemme todentaneet lokitiedosta, että kyseessä on sisäisen toimijan tahallaan tekemä vihamielinen teko. Käyttäjätunnuksen 'esimerkkiadmin' haltija on käyttänyt tekoon Esimerkkitien toimipisteen laitetta.

Aikaleimojen perusteella olemme myös pystyneet rajaamaan vihamielisen käyttäjän henkilöllisyyden kameravalvontaa hyödyntäen.

Kuva 12 Väliraportti

2.4 Loppuraportti

Loppuraportti on täytettävä kuukauden (1 kk) kuluessa jatkoilmoituksen toimittamisesta tai, jos kyseessä on pitkäkestoinen poikkeama, kuukauden (1 kk) kuluessa poikkeaman käsittelyn päättymisestä. Tämän ilmoitustyypin tarkoituksena on toimia viimeisenä raporttina valvovalle viranomaiselle, jossa kuvaillaan poikkeamaan liittyvät tiedot ns. täydellisenä.



Kuva 13 Kesto & Henkilömäärät

Loppuraportin toisessa kentässä pyydetään arvioimaan tietoturvapoikkeaman vaikutusta käyttäjäkohtaisesti kunkin kyberturvallisuuslaissa valvottavan sektorin osalta. Tätä vaikutusarviota tehdessä on kuitenkin huomioitava, ettei vaikutuksen täydellisten vaikutusten arviointi ole välttämättä mahdollista. Näin ollen, edellä mainitussa kentässä voitte antaa pyöristetyn arvion poikkeaman vaikutuksista, jonka tarkkuus määrittyy olemassa olevan tiedon sekä poikkeaman vakavuus- ja vaikutusasteikon mukaisesti.

Arvioidessanne vaikutuksen kestoa kolmannessa kentässä, voitte esimerkiksi käyttää Kuvassa 13 esiteltyä aikajana-tapaa poikkeaman keston kuvailemisessa.

Edellä mainitussa kentässä voi myös kuvailla erillisiä ajanjaksoja, jos poikkeaman vaikutukset ovat esimerkiksi rajautuneet kolmeen erillisen ajanjaksoon poikkeaman johdosta. Erillisten vaikutusaikojen kuvaileminen on hyvinkin tarkoituksenmukaista esimerkiksi DDoS-palvelunestohyökkäyksistä johtuvissa poikkeamailmoituksissa, joissa on yleistä, ettei poikkeaman vaikutus ole yhtäjaksoista vaan aaltoilevaa riippuen DDoS-hyökkäyksen volyymistä.

"Yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista"-kentän voi täyttää oheisen ohjeen mukaisesti, sekä seuraten Kuvassa 14 annettua esimerkkiä.

Kuvailkaa tarkasti, mitä on tapahtunut. Mainitse mahdolliset virheet, häiriöt tai odottamattomat tapahtumat. Arvioi, kuinka merkittävä tai kriittinen poikkeama on toiminnan kannalta. Voitte käyttää asteikkoa (esim. vähäinen, kohtalainen, vakava) tai kuvata vakavuutta sanallisesti. Kuvaa, mitä vaikutuksia poikkeamalla on ollut tai voi olla. Pohdi esimerkiksi, miten poikkeama on vaikuttanut toimintaan, tuotteisiin, palveluihin tai turvallisuuteen. Jos poikkeamalla on taloudellisia tai ajallisia seurauksia, mainitse myös nämä.

Poikkeaman juurisyynä oli sisäisen toimijan aiheuttama lunnaskiristysohjelma, joka asennettiin sisäisiä järjstelmänvalvoja-tunnuksia käyttäen. Edellä mainittu lunnaskiristysohjelma salasi suurimman osan tuotantojärjestelmistämme.

Poikkeaman vaikutukset olivat liiketoimintakriittisiä yrityksen toiminnalle, sillä kaikki yrityksen tuotantojärjestelmät poistuivat käytöstä ennen varajärjestelmien nousua. Käytännöllisesti katsoen, suurin osa yrityksemme palveluista oli keskeytynyt poikkeaman johdosta.

Poikkeamalla oli myös laajoja finansiaalisia sekä ajankäytöllisiä vaikutuksia yrityksemme toimintaan, sillä poikkeamasta johtuen useampi asiakasyrityksiemme palvelutasosopimuksiin liitetyt sanktiomenettelyt käynnistyivät poikkeaman johdosta. Poikkeamasta aiheutui myös n. 120 henkilötyötunnin päivystysluontoista työtä sekä ulkoisen tietoturvapalveluntarjoajan asiantuntijoille että yrityksemme työntekijöille.

Poikkeaman tutkinnan aikana todettiin, että yrityksemme tietoturvapolitiikasta löytyi puutteita erityisoikeudellisten käyttäjätunnuksien hallinnan ja valvonnan osalta sekä ulkoisten USB-muistien käyttöpolitiikassa. Nämä puutteet on huomioitu poikkeaman jälkimainingeissa luodussa jälkiraportissa sekä niiden mukaiset korjaustoimenpiteet on tehty, jottei samanlaista poikkeamaa voisi toteutua jatkossa.

Kuva 14 Kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista *

Täyttäessäsi Kuvan 15 mukaisia kategorisointikenttiä, valitse kaikki kentät, jotka kuvailevat poikkeamassa esiintyneitä asianhaaroja. Referenssitapauksessa pääasiallinen ryhmittely sopisi vaihtoehtoon "Tarkoitukselliset sisäiset teot", mutta tapauksen luonteen vuoksi on myös valittu fyysisen vahingoittamisen/hyväksikäytön/varkauden vaihtoehto, sillä mahdollisen kiristyshaittaohjelman tarkoituksena on voinut olla kiristysvaatimuksen esittäminen poikkeaman kohteena olleelle organisaatiolle.

Osoitus juurisyykategoriasta *

Vihamieliset teot

Juurisyyn alakategoria *

Tarkoituksellinen fyysinen vahingoittaminen/hyväksikäyttö/varkaus, Tarkoitukselliset sisäiset teot

Tietoa vaikutuksen kohteena olleista teknisistä omaisuuseristä *

Palvelimet ja verkkoalueohjaimet, Sovellus, Teollisuusjärjestelmä, Työasema, Verkkosivu

Poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyyppi

Pääasiallinen juurisyy: Vihamielinen teko, sisäinen uhka
Lisätekijä: Puuttellinen prosessi irtisanomistilanteissa korotettujen käyttöoikeuksien osalta.

Kuva 15 Poikkeaman juurisyiden sekä vaikutuksien kategorisointi.

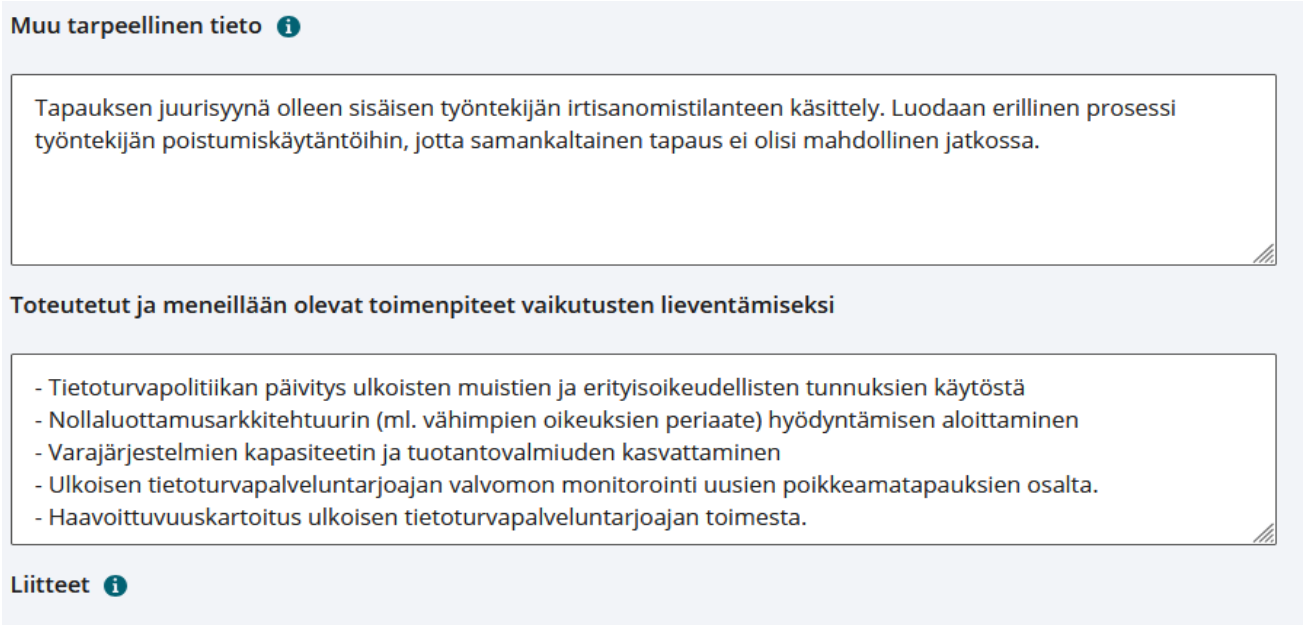
Valitessanne vaikutuksen kohteena olevia teknisiä omaisuuseriä, valitsettehan järjestelmät, joihin kohdistui merkittävää vaikutusta poikkeaman johdosta.

Referenssitapauksessa vaikutuksen ollessa laaja-alainen on huomioitava, että pääasiallinen vaikutus kohdistui ensimmäisenä valittuun kategoriaan, eli "Palvelimet ja verkkoalueohjaimet"-vaihtoehtoon.

Kuvaa, mikä todennäköisesti aiheutti poikkeaman. Jos poikkeama johtui useammasta uhasta tai juurisyystä, valitse pääasiallinen syy ja mainitse myös muut mahdolliset tekijät. Voitte täyttää edellä mainitun kentän esimerkiksi oheisen mukaisesti:

- *'Pääasiallinen syy: Inhimillinen virhe, lisätekijä: Puutteellinen prosessi.'*

Jos olette toteuttaneet poikkeaman selvityksen yhteydessä laajemman juurisyyanalyysin, kuvailu voi sisältää tarkempia yksityiskohtia poikkeamaan johtaneista juurisyistä sekä niihin liittyvistä prosesseista.



Kuva 16 Muut tiedot ja toimenpiteet

Muun tarpeelliseen tiedon kenttään voitte kirjoittaa kaiken sellaisen tiedon, joka ei sopinut aiempiin kenttiin, mutta joka on kuitenkin tärkeää poikkeaman käsittelyn kannalta. Tämä voi sisältää esimerkiksi erityistilanteet, taustatiedot tai lisähuomiot, jotka selkeyttävät poikkeaman laajuutta tai sen syitä.

"Toteutetut ja meneillään olevat toimenpiteet vaikutusten lieventämiseksi"-kenttään voitte kuvailla yrityksenne toteuttamien toimenpiteiden nykytilannetta, sekä kyseisten toimenpiteiden jatkuvuutta tulevaisuudessa. Kuvan 16 mukaisesti voitte myös kertoa tässä kentässä, jos olette jatkaneet toimintaa esimerkiksi ulkoisen tietoturvapalveluntarjoajan kanssa poikkeaman jälkeenkin.

Lisää liitteeksi asiakirjat, raportit, kuvat tai muut tiedostot, jotka tukevat tai täydentävät poikkeaman kuvausta. Varmista, että liitteet ovat hyväksyttävissä tiedostomuodoissa (esim. PDF, DOCX, XLSX, JPG, PNG). Nimeä tiedostot selkeästi ja kuvaavasti, jotta niiden sisältö on helposti ymmärrettävissä.

Huomioi mahdolliset tiedostokokorajoitukset. Jos tiedostosi on suuri, harkitse sen pienentämistä tai jakamista useampaan osaan, jotta liitteiden lataaminen sujuu

ongelmitta. Voitte lisätä loppuraportin liitteeksi myös sisäisiä raportteja, juurisyyanalyysejä sekä muita poikkeamaan liittyviä dokumentteja

2.5 Vapaaehtoinen ilmoitus valvovalle viranomaiselle

Tässä kohdassa voit tehdä vapaaehtoisen ilmoituksen valvovalle viranomaiselle muista häiriöistä kuin merkittävistä poikkeamista. Tiedot välittyvät myös Traficomin Kyberturvallisuuskeskuksen CSIRT-yksikölle. Jos kuitenkin haluat tehdä ilmoituksen vain CSIRT-yksikölle, löydät vapaaehtoisen ilmoituksen myös suoraan Kyberturvallisuuskeskuksen etusivulta.

Kaikki saavat tehdä vapaaehtoisia ilmoituksia poikkeamista, uhkista ja läheltä piti -tilanteista. Vapaaehtoisen ilmoituksen voi tehdä esimerkiksi kyberturvallisuuslain mukainen toimija, yhteiskunnalle tärkeällä toimialalla toimiva pienyritys tai yksityishenkilö.

Näiden ilmoituksien avulla Kyberturvallisuuskeskus saa hyödyllistä tietoa kansallisessa kyberympäristössä tapahtuvista ilmiöistä ja kehityssuunnista, joten toivomme teidän tekevän myös vapaaehtoisia ilmoituksia matalalla kynnyksellä.

Vapaaehtoinen ilmoitus on jaettu kolmeen erilliseen kategoriaan.

2.5.1 Poikkeama

Vapaaehtoisen poikkeamailmoituksen käyttötarkoitus on ilmoittaa valvovalle viranomaiselle ei-merkittävästä poikkeamasta.

Kyberturvallisuuslaissa poikkeama on määritelty-oheisesti:

"Poikkeamalla tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden;"

Ei-merkittävän poikkeaman osalta tarkoitetaan poikkeamaa, jonka vaikutus yrityksen toimintaan on vähäinen. Tämänkaltaisia tilanteita ovat esimerkiksi yksittäisen työntekijän ei-erityisoikeudellisen käyttäjätunnuksen ja salasanan kalastusyrityksen (engl. phishing) onnistuminen.

2.5.2 Kyberuhka

Voit myös ilmoittaa valvovalle viranomaiselle kyberuhkista, jotka ovat tulleet esille yrityksenne toiminnassa, kuten esimerkiksi tietoturvatutkinnassa esille tulleet uudet haavoittuvuudet ohjelmistoissa.

Kyberturvallisuuslaissa kyberuhka on määritelty oheisesti:

"Kyberuhkalla tilannetta, tapahtumaa tai toimintaa, joka toteutuessaan voi vahingoittaa tai häiritä viestintäverkkoja tai tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita henkilöitä tai muulla tavoin vaikuttaa näihin haitallisesti;"

Käytännön esimerkkinä kyberuhasta voi myös olla esimerkiksi yrityksen sähköpostisoitteisiin tehty laajamittainen tietojenkalastusviestikampanja, jolla ei ole saavutettu tunnuksien haltuunottoa.

2.5.3 Läheltä piti-tilanne

Läheltä piti-tilanne on tarkoitettu tilanteisiin, jossa tapahtuma, joka olisi voinut vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden mutta jonka toteutuminen onnistuttiin estämään tai joka ei toteutunut satunnaisen syyn vuoksi.

Tämänkaltaisia tilanteita ovat esimerkiksi työntekijän salasanan kalasteluyrityksen (engl. phishing) -hyökkäyksen onnistuminen, mutta kuitenkin niin, ettei tällä tavoin haltuun saatuja tunnuksia ole voitu hyödyntää esimerkiksi siitä syystä, että käytössä on monivaiheinen tunnistautuminen (engl. 2FA/MFA).

Mahdolliset kehitysideat ja palautteet tästä ohjeistuksesta voi lähettää sähköpostitse osoitteeseen nis.valvonta.ktk@traficom.fi.

Käytäthän sähköpostisi otsikossa oheista tunnistetta: [NISLO]