POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

Tietoverkkorikos, teenkö rikosilmoituksen?

rikosylikomisario Tero Muurman

Keskusrikospoliisi, Kyberrikostorjuntakeskus

Yleistä tietoverkkorikollisuudesta

- Tietoverkkorikollisuudessa piilorikollisuuden määrä on todennäköisesti suuri
  - Yritysten tekemät ilmoitukset ovat aliedustettuja yksityishenkilöiden tekemiin ilmoituksiin nähden
- Organisaatioissa rikosilmoituksen hyötyjä ja haittoja punnitaan tarkoin
  - Maineriski?
  - Maksaako rikosprosessi vaivan? Onko edullisempaa paikata aukot, siivota jäljet ja jatkaa eteenpäin?

Entä sitten?

- Mitä tilastot kertovat päättäjille?
  - Vähän ilmoituksia, joten "kaikki on siis kunnossa" …
    …. Vai onko?
- Korkea ilmoituskynnys on ongelmallinen tietoverkkorikollisuuden tilannekuvan kannalta
  - Toiminnan ohjaaminen..
  - Kouluttautuminen …
  - Työkalujen hankkiminen….
  - Resurssit…

  → valmiuskysymys; olemmeko valmiita, jos/kun alkaa tapahtua?

Miksi tehdä rikosilmoitus

- Yhteiskuntavastuun näkökulma??
  - Osoitetaanko paheksuntaa rikollista tekoa kohtaan vai painetaanko asia niin sanotusti villaisella
  - Valtionhallinnolla korostunut yhteiskuntavastuu

- Rikostutkinta on palapelin kokoamista
  - Uusi rikostutkinta voi tuoda uutta tietoa vanhojen tapausten selvittämiseen
  - Tutkinnassa voi selvitä myös kokonaan uusia tekoja

Miksi tehdä rikosilmoitus?

- Esitutkinta on erinomainen tiedonhankintakeino
  - Ketkä ovat tietoverkkorikosten tekijöitä?
  - Tehdäänkö rikokset ulkomailta, millaista osaamista meillä on Suomessa?
  - Mitä tekotapoja on käytetty, millaisia työkaluja tekijöillä on?
  - Rikollisten verkostot?
  - Rikoshyödyn määrä, poisottaminen?
  - jne…

→ Esitutkinta tuottaa rikosvastuun toteuttamiseen tarvittavan tiedon ohella myös **suojautumisen ja varautumisen** kannalta tärkeää tietoa!

Havaittuja ongelmia

- Logit usein riittämättömiä tai olemattomia
- Ulkoistaminen & palveluketjut
  - Ei tiedetä missä omat tiedot ovat
- Logien omistajuus ja saatavuus
  - Sopimuksissa ei ole huomioitu tietoturvapoikkeamien selvittelyä ja tähän liittyen datan omistajuutta
- Järjestelmien dokumentaation puutteet
  - dokumentaation taso huolellisuuden mittarina

Alkutoimet epäiltäessä tietoverkkorikosta

- Mitä on tapahtunut?
- Mihin tietojärjestelmään tai -verkkoon teko tai tapahtuma on kohdistunut?
- Milloin teko alkoi?, jatkuuko teko tai tapahtuma yhä?
- Millaiset vaikutukset teolla/tapahtumalla on tietojärjestelmään, siinä olevaan dataan tai siihen kytkettynä oleviin muihin laitteisiin, järjestelmiin tai laitoksiin
- Yhteys ViVi:n Kyberturvallisuuskeskukseen ja Poliisiin
  - Huom!! KTK ei ilmoita tietoja Poliisille automaattisesti, eikä koskaan ilman suostumusta.

Tutkinnan turvaaminen

- Varmista, että tietojärjestelmien logit ovat käytettävissä tapahtumien todentamiseksi ja selvittämiseksi
- Logit on tallennettava mahdollisimman kattavasti
- Tiedot mielellään sellaisenaan "raakadatana", toimitustapa voidaan sopia erikseen
  - esim. isot tietomassat
- Perinteisen rikospaikkatutkinnan turvaaminen, jos on viitteitä
  - Fyysisestä tunkeutumisesta tiloihin / muu fyysisen pääsyn hankkiminen tietojärjestelmiin (kodit, autot jne…)
  - Fyysisen tietovälineen tms. avulla tapahtuneesta tunkeutumisesta

Tutkinnan turvaaminen

- Toimenpiteiden dokumentointi
  - Mitä toimenpiteitä on tehty?
  - Kuka on suorittaja?
  - Milloin toimenpiteet on tehty?
- Onko havaintoja tai epäilyjä tekijästä? Mihin em. epäilyt perustuvat?
  - SOME , poikkeamailmoitukset … jne

HUOM! Rikostutkinnassa täsmällisesti tehdyn dokumentaation merkitys on erittäin suuri.

Kiitos

tero.muurman@poliisi.fi
twitter: @TeeJiiM

cybercrime.nbi@poliisi.fi
@kyberkeskus