Kyberrikos on poliisiasia

Opas yrityksille kyberrikostutkinnan kulusta

oletietoinen.fi

Opetus- ja kulttuuriministeriö

POLIISI
POLIISIAMMATTIKORKEAKOULU

JYVSECTEC
by jamk

Sisällysluettelo

Julkaistu: maaliskuu 2021

Johdanto

Kyberrikollisuus* on varteenotettava riski toimialasta ja koosta riippumatta kaikille yrityksille Suomessa. Kyberrikollisuuden määrä on kasvanut jatkuvasti ja yksittäisten tekojen vaikutukset yrityksille vaihtelevat tapauksen mukaan vähäisestä kriittiseen. Rikoksen kohteeksi joutuminen on epämiellyttävä yllätys, mutta sen vaikutuksia voi lieventää varautumalla ennakolta ja laatimalla toimintasuunnitelman.

Nyrkkisääntö on, että epäilty rikos kannattaa aina ilmoittaa poliisille.

Tämä opas johdattaa lukijan yrityksiin kohdistuvan kyberrikollisuuden esitutkintaan poliisissa. Oppaan tarkoituksena on motivoida yrityksiä ilmoittamaan kyberrikokset poliisille ja omaksumaan toimintatapoja, jotka parantavat kyberrikosten selvittämismahdollisuuksia sekä tarjota tietoa esitutkinnan kulusta. Opas on kirjoitettu paitsi tiedonlähteeksi, myös keskustelun välineeksi yritysten sisällä vastuu- ja avainhenkilöiden ja ICT-ammattilaisten sekä ostopalvelusopimusten kautta toimivien palveluntarjoajien välillä. Parhaan hyödyn oppaasta saa käsittelemällä sitä yhdessä yrityskohtaisesti mietityllä kokoonpanolla ja pohtimalla vastauksia kunkin teeman alla esitettyihin kysymyksiin.

Oppaalle on tarvetta, koska käytäntö Suomessa ja kansainvälisesti osoittaa, että yritykset eivät ilmoita läheskään kaikista kyberrikoksista poliisille. Syitä ilmoittamatta jättämiseen on monia ja käymme niitä läpi tässä oppaassa. Nyrkkisääntö on, että epäilty rikos kannattaa aina ilmoittaa poliisille. Ilmoittaminen on samalla yhteiskunnallinen viesti, että rikosta ei hyväksytä, vaan tekijä halutaan rikosoikeusjärjestelmän kautta vastuuseen teostaan. Rikoksen uhriksi joutuminen ei ole häpeä ja saattamalla rikoksen viranomaisten tietoon voi estää muita joutumasta uhriksi.

Osa I esittelee lyhyesti kyberrikoksia sekä havainnollistaa miksi niistä kannattaa ilmoittaa poliisille ja toisaalta, mitkä syyt vaikuttavat siihen, että rikoksista ei ilmoiteta.

Osa II avaa esitutkintaa osana rikosprosessia ja kuvaa kahden fiktiivisen esimerkin kautta yrityksiin kohdistuvia kyberrikostilanteita sekä niiden esitutkintaa.

Osa III keskittyy käytännön ohjeisiin. Siinä käydään läpi mille viranomaisille tietoturvalouk-kauksista ja kyberrikoksista kuuluu ilmoittaa. Lisäksi ohjeistetaan rikosilmoituksen tekemisestä poliisille ja kerrotaan, millaista tietoa poliisi tarvitsee kyberrikostutkinnan aikana. Lopuksi keskitytään kyberrikoksiin varautumiseen ja annetaan vinkkejä, mistä yritykset saavat apua sekä esitellään hyviä käytäntöjä, miten madaltaa ilmoittamisen kynnystä suunnittelemalla ilmoittamispolitiikka etukäteen sekä kuinka parantaa rikosten selvittämismahdollisuuksia.

- Hyvät käytännöt on laadittu yhdessä viranomaisten ja yritysten kanssa syksyllä 2020.
- Lisää oppaan luontiprosessista ja CYBERDI-hankkeesta sivulla 47.

* Kyberrikollisuus on tieto- ja viestintäjärjestelmiin kohdistuvaa tai niitä hyväksikäyttäen tehtyä rikollisuutta.

OSA I

Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

Rikokset ja motiivit

Kyberrikokselle ei ole erillistä määritelmää rikoslaissa (RL), vaan teot kattavat joukon tunnusmerkistöjä. Monet kyberrikoksiksi mielletyt teot, mutta ei kaikki, löytyvät rikoslain luvusta 38 ”Tieto- ja viestintärikokset”. Arkikielessä kyberrikokset jaotellaan tieto- ja viestintäjärjestelmiin kohdistuviin ja niitä hyväksikäyttäen tehtyihin rikoksiin.

Käytännössä monet teot ovat osa tapahtumaketjua, jossa yhdistyy useammanlaista rikollista toimintaa. Yrityksen ei ole aina helppo havaita niitä tai tunnistaa tapahtumien välistä yhteyttä, sillä aikajänne voi olla jopa kuukausia tai vuosia. Kyberrikoksen kohteeksi voivat joutua kaiken kokoiset yritykset miltä tahansa toimialalta.

Tiesitkö että...

Tietojärjestelmään kohdistuvan rikoksen tunnusmerkistön haarukointi alkaa yleensä kuudesta rikosnimikkeestä: tietomurto (RL 38:8)*, luvaton käyttö (RL 28:7), datavahingonteko (RL 35:3a), vaaran aiheuttaminen tietojenkäsittelylle (RL 34:9a), tietoliikenteen häirintä (RL 38:5) ja tietojärjestelmän häirintä (RL 38:7a).

- **Tietomurto** tulee kyseeseen tapauksissa, joissa tietojärjestelmään on tunkeuduttu oikeudettomasti.
- **Luvaton käyttö** viittaa laitteen tai muun omaisuuden käyttöön ilman lupaa.
- **Datavahingonteko** on vahingoittamistarkoituksessa tehtyä datan vahingoittamista, kuten sen hävittämistä, muuttamista tai käyttökelvottomaksi saattamista.
- **Vaaran aiheuttaminen tietojenkäsittelylle** käsittää tekoja, joiden tarkoitus on ollut haitan tai vahingon aiheuttaminen tietojenkäsittelylle taikka tieto- ja viestintäjärjestelmän toiminnalle tai turvallisuudelle. Kyseessä voi olla esimerkiksi tietoverkkorikosvälineiden hankinta, valmistaminen ja levittäminen.
- **Tietoliikenteen häirintä** viittaa esimerkiksi televiestiliikenteen oikeudettomaan häirintään tai estämiseen.
- **Tietojärjestelmän häirinnässä aiheutettu haitta tai vahinko** kohdistuu tietojärjestelmän toimintaan.

Osalle mainituista rikosnimikkeistä on myös törkeä ja lievä tekomuoto, mitkä viittaavat perusmuotoista vakavampaan ja lievempään rikokseen. Kyberrikoksiin yhdistyy usein myös muita rikosnimikkeitä. Esimerkiksi **törkeä kiristys** (RL 31:4), **petos** (RL 36:1), **vakoilu** (RL 12:5) tai **yritysvakoilu** (RL 30:4) voivat tulla kyseeseen rikoksen laadusta riippuen. Eli kyberrikoksen taustalla on usein tietojärjestelmään kohdistuvia esirikoksia, joita tarvitaan varsinaisen tavoitteen saavuttamiseksi.

Katso tarkat tunnusmerkistöt rikoslaista.

- Ajantasaiset säädökset (rikoslaki 39/1889) osoitteessa finlex.fi.

* luku: pykälä

Pohdittavaksi

Millainen vaikutus seuraavilla rikoksilla olisi yrityksemme toimintaan?

Rikollinen löytää yrityksen tietojärjestelmästä tunnetun, mutta paikkaamatta jääneen haavoittuvuuden, murtautuu tietokantaan, kopioi sen ja kiristää yritystä.

- **Millä tiedolla meitä voisi kiristää tehokkaimmin?**

Verkkokauppaan kohdistunut palvelunestohyökkäys estää asiakkaiden pääsyn ostoksille ja pysäyttää myynnin.

- **Miten palvelunestohyökkäys näkyisi asiakkaillemme ja millaisia vaikutuksia sillä voisi olla?**

Työntekijän tietokoneelle asennetaan vakoiluhaittaohjelma, joka kopioi ja lähettää eteenpäin hänen näppäimenpainalluksensa, myös salasanat ja käyttäjätunnukset.

- **Mihin kaikkeen rikollinen saisi organisaatiossamme pääsyn?**

Maajohtaja pyytää sähköpostitse tekemään kiireellisen tilisiirron pitkäaikaiselle ulkomaalaiselle alihankkijalle. Tilisiirron tekemisen jälkeen havaitaan, että alihankkijan tilinumero oli väärennetty eikä maajohtaja lähettänyt viestiä.

- **Menisikö huijaus läpi myös meidän organisaatiossamme ja minkä suuruisen taloudellisen menetyksen kestäisimme?**

Yrityksen ulkoisten verkkosivujen sisältöä muokataan luvatta.

- **Miten sotketut sivut voisivat vaikuttaa maineeseemme? Ja oliko tässä kaikki? Pääseekö verkkosivujemme kautta tekemään muuta vahinkoa?**

Vaihtelevat motiivit

Kyberrikosten motiivit vaihtelevat. Joskus vakavakin teko voi olla ajattelemattoman ja kokeilunhaluisen tekijän aikaansaannos, mutta usein kyse on taloudelliseen hyötyyn tähtäävästä ammattimaisesta tai puoliammattimaisesta rikollisuudesta. Uhri voi olla joko satunnainen tai harkittu kohde.

Ei ole tavatonta, että yritystä käytetään väliaskelmana, jonka kautta päästään käsiksi varsinaiseen kohteeseen.

Rikolliset etsivät usein verkosta automaattityökalujen avulla haavoittuvia järjestelmiä ja valitsevat löydösten joukosta kiinnostavimmat kohteet. Tällöin jo kyberturvallisuuden perustason ylläpitäminen torjuu osan rikoksista. Taloudellinen hyöty, kilpailevan yrityksen vahingoittaminen, muu kilpailuedun tavoittelu tai ideologiset syyt voivat löytyä rikoksen taustalta. Joskus kyse voi olla myös valtiollisesta vakoilusta tai muusta valtioon kohdistuvasta vaikuttamispyrkimyksestä.

Motiivin ja epäillyn selvittäminen auttavat arvioimaan yritykseen kohdistuvan uhkan laajuutta ja vakavuutta. Ei ole tavatonta, että rikoksen todellinen kohde onkin jokin muu ja esimerkiksi alihankkijayritystä käytetään väliaskelmana, jonka kautta päästään käsiksi suurempaan kohteeseen. Myös satunnaisen yrityksen kybertoimintaympäristön osat, esimerkiksi palvelimet ja työasemat, voivat itsessään kiinnostaa rikollista, sillä murrettuja laitteita voidaan etähallita ja valjastaa työkaluiksi muuhun rikollisuuteen.

Pohdittavaksi

- **Mitä rikollisen kannalta kiinnostavaa meillä on?**
- **Ovatko asiakkaamme tai liikekumppanimme kiinnostavia kohteita?**
- **Olemmeko helppo uhri? Testaammeko esimerkiksi verkossa olevia tietojärjestelmiämme haavoittuvuuksien varalta ja huolehdimmeko päivityksistä?**
- **Uskaltaako ja ymmärtääkö henkilökuntamme ilmoittaa poikkeavista havainnoistaan tai mahdollisista virheistään? Miten työntekijän tulisi toimia, jos sähköpostin avattu liitetiedosto epäilyttää?**

Miksi kyberrikoksesta kannattaa ilmoittaa poliisille?

Ilmoittaminen on oikeus

Monet yritykset toivovat selkeää ohjetta, milloin kyberrikoksesta kannattaa ilmoittaa poliisille. Lähtökohtaisesti uhrilla on aina oikeus ilmoittaa poliisille epäilemästään rikoksesta ja poliisi kannustaa ilmoittamaan matalalla kynnyksellä kaikki rikokset. Ilmoitus kannattaa tehdä heti kun rikos havaitaan, sillä epäillyn jäljet haihtuvat nopeasti verkkoympäristöstä. Uhrin ei tarvitse pohtia, oliko teko esimerkiksi tarpeeksi vakava tai voiko epäiltyä tavoittaa, vaan poliisi arvioi tilanteet tapauskohtaisesti. Rikosten tutkinnan prioriteettiin vaikuttaa esimerkiksi jutun kiireellisyys, selvittämismahdollisuudet, aiheutuneet vahingot ja poliisin resurssit.

Ilmoittamatta jättäminen vahingoittaa rikosoikeusjärjestelmän toimintaa

Rikoslain tarkoitus on ohjata ihmisten käyttäytymistä osoittamalla millaiset teot ovat yhteiskunnan arvojen ja moraalin vastaisia ja millainen seuraamus, toisin sanoen rangaistus, niistä aiheutuu. Seuraamuksilla tavoitellaan vaikutusta, joka ohjaa käyttäytymistä poispäin epätoivotusta. Jos rikoksista ei ilmoita poliisille, vahvistetaan käsitystä, että yhteiskunta hyväksyy tällaisen rikollisuuden, mikä puolestaan kannustaa paitsi kotimaisia myös ulkomaisia rikollisia toimimaan Suomessa.

Ilmoitetut rikokset kehittävät ja suuntaavat poliisitoimintaa

Suurin osa poliisin tietoon tulleista rikoksista tulee ilmoitusten kautta. Rikoslajikohtainen rikosten määrä vaikuttaa esimerkiksi poliisin resursseihin ja niiden suuntaamiseen eri toimintoihin. Kertyvä kokemus auttaa tutkimaan kyberrikoksia myös jatkossa ja oppimaan uusia menetelmiä. Oikeuskäytäntö ja käsitys tarvittavasta todistusaineistosta rakentuu tuomioiden kautta. Näkemys poliisin tehtäväkentästä vaikuttaa pitkällä tähtäimellä poliisikoulutuksen opetussisältöihin, arvioitaessa minkälaisista taidoista ja valmiuksista on hyötyä tulevaisuudessa. Vääristynyt tilannekuva voi siten johtaa virheellisiin strategisiin valintoihin.

Ilmoittaminen auttaa sarjoittamaan rikoksia myös ulkomaille

Vaikka yksittäisen rikoksen merkitys tai siitä aiheutunut taloudellinen tappio tuntuisi pieneltä, saman rikoksen kohteeksi joutuneita tahoja voi paljastua ympäri maailmaa. Poliisi on kansainvälisesti verkostoitunut viranomainen, jonka on mahdollista paitsi saada tietoa ulkomailla sijaitsevasta epäillystä, myös yhdistää Suomessa tapahtuneita rikoksia osaksi laajempaa kansainvälistä rikossarjaa. Rikolliset luottavat siihen, että viranomaisten toimivalta loppuu valtion rajalla, mutta yhdistämällä tiedot ja välillä myös tutkinnat, rikolliset voidaan saattaa edesvastuuseen eri maissa tapahtuneesta kokonaisuudesta. Mitä useammasta rikoksesta saadaan kerättyä todistusaineistoa, sitä todennäköisempää on epäillyn tunnistaminen.

Poliisin keinovalikoima on muita laajempi

Vaikka epäillyn henkilöllisyys ei olisi uhrin tiedossa, poliisilla on yrityksiä ja muita viranomaisia laajemmat tiedonsaantioikeudet selvittää rikoksesta epäillyn henkilöllisyyttä.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

Kiinnijääminen voi muuttaa rikoksentekijän tulevaisuuden

Saman tekijän kontolle kertyy yleensä useita kyberrikoksia. Kyberrikoksesta epäillyt ovat tyypillisesti nuorehkoja miehiä, joista osa on vielä alaikäisiä. Nuoren voi olla vaikea hahmottaa tekonsa vakavuutta ja seurauksia, jos yleinen käsitys on, että kiinnijäämisriski on matala eivätkä edes uhrit ilmoita rikoksista. Rikoskierteen katkaisu on helpompaa varhaisessa vaiheessa ja esimerkiksi moni uravalinta edellyttää nuhteetonta taustaa. Tämän vuoksi myös taitamattomilta vaikuttavat teot kannattaa ilmoittaa poliisille.

Rikosilmoitus on merkki vastuullisuudesta

Rikoksesta ilmoittaminen poliisille saa yrityksen todennäköisesti arvioimaan yksittäistä tapausta huolellisemmin kuin se muuten olisi tehnyt. Vähäpätöiseltä vaikuttanut tapaus voi osoittautua myöhemmin merkittäväksi ja osaksi laajempaa tapahtumaketjua. Siksi kaikki tapaukseen liittyvä dokumentaatio on tärkeää. Lisäksi, jos tapauksesta tulee jälkikäteen julkinen, ilmoituksen tehneen yrityksen on helpompi osoittaa toimenpiteidensä riittävyys ja vastuullisuus. Tällöin ei tarvitse perustella, miksei yritys ilmoittanut esimerkiksi aiemmin tapahtuneesta tietomurrosta. Poliisille ilmoittamisella voi olla myös rauhoittava vaikutus: asiat saavat oikean perspektiivin, kun tilannetta ratkotaan yhdessä.

Vähäpätöiseltä vaikuttanut tapaus voi osoittautua myöhemmin merkittäväksi ja osaksi laajempaa tapahtumaketjua.

Miksi poliisille ei aina ilmoiteta rikoksesta?

Hyötyjen ja haittojen punnintaa

Käytännössä kaikista rikoksista ei ilmoiteta poliisille, vaikka ilmoittaminen on toivottavaa ja yhteiskunnallisesti merkityksellistä. Yritykset punnitsevat ilmoittamisen hyötyjä ja haittoja liiketoimintansa kannalta. Esimerkiksi vakuutuskorvauksen saaminen voi edellyttää ilmoituksen tekemistä. Toisaalta yrityksiltä voi puuttua ilmoittamista tukevat prosessit, eikä poliisille ilmoittamista ole mielletty osaksi tietoturvaloukkausten käsittelyprosessia tai selvitetty ennakolta, miten ilmoitus tehdään. Lisäksi rikostutkinnan aikaiseen yhteistyöhön poliisin kanssa kuluu myös uhrin resursseja, kuten henkilöstön työaikaa, vaikka tutkinta pyritään tekemään niin, että siitä on mahdollisimman vähän haittaa yritykselle.

Epäröintiä prosessin käynnistämisessä

Ilmoitukset viivästyvät, jos uhri epäröi haluaako se rikoksen tutkittavaksi vai ei. Tilanne voi tulla kyseeseen erityisesti silloin, jos kyse on virallisen syytteen alaisesta rikoksesta. Poliisilla on lakiin sidottu velvollisuus tutkia virallisen syytteen alaiset rikokset, kun ne ovat tulleet sen tietoon, eikä uhri voi vetää ilmoitusta pois prosessista. Sen sijaan asianomistajarikoksissa uhrin päätös olla vaatimatta rangaistusta epäillylle päättää tutkinnan, ellei erittäin tärkeä yleinen etu vaadi sen jatkamista. Jos asianomistajaa arveluttaa rikosprosessin julkisuus, on syytä huomioida, että rikoksen ilmoittamatta jättäminen poliisille ei tarkoita suoraan sitä, että rikos ei paljastuisi ulkopuolisille, vaan kyberrikoksen uhri voi joutua esimerkiksi rikollisen kiristyksen, tietovuodon tai muun vahingonteon kohteeksi pitkänkin ajan jälkeen.

Pelkoa omien virheiden paljastumisesta

Joskus yritystä voi arveluttaa rikosilmoituksen tekeminen, koska se pelkää omien virheidensä, esimerkiksi puutteellisesti hoidetun tietoturvan tai hyväuskoisuuden, paljastumista. Pelon ei saisi kuitenkaan antaa estää rikoksen uhria hakemasta apua ja saamasta oikeutta. Rikoksessa on monesti kyse tapahtumaketjusta, jonka toteutumiseen on vaikuttanut moni asia ja uhria on erehdytetty taitavasti. Peittely ja salailu voivat tehdä lopputuloksesta moninkertaisesti pahemman, kun vahingot pääsevät leviämään tai paljastuvat myöhemmin, jolloin myös tilanteen aiempi käsittely tulee esille.

Monesti rikoksista ilmoittamiseen liittyvät huolet ja pelot saavat suuremmat mittasuhteet kuin on tarpeellista.

Kyberrikokset ovat yleistyneet niin paljon, että uhriksi voi joutua mikä tahansa organisaatio. Siksi on tärkeää, että kaiken kokoiset yritykset miettivät, mitä kyberrikoksen kohteeksi joutuminen voi tarkoittaa omalta kannalta, miten silloin toimitaan ja toisaalta, miten asiaan suhtaudutaan. Monesti rikoksista ilmoittamiseen liittyvät huolet ja pelot saavat suuremmat mittasuhteet kuin on tarpeellista.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

Pohdittavaksi

Miten meidän organisaatiossamme arvioidaan kyberrikosten ilmoittamista poliisille?

- **Vaikuttavatko punnintaamme enemmän yhteiskunnalliset vai yrityslähtöiset syyt?**
- **Haluammeko antaa poliisille mahdollisuuden tutkia meihin kohdistuneet rikokset? Eroaako ajattelumme kyberrikosten osalta muusta rikollisuudesta? Jos eroaa, niin miksi?**
- **Pyrimmekö tunnistamaan mahdolliset rikokset?**
- **Onko toimintakäytännöissämme heikkouksia, joiden paljastuminen olisi kiusallista tai voisi johtaa jopa seuraamuksiin? Estävätkö ne avun pyytämisen viranomaisilta? Kuinka voimme korjata toimintakäytäntömme ja kenen johdolla?**
- **Vaikuttaako päätökseemme teon vakavuus tai aiheutuneet vahingot?**
- **Voimmeko saada vakuutuskorvauksia ja edellyttääkö niiden saaminen rikosilmoitusta?**
- **Voimmeko saada vahingonkorvauksia rikosprosessin kautta epäillyltä?**
- **Pelkäämmekö rikosprosessin aikaista julkisuutta? Voimmeko vaikuttaa julkisuuskuvaan omilla toimillamme?**
- **Tunnistammeko rikosilmoituksen muut hyödyt, vaikka epäiltyä ei tavoitettaisi?**
- **Pelkäämmekö rikollisen kostoa, jos ilmoitamme poliisille?**
- **Tiedostammeko, että samasta tapauksesta voi olla tarpeellista ilmoittaa usealle viranomaiselle? (lue lisää sivulta 17)**
- **Miten arvioimme odotettua kokonaishyötyä suhteessa poliisitutkinnan aiheuttamaan vaivaan yrityksessä?**

OSA II

Kyberrikoksen esitutkinta

Esitutkinta osana rikosprosessia

Rikosprosessi on viranomaistoiminnan muodostama ketju, jonka tarkoituksena on varmistaa, että rikosepäilyt selvitetään, syytetään ja tuomitaan lain mukaisesti sekä mahdolliset rangaistukset pannaan täytäntöön. Rikosprosessi kokonaisuutena voi kestää useamman vuoden. Kestoon vaikuttavat esimerkiksi tapauksen laajuus ja viranomaisten resurssit. Seuraavaksi käydään läpi pääpiirteittäin, miten ilmoitettu rikos etenee esitutkinnan aikana syyteharkintaan.

1. Esitutkinta

2. Syyteharkinta

3. Oikeudenkäynti

4. Rangaistuksen täytäntöönpano

▸ Lue lisää esitutkinnasta osana rikosprosessia teoksesta Rantaeskola, Satu (2019). Rikos ja rikosprosessi. Warelia: Sastamala.

Rikosprosessin neljä vaihetta ovat esitutkinta, syyteharkinta, oikeudenkäynti ja rangaistuksen täytäntöönpano.

Esimerkki yrityksen tekemän rikosilmoituksen etenemisestä esitutkinnassa:

1. Rikos-ilmoitus

Yritys tekee poliisille rikosilmoituksen epäilemästään rikoksesta.

2. Kirjallinen vahvistus

Poliisi on velvollinen kirjaamaan tapahtuman, jota ilmoittaja epäilee rikokseksi ja antamaan kirjallisen vahvistuksen ilmoitetusta tapahtumasta (ETL 3:1).

3. Onko syytä epäillä rikosta?

Kyllä: Esitutkinta on toimitettava (ETL 3:3:1). Asianomistajalle ilmoitetaan mahdollisuuksien mukaan mihin toimenpiteisiin rikosepäilyn osalta ryhdytään (ETL 11:9:1).

Ei: Prosessi päättyy ja siitä ilmoitetaan asianomistajalle. (ETL 10:2:2 ja 4:18:7)

4. Onko kyse virallisen syytteen alaisesta rikoksesta?

Kyllä: Tutkinta etenee.

5. Vaatiiko asianomistaja rangaistusta?

Ei: Asianomistajarikoksen esitutkinta toimitetaan, jos asianomistaja vaatii rangaistusta rikokseen syyllistyneelle. Yleisen edun vaatiessa syyttäjä voi nostaa syytteen asianomistajarikoksesta ilman asianomistajan rangaistusvaatimusta, jolloin esitutkinta toimitetaan syyttäjän pyynnöstä. (ETL 3:4)

Ei: Prosessi päättyy ja siitä ilmoitetaan asianomistajalle. (ETL 10:2:2 ja 4:18:7)

Kyllä: Tutkinta etenee.

6. Onko esitutkinnan rajoittamiselle tarvetta?

Kyllä: Esimerkiksi jos kustannukset ovat selvässä epäsuhteessa tutkittavana olevan asian laatuun ja siitä mahdollisesti odotettavaan seuraamukseen tai on todennäköistä, että syytettä ei nosteta, esitutkintaa voidaan rajoittaa (ETL 3:10). Tutkinnan rajoittamisesta ilmoitetaan asianomistajalle.

Ei: Tutkinta etenee.

7. Onko esitutkinnan keskeyttämiselle tai lykkäämiselle tarvetta?

Kyllä: Esitutkinta voidaan keskeyttää, jos rikoksesta ei epäillä ketään tai asiaan vaikuttavaa selvitystä ei ole saatavissa (ETL 3:13). Lykkääminen myöhemmäksi voi tulla kysymykseen, jos se on välttämätöntä toisen tutkittavan rikoksen takia eikä siitä aiheudu laissa määriteltyä vaaraa tai vahinkoa (ETL 3:12). Keskeyttämisestä ja lykkäämisestä ilmoitetaan asianomistajalle.

Ei: Tutkinta etenee.

8. Esitutkinta-pöytäkirja

Poliisi tutkii rikoksen ja laatii esitutkinta-pöytäkirjan, joka sisältää tutkinnan kannalta merkitykselliset tiedot tapauksesta mm. kuulustelupöytäkirjat, selostukset tutkintatoimenpiteistä ja tehdyistä havainnoista sekä olennaiset liitteet ellei laissa toisin säädetä (ETL 9:6).

9. Loppu-lausunnot

Poliisi pyytää tarvittaessa asianosaisilta loppulausunnon ennen esitutkinnan päättämistä. Loppulausunnossa asianosaiset arvioivat mm. esitutkinta-aineiston riittävyyttä ja muita tärkeitä tutkinnan toteutuksen seikkoja (ETL 10:1). Myös asianosainen voi pyytää esitutkintatoimenpiteitä, kuten kuulusteluja, jos hän voi osoittaa, että ne saattavat vaikuttaa asiaan ja jos niistä ei aiheudu asian laatuun nähden kohtuuttomia kustannuksia (ETL 3:7).

10. Siirtyykö asia syyteharkintaan?

Kyllä: Syyteharkinnassa syyttäjä päättää, nostaako se syytteen epäillystä rikoksesta vai ei.

Ei: Asia ei etene syyteharkintaan, jos rikosta ei ole tapahtunut tai syytettä ei voi nostaa ketään vastaan, esimerkiksi epäilty on jäänyt tuntemattomaksi (ETL 10:2:2–10:2:3). Asianomistaja saa tiedon jutun tilasta.

Esitutkinnan tarkoitus

Poliisin rooli rikosprosessissa on suorittaa esitutkinta eli tehdä pohjatyö, jonka perusteella mahdollinen rikos voi edetä prosessissa. Esitutkinnan aikana selvitetään epäillyn rikoksen tapahtumakulku, siihen liittyvät henkilöt, saatu rikoshyöty, aiheutunut vahinko ja asianomistajan eli uhrin vaatimukset.

Ilmoitus tuo rikosepäilyn poliisin tietoon

Kyberrikokset tulevat poliisin tietoon tyypillisesti uhrin ilmoittamana. Poliisi on velvollinen kirjaamaan ilmoitetun tapauksen ja antamaan kirjallisen vahvistuksen tehdystä ilmoituksesta. Ensimmäiseksi poliisi arvioi, onko ilmoitetussa tapauksessa syytä epäillä rikosta. Jos ei, esitutkintaa ei aloiteta ja siitä ilmoitetaan asianomistajalle.

Virallisen syytteen alainen vai asianomistajarikos?

Rikoslain mukaiset rikokset jaetaan Suomessa kahteen tyyppiin: asianomistajarikoksiin ja virallisen syytteen alaisiin rikoksiin. Esitutkintalain (ETL) 3:4 (luku:pykälä) mukaan asianomistajarikoksen esitutkinta toimitetaan, jos asianomistaja vaatii rangaistusta rikokseen syyllistyneelle eli toisin sanoen, asianomistaja päättää tutkitaanko rikos vai ei. Poikkeuksen tähän tekee tapaus, jossa syyttäjän on pyydettävä tutkintaa ja nostettava syyte yleisen edun vuoksi. Käytännössä monien asianomistajarikosten syytekynnyksen ylittyminen ilman asianomistajan rangaistusvaatimusta edellyttää erittäin tärkeää yleistä etua (ks. esim. RL 38:10). Virallisen syytteen alaiset rikokset tutkitaan asianomistajan vaatimuksesta riippumatta. Kyberrikosten joukossa on molempia syytetyyppejä. Pääpiirteittäin vakavimmat rikokset ovat virallisen syytteen alaisia. Myös käytettävissä oleva tutkintakeinovalikoima kasvaa rikoksen vakavuuden myötä.

Poliisi tekee usein kansainvälistä yhteistyötä kyberrikostutkinnan aikana, vaikka ei vielä tiedetä onko epäilty ulkomailla vai Suomessa.

Kyberrikoksen jäljet johtavat usein ulkomaille

Rikokset ovat erilaisia ja niiden selvittämismahdollisuudet vaihtelevat. Kyberrikoksille on tyypillistä, että niiden tekijä on uhrille tuntematon ja rikoksen jälkiä löytyy ulkomailta. Vaikka ei vielä tiedetä, onko epäilty ulkomailla vai Suomessa, poliisi tekee usein kansainvälistä yhteistyötä kyberrikostutkinnan aikana. Poliisi voi tehdä esimerkiksi tietopyyntöjä ulkomaalaisille palvelun-tarjoajille, kartoittaa kansainvälisten poliisiviranomaisten verkostojen kautta tekotapoja ja niihin liittyviä jälkiä sekä pyytää kansainvälisen oikeusapupyynnön kautta apua toisen valtion poliisilta, jos esimerkiksi epäilty oleskelee kyseisessä valtiossa. Tiivein yhteistyön muoto on eri valtioiden toimivaltaisista viranomaisista koottu yhteinen tutkintaryhmä (joint investigation team, JIT), joka voidaan perustaa eri maiden alueille ulottuvan rikostapauksen esitutkinnan toimittamista varten.

Esitutkinnan laajuus vaihtelee

Tietyissä tilanteissa esitutkinta voidaan jättää toimittamatta, suorittaa suppeana tai lopettaa. Esitutkintaa voidaan myös rajoittaa, siirtää ajallisesti tai se voidaan keskeyttää. Rajoituksilla pyritään turvaamaan vakavien rikosten tutkinta ja toisaalta varmistamaan kustannustehokkuus. Lisätietoja rajoittamisesta löytyy valtakunnansyyttäjän ohjeesta https://syyttajalaitos.fi/vks-2016-5-esitutkinnan-rajoittaminen. Tässä oppaassa esitetään vain osa tilanteista.

Tutkinnan rajoittaminen voi tulla kysymykseen esimerkiksi silloin, jos on todennäköistä ettei asiasta nosteta syytettä tai tutkinnan kustannukset ovat liian korkeat suhteessa tutkittavan asian laatuun ja mahdollisiin odotettaviin seuraamuksiin (ETL 3:10). Lisäksi esitutkinta voidaan keskeyttää tilapäisesti, jos rikoksesta ei epäillä ketään ja jos asiaan vaikuttavaa selvitystä ei ole saatavissa (ETL 3:13). Myös esitutkinnan lykkääminen toiseen ajankohtaan on mahdollista tiettyjen kriteerien täyttyessä, esimerkiksi että siirtäminen on välttämätön toisen tutkittavan rikoksen vuoksi eikä siirtämisestä aiheudu vaaraa hengelle tai terveydelle (ETL 3:12). Poliisi ilmoittaa esitutkinnan vaiheista asianomistajalle.

Esitutkintapöytäkirja ja loppulausunto

Poliisi kokoaa tekemänsä tutkinnan esitutkintapöytäkirjaksi, jonka liitteeksi laitetaan tutkinnan kannalta olennaiset dokumentit, kuten asiakirjat ja raportti tietoteknisestä tutkinnasta. Myös asianosainen on voinut pyytää esitutkinnan aikana tutkintatoimenpiteitä, jos hän osoittaa, että ne saattavat vaikuttaa asiaan, ja jollei niistä aiheudu asian laatuun nähden kohtuuttomia kustannuksia (ETL 3:7:1). Ennen esitutkinnan päättämistä asianosaisille saatetaan tutkittavan tapauksen laadusta ja laajuudesta riippuen antaa mahdollisuus jättää kirjallinen loppulausunto. Loppulausunnossa asianosaiset voivat ottaa kantaa esitutkinta-aineiston riittävyyteen, näytön arviointiin, asiaan liittyviin oikeuskysymyksiin sekä muihin asian käsittelyn kannalta tärkeisiin seikkoihin. (ETL 10:1.) Poliisi ilmoittaa asianosaisille jutun siirtymisestä syyteharkintaan.

Poliisi ja syyttäjä työskentelevät yhdessä

Poliisi on velvollinen pitämään syyttäjän ajan tasalla tutkinnan edistymisestä ja esitutkintatoimenpiteistä asian laadun tai laajuuden edellyttämällä tavalla (ETL 5:3:1). Yhteistyön merkitys korostuu erityisesti laajojen ja haastavien rikosten esitutkinnassa, sillä syyttäjällä on paras käsitys siitä, minkälaista näyttöä tarvitaan, että juttu menestyisi oikeudessa, kun taas poliisi on tutkintamenetelmien ja -taktiikoiden asiantuntija.

Esitutkinta päättyy syyteharkintaan

Syyteharkinnan aikana syyttäjä päättää esitutkinnassa selvitettyjen seikkojen perusteella syytteen nostamisesta. Syyttäjä voi myös määrätä lisätutkimuksia jo päättyneeseen esitutkintaan. Laki oikeudenkäynnistä rikosasiassa (ROL) 1:6 määrittää, että syyte on nostettava, jos epäilty rikos on lain mukaan rangaistava, syyteoikeus on voimassa eli rikos ei ole vanhentunut ja epäilyn syyllisyyden tueksi on olemassa todennäköisiä syitä. Asianomistajarikoksen syyteoikeuteen vaikuttaa myös se, tekeekö asianomistaja syyttämispyynnön (ROL 1:6a:3). Syyttäjällä on lisäksi harkintavaltaa olla nostamatta syytettä tapauksissa, joissa tärkeä yleinen tai yksityinen etu ei sitä vaadi ja jokin laissa määritetty syyttämättä jättämisen kriteeri täyttyy, esimerkiksi kyse on alaikäisenä tehdystä lievästä rikoksesta, jonka voidaan katsoa johtuneen ymmärtämättömyydestä tai harkitsemattomuudesta (ROL 1:7-8).

Yleisöjulkisuus rikosprosessin aikana

Julkisuus rikosprosessin aikana jaetaan kahteen tyyppiin: asianosais- ja yleisöjulkisuuteen. Yleisöjulkisuuden piiriin kuuluvat kaikki muut tahot kuin kyseisen rikoksen asianosaiset eli esimerkiksi tiedotusvälineet, asiasta uteliaisuuttaan kiinnostuneet ja todistajat, koska heiltä puuttuu omakohtainen intressi rikokseen nähden. Viranomaisten asiakirjat ovat lähtökohtaisesti yleisöjulkisia, mutta niiden julkisuutta on voitu rajoittaa lailla välttämättömästä syystä, esim. muun perusoikeuden suojaamiseksi. (Rantaeskola 2019, 33-36.)*

* Rantaeskola, Satu (2019). Rikos ja rikosprosessi. Warelia: Sastamala.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

Laissa viranomaistoiminnan julkisuudesta (621/1999, jatkossa JulkL) 24 § määrittää, että esimerkiksi rikosilmoitus sekä esitutkintaa varten laaditut tai saadut asiakirjat ovat salassa pidettäviä tuomioistuimen istuntoon saakka, joten mahdollinen yksittäisestä rikoksesta tiedottaminen esitutkinnan aikana tapahtuu tarkkojen kriteerien mukaan (JulkL 24.1 § 3 kohta; ETL 11:7; Rantaeskola 2019, 40). Jos juttu ei etene oikeuteen asti, tämä määräaikainen salassapito päättyy syyttämättäjättämispäätökseen tai kun asia on jätetty esitutkinnassa sikseen. (JulkL 24.1 § 3 kohta.)

On huomionarvoista, että yleisen salassapidon päätyttyä esitutkinta- ja syyteharkinta-aineiston (tai osan siitä) salassapito saattaa kuitenkin jatkua julkisuuslain tai muun lain salassapitosäätelyn perusteella. Lisäksi, vaikka oikeudenkäynti ja siihen liittyvät asiakirjat ovat lähtökohtaisesti julkisia, myös oikeudenkäynnin yleisöjulkisuutta voidaan rajoittaa, jos rajoittamisen perusteet täyttyvät. Tämä edellyttää yleensä asianomistajan pyyntöä, koska salaaminen tehdään eri lain* perusteella kuin rikosprosessin aikaisemmassa vaiheessa. (Rantaeskola 2019, 37-41.)

Oikeudenkäynti ja rangaistuksen täytäntöönpano

Jos syyte nostetaan, rikosasia käsitellään oikeudessa. Oikeudenkäynnin lopuksi tuomioistuin antaa ratkaisunsa tapauksesta. Tuomiossa perustellaan ne seikat ja oikeudellinen päättely, mihin ratkaisu perustuu. Lievemmät rikosasiat voidaan toisinaan käsitellä myös kirjallisessa menettelyssä. Rangaistuksen täytäntöönpano kuuluu Oikeusrekisterikeskukselle ja Rikosseuraamuslaitokselle.

Keskeisiä lakeja, jotka vaikuttavat esitutkintaan, poliisin toimivaltuuksiin, rikosprosessin julkisuuteen ja syyteharkintaan:

- Esitutkintalaki (805/2011)
- Laki oikeudenkäynnistä rikosasioissa (689/1997)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Pakkokeinolaki (806/2011)
- Poliisilaki (872/2011)
- Laki viranomaistoiminnan julkisuudesta (621/1999)
- Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa (370/2007)

Ajantasainen lainsäädäntö osoitteessa finlex.fi.

* laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa (370/2007)

Tiesitkö, että...

...rikoksen tutkii pääsääntöisesti se poliisilaitos, jonka alueella rikos on tapahtunut. Jokaisella poliisilaitoksella on valmiudet vastaanottaa rikosilmoitus sekä ohjeistaa todistusaineiston turvaaminen kyberrikosten osalta. Vakavien, kansainvälisten tai paljon erityisresursseja vaativien rikosten tutkinta voidaan myös siirtää Keskusrikospoliisissa sijaitsevan Kyberrikostorjuntakeskuksen tutkittavaksi tai paikallispoliisi voi konsultoida sitä tarvittaessa. Kyberrikostorjuntakeskus voi myös pyytää paikallispoliisilta apua esimerkiksi digitaalisen todistusaineiston keräämisessä ympäri maata tai jakaa juttuja poliisilaitosten tutkittavaksi, esimerkiksi jos se on saanut kansainväliseltä kumppanilta ilmiannon mahdollisesta rikoksesta tietyn poliisilaitoksen alueella.

Fiktiivinen tapausesimerkki kiristyshaittaohjelman esitutkinnasta

Miltä tuntuisi saada viesti, jossa vaaditaan maksamaan seuraavan 48 tunnin aikana 350 000 € tai liikesalaisuuksia koskevat tiedot vuodetaan julkisuuteen? Vaadittu summa kasvaa kuuden tunnin välein 30 %.

1. Rikos havaitaan

RealSignal on 50 henkilöä työllistävä suunnittelutoimisto, joka huolehtii kybertoimintaympäristöstään itse. Toimitusjohtaja saa aamulla kännykkäänsä sähköpostin, jonka mukaan yrityksen tietojärjestelmiin on tunkeuduttu, tietoja kopioitu ja haittaohjelma lukinnut työasemia. Viestissä vaaditaan maksamaan seuraavan 48 tunnin aikana 350 000 € kryptovaluuttana tai lukitusta ei avata ja liikesalaisuuksia koskevat tiedot tullaan vuotamaan julkisuuteen. Vaadittu summa kasvaa kuuden tunnin välein 30 %.

Sama viesti ilmestyy myös toimitusjohtajan tietokoneen näytölle. Toimitusjohtaja, kaksihenkinen ICT-tiimi, toimialapäälliköt ja viestintävastaava kokoontuvat selvittämään tilannetta. Myös hallitukselle ilmoitetaan välittömästi. Tilanne on yrityksen liiketoiminnan kannalta vakava. Kiristyshaittaohjelma on levinnyt laajasti järjestelmiin, eikä yhtään työasemaa ole onnistuttu vielä avaamaan.

▸ Rikostutkinta perustuu lakiin, mutta on aina tapauskohtainen prosessi. Niinpä tapauksen käsittelyyn voivat vaikuttaa monet asiat, eikä tutkinta etene aina tässä fiktiivisessä esimerkissä kuvatulla tavalla. Esimerkin tarkoitus on havainnollistaa, millaisena kyberrikos ja sen esitutkinta voivat näyttäytyä yrityksen näkökulmasta menemättä tutkintataktiikoihin.

RealSignal on suunnitellut etukäteen toimintamallin kyberrikostilanteessa. Sitä noudattaen yrityksen vastuuhenkilöt päättävät, että he haluavat poliisin tutkivan tapauksen, vaativat tekijälle rangaistusta sekä pyytävät apua tilanteen ratkaisuun Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselta ja sallivat viranomaisten työskentelevän yhdessä tapauksen ratkaisemiseksi. Yrityksen vastuuhenkilöt tiedostavat, että myös henkilötietoja on voinut vaarantua, mikä edellyttää ilmoituksen tekemistä Tietosuojavaltuutetun toimistoon ilman aiheetonta viivästystä, viimeistään 72 tunnin kuluessa.

2. Rikosilmoitus tehdään

RealSignalin toimitusjohtaja kertoo poliisiasemalla mitä on tapahtunut. Hänellä on mukanaan henkilöllisyystodistus, kuva näytölle ilmestyneestä kiristysviestistä, kiristyssähköposti ja ICT-päällikön yhteystiedot.

Rikosilmoituksen vastaanottaja konsultoi heti poliisin tietotekniikkatutkijaa. Jutusta kirjataan alustavat rikosnimikkeet: törkeä kiristys, törkeä luvaton käyttö ja datavahingonteko. Toimitusjohtaja kertoo, että myös Traficomin Kyberturvallisuuskeskukselta on pyydetty apua ja antaa luvan tiedonvaihtoon.

RealSignalissa oli päätetty ennen poliisille ilmoittamista, että juttu halutaan tutkittavaksi. Törkeä kiristys on virallisen syytteen alainen rikos, joten asianomistajan kanta rangaistusvaatimukseen ei vaikuta tutkinnan aloittamiseen.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

3. Todistusaineiston turvaaminen

Poliisin tietotekniikkatutkija soittaa RealSignalin ICT-päällikölle. He keskustelevat tapauksen nykytilasta, yrityksen kybertoimintaympäristön rakenteesta ja pohtivat yhdessä, mistä kaikkialta todistusaineistoa voi olla saatavilla. Tietotekniikkatutkija haluaa myös varmistaa, että yrityksessä tiedetään, miten estää vahinkojen leviäminen ja käynnistää toipuminen.

RealSignalissa poimitaan ja dokumentoidaan poliisin ohjeistamana lokitiedot ja varmuuskopiot sekä luovutetaan saastunut työasema haittaohjelma-analyysia varten. Kun todistusaineisto on turvassa, yrityksessä ei tarvitse pelätä, että järjestelmän uudelleenasennus tuhoaisi todistusaineistoa.

4. Tutkinta käynnistyy

Jutulle nimetään tutkija ja tutkinnanjohtaja paikallispoliisissa. Tapaus menee tiedoksi syyttäjälle, jonka kanssa tehdään yhteistyötä jo tutkinnan aikana. Tutkija on yhteydessä tietotekniikkatutkijaan, joka ohjeisti todistusaineiston turvaamisen tietojärjestelmistä, Kyberrikostorjuntakeskukseen sekä RealSignalin luvalla Traficomin Kyberturvallisuuskeskukseen. Hän ottaa yhteyttä myös RealSignalin toimitusjohtajaan ja kertoo tapauksen tutkinnan käynnistymisestä sekä seuraavista vaiheista.

5. Tutkinta etenee

Poliisi puhuttaa RealSignalin henkilökuntaa sekä alkaa selvittää tapahtumakulkua digitaalisen todistusaineiston avulla. Yrityksen apua tarvitaan heidän kybertoimintaympäristönsä ymmärtämisessä. Poliisi kartoittaa, onko samankaltaisia tapauksia tapahtunut aiemmin kotimaassa tai ulkomailla.

Lokitiedot paljastavat työntekijän avanneen haitallisen sähköpostin liitetiedoston, jonka pitkäaikainen alihankkija, SatakuntaVision, oli lähettänyt. Liite oli ujutettu osaksi pidempää, suomenkielistä viestiketjua.

6. Tutkinta laajenee alihankkijayritykseen

Poliisi ottaa yhteyttä SatakuntaVisioniin. Tutkinta laajenee, sillä kukaan yrityksestä ei ollut huomannut tapausta. On selvitettävä, onko ulkopuolisella pääsy työntekijän sähköpostiin ja ovatko tietojärjestelmät vaarantuneet. SatakuntaVision on NIS-direktiivin tarkoittama yhteiskunnan kannalta kriittinen toimija, joten se tekee myös lakisääteisen ilmoituksen valvovalle viranomaiselleen Traficomin Kyberturvallisuuskeskuksen kautta. Office 365 -tilin kautta rikollisella on ollut pääsy myös henkilötietoihin, joten myös Tietosuojavaltuutetun toimistoon on tehtävä ilmoitus.

Tiesitkö, että...

Keskeisten organisaatioiden nimissä voi piillä sekoittumisvaara, jos ei ole tarkkana? Keskusrikospoliisissa sijaitsee Kyberrikostorjuntakeskus, kun taas Liikenne- ja viestintävirasto Traficomissa on Kyberturvallisuuskeskus. Muistisääntönä toimii organisaatioiden nimissä näkyvät tehtäväkentät: poliisi käsittelee rikoksia. Kyberturvallisuuskeskus puolestaan huolehtii laajemmin kyberturvallisuuden ylläpidosta.

7. Kumppaniin kohdistunut huijaus vaaransi RealSignalin

Yhteistyössä SatakuntaVisionin palveluntarjoajan, Traficomin Kyberturvallisuuskeskuksen ja poliisin kanssa selviää, että SatakuntaVisionin työntekijän Office 365 -tili oli kaapattu jo neljä kuukautta aiemmin. Viestit on uudelleenlähetetty sähköpostiosoitteeseen, joka viittaa suomen kielen taitoon.

RealSignalin lokit osoittavat, että rikollinen on päässyt liitteen avanneen työntekijän työasemaa hyväksikäyttäen etenemään tietojärjestelmässä ja löytänyt muutaman salasanatiivisteen, joista yksi kuului järjestelmän ylläpitäjälle. Rikollisen onnistui murtaa ylläpitäjän **heikko salasana Real$ignal2018**, ja saamaan haltuunsa yrityksen verkkotunnuksen, realsignal.fi. Tiedostojen käsittelystä koottava loki paljastaa, että rikollinen on ladannut työasemilta, levypalvelimilta ja sähköposteista yhteensä 45 gigatavua materiaalia ja siirtänyt sen Amazon-pilvipalvelussa sijaitsevaan palvelimeen. Hän ehti levittää kiristyshaittaohjelman kaikkiin verkossa kiinni olleisiin työasemiin ja palvelimiin.

8. Poliisi jatkaa epäillyn henkilöllisyyden selvittämistä

Poliisi etsii digitaalisten jälkien joukosta muita viitteitä epäillyn henkilöllisyydestä ja selvittää yhteistyötahojen kanssa haittaohjelman käyttöä ja rakennetta. Poliisi lähettää ulkomaisille palveluntarjoajille tietopyyntöjä esimerkiksi Amazon-pilvipalvelussa sijaitsevasta palvelimesta, osoitteesta, johon SatakuntaVisionin työntekijän viestit on ohjattu sekä osoitteesta, josta RealSignalin toimitusjohtaja sai kiristysviestin. Poliisia kiinnostaa esimerkiksi mistä IP-osoitteesta ja kuka henkilö on kirjautunut tilille ja liittyvätkö samat elementit johonkin toiseen rikokseen.

Lopuksi

Tässä fiktiivisessä esimerkkitapauksessa poliisi sai osoitettua tapahtumakulun yhteistyössä muiden tahojen kanssa ja jatkaa nyt epäillyn henkilöllisyyden selvittämistä. Suuri merkitys tapahtumakulun selvittämisen onnistumisessa oli RealSignalin kattavilla lokituskäytännöillä sekä heidän ymmärryksellä, että todistusaineiston talteenotto rikoksen jäljiltä. Yhteydenotto viranomaisiin varmistaa oikean toiminnan. Erillään säilytetyt, laajat varmuuskopiot puolestaan auttoivat RealSignalia toipumisessa eikä liiketoiminnalle aiheutunut siten ylitsepääsemätöntä vahinkoa, vaikka rikos vakava isku olikin. RealSignal oppi tapauksesta paljon, mikä johti toimintatapojen kriittiseen arvioon ja muuttamiseen. SatakuntaVision otti käyttöön kaksivaiheisen tunnistautumisen, jotta Office 365 -tilille ei pääse kirjautumaan pelkän salasanan ja käyttäjätunnuksen avulla.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

Fiktiivinen tapausesimerkki yritysvakoilun esitutkinnasta

Miltä tuntuu kun yrityksessä havahdutaan siihen, että ulkopuolinen taho näyttää saaneen haltuunsa kaiken kehitys- ja tutkimusdatan uudesta prototyypistä? Tiedon vuotaminen kilpailijalle ja tuotteen kopioiminen aiheuttaisi merkittävän taloudellisen uhan yrityksen kilpailukyvylle.

1. Outo sattumus saa työntekijän toimimaan

Tuotekehitystiimin työntekijä tekee poikkeamailmoituksen tietoturvavalvomoon (SOC) saamastaan sähköpostiviestistä. Viestin lähetti markkinointitiimissä työskentelevä Tommi, jonka tiedetään olevan pidemmällä lomalla. Tommi ei kuitenkaan vastaa yhteydenottoihin.

2. Tietoturvaryhmä selvittelee tapausta

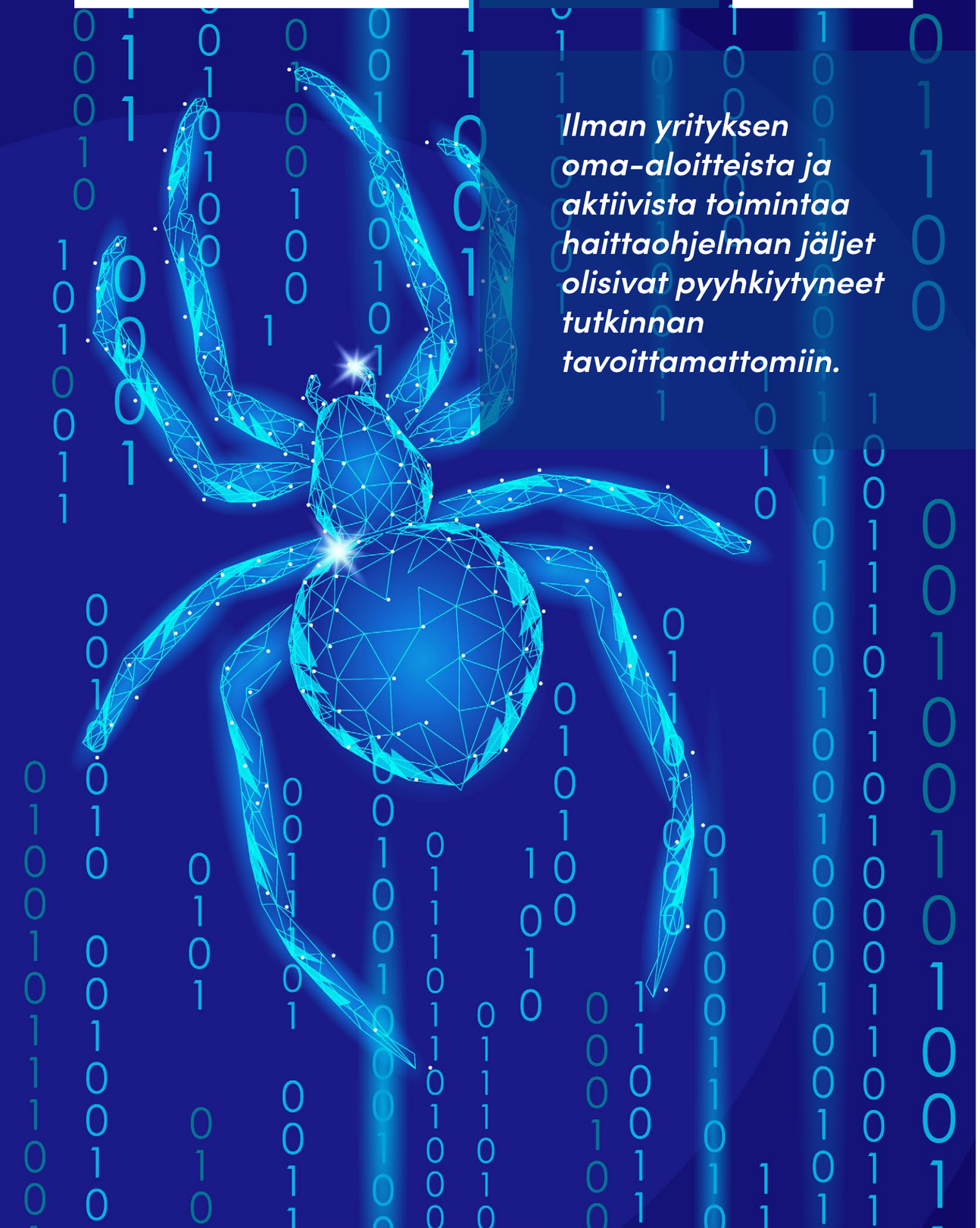
SOC suosittelee Ekorenkaiden tietoturvaryhmää tutkimaan tapauksen. Tommia ei tavoiteta ja henkilöstöhallinto vahvistaa hänen olevan lomalla. Tietoturvaryhmä pyytää ilmoittajalta Tommin viestin liitteineen ja selvittää sen muut vastaanottajat. Sähköpostipalvelinlokeista paljastuu, että Tommin Office 365 -tilille on kirjauduttu ulkomailta ja viestin liitteenä ollut Word-dokumentti sisältää makron automatisoidusta ohjelmakäskystä, joka yrittää ottaa yhteyttä käytöstä poistettuun verkkotunnukseen. Lopulta Tommi vahvistaa, ettei hän ole käyttänyt mitään työvälineitä lomansa aikana. Tietoturvaryhmä selvittää yhdessä työasemaylläpidon palveluntarjoajan kanssa viestin vastaanottajien työasemat sekä pyrkii saamaan tiedon käyttäjiltä liitetiedoston avaamisesta.

Taustaa

Ekorenkaat on merkittävä rengasvalmistaja ja pörssiyhtiö, jonka uusi, ympäristöystävällinen rengasprototyyppi on pian valmis. Kilpailu markkinoilla on kovaa ja ennusteet osoittavat, että ekologisuudesta on kehittymässä alalla erityinen kilpailuvaltti.

Ekorenkaiden työasemaylläpito, eli leasing-työasemat ja niiden hallintapalvelu, on ollut ulkoistettuna samalle toimijalle jo vuosia. Lisäksi Ekorenkaat ostaa tietoturvayhtiöltä tietoturvavalvomopalveluita (SOC – Security Operations Center) koko kybertoimintaympäristöönsä.

▶ Rikostutkinta perustuu lakiin, mutta on aina tapauskohtainen prosessi. Niinpä tapauksen käsittelyyn voivat vaikuttaa monet asiat, eikä tutkinta etene aina tässä fiktiivisessä esimerkissä kuvatulla tavalla. Esimerkin tarkoitus on havainnollistaa, millaisena kyberrikos ja sen esitutkinta voivat näyttäytyä yrityksen näkökulmasta menemättä tutkintataktiikoihin.



Ilman yrityksen oma-aloitteista ja aktiivista toimintaa haittaohjelman jäljet olisivat pyyhkiytyneet tutkinnan tavoittamattomiin.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

3. Tietoturvaryhmä konsultoi Kyberturvallisuuskeskusta

Traficomin Kyberturvallisuuskeskus kehottaa sulkemaan Tommin Office 365 -tunnukset, estämään liikenteen verkkotunnukseen, jonne makro yrittää saada yhteyden, puhdistamaan saastuneet työasemat sekä pyytää tutustumaan tekemäänsä ohjeistukseen Office 365 -huijauksien käsittelystä. He myös tarkastavat verkkotunnuksen ja huomaavat sen olevan varsin tuore ja rekisteröity anonyymisti.

Kyberturvallisuuskeskuksen mukaan kyse on rikoksesta, joten he suosittelevat yhteydenottoa poliisiin ja kertovat, että jos yritys haluaa selvittää tapahtumakulkua tarkemmin, se voi palkata avukseen myös it-forensiikkaan erikoistuneen yrityksen. Tietoturvaryhmä esittelee tapauksen johtoryhmälle ja tapauksesta kerrotaan yrityksen hallitukselle. Myös mahdollista henkilötietojen vaarantumista ja sitä kautta Tietosuojavaltuutetulle ilmoittamisen tarpeellisuutta selvitetään.

4. Virustorjuntajärjestelmä hälyttää

Tietoturvavalvomo tunnistaa, että hälytyksen aiheutti kahdesta tuotekehityksen työasemasta löytynyt Citrix-ympäristön haavoittuvuutta hyväksikäyttävä haittaohjelma. Haittaohjelma on vastajulkaistu ja sen tiedetään kirjoittavan ainoastaan keskusmuistiin.

Tietoturvaryhmä löytää työasemien verkkoliikennelokeista osumia Tommin viestissä olleen liitetiedoston käyttämään verkkotunnukseen. Tuotekehityksen Citrix-työskentely-ympäristön hyväksikäyttö alkaa näyttää todennäköiseltä. Tietoturvaryhmä ottaa reaaliaikaisen kopion Citrix-työskentely-ympäristöstä ennen laitteiden sammuttamista, koska muutoin haittaohjelman toiminnasta aiheutuneet jäljet katoaisivat pysyvästi.

5. Ekorenkaat tekee rikosilmoituksen

Ekorenkaat valtuuttaa lakimiehensä täyttämään sähköisen rikosilmoituksen, koska epäilee tietomurtoa heidän liikesalaisuuksiansa sisältävään tuotekehityksen palvelinjärjestelmään. Lakimies toimii yhteyshenkilönä poliisin suuntaan ja tietoturvatiimin vetäjä varautuu vastaamaan tietojärjestelmiä koskeviin kysymyksiin.

Ekorenkaat selostaa rikosilmoituslomakkeeseen havaitsemansa tapahtumat ja toteaa, ettei yrityksellä ole vielä tarkkaa kuvaa siitä, mihin kaikkeen tietoon on päästy käsiksi tai onko tietoja päästy varastamaan, mutta lokitietoja on pyritty taltioimaan systemaattisesti. Pahimmassa tapauksessa ulkopuolinen taho on saanut haltuunsa kaiken kehitys- ja tutkimusdatan uudesta rengasprototyypistä. Tiedon vuotaminen kilpailijalle ja tuotteen kopioiminen aiheuttaisi merkittävän taloudellisen uhan yrityksen kilpailukyvylle. Pörssiyhtiönä Ekorenkaat on myös velvollinen antamaan julkisen tulosvaroituksen, jos tulosennuste muuttuu odottamatta.

6. Poliisi kirjaa rikosilmoituksen

Rikosilmoituksen vastaanottaja kirjaa ilmoituksen rikosilmoitusjärjestelmään. Annettujen esitietojen perusteella hän päättelee, että kyseeseen voisi tulla tietomurto, luvaton käyttö ja vaaran aiheuttaminen tietojenkäsittelylle. Lisäksi on selvitettävä, voiko kyse olla yritysvakoilusta. Jutulle nimetään tutkija ja tutkinnanjohtaja. Siitä ilmoitetaan myös syyttäjälle ja keskustellaan tietotekniikkatutkijan kanssa. Vaaran aiheuttaminen tietojenkäsittelylle on virallisen syytteen alainen rikos, joten asianomistajan mahdollinen rangaistusvaatimus ei vaikuta tutkinnan aloittamiseen.

7. Rikostutkinta alkaa

Jutun tutkija soittaa Ekorenkaiden lakimiehelle odotettavissa olevista tutkintatoimista. Samalla tietotekniikkatutkija pyytää tietoturvatiimin vetäjältä päivitystä tilannekuvaan ja he keskustelevat voiko tietojärjestelmistä tallentaa vielä muita jälkiä kuin jo tallennetut. Tietotekniikkatutkija kiittää Ekorenkaita Citrix-ympäristön kopiosta, mitä ilman haittaohjelman jäljet olisivat pyyhkiytyneet tutkinnan tavoittamattomiin.

8. Tilanteen vakavuus säikäyttää

Tilanteen vakavuus alkaa valjeta, kun havaitaan, että rikollinen on paitsi saanut jalansijan tuotekehitystyöasemiin, joiden käyttäjät avasivat Tommilta tulleen sähköpostin liitetiedoston myös onnistunut nostamaan saastuneiden koneiden käyttöoikeudet ja selvittämään työasemien käyttäjien salasanat salasanojen urkintaan suunnitellulla haittaohjelmalla. Hyvän lokituksen ansioista nähdään, että hyökkääjä onnistui kopioimaan kaikki uuteen rengasprototyyppiin liittyvät dokumentit ja lähettämään ne eteenpäin.

9. Kyberrikostutkinta sisältää paljon perinteistä poliisityötä

Rikostutkinnan tarkoitus on selvittää ja osoittaa tapahtumakulku ja siihen liittyvät henkilöt näytön avulla. Tietojärjestelmiin kohdistuneiden rikosten tutkinnassa yhdistyy tyypillisesti kahden tyyppistä tutkintaa: tietoteknistä, joka kohdistuu todistusaineiston taltiointiin tietojärjestelmistä ja sen analysointiin sekä taktista, joka kattaa rikostutkinnan muut osa-alueet, kuten tutkintalinjojen ja -taktiikoiden valinnan sekä henkilöiden puhuttamisen ja kuulustelut.

Poliisi puhuttaa Ekorenkaiden avainhenkilökuntaa sekä Tommia. Varmistuu, että Tommi ei ole voinut itse käyttää Office 365 -tunnuksia kyseisenä ajankohtana. Hän myös kertoo säilyttävänsä salasanaansa näppäimistön alla. Lisäksi selviää, että Ekorenkaissa on sattunut muitakin turvallisuuspoikkeamia lähikuukausien aikana. Poliisi pyytää nähtäväksi raportin tuotekehitystiimiin kohdistuneesta kalastelukampanjasta, johon kukaan ei langennut lokitietojen perusteella. HR-osasto puolestaan tiesi kertoa, että yhdelle työntekijälle annettiin varoitus toimintaohjeiden rikkomisesta. Varastotyöntekijä Kikka oli vienyt SER-jäteastiasta kannettavan tietokoneen ja useampia kiintolevyjä. Asia oli selvitetty sisäisesti.

10. Epäily kohdistuu varastotyöntekijään

Poliisi kuulustelee hermostunutta Kikkaa, joka kertoo etsineensä jäteastiasta vain omassa käytössään olleita laitteita tarkoituksenaan poimia talteen niille unohtamansa tiedostot. Lokitiedoista selviää, että Kikan käyttäjätunnuksella on yritetty päästä tuotekehitysraportteihin, joihin hänellä ei ole käyttöoikeuksia. Yritysten määrä ei ylittänyt automaattisen hälytyksen kynnystä. Poliisi selvittää myös, että Kikan on onnistunut ladata yksittäisiä tiedostoja.

Kikan tilitiedoista paljastuu, että hän on saanut kaksi tilisiirtoa ulkomailta rahansiirtoyrityksen kautta. Ensimmäinen tapahtui kolme päivää sen jälkeen, kun lokeihin jäi merkintä tuotekehityksen tiedostojen lataamisesta. Toinen tilisiirto on tehty myöhemmin, vähän ennen sitä, kun haittaohjelman sisältävä liite lähetettiin Tommin sähköpostista.

11. Kikka tunnustaa

Toisessa poliisikuulustelussa Kikka murtuu ja kertoo tutustuneensa mukavaan mieheen netissä. Alkuun he olivat jutelleet muista asioista, mutta kuultuaan Kikan ongelmista ja pikavippikierteestä, mies oli sanonut tietävänsä kaverin, joka pystyisi auttamaan. Kikka kertoo kaverin soittaneen hänelle ja tarjonneen tilaisuutta ansaita rahaa. Vastineeksi piti hankkia Ekorenkaiden tuotekehitykseen liittyviä tiedostoja kehitteillä olevasta rengasprototyypistä.

Kikka kertoo ajatelleensa, ettei hän varastotyöntekijänä pääsisi kuitenkaan käsiksi mihinkään kovin tärkeään, joten päätti rahapulassa suostua. Lähettämällä muutaman, ei kovin tärkeän oloisen, tiedoston ilmoitettuun sähköpostiin, hänen tililleen oli ilmestynyt rahaa. Siksi hän oli yrittänyt etsiä SER-jäteastiasta laitteita uusien tietojen toivossa. Kikka oli kuullut sattumalta, että Tommi säilyttää salasanaansa näppäimistön alla ja myönsi lähettäneensä sen saamaansa sähköpostisoitteeseen. Korvaus oli vieläkin parempi. Kikan mukaan se oli viimeinen yhteydenotto.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

12. Rikostutkinta jatkuu

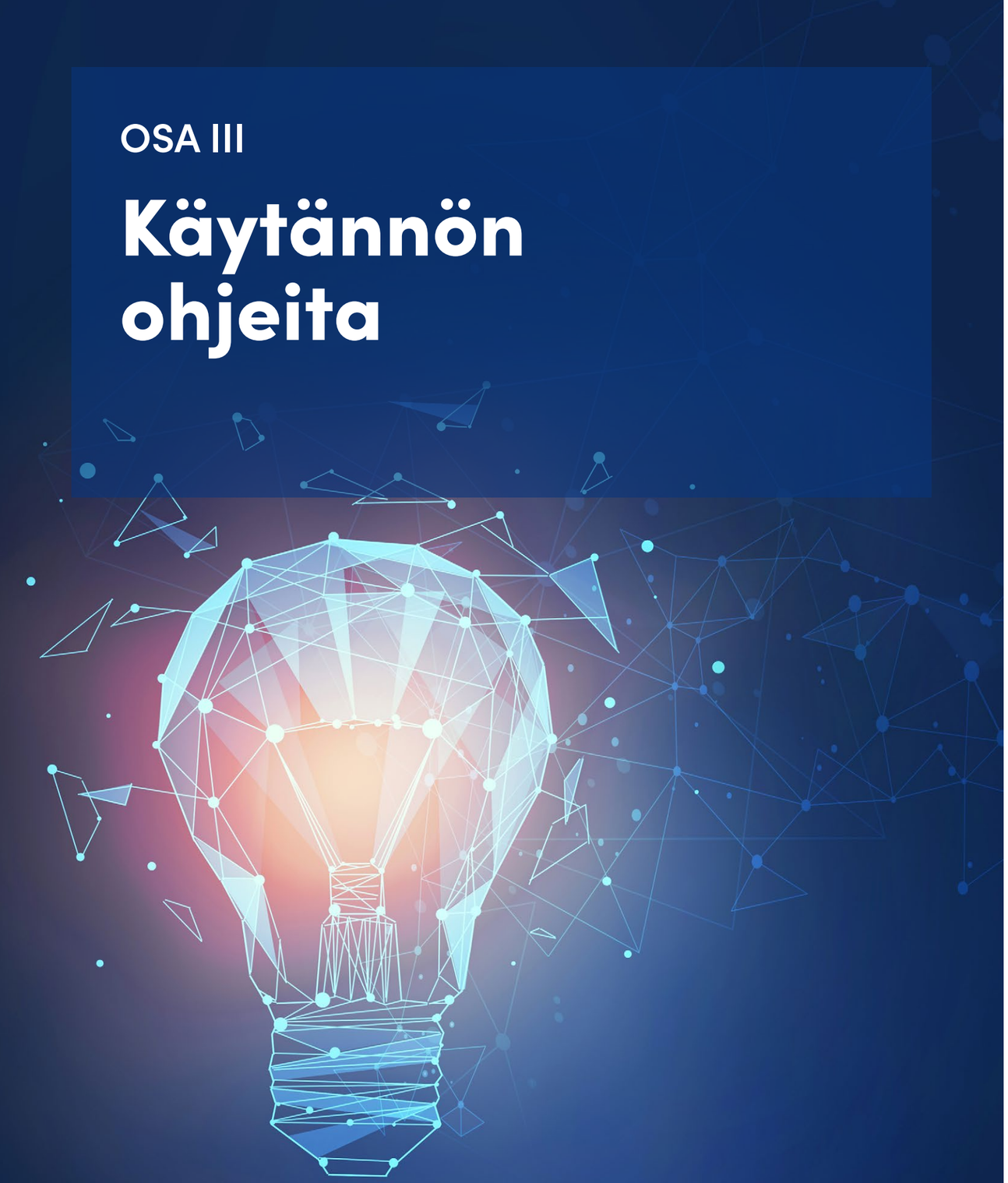
Poliisi tutkii Kikan puhelimen ja läppärin sekä selvittää yhteydenpitoväitteiden paikkansapitävyyden. Niistä löytyy näyttöä kertomukselle sekä ulkomainen puhelinnumero ja sähköpostit, jotka Kikka oli yrittänyt poistaa. Poliisi jatkaa tapauksen selvittämistä esimerkiksi kansainvälisten oikeusapupyyntöjen avulla ja yrittää saada selville, kuka houkutteli Kikan hämärähommiin.

Lopuksi

Fiktiivinen tapaus Ekorenkaista viittaa vahvasti yritysvakoiluun ja osoittaa, että rikollinen voi hyödyntää monia väyliä yrittäessään päästä käsiksi uhriinsa. Jälkien perusteella rikollinen on ollut kiinnostunut juuri tuotekehitysympäristöstä ja etsinyt Ekorenkaiden työntekijöiden sosiaalisen median profiileja verkosta, koska myöhemmin paljastui, ettei Kikka ollut ainoa työntekijä, johon hän oli ollut yhteydessä. Kikan tilapäisesti haastava elämäntilanne teki hänestä kuitenkin alttiin vaikutusyrityksille. Kikan ja rikollisen viestittely muistutti luonteeltaan rakkaushuijausta. Pala palalta rikollisen onnistui rakentaa luottamus Kikkaan ja vakuuttaa, että hänellä on ratkaisu tämän ongelmiin. Vaikka tapauksen selvittely oli vielä kesken, Ekorenkaat aloitti käytäntöjensä muuttamisen. Yritys otti käyttöön kaksivaiheisen tunnistautumisen Office 365 -ympäristöön, lisäsi henkilöstön tietoturvakoulutusta erilaisista vaikuttamisyrityksistä verkossa sekä kehitti yhteistyötä fyysisen turvallisuuden ja tietoturvaryhmän välillä, jotta kokonaiskuva turvallisuuspoikkeamista olisi jatkossa samassa paikassa.

OSA III

Käytännön ohjeita



Kyberrikos, tietoturvaloukkaus… minne ilmoitetaan mitäkin?

Kyberrikosten lisäksi kyberturvallisuudessa puhutaan usein poikkeamista ja tietoturvaloukkauksista. Sanastokeskus TSK on määrittänyt Kyberturvallisuuden sanastossaan, että **tietoturvaloukkaus on ”oikeudeton puuttuminen tietoon tai tietojärjestelmään”***. Poikkeamaksi voidaan kutsua tapahtumaa, joka eroaa normaalista.

Kaikki poikkeamat eivät ole haitallisia. Aina ei ole helppo tunnistaa, milloin poikkeamasta tulee tietoturvaloukkaus, joten se vaatii selvittämistä. Jos tietoturvaloukkaus johtuu jonkun oikeudettomasta, luvattomasta toiminnasta, sama tapaus on mitä todennäköisimmin myös rikos. Tällaisia ovat esimerkiksi tilanteet, joissa tietojärjestelmään on tunkeuduttu tai yritetty tunkeutua oikeudetta, palvelua on häiritty tahallaan tai järjestelmiä on käytetty luvatta.

Toisinaan tapauksesta tulee ilmoittaa usealle viranomaiselle

Suomessa on useita viranomaisia, joille ilmoittaminen on lakisääteistä tai suotavaa tietoturvaloukkauksen osuessa kohdalle. Saman tapauksen raportoiminen usealle viranomaiselle ja luvan antaminen tapauksen käsittelyyn yhdessä on monesti hyödyllistä. Ilmoitusten laatimisesta aiheutuvan vaivannäön jälkeen yhteistyö voi säästää selvityksiin käytettyä aikaa ja resursseja. Valitettavasti Suomessa ei ole vielä mahdollista ilmoittaa kaikille tarvittaville viranomaisille yhdellä lomakkeella.

▸ **Kenelle ilmoittaa mitäkin? Katso vinkit seuraavalta sivulta.**

* Sanastokeskus TSK (2018). Kyberturvallisuuden sanasto. TSK 52, s. 17. Saatavilla 15.1.2021: https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Tietoturvaloukkaus osui kohdalle, kenelle ilmoitamme?

- Ilmoittakaa rikosepäilyt poliisille matalalla kynnyksellä

https://poliisi.fi/tee-rikosilmoitus

- Ilmoittakaa tietoturvaloukkaukset Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle. Kyberturvallisuuskeskus tarvittaessa auttaa ja opastaa tietoturvaloukkauksen uhria. Yhteydenotot käsitellään luottamuksellisesti

https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

- Henkilötietojen tietoturvaloukkauksesta on dokumentointivelvollisuus ja tapauksesta tulee ilmoittaa Tietosuojavaltuutetun toimistoon ilman aiheetonta viivytystä mahdollisuuksien mukaan 72 tunnin kuluessa tapauksen huomaamisesta, jos siitä aiheutuu riski kohteeksi joutuneille henkilöille. Jos riski on korkea, myös loukkauksen kohteena oleville henkilöille on ilmoitettava.

https://tietosuoja.fi/tietoturvaloukkaukset

- NIS-direktiivin tarkoittamille yhteiskunnan kannalta kriittisille toimijoille on asetettu oma ilmoitusvelvollisuus valvovalle viranomaiselle. Voitte tarkistaa toimialakohtaiset valvontaviranomaiset ja tehdä lakisääteisen ilmoituksen Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen sivuilla. Samalla lomakkeella voi antaa tapauksen tiedoksi myös Kyberturvallisuuskeskukselle.

https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkosto-johtaminen/nis-koordinointi-ja-viranomaisyhteistyo

Pohdittavaksi

- **Olemmeko velvollisia tai onko suotavaa ilmoittaa vielä muualle?**
- **Mitä meitä koskeva, esimerkiksi toimialakohtainen, lainsäädäntö sanoo asiasta?**
- **Mihin tekemämme sopimukset ja antamamme sitoumukset velvoittavat?**
- **Onko luokiteltua viranomaistietoa voinut päätyä vääriin käsiin?**
- **Voivatko myös kumppanimme tai asiakkaamme olla vaarassa?**

Rikosilmoituksen tekeminen

Ilmoittakaa kyberrikoksesta matalalla kynnyksellä ja mahdollisimman tuoreeltaan, että todistusaineisto paitsi tapahtumakulusta myös epäillyn toimista saadaan turvatuksi oikeusvarmalla tavalla. Huomioikaa, että todistusaineistoa voi helposti kadota tai sen luotettavuus voi vaarantua, jos ette ole varma sen oikeasta käsittelystä. Ottakaa yhteyttä poliisiin, vaikka jokin muu taho taltioisi jo jälkiä, sillä taltioinnin painopiste on erilainen aineiston käyttötarkoituksesta riippuen.

Tehkää ilmoitus samalla tavalla kuin muidenkin rikosten osalta: käymällä poliisilaitoksella tai täyttämällä sähköinen rikosilmoitus.

Tuokaa selvästi esille, että kyseessä on tietojärjestelmään kohdistunut rikos ja tilanteen välittömät vaikutukset. Arvio asian kiireellisyydestä ja minkälaista asiantuntemusta rikoksen selvittämisen alkutoimet edellyttävät, tehdään ilmoituksen perusteella. Parhaassa tapauksessa rikosilmoituksen vastaanottaja pystyy konsultoimaan tietotekniseen tutkintaan erikoistunutta poliisihenkilöstöä välittömästi.

Rikosilmoituksen tekeminen edellyttää tunnistautumista. Esimerkiksi sähköisen rikosilmoituksen voi täyttää henkilö, jolla on oikeus asioida yrityksen puolesta. Valtuutuksen voi tehdä Suomi.fi-verkkopalvelussa.

Antakaa mahdollisimman tarkat alkutiedot tapahtumasta sen hetkisen käsityksen perusteella. Niitä voi täydentää jälkikäteen. Havaitusta tapauksesta on parempi tehdä rikosilmoitus vajaammin tiedoin kuin jättää ilmoittamatta tai lykätä ilmoittamista. Esimerkiksi tietojärjestelmään tunkeutumisen tapahtumakulusta ja vaikutuksista harvoin tiedetään aluksi muuta kuin merkit, joista se on havaittu.

Jos ette voi olla heti yhteydessä poliisiin, pitäkää rikoksen kohteeksi joutuneet laitteet mahdollisuuksien mukaan käynnissä, mutta irrottakaa ne verkosta vahinkojen rajaamiseksi.

- **Millaista tietoa poliisi tarvitsee kyberrikostutkinnan aikana? Lisää sivulla 33.**

- **Poliisilaitosten yhteystiedot**
https://poliisi.fi/yhteystiedot
- **Poliisin sähköinen rikosilmoitus** – tapauksille, jotka eivät vaadi välittömiä poliisin toimenpiteitä https://asiointi.poliisi.fi.
- **Nettivinkki** – kiireettömille tapauksille, joissa rikosilmoituksen kynnys ei vielä ylity. Nettivinkki ei ole rikosilmoitus, vaan sillä voi ilmoittaa esim. vihjetietoa, kuten laitonta materiaalia verkossa. Nettivinkin voi tehdä myös anonyymisti https://poliisi.fi/nettivinkki.

Ajantasainen yleisohjeistus rikosilmoituksen tekemiseen löytyy poliisin verkkosivuilta.

Varautukaa kertomaan rikosilmoituksessa seuraavista asioista

1. Vapaamuotoinen kuvaus tapahtumista ja tehdyistä toimenpiteistä sellaisena kuin tiedossa

- Mitä on tapahtunut, kenelle ja miten? Mitkä ovat tapahtuman vaikutukset ja vahingot? Onko yritys jo palannut normaalitilaan vai onko tapahtuma vielä käynnissä? Onko jotain tietoa voinut vaarantua – minkälaista ja miten paljon, esim. henkilötietoja tai liikesalaisuuksia? Miten tapahtuma huomattiin? Mihin toimenpiteisiin tapahtuman johdosta on ryhdytty? Onko muihin viranomaisiin oltu yhteydessä? Onko jokin yksityiskohta kiinnittänyt huomiota tai onko yrityksessä tapahtunut muuta poikkeavaa?

2. Tapahtumakulusta kertovat todisteet

- Todistusaineiston taltioinnin suunnittelu on poliisin tehtävä, mutta digitaaliset jäljet katoavat valitettavan nopeasti. Jos yrityksellä on antaa jotain materiaalia, siitä voi mainita rikosilmoituksen yhteydessä tai – ilmoitustavasta riippuen – toimittaa materiaalin suoraan poliisille. Tällaista tietoa voi olla esimerkiksi kopiot tai kuvat epäilyttävistä viesteistä tai muusta näytöllä näkyvästä toiminnasta, joka viittaa rikokseen. Myös lokitietoja, tehtyä dokumentaatiota, analyysia tai esimerkiksi haittaohjelmanäytteen voi toimittaa.

3. Yhteystiedot ja osoitteet

- Missä yritys ja sen toimipisteet sijaitsevat? Entä missä rikoksen kohteeksi joutuneet tietojärjestelmät sijaitsevat – onko kyse yrityksen omista järjestelmistä vai palveluntarjoajalta tilatuista ostopalveluista? Keneltä voi kysyä lisätietoja sekä tapauksesta yleensä että tietojärjestelmille koituneista vahingoista?

4. Milloin tapahtuma huomattiin?

- Mihin ajankohtaan ja kellonaikaan ensihavainnot tapahtumasta tehtiin. Rikoksen tekoaika ja sen havaitsemisaika voivat erota toisistaan.

5. Onko yrityksellä käsitystä, kuka voisi olla rikoksen takana?

- Onko merkkejä, että kyse voisi olla kohdennetusta hyökkäyksestä? Kyberrikosten tekijä on uhrille usein tunnistamaton tai tuntematon.

6. Vaaditko rangaistusta?

- Osa kyberrikoksista on virallisen syytteen alaisia ja osa asianomistajarikoksia. Asianomistajarikoksen tutkiminen edellyttää pääsääntöisesti asianomistajan eli uhrin rangaistusvaatimusta. Jos asianomistaja ilmoittaa poliisille eikä vaadi rangaistusta, tutkintaa ei aloiteta, ellei erittäin tärkeä yleinen etu niin vaadi. Asianomistaja menettää syyteoikeutensa, jos hän ei vaadi rangaistusta asianomistajarikoksessa. Sen sijaan virallisen syytteen alaisen rikoksen tutkinnan aloittamiseen asianomistaja ei voi vaikuttaa ilmoituksen tekemisen jälkeen. Näin ollen virallisen syytteen alaisesta rikoksesta tehtyä ilmoitusta ei voi myöskään perua.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

Millaista tietoa poliisi tarvitsee kyberrikostutkinnan aikana?

Tieto- ja viestintäjärjestelmään kohdistuvan rikoksen esitutkinta yrityksessä edellyttää poliisin ja yrityksen yhteistyötä. Käytännössä se tarkoittaa, että myös yritykseltä kuluu resursseja tähän yhteistyöhön. Rikostutkinnassa yhdistyy perinteisen poliisitoiminnan, kuten asiasta tietävien henkilöiden puhuttamisen ja tietopyyntöjen lisäksi tietoteknisen tutkinnan menetelmiä. Puhuttamalla ja kuulustelemalla poliisi kartoittaa esimerkiksi mitä yrityksen henkilökunta tietää tapahtumista ja millaisia havaintoja yrityksessä on tehty. Tietopyyntöjen tarkoitus on saada viitteitä epäillyn henkilöllisyydestä ja pyrkiä yhdistämään tapaus muihin kotimaisiin tai kansainvälisiin rikostapauksiin.

Parhaassa tapauksessa yrityksen ja viranomaisten toimet tukevat toisiaan ja voimien yhdistämisellä saavutetaan lopputulos, johon mikään taho ei olisi yksin pystynyt.

Tietotekninen tutkinta puolestaan rakentaa käsityksen rikoksen kohteeksi joutuneesta kybertoimintaympäristöstä ja taltioi sekä analysoi sieltä löytyviä jälkiä tapahtumakulusta ja epäillyistä henkilöistä oikeusvarmalla tavalla. Parhaassa tapauksessa yrityksen omat ja viranomaisten toimet tukevat toisiaan ja voimien yhdistämisellä saavutetaan lopputulos, johon mikään taho ei olisi yksin pystynyt.

Poliisilta kysytään usein yleisohjetta, miten uhriksi joutunut yritys voi taltioida tieto- ja viestintäjärjestelmään kohdistuneen rikoksen jäljet. Kulloinkin relevantti todistusaineisto sekä toimenpiteet ovat kuitenkin tapauskohtaisia ja poliisi ohjeistaa tai suorittaa todistusaineiston taltioinnin ja muut tarvittavat toimenpiteet tilanteen mukaan. Varhainen yhteydenotto poliisiin on tärkeää, etteivät nämä jäljet tuhoudu tai sotkeudu.

1. Tiedetäänkö ja millä perustein, onko tilanne jo asianomistajalla hallinnassa vai onko hyökkääjällä edelleen pääsy järjestelmiin?

- Onko asianomistajalla jo toimintasuunnitelma? Millainen?

2. Millaista vahinkoa asianomistajalle on aiheutunut ja miten laajasta vahingosta arvioidaan olevan kyse?

- Voiko ongelma laajentua yrityksen ulkopuolelle?

3. Millainen rakenne ja millaiset yhteydet sekä keskinäisriippuvuudet järjestelmillä on?

- Ovatko järjestelmät yrityksen omia vai mitä palveluntarjoajia on mukana?
- Miten eri tahojen vastuut ja roolit on rajattu? Kuka omistaa minkäkin datan ja mitä sen käsittelystä on sovittu?
- Jos järjestelmissä on riippuvuuksia ulospäin esimerkiksi toisen yrityksen järjestelmiin, onko lokit näistä tiedonsiirroista saatavilla?
- Millaisin tietoturvaratkaisuin järjestelmiä ja dataa on suojattu? Onko tietoturvaratkaisuista tullut hälytyksiä, jotka voisivat liittyä asiaan?
- Myös järjestelmien ylläpito, versiot, päivitysyklit ja kellonaikojen erot ovat tärkeää tietoa.

4. Onko todistusaineiston taltiointia ja selvittämistä jo tehty, kuka sen on tehnyt ja miten toimenpiteet on dokumentoitu?

- Onko tapahtumia ja toimenpiteitä laitettu esimerkiksi aikajanalle?
- Onko jokin muu taho, kuten Traficomin Kyberturvallisuuskeskus tai yksityinen tietoturva-alan yritys tehnyt jotain analyysia?

5. Millainen lokituspolitiikka yrityksen tietojärjestelmissä ja sen osissa on ollut?

- Onko vielä saatavissa muita jälkiä kuin jo tallennetut?
- Onko jotain tapaukseen liittyviä laitteita irrotettu jo verkosta, mutta pidetty vielä käynnissä, että niistä voisi taltioida todistusaineistoa?
- Onko jotain jälkiä mahdollisesti jo kadonnut esimerkiksi laitteiden sulkemisen tai uudelleenasennuksen takia?
- Onko lokituksen yksityiskohtaisuutta tarpeellista tai mahdollista nostaa tilapäisesti?

6. Millaisia varmuuskopioita on saatavilla?

- Kattavatko ne toiminnot ja järjestelmät, jotka voivat liittyä tapaukseen? Ovatko aikajänteet riittävän pitkät?

7. Voiko muuta todistusaineistoa olla vielä joillakin laitteilla?

- Poliisi voi pyytää rikostutkinnan aikana tutkittavaksi esimerkiksi haittaohjelman saastuttaneita laitteita tai ottaa niistä kopiot. Työ pyritään hoitamaan niin, että siitä aiheutuu mahdollisimman vähän haittaa liiketoiminnalle.

8. Voiko sisäisen epäillyn sulkea pois?

- Onko joillakin henkilöillä pääsy käsittelemään tietojärjestelmiä niin, että sillä voi olla vaikutusta todisteisiin?
- Keillä henkilöillä on ylläpitotason oikeudet?
- Keillä on pääsy tietojärjestelmä- ja tietoturvallisuuskuvauksiin sekä dokumentaatioon?
- Onko kenenkään käyttäjätunnuksilla kirjauduttu poikkeavasti?
- Onko yhteistyökumppaneilla pääsy yrityksen tietojärjestelmiin? Mihin?
- Onko entisten työntekijöiden käyttäjätunnukset suljettu?

9. Onko käsitystä, millaista luottamuksellista aineistoa on voinut vaarantua?

- Kuka voisi hyötyä luottamuksellisesta aineistosta?

10. Millaisesta hyökkäyksestä on kyse?

- Onko merkkejä, että kyse olisi kohdennetusta hyökkäyksestä?
- Voiko varsinainen kohde tai tarkoitusperä olla muu kuin ensisilmäyksellä vaikuttaa?

11. Onko yritys ollut aiemmin kyberrikoksen kohteena?

- Ilmoitettiinko asiasta tuolloin poliisille tai muille viranomaisille?

12. Onko henkilökunta tai valvontakamerat havainneet mitään erikoista?

- Liikkuuko yrityksen tiloissa ulkopuolisia henkilöitä? Onko havaittu poikkeavia tapahtumia?
- Onko havaittu poikkeavia mainintoja sosiaalisessa mediassa tai mahdollisia tietojenkalasteluyrityksiä?
- Onko henkilökunta osallistunut yrityksen ulkopuolisiin tilaisuuksiin, joissa laitteita olisi voinut saastua?

13. Onko asiasta tiedottamistarvetta?

- Poliisin kanssa on syytä keskustella esitutkinnan aikaisesta ulkoisesta viestinnästä ja sen mahdollisista vaikutuksista tutkintaan ennen toimenpiteitä.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

Kuinka varautua kyberrikoksiin?

Yrityksen johdon, henkilökunnan ja kumppanien on tärkeä tiedostaa, että kyberrikos voi käynnistää tapahtumaketjun, jossa liiketoiminnalle aiheutuu vakavia häiriöitä tai vahinkoja (fiktiiviset tapahtumakuvaukset kiristyshaittaohjelmasta ja yritysvakoilusta sivuilla 20–27).

Yrityksen koosta ja toimialasta riippumatta on tärkeää, että tunnistetaan kyberturvallisuuden kehittämisen merkitys osana riskienhallintaa.

Tämä opas käsittelee ensisijaisesti kyberrikosten ilmoittamista poliisille ja kuinka yritys voi omilla toimillaan tukea rikostutkinnan onnistumista. Kyberrikollisuuteen varautuminen on kuitenkin vain yksi kyberturvallisuuden osa-alue. Rikoksen kohteeksi joutumisen todennäköisyyttä ja haitallisia vaikutuksia voi vähentää samalla tavalla kuin muidenkin kyberriskien eli huolehtimalla kyberturvallisuudesta yleisesti. Yrityksen koosta ja toimialasta riippumatta on tärkeää, että yrityksessä on tunnistettu kyberturvallisuuden kehittämisen merkitys osana riskienhallintaa.

Avun pyytäminen

Kyberrikoksen kanssa ei tarvitse jäädä yksin. Seuraavalle sivulle on koottu keskeisiä toimijoita ja niiden tehtäviä, miltä yritys voi saada apua kyberrikospulmiin. Huomatkaa, että osalla toimijoista rooli painottuu ennaltaehkäisyyn ja varautumiseen, kun taas toisista on apua akuutin tilanteen ratkaisussa.

Ostopalveluista ja avusta huolimatta kyberturvallisuus on ennen kaikkea yrityksen itsensä asia, joka vaatii perehtymistä koko organisaation tasolla. Kyberturvallisuuden arviointia ja kehittämistä varten on myös olemassa useita erilaisia kaupallisia ja vapaasti saatavilla olevia itsearviointityökaluja, joiden avulla yritys voi arvioida kyberturvallisuutensa nykytilan sekä määrittää kehitystarpeet. Esimerkiksi Traficomin Kyberturvallisuuskeskuksen tarjoama Kybermittari sekä JYVSECTECin* ylläpitämä Finnish Cyber Security Certificate -sertifiointijärjestelmä, FINCSC, ovat tällaisia työkaluja. Itsearvioinnissa on syytä olla rehellinen, jotta arvioinnin tulos todella kuvaa nykytilaa.

- **Lisätietoja Kybermittarista** https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari
- **Lisätietoja FINCSC:sta** https://www.fincsc.fi

* JYVSECTEC on Jyväskylän ammattikorkeakoulussa toimiva kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus.

Keskeisiä toimijoita, jotka auttavat yrityksiä kyberrikostilanteessa ja siihen varautumisessa

Poliisi

Poliisin tehtäviä ovat rikosten selvittäminen, syyteharkintaan saattaminen, ennalta estäminen ja paljastaminen. Esitutkinnan aikana selvitetään epäillyn rikoksen tapahtumakulku, siihen liittyvät henkilöt, saatu rikoshyöty, aiheutunut vahinko ja asianomistajan eli uhrin vaatimukset.

Poliisille ilmoitetaan rikosepäilyistä tekemällä rikosilmoitus. Poliisi vastaanottaa myös vihjetietoa kyberrikoksista. Esimerkiksi epäilyttävästä materiaalista verkossa voi ilmoittaa poliisin Nettivinkin kautta.

Kyberrikoksia tutkitaan paikallispoliisissa ja Keskusrikospoliisin (KRP) yhteydessä toimivassa Kyberrikostorjuntakeskuksessa. KRP:ssä keskitytään vakavien, kansainvälisten tai paljon erityisresursseja vaativien rikosten tutkintaan.

poliisi.fi

Suojelupoliisi

Suojelupoliisin tehtäviä ovat kaikkein vakavimpien kansallisen turvallisuuden uhkien, kuten valtiollisen vakoilun ja terrorismin, ennaltaehkäisy ja torjunta. Valtion laiton tiedustelu voi kohdistua myös yrityksiin. Supo tekee myös henkilö- ja yritysturvallisuusselvityksiä.

Suojelupoliisi on tiedusteluviranomainen ja yhteydenotto siihen tapahtuu usein muiden viranomaisten kautta, mutta myös suora yhteydenotto on mahdollista vakavissa kansallisen turvallisuuden uhkissa.

supo.fi

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus

Kyberturvallisuuskeskuksen tehtäviä ovat tietoturvallisuuden tilannekuvan ylläpito, tietoturvallisuusuhkista viestiminen sekä auttaminen tietoturvaloukkauksen selvittämisessä, tutkimisessa ja toimenpiteiden koordinoimisessa. Keskus julkaisee ohjeita ja parhaita käytänteitä organisaatioille kyberturvallisuuden arvioimiseksi ja kehittämiseksi sekä kyberturvallisuusuhkilta suojautumiseksi.

Kyberturvallisuuskeskus vastaa myös viestintäverkkojen ja -palvelujen, vahvojen sähköisten tunnistuspalvelujen ja sähköisten luottamuspalvelujen sekä muiden digitaalisten palveluiden luotettavuuden ja tietoturvallisuuden ohjauksesta ja valvonnasta kuin myös kyberturvallisuusuhkiin ennakolta varautumisesta.

Kyberturvallisuuskeskus vastaanottaa ilmoituksia tietoturvaloukkauksista. Yhteiskunnan kannalta kriittiset toimijat voivat tehdä sen kautta myös NIS-direktiivin velvoittamat ilmoitukset valvoville viranomaisilleen.

kyberturvallisuuskeskus.fi

Tietosuojavaltuutetun toimisto

Tietosuojavaltuutetun toimisto opastaa, mitä kaikkien organisaatioiden on huomioitava henkilötietojen käsittelyssä ja valvoa, että tietosuojalainsäädäntöä noudatetaan.

Henkilötietojen tietoturvaloukkauksesta on dokumentointivelvollisuus ja tapauksesta tulee ilmoittaa Tietosuojavaltuutetun toimistoon ilman aiheetonta viivytystä mahdollisuuksien mukaan 72 tunnin kuluessa tapauksen huomaamisesta, jos siitä aiheutuu riski kohteeksi joutuneille henkilöille. Jos riski on korkea, myös loukkauksen kohteena oleville henkilöille on ilmoitettava.

tietosuoja.fi

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

Huoltovarmuuskeskus

Huoltovarmuuskeskus ylläpitää ja kehittää huoltovarmuuden ylläpitämiseen liittyvää suunnittelua, toteutusta ja operatiivista varautumistoimintaa, missä digitaalinen turvallisuus sisältäen kyberturvallisuuden on yksi merkittävä osa-alue. Kyberuhkiin liittyvästä varautumisesta huolehtii Infrastruktuuriosasto.

Huoltovarmuuskeskuksen alaisuudessa toimii Huoltovarmuusorganisaatio, joka koostuu toimialakohtaisista pooleista. Poolit ovat elinkeinoelämän, keskeisten viranomaisten ja järjestöjen muodostamia verkostoja, jotka vastaavat operatiivisesta varautumisesta, kuten yrityksille järjestettävistä koulutuksista, harjoituksista ja ohjeistuksesta. Kyberturvallisuuteen liittyen keskeinen toteuttaja on Digipooli, mutta kehitystarpeiden osalta yhteistyö on kiinteää kaikkien poolien kanssa.

Huoltovarmuuskeskus rahoittaa projekteja ja toimintaa, jotka kehittävät kriittisen infrastruktuurin kyberturvallisuuden toteutumista. Rahoituksella tuetaan mm. Traficomin Kyberturvallisuuskeskuksen palveluiden tuottamista ja kehitystä elinkeinoelämän tarpeisiin. Vuosina 2021-2025 rahoitusta ohjataan Digitaalinen Turvallisuus 2030 -ohjelman kautta.

huoltovarmuuskeskus.fi

Vertaistuki

Kyberrikoksen kohteeksi joutumisesta uskalletaan kertoa aiempaa avoimemmin. Muiden kokemusten kuuleminen auttaa uhriksi joutunutta yritystä huomaamaan, ettei se ole suinkaan tilanteessaan ainoa. Lisäksi muiden kokemuksista voi oppia.

Omalle kohdalle osuneesta kyberrikoksesta selvittyämme, olisimmeko valmiita antamaan vertaistukea joko suoraan jollekin toiselle yritykselle tai kertomaan kokemuksestamme laajemmalle kuulijakunnalle?

Yksityiset yritykset

Monet organisaatiot ovat ulkoistaneet kaupallisille palveluntarjoajille esimerkiksi kybertoimintaympäristönsä – tai niiden osan – rakentamisen, laitekannan, ylläpidon sekä ostavat myös tarvitsemansa palvelut, kuten sähköpostijärjestelmän, tallennus- ja työtilat, sisäiset ja ulkoiset verkkosivut sekä käyttämänsä sovellukset.

Ostopalveluina on mahdollista hankkia lisäksi esimerkiksi tietoturvaratkaisuja, järjestelmien haavoittuvuuksien kartoittamista, haittaohjelma-analyysia, kybertoimintaympäristöjen auditointia, tietoturvapoikkeamien reaaliaikaista havaitsemista ja ratkaisua sekä vahingoittuneiden järjestelmien palauttamista.

Ostettujen palvelujen sisällöt, rajoitukset ja vastuut määritellään sopimuksissa. Mitä solmimamme sopimukset sanovat kyberrikoksista? Millaista varautumista ja apua voimme odottaa niiden perusteella? Entä jääkö sopimuksiin katvealueita, joihin meidän tulisi varautua?

Kolmannen sektorin toimijat voivat valvoa yritysten etuja ja levittää tietoisuutta kyberrikoksista ja niihin varautumisesta. Lisäksi Suomessa on vapaaehtoistoimijoita, jotka auttavat organisaatioita myös akuuteissa tietoturvaloukkauksissa.

Pohdittavaksi

- **Mitkä ovat yrityksellemme tärkeät tahot, joilta saamme tai pyydämme apua kyberrikollisuuteen varautumisessa? Entä tilanteen ollessa akuutti?**
- **Tiedämmekö miten ja minne otamme yhteyttä?**
- **Onko vielä muita, juuri meille tärkeitä tahoja, kuin edellä mainitut?**

Rikosilmoituksen tekeminen on yksinkertaisempaa, kun yrityksellä on toimintamallit valmiina.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

Suunnitelkaa rikoksesta ilmoittaminen etukäteen

On normaalia, että rikoksen kohteeksi joutuminen säikäyttää. Tilanne voi herättää paljon kysymyksiä, pelkoja ja pakottaa tekemään paineen alla päätöksiä, jotka eivät jälkikäteen pohdittuna olleet välttämättä niitä parhaita. Rikosilmoituksen tekeminen on yksinkertaisempaa, kun yritys on valmistautunut siihen etukäteen ja määritellyt päätöksentekoprosessin ja politiikan, millaiset tapaukset ilmoitetaan poliisille.

1. Millaiset kyberrikokset ilmoitamme poliisille? Miksi tai miksi emme?

- Rikoksesta ilmoittaminen poliisille on uhrin oikeus ja tärkeä osa rikosoikeusjärjestelmän toimintaa, mutta samalla päätös, jossa vastakkain voi olla useita intressejä.
- Sivuilla 8–11 kerrotaan, miksi rikoksesta kannattaa ilmoittaa ja toisaalta, miksi näin ei aina tapahdu.

2. Miten toimimme, jos havaittu tietoturvaloukkaus saattaa täyttää myös rikoslain tunnusmerkistön?

- Keiden yrityksessämme pitää saada tieto asiasta ja miten nopeasti?
- Keillä on valtuudet tehdä nopeitakin päätöksiä tietoturvaloukkauksen eskaloituessa?
- Onko todistusaineiston turvaamisen alkutoimien järjestämistä pohdittu?

3. Kuka tai ketkä yrityksessämme päättävät poliisille ilmoittamisesta?

- Tiedämmekö missä ja miten rikosilmoitus tehdään, kuka sen tekee ja mitä tietoa ilmoitusta varten tarvitaan? Lue lisää sivuilta 31–34 .
- Keillä on valtuudet toimia yhteyshenkilöinä esimerkiksi kybertoimintaympäristön, toimitilaturvallisuuden, viestinnän ja yrityksen johdon näkökulmista tutkinnan aikana?

4. Miten viestimme kyberrikoksesta sisäisesti ja yrityksen ulkopuolelle?

- Harkittu ulostulo ajoissa on yleensä parempi kuin reagoiminen esimerkiksi rikollisen jo vuotamaan tietoon. Lisäksi sähköiset viestintäkanavat voivat olla pois käytöstä rikoksen johdosta.
- Tutkinnanjohtaja päättää esitutkinnasta tiedottamisesta, joten esitutkinta voi vaikuttaa myös ulkoiseen viestintäämme.
- Rikosprosessin kautta tapauksesta tulee julkinen ja se voi herättää median kiinnostuksen.

5. Tiedämmekö asianomistajarikosten ja virallisen syytteen alaisten rikosten eron?

- Osa tieto- ja viestintäjärjestelmiin kohdistuvista rikoksista on asianomistajarikoksia ja osa virallisen syytteen alaisia rikoksia. Asianomistajarikoksen eteneminen rikosprosessissa edellyttää pääsääntöisesti asianomistajan eli uhrin rangaistusvaatimusta. Jos asianomistaja ilmoittaa tapauksesta poliisille, mutta ei vaadi rangaistusta, tutkintaa ei aloiteta, ellei erittäin tärkeä yleinen etu niin vaadi. Toisin sanoen, luopumalla rangaistusvaatimuksesta uhri luopuu oikeudestaan saattaa mahdollinen rikos syytettäväksi. Tällöin uhri ei voi nostaa myöhemmin myöskään siviilikannetta samasta asiasta.
- Jos uhri haluaa keskeyttää asianomistajarikoksen tutkinnan tai estää syytteen nostamisen, se onnistuu ilmoittamalla, ettei vaadi enää tekijälle rangaistusta. Sen sijaan virallisen syytteen alaisen rikoksen tutkinnan aloittamiseen asianomistaja ei voi vaikuttaa, eikä siten myöskään vaatia tutkinnan keskeyttämistä.

Keinoja parantaa rikoksen selvittämismahdollisuuksia

Tieto- ja viestintäjärjestelmät rikospaikkana edellyttävät samanlaista ymmärrystä ympäristöstä ja siellä tapahtuvista asioista kuin fyysinen rikospaikka. Yritys tuntee toimitilojensa pohjapiirroksen, tietää missä arvokkaat tavarat sijaitsevat, keillä on pääsy niihin ja miten sitä valvotaan.

Samanlainen tuntemus on tärkeä myös kybertoimintaympäristön osalta. Ilman ymmärrystä rikospaikasta ja sinne suunnitelmallisesti asetettuja valvontakeinoja on vaikea selvittää mitä tapahtui, miten ja kuka oli asialla.

Poliisille voi ilmoittaa rikoksesta aina, eikä ilmoittamista tarvitse lykätä tai jättää tekemättä sen takia, ettei jotain tietoja olisi valmiina tai saatavilla. Mutta mitä paremmin rikoksen uhriksi joutunut yritys – tai yrityksen palveluntarjoaja, jolta kybertoimintaympäristö tai palvelu on hankittu – tuntee ja on dokumentoinut ympäristönsä sekä sen sisältämät kriittiset tiedot jo ennen kuin mitään rikosta on tapahtunut, sen nopeammin rikostutkinnassa päästään itse asiaan eli selvittämään tapahtumakulkua ja saattamaan rikollinen vastuuseen teoistaan.

Myös pk-yritysten on tärkeä ymmärtää IT-palveluntarjoajien kanssa tekemänsä sopimukset, niiden sisältö ja rajoitukset. Sopimusten kautta määritellään esimerkiksi vastuita ja toimenpiteitä. Yritykselle voi tulla yllätyksenä, ettei sopimukseen välttämättä kuulu esimerkiksi kattava lokitietojen kerääminen. On tärkeä osa liiketoimintaa tietää, miten palveluntarjoaja huolehtii yrityksen datasta paitsi asioiden normaalitilassa, myös tietoturvaloukkauksen sattuessa.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

Yrityksen oman kybertoimintaympäristön ja sen sisältämien kriittisten tietojen tunteminen nopeuttaa varsinkin rikostutkinnan alkuvaiheita.

Yrityksen valmiudet kyberrikostutkinnan edistämiseksi

Seuraaviin kysymyksiin vastaaminen havainnollistaa yrityksen valmiuksia auttaa poliisia kyberrikostutkinnassa. Monet kohdista saattavat tuntua haastavilta. Todennäköisesti kaikkiin kysymyksiin ei löydy valmista vastausta. Kysymykset auttavat kuitenkin tunnistamaan ongelmakohtia. Sitoutuminen kyberturvallisuuden laajempaan kehittämiseen parantaa samalla myös mahdollisten rikosten selvittämismahdollisuuksia. Apuna voi käyttää esimerkiksi aiemmin mainittuja itsearviointityökaluja (s. 35).

1. Olemmeko kybertoimintaympäristömme paras asiantuntija?

- Onko kybertoimintaympäristömme rakenne ja sen keskinäisriippuvuudet, ylläpito, päivityssyklit, tietoturvaratkaisut sekä yhteydet ulospäin dokumentoitu ajantasaisesti?
- Kenellä on käsitys normaalista verkkoliikenteestämme, jotta poikkeamat pystytään tunnistamaan?
- Ketkä hallitsevat kokonaisuuden? Kokonaisuus voi koostua useista eri ostopalveluista ja omista järjestelmistä, jolloin kokonaiskuva on erityisen tärkeä.

2. Olemmeko määritelleet, suojanneet ja rajoittaneet pääsyä liiketoiminnan kannalta kriittiseen tietoon?

- Kriittistä tietoa voivat olla esimerkiksi tuotekehitys- ja henkilötiedot.
- On helpompi arvioida esimerkiksi tietomurrosta aiheutuneita vahinkoja, kun tiedetään missä erilaista tietoa on, miten se on suojattu ja miten pääsyä on rajattu sekä valvottu.

3. Mikä on yrityksemme (tai palveluntarjoajiemme) kyky valvoa ja tallentaa tietojärjestelmissä tapahtuvia muutoksia?

- Kuinka tunnistamme ja raportoimme poikkeavat tapahtumat?
- Keräämmekö riittävän laajasti lokitietoja tärkeistä toiminnoista ja säilytämmekö ne riittävän pitkään sekä erillään muusta järjestelmästä? Entä onko pääsy lokeihin rajoitettu ja niiden muokkaaminen estetty?
- Onko meillä (tai palveluntarjoajillamme) valmius ottaa kopio lokitiedostoista tarvittaessa ja säilyttää se koskemattomana, esimerkiksi tilanteessa, jossa päätöstä rikostutkinnasta ei ole vielä tehty, mutta kyberrikos alkaa vaikuttaa todennäköiseltä?

4. Olemmeko sopineet palveluntarjoajiemme kanssa lokitiedostojen keruusta ja käytöstä?

- Kuka omistaa lokitiedostot, millä edellytyksin ne ovat saatavilla ja mitä on saatavilla, jos tietojärjestelmään kohdistuu rikos?
- Palveluntarjoajien kanssa voi sopia ennakolta myös velvollisuudesta kerätä dokumentaatiota hyökkäyksestä, mikä tähtää tapauksen selvittämiseen.

OSA I
Kyberrikokset yrityksissä ja ilmoittamiseen vaikuttavat tekijät

OSA II
Kyberrikosten esitutkinta

OSA III
Käytännön ohjeita

5. Miten huolehdimme varmuuskopiointikäytännöistä?

- Otammeko varmuuskopioita säännöllisesti ja säilytämmekö ne riittävän pitkän ajan sekä erillään muusta tietojärjestelmästä? Erillään säilyttäminen vähentää riskiä, jotta esimerkiksi kiristyshaittaohjelma ei lukitse myös varmuuskopioita tai palvelinrikko tuhoa niitä.
- Onko varmuuskopiomme myös suojattu salauksella (kryptattu) ja salasanalla, jolloin ne eivät voi vuotaa selkokielisenä ulos yrityksestä?

6. Tiedostammeko, että monet digitaaliset jäljet, joita voisi käyttää todistusaineistona rikoksesta, katoavat varsin nopeasti?

- Poliisiin on tärkeä olla yhteydessä mahdollisimman tuoreeltaan, jotta tarpeellinen todistusaineisto voidaan ottaa talteen rikostutkintaa varten oikeusvarmalla tavalla.

7. Mitä teemme äkillisissä, merkittävissä kyberrikoksissa, joissa päätökset on tehtävä nopeasti?

- Äkillisten tapausten varalle on hyvä sopia toimintatavat etukäteen, esimerkiksi ketkä tekevät päätökset ja mitä päätöksissä painotetaan. Ratkaisevat päätökset voidaan joutua usein tekemään vajain tiedoin.
- Saastuneen laitteen irrottaminen verkosta voi olla ainoa tapa pysäyttää hyökkäys ja estää laajemmat vahingot. Toisaalta laitteen irrottaminen verkosta saattaa samalla antaa rikolliselle merkin, että on aika siivota jäljet, kun teko on paljastunut. Lisäksi olennaista todistusaineistoa häviää helposti, kun saastunut laite irrotetaan verkosta ja sammutetaan.
- Joissakin tapauksissa kopion ottaminen ei kestä muutamaa minuuttia kauempaa eikä muuta kokonaistilannetta. Jokainen tilanne on omanlaisensa eikä yleispätevää ohjetta voi antaa.

8. Tiedostammeko, että kyberrikoksilla ja fyysisen maailman tapahtumilla voi olla yhteys?

- Onko toimitilaturvallisuutemme kunnossa?
- Kannustammeko työntekijöitämme ilmoittamaan verkon ja fyysisen maailman poikkeamista?
- Kenellä yrityksessämme on kokonaiskuva kaikista poikkeamista?

9. Tiedämmekö esitutkinnan tarkoituksen?

- Poliisin suorittaman esitutkinnan tarkoitus on selvittää ja osoittaa todistein tapahtumakulku sekä löytää rikoksesta epäilty.
- Kaikkia rikoksen kohteeksi joutuneita kannustetaan ilmoittamaan nopeasti poliisille. Erityisen tärkeää se on tapauksissa, joissa digitaalisten jälkien alkutaltioinnista ei pystytä muutoin huolehtimaan.
- Mitkä ovat yrityksemme tai palveluntarjoajamme valmiudet tunnistaa ja taltioida digitaalista todistusaineistoa, dokumentoida tehdyt toimenpiteet ja säilyttää kopiot mahdollisimman koskemattomina ja muuttumattomina?

Keskeinen käsitteistö

Asianosainen

”Esitutkinnassa asianosaisia ovat: 1) asianomistaja, 2) rikoksesta epäilty; 3) muu henkilö, jonka oikeuksiin, etuihin tai velvollisuuksiin rikos tai sen selvittäminen voivat vaikuttaa” (ETL 2:5).

Asianomistaja

Asianomistajalla tarkoitetaan rikoksen uhria eli luonnollista tai oikeushenkilöä (esim. yritystä), johon rikos on kohdistunut.

Haavoittuvuus

Haavoittuvuus on alttius tietoturvaan kohdistuville uhkille. Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa.” Sanastokeskus TSK (2018, 15)

Henkilötiedot

Henkilötiedoilla tarkoitetaan ”kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön [...] liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella” EU:n yleinen tietosuoja-asetus (2016/679/EU) (GDPR) artikla 4, kohta 1.

Kohdennettu hyökkäys

Monivaiheinen tietoverkkohyökkäys, joka kohdistuu tiettyyn rajattuun kohteeseen ja joka tehdään haittaohjelmien sekä muiden toimintojen avulla. Kohdistettu haittaohjelmahyökkäys voi suuntautua esimerkiksi yritykseen, toimialaan, valtionhallinnon organisaatioon tai rajattuun joukkoon henkilöitä. Tavoitteena on usein kohteen kriittisen tiedon haltuun saaminen tai kohteen toiminnan muuttaminen. Sanastokeskus TSK (2018, 39)

Kyberrikollisuus

Kyberrikollisuus on tieto- ja viestintäjärjestelmiin kohdistuvaa tai niitä hyväksikäyttäen tehtyä rikollisuutta.

Kybertoimintaympäristö; kyberympäristö

Kybertoimintaympäristö on ”yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva toimintaympäristö.” Sanastokeskus TSK (2018, 21)

Kyberturvallisuus

Kyberturvallisuus on ”tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.” Sanastokeskus TSK (2018, 22)

NIS-direktiivi

NIS-direktiivi on EU:n verkko- ja tietoturvadirektiivi.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. OJ L 194, 19.7.2016, p. 1–30

Palvelunestohyökkäys

Palvelunestohyökkäys on ”tietoverkkohyökkäys, jolla pyritään kuormittamaan ja siten lamaannuttamaan jokin palvelu tai tietojärjestelmä” TSK (2018, 31)

Tietoturvaloukkaus

Tietoturvaloukkaus on ”oikeudeton puuttuminen tietoon tai tietojärjestelmään” TSK (2018, 17)

- Sanastokeskus TSK (2018). Kyberturvallisuuden sanasto. TSK 52. Saatavilla 15.1.2021:

  https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Hyödyllistä lukemistoa

Ohessa linkkejä hyödyllisiksi koettuihin dokumentteihin. Linkkien toiminta on tarkastettu 24.3.2021.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on julkaissut monia hyödyllisiä oppaita, jotka on tarkoitettu eri kohderyhmille: yrityksille ja organisaatioille, tietoturva-ammattilaisille ja yksityishenkilöille. Niiden aihepiirit käsittelevät esimerkiksi etätyön tietoturvaa, tietomurroilta suojatumista ja tietoturvan sertifiointia. Tutustu oppaisiin Kyberturvallisuuskeskuksen sivuilla https://www.kyberturvallisuuskeskus.fi/fi/ohjeet. Lisäksi alle on koottu muutamia esimerkkejä, jotka voivat hyödyttää erityisesti tämän oppaan lukijakuntaa.

- **Kyberturvallisuus ja yrityksen hallituksen vastuu.** Traficomin julkaisuja 2/2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

- **Näin keräät ja käytät lokitietoja.** Tietoturva-ammattilaisille, Traficom. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja

- **Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille.** Traficomin julkaisuja 123/2019. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_pilvipalvelujen_turvallisuudesta_123-2019.pdf

- **Opas tietomurtojen havaitsemiseen.** Tietoturva-ammattilaisille, Traficom. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Opas-tietomurtojen-havaitsemiseen.pdf

- **Pienyritysten kyberturvallisuusopas.** Traficomin julkaisuja 228/2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

- **Suojautuminen Microsoft Office 365 –tunnusten kalastelulta ja tietomurroilta.** Traficomin julkaisuja 12/2019. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Suojautuminen%20Microsoft%20Office%20365%20-tunnusten%20kalastelulta%20ja%20tietomurroilta%20web.pdf

Lainsäädäntö ohjeistaa tietoturvasta huolehtimiseen, tietoturvaloukkauksista ilmoittamiseen ja henkilötietojen käsittelyyn

- **EU:n verkko- ja tietoturvadirektiivi** (2016/1148/EU) – ”NIS-direktiivi” tietoturvavelvollisuuksista ja häiriöraportoinnista. Koskee seuraavia toimialoja: liikenne, energiahuolto, terveydenhuolto, finanssiala, finanssialan infrastruktuuri, vesihuolto, digitaalinen infrastruktuuri ja digitaaliset palvelut.
- **EU:n yleinen tietosuoja-asetus (2016/679/EU)** (GDPR) – henkilötietojen käsittelystä EU:n alueella
- **Laki sähköisen viestinnän palveluista (917/2014)** – sähköisen viestinnän palveluiden laadusta, tietoturvasta ja viestinnän luottamuksellisuudesta. Laki koskee teleyrityksiä, viestinnän välittäjiä, yhteisötilaajia ja verkkotunnusvälittäjiä. Huom! Monet yritykset ovat yhteisötilaajia. Yhteisötilaaja tarkoittaa ”viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä ja yhteisöä, joka käsittelee viestintäverkossaan käyttäjien viestejä, välitystietoja tai sijaintitietoja” (1:3:41). Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus ohjeistaa https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/saantelyn-kohteet, että yritys on yhteisötilaaja, jos se esimerkiksi tarjoaa WLAN-yhteyden toimipisteessään vieraileville, puhelin- ja laajakaistaliittymät työntekijöilleen ja käsittelee sisäverkossaan viestinnän välitystietoja.
- **Tietosuojalaki (1050/2018)** – henkilötietojen käsittelystä
- Katso myös **Rikoslaki (39/1889)** 38:9 ”Tietosuojarikos”.

Oppaan luontiprosessista ja CYBERDI-hankkeesta

Tämä opas on luotu Opetus- ja kulttuuriministeriön rahoittaman CYBERDI-hankkeen aikana 2020 - 2021. Oppaan ovat toteuttaneet Poliisiammattikorkeakoulu (Polamk) ja Jyväskylän ammattikorkeakoulu (JAMK). Lisäksi oppaan tarpeellisuudesta ja sisällöistä on käyty keskusteluja muun muassa Keskusrikospoliisissa sijaitsevan Kyberrikostorjuntakeskuksen, Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen ja Suojelupoliisin kanssa.

Olennainen osa oppaan valmisteluprosessia oli syksyllä 2020 toteutettu sähköinen Delfoi-paneeli ja sitä tukevat haastattelut, joihin ilmoittautui yhteensä yli 40 asiantuntijaa yksityiseltä ja julkiselta sektorilta. Panelistit vastasivat loka-marraskuussa kahteen kyselylomakkeeseen. Ensimmäinen kyselylomake perustui oppaassa esitettyihin, fiktiivisiin tapauskuvauksiin kiristyshaittaohjelmasta ja yritysvakoilusta. Kyseisten tapausten kontekstissa osallistujilta tiedusteltiin esimerkiksi viranomaisille ilmoittamista, suhtautumista julkisuuteen sekä pyydettiin arvioimaan luonnostelemiamme ohjeita poliisille ilmoittamisessa, tutkinnan etenemisessä ja varautumisessa rikoksen kohteeksi joutumiseen. Muokkasimme ohjeita osallistujien kommenttien perusteella ja esitimme ne sekä oppaan sisältöehdotuksia toisella paneelikierroksella. Hyödynsimme annettuja vastauksia oppaan laatimisprosessissa, sekä käytimme myös joitain yksittäisiä, hyvin muotoiltuja virke-ehdotuksia osana tätä opasta. Lähetimme vielä oppaan luonnosversion osallistujille kommentoitavaksi alkuvuodesta 2021.

CYBERDI – Cybercrime prevention, awareness raising and capacity building by RDI on modern cyber attacks on JAMKin ja Polamkin yhteisprojekti. Projektissa kehitetään teknologisesti ja toiminnallisesti parhaita käytäntöjä kyberrikosten estämiseen, tutkimiseen ja selvittämiseen sekä kasvatetaan käyttäjälähtöisesti tietoisuutta digitaalisen maailman uhkista ja rikollisuudesta.

Rahoitus: Opetus- ja kulttuuriministeriö
Toteutus: 10/2018 – 12/2021

Kiitokset

Oppaan työstämiseen osallistuivat Aktia Oy (Henri Heinonen, Keijo Korte ja Timo Wiander), Cinia Oy (Anssi Kärkkäinen), Epec Oy (Keijo Ekola ja Mika Heiskanen), Fingrid Oyj (Jyrki Pennanen), Huld Oy (Riku Nykänen), Kaisanet Oy, Jussi Jaakonaho, Kyberrikostorjuntakeskus (Marko Leponen), Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus (Jukka-Pekka Juutinen ja Miikka Salonen), Lounais-Suomen poliisilaitos (Jami Toivonen), Oy Karl Fazer Ab, S-Pankki Oy (Juha Nieminen ja Petteri Ruohomäki), Steveco Oy, Terveyden ja hyvinvoinnin laitos (THL), Tietosuojavaltuutetun toimisto (Heikki Partanen), Valio Oy (Mika Arvonen) ja Viria Security Oy.

Lisäksi oppaan laadintaan osallistui lukuisa joukko muita toimijoita. Lämmin kiitos kaikille osallistuneille!

CYBERDI-projektitiimin jäsenet

Oppaan laatija: Anna Leppänen | Graafinen suunnittelu: Heli Sutinen | Fiktiiviset tarinat: Joni Ahonen, Heikki Salo, Marko Vatanen ja Jarmo Viinikanoja | Asiantuntijakommentit ja palautteet: Salla Huikuri, Toni Kranz, Tuukka Laava, Jani Peltola, Tommi Rautanen ja Tero Toiviainen.

Oppaan laatija: Anna Leppänen, Polamk | Graafinen suunnittelu: Heli Sutinen, JAMK

Opasta koskeva palaute ja tiedustelut

tutkimus.polamk@poliisi.fi

oletietoinen.fi

Opetus- ja kulttuuriministeriö

POLIISI
POLIISIAMMATTIKORKEAKOULU

JYVSECTEC
by jamk