Yhteydenotto poliisiin

Hätätilanne/kiireellinen tilanne: 112

Kiireetön rikosilmoitus:

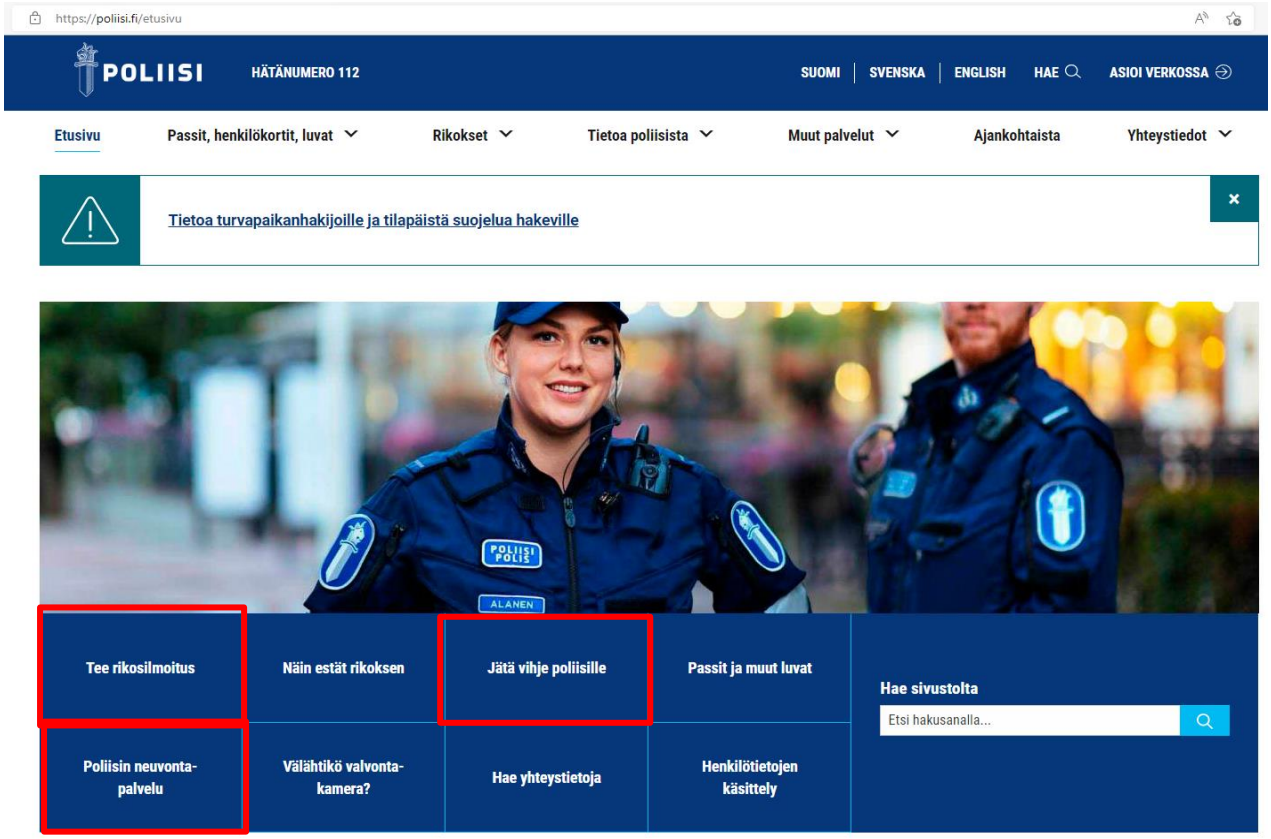
- Ensisijaisesti: Sähköinen rikosilmoitus: https://asiointi.poliisi.fi/fi/yritys/rikos
- Palvelu on poissa käytöstä klo 22.45 - 06.00.
- Sähköisen rikosilmoituksen asiointipalveluun kirjautuminen edellyttää vahvaa tunnistautumista

- Puhelimitse poliisiaseman palvelupäivystykseen (vain jos muita ilmoituskanavia ei ole käytössä)
- Paikan päällä poliisiaseman palvelupäivystykseen

Yleisneuvonta ja apu kiireettömissä asioissa (esim apua rikosilmoituksen tekoon): Poliisin valtakunnallinen neuvontapuhelin 0295 419 800 (arkisin klo 8-16.15). Lisätietoa: https://poliisi.fi/neuvontapalvelu

Rikoksiin liittyvät vihjeet (myös anonyymi ilmoitus onnistuu):

- Poliisin Nettivinkki: https://poliisi.fi/nettivinkki
- Vihjeyhteystiedot poliisilaitoksittain: https://poliisi.fi/vihjeyhteystiedot



Pikalinkit em. palveluihin löytyvät www.poliisi.fi-verkkosivuston etusivulta

Alkutoimiohjeet asianomistajaorganisaatiolle tietoverkkorikostapauksessa

Tietojärjestelmiin tai muuhun tietotekniseen ympäristöön kohdistuneiden rikosten selvittämisessä hyödynnetään samankaltaisia tietoja kuin teknisen häiriötilanteen diagnostiikassakin. Esimerkiksi palvelunestohyökkäyksessä rikostutkinnan tukena toimivat hyvin lokit, joissa perusasiat ovat hyvällä tasolla. Palvelunestohyökkäyksen lisäksi tietoverkkorikoksia ovat esimerkiksi yritykseen kohdistuneet tietomurrot ja haittaohjelmat. Mikäli epäilee rikosta, on asiasta hyvä ilmoittaa poliisille epäselvissäkin tapauksissa. Poliisi arvioi ilmoituksen jälkeen, täyttääkö teko jonkin rikoksen tunnusmerkistön.

Pitkäkestoisen ja laajan rikosasian esitutkinnan turvaamisen kannalta tärkeimmät asiat voidaan jakaa kahteen kategoriaan: 1. Rikoksen kohteena olevaa organisaatiota eli rikosasian varsinaista asianomistajaa koskeviin tietoihin. Näihin kuuluvat tiedot sekä organisaatiosta että sitä edustavista henkilöistä. 2. Rikoksen kohteena olevaa tietojärjestelmää koskeviin tietoihin.

Poliisi suosittelee, että organisaatiossa otettaisiin rikosilmoituksen tekeminen ja todistusaineiston talteenotto osaksi tietoturvaprosesseja. Mikäli mahdollista, rikosta epäiltäessä esitutkinnan turvaamiseksi asianomistajaa pyydetään olemaan tekemättä korjaavia toimenpiteitä ennen kuin tutkinnan kannalta tarvittavat taltioinnit (kappaleet 3.1-3.5) on tehty. Tässä dokumentissa on kerrottu, mitä alkutoimia ja taltiointeja organisaation olisi hyvä suorittaa tietoverkkorikostapauksessa.

1. Tekotapa ja vaikutukset

- Tapahtumakuvaus epäillystä rikoksesta, hyökkäyksen vaikutuksista ja sen kestosta sekä ilmoitus rangaistusvaatimuksesta.
- Alustava arvio aiheutuneista vahingoista. Tarkka tieto vahinkojen määrästä ja vahingonkorvausvaatimuksesta tarkentuu tutkinnan edetessä, mutta alustava arvio auttaa esitutkinnan alkuvaiheessa. Vahingonkorvauksen määrää arvioitaessa kannattaa huomioida myös kaikki tilanteeseen käytetyt henkilötyötunnit.

2. Tiedot organisaatiosta

- Organisaation eli oikeushenkilön tiedot
- Virallinen nimi
- Y-tunnus
- Organisaation kotipaikka sekä toimipisteen nimi ja sijainti
- Organisaation laillinen edustaja

2.1 Organisaation edustajan ja varahenkilön tarkat yhteystiedot:

- Sukunimi, etunimi, henkilötunnus
- Tehtävänimike
- Puhelinnumero ja sähköpostiosoite
- Edustusoikeuden peruste (esim. asemavaltuutus)
- Varsinaisen edustajan lisäksi organisaation olisi hyvä valita myös tekninen yhteyshenkilö, joka osaa vastata järjestelmiin liittyviin kysymyksiin
- Teknisen yhteyshenkilön yhteystiedot

2.2 Tiedot mahdollisista alihankkijoista ja asiakkaista sekä niiden yhteyshenkilöt

- Vastaavat tiedot kuin kohdissa 2. ja 2.1
- Alihankkijalla tarkoitetaan mm. rikoksen kohteena olevan palvelun taustalla olevaa konesalipalveluntarjoajaa.

- Asiakkaalla tarkoitetaan palvelun omistajaa.
- Rikoksen kokonaiskuvan hahmottamiseksi, asianomistajien selvittämiseksi ja esitutkinnan suorittamiseksi on tärkeää ilmoittaa myös kaikista niin sanotuista ”sijaiskärsijöistä”, jotka eivät ole olleet esim. varsinaisen hyökkäyksen kohteena, mutta joiden toiminta on verkon-rakenteesta johtuen kärsinyt.

2.3 Lupa jakaa tietoja muiden tapahtuman selvittelyyn osallistuvien tahojen kanssa

- Poliisi ja muut tapauksen selvittelyyn liittyvät tahot (esim. Kyberturvallisuuskeskus tai SOC) tarvitsevat organisaation luvan, jotta voivat jakaa tietoja ja havaintoja ristiin. Mikäli organisaatio antaa luvan tietojen vaihtoon, asian voi ilmoittaa jo rikosilmoituksen tekovaiheessa.

3.1 Tiedot tietojärjestelmästä ja sen roolin kuvaus

- Rikoksen kohteena olevasta tietojärjestelmästä ja sen käyttötarkoituksesta tulisi laatia lyhyt ja ajantasainen kuvaus pelkän palvelunimen lisäksi. Palvelun käyttötarkoitus voi olla olennainen tieto rikosasian selvittämisen kannalta.
- Lyhyt kuvaus hyökkäyksen/poikkeaman vaikutuksista organisaatioon, jotta poliisi osaa arvioida teon vakavuutta.
- Kuvaus hyökkäyksen kohteena olevan tietojärjestelmän teknisistä yhteyksistä ja rajapinnoista (verkko- ja palvelindokumentaatio) sillä tarkkuudella, että hyökkäyksen todellinen kohde ja hyökkäyksessä mahdollisesti lamaantunut laitteisto voidaan tunnistaa. Tarvittaessa myös tieto, mistä kohdista on olemassa lokia ja mitä on varmuuskopioitu minnekin.
- Mikäli käytössä on virtuaalikoneita, RAM-dumpin ottaminen, snapshotin ottaminen ja jäädyttäminen rikoksen kohteena olleesta koneesta. Tätä kannattaa harjoitella jo etukäteen.
- Rautakoneiden osalta suunnitelma siitä, kuka tekee ensitoimet. Tämän henkilön ei tarvitse olla poliisi, jos omasta SOC-toiminnosta tai vastaavasta löytyy osaaminen ottaa muistidumppi yms.

Karkeimmillaan dokumentaatiosta tulisi käydä ilmi yhteys ulkoverkon reitittimeltä hyökkäyksen kohteeseen ja niiden käyttämät IP-osoitteet sekä muut tekniset tiedot. Muita teknisiä tietoja voivat olla esimerkiksi reitittimen tyyppi ja palvelimen käyttämät ohjelmistot kuten WEB-palvelimen tuotteet.

3.2 Tapahtumalokit

Organisaation tulisi omistaa omat lokinsa ja retentioaikojen olla tarpeeksi pitkiä (mieluiten vuosia). Jos palvelimen edustalle on asennettu kuormantasaajia tai palomuurilaitteistoa, joka kirjoittaa tapahtumalokia, kannattaa lokin sisältö tarkastaa hyvissä ajoin, jotta voidaan varmistua, että lokitetaan oikeita asioita. Esimerkiksi osa yleisesti käytössä olevista kuormantasaus- ja palomuurilaitteistoista kirjoittaa lokia verkkoyhteyksistä siten, että se maskeeraa sisään tulevat verkkoyhteydet omalla sisäverkon IP-osoitteella.

Lokin sisällöstä on hyvä varmistaa myös se, että se sisältää tarkat aikaleimat, lähde- ja kohdeosoitteet ja muut perusasiat. Lisäksi lokien formaatti kannattaa dokumentoida ja lokien käytettävyys varmistaa siltä osin, että ne ovat saatavissa laitteistosta luettavassa (teksti)muodossa ulos ja niiden käsittely onnistuu tavallisilla työkaluilla. Lokit tulisi toimittaa poliisille aina sellaisenaan, mutta kaikki stilisoitu tai analysoitu lokitietokin otetaan mielellään vastaan alkuperäisen lisäksi. Kaikki alkuperäisestä muuttunut data tulee kuitenkin merkitä selvästi muokatuksi ja sen tulisi toimia vain alkuperäisen datan tukena. Lokia tarvitaan usein myös selvästi hyökkäystä tai poikkeamaa edeltävältä ajalta sekä sen jälkeen, jotta saadaan näyte ns. normaalista tilasta.

Jos tietyllä ajanjaksolla havaitaan tavallista enemmän poikkeavaa verkkoliikennettä, kuten matalan volyymin palvelunestohyökkäyksiä tai porttiskannauksia, kannattaa tapahtumalokit ottaa talteen.

Mikäli organisaatio on tehnyt hyökkäyksestä alustavaa analyysiä ja tunnistanut tietoturvapoikkeamaan/verkkohyökkäykseen liittyviä tunnisteita, kuten hyökkäyksessä käytetyn IP-osoitteen, tulisi tiedot niistä toimittaa poliisille niin pian kuin mahdollista. Tämä mahdollistaa poliisin tutkintatoimien nopean käynnistämisen.

3.3 Verkkolokit tietoliikenneoperaattorilta tai palomuurilaitteistosta

Verkkoliikenteestä kirjoitetaan ymmärrettävästi hyvin eri tasoista lokia liikennemääristä riippuen, mutta varsinkin palvelunestohyökkäyksissä niistä tulisi olla perustiedot saatavilla.

- Hyökkäyksen tarkat aikaleimat aikavyöhyketietoineen
- Hyökkäyksen lähde- (myös väärennetyt) ja kohdeosoitteet
- Tietoliikenteen tyyppi: protokolla- / porttitiedot
- Hyökkäyksen volyymi: ppt- / bps-tiedot (numeeriset ja graafiset jos mahdollista)

3.4 Sähköpostit

Mikäli tutkittavaan tapaukseen liittyy sähköpostiviesti, esim. kalasteluviesti tai haitallinen liitetiedosto, tulee se ehdottomasti säilyttää tutkintaa varten. Se kannattaa tallettaa kokonaisena viestitiedostona liitteineen ja header-tietoineen poliisille toimittamista varten. Viestin välittäminen suoraan sähköpostiohjelmasta poliisin sähköpostiosoitteeseen ”välitä”-toiminnon avulla ei ole oikea toimintatapa, sillä se muuttaa alkuperäisen viestin header-tiedot ja haitallinen liitetiedosto aiheuttaa myös riskin.

3.5 Muut mahdolliset tiedot

Lisäksi pyydämme toimittamaan meille kaiken muun kiinnostavan materiaalin, mikä teidän mielestänne liittyy epäiltyyn rikokseen. Tässä tapauksessa olemme esimerkiksi kiinnostuneita mahdollisista lunnasvaatimuksista yms.