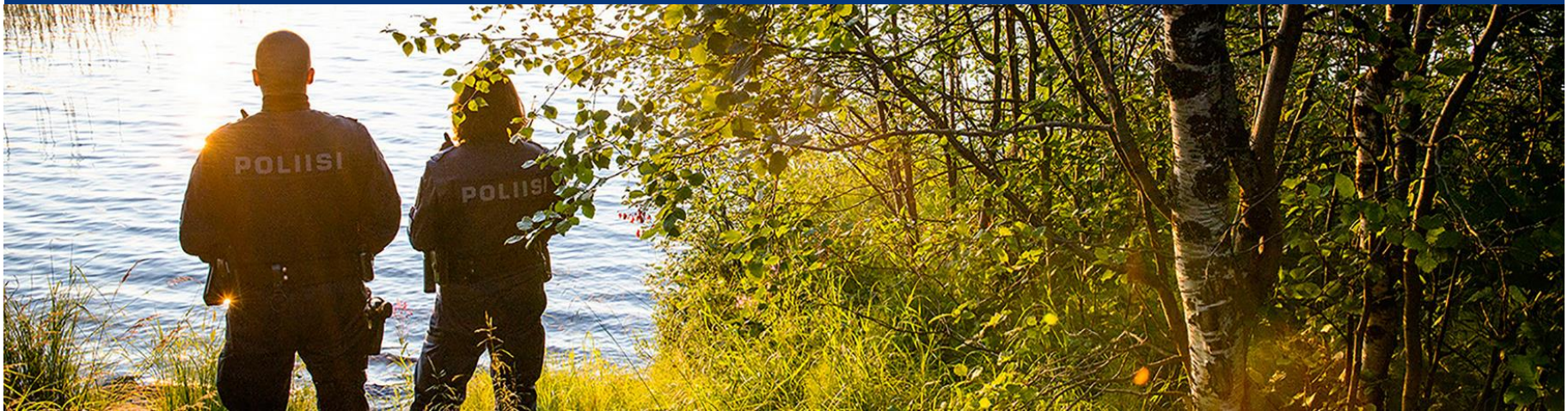
POLIISI
LOUNAIS-SUOMI

Lainvalvojan näkökulmaa kyberturvallisuuteen

- mitä tulisi osata paremmin?

Rikoskomisario Matti Airaksinen



Kyberrikollisuus

Miten suojaan itseni ja työni?

Mitä on osattava paremmin?

Kyberrikollisuus

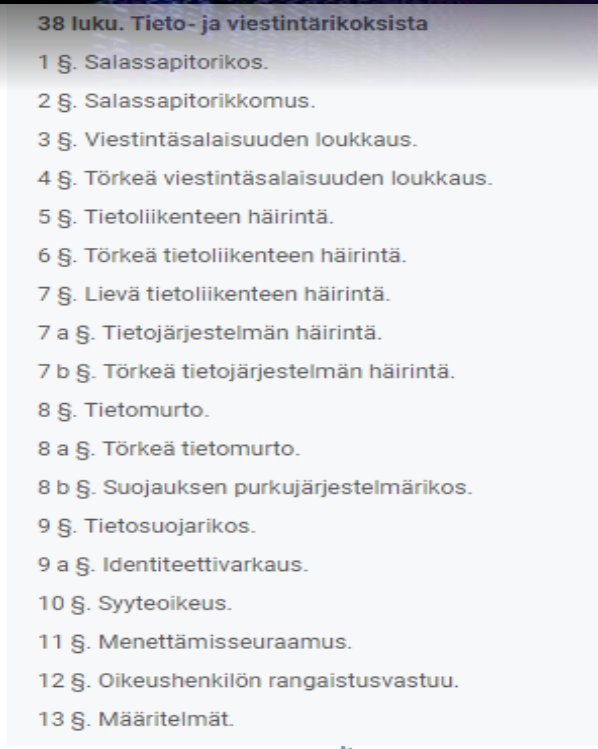
Kyberrikos

Ei ole virallista määritelmää.

Kyberrikokset ovat usein jaoteltuina:

a) tietoverkkoympäristöön kohdistuviin tietoverkkorikoksiin

b) tietoverkkoympäristöä hyväksikäyttäviin rikoksiin



POLIISI
LOUNAIS-SUOMI

Kyberrikos

Ei ole määriteltyä.

Kyb

orikoksiin

n

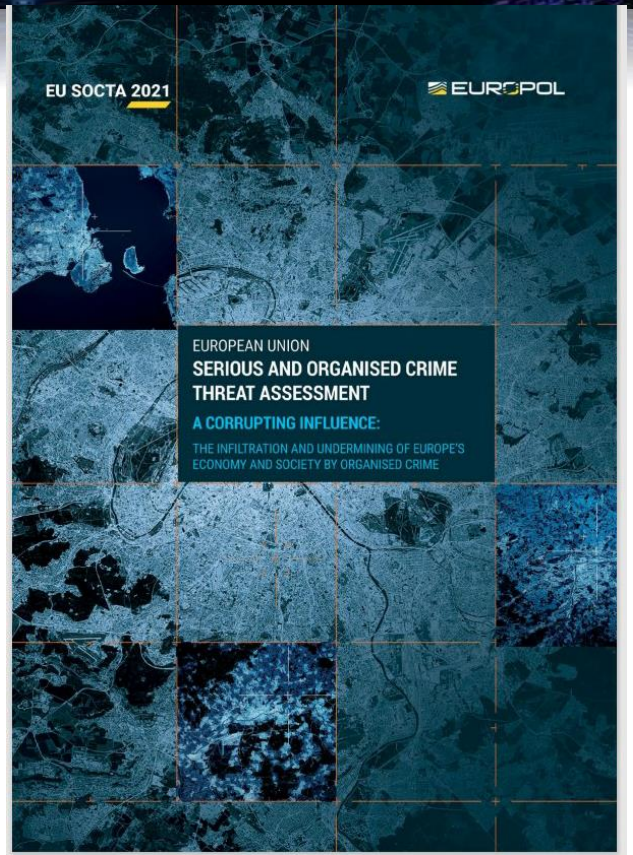
38 luku. Tieto- ja viestintärikoksista
1 §. Salassapitorikos.
2 §. Salassapitorikkomus.
3 §. Viestintäsalaisuuden loukkaus.
4 §. Törkeä viestintäsalaisuuden loukkaus.
5 §. Tietoliikenteen häirintä.
6 §. Törkeä tietoliikenteen häirintä.
7 §. Lievä tietoliikenteen häirintä.
7 a §. Tietojärjestelmän häirintä.
7 b §. Törkeä tietojärjestelmän häirintä.
8 §. Tietomurto.
8 a §. Törkeä tietomurto.
8 b §. Suojauksen purkujärjestelmärikos.
9 §. Tietosuojarikos.
9 a §. Identiteettivarkaus.
10 §. Syyteoikeus.
11 §. Menettämisseuraamus.
12 §. Oikeushenkilön rangaistusvastuu.
13 §. Määritelmät.

Kyberrikollisuus
- eli tietotekniikkarikollisuus tarkoittaa tietotekniikkaan tai tietoverkkoihin kohdistuvia rikoksia tai tietotekniikkaa ja tietoverkkoja hyväksi käyttäen tehtäviä rikoksia
- / SM/ intermin.fi

POLIISI
LOUNAIS-SUOMI

Vakava- ja järjestäytynyt rikollisuus EU:ssa

“The threat from cyber-dependent crime has been increasing over the last years, not only in terms of the number of attacks reported but also in terms of the sophistication of attacks. Cyber-dependent crime is likely significantly underreported”.

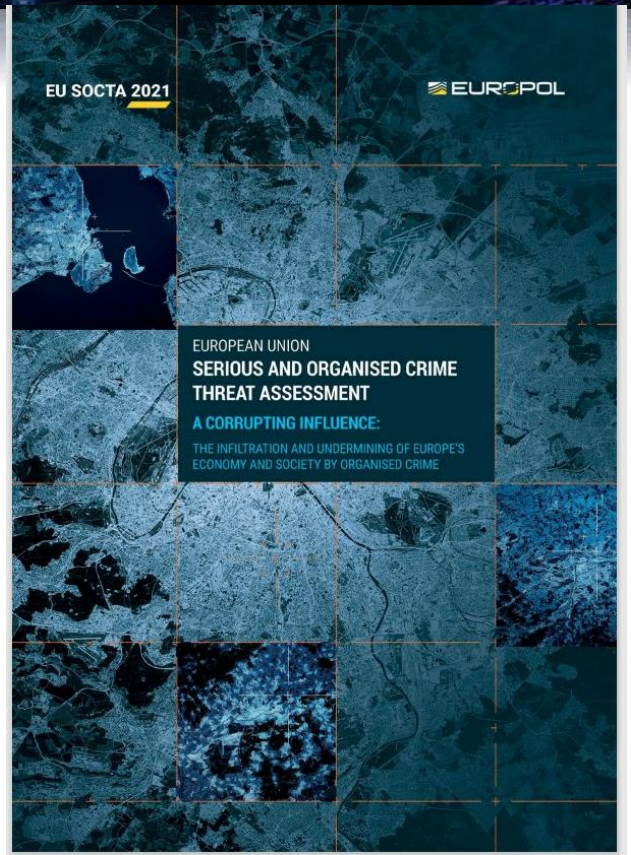


POLIISI
LOUNAIS-SUOMI

Vakava- ja järjestäytynyt rikollisuus EU:ssa

“The threat from cyber-dependent crime has

Businesses are increasingly the targets of cyberattacks. Public institutions, including critical infrastructures such as health services, continue to be targeted by cybercriminals. A potential leak of data or service disruptions in these sectors could result in very high financial and social costs.



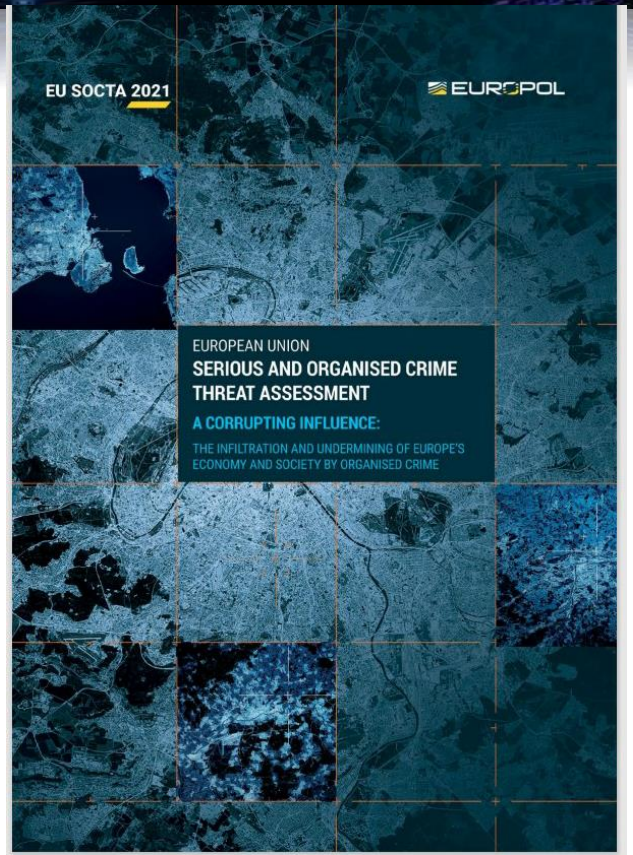
POLIISI
LOUNAIS-SUOMI

Vakava- ja järjestäytynyt rikollisuus EU:ssa

"The threat from cyber-dependent crime has

Businesses are increasingly the targets of cyber-dependent crime. Cyber-dependent crime can result in very high financial and social costs.

There has been a continuous increase in activities related to online child sexual abuse over recent years. Child sexual exploitation targets the most vulnerable members of society.



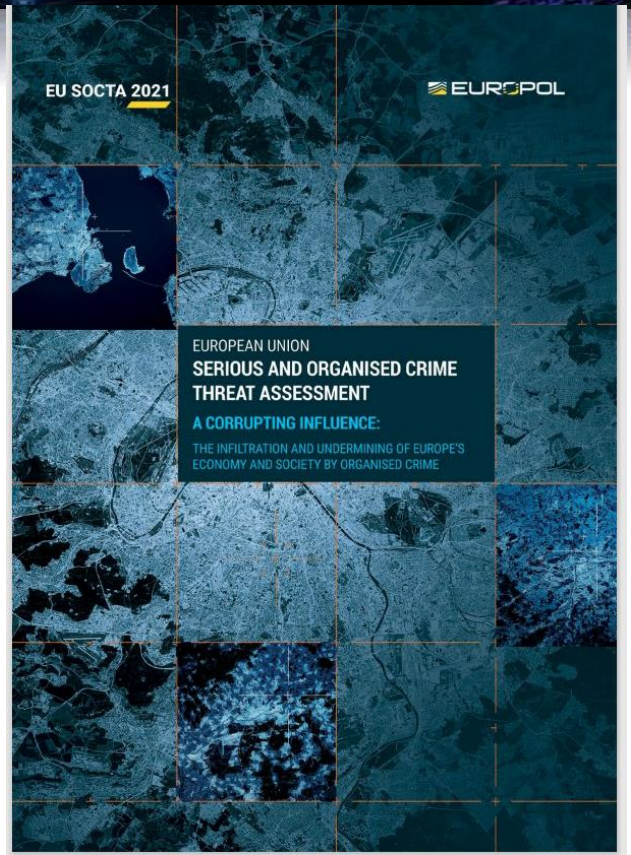
POLIISI
LOUNAIS-SUOMI

Vakava- ja järjestäytynyt rikollisuus EU:ssa

"The threat from cyber-dependent crime has

Businesses are increasingly the targets of

The move toward cashless economies creates powerful incentives for payment fraudsters. Cybercriminals seek to compromise online payments, internet and mobile banking, online payment requests, contactless payments (both card-present and not) and mobile applications



POLIISI
LOUNAIS-SUOMI

Tietoverkkorikosten määrä on jatkanut kasvuaan – taustalla näkyy uuden teknologian hyödyntäminen ja rikollisen toiminnan muuttuminen järjestäytyneemmäksi / poliisi.fi 5.10.2021

Kyberhyökkäysten määrä on lisääntynyt globaalisti, koska se on kannattavaa liiketoimintaa. / Antti Partanen; IBM/ 14.8. 2022 HS.

Tietoverkkoavusteiset petokset yhä laajeneva ongelma / Rahanpesun selvittelykeskuksen vuosikertomus 2021

Vastaamo -> 33.000 ihmisen tiedot/ 22.000 tutkintapyyntöä

– Sanoisin, että jossakin kohtaa kyberrikollisuus ohittaa perinteisen rikollisuuden määrällisesti. Se saattaa olla jo sen tehnyt, mutta kun rikoksista ei tehdä ilmoituksia, poliisi ei pysty sitä todentamaan. / Timo Piiroinen/ KPMG:n forensiikkapalvelujohtaja; 22.1.2021; Yle

Silkkitie 2019 –> Poliisi löysi 7000 vanhaa huumerikosta ja joutui aloittamaan tutkinnan niistä kaikista – Poliisi toivoo nyt lakimuutosta /Reinboth, Susanna/ HS 28.8.2022

POLIISI
LOUNAIS-SUOMI

Lähde: [Kyberrikos on poliisiasia - Opas yrityksille kyberrikostutkinnan kulusta (polamk.fi)]

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

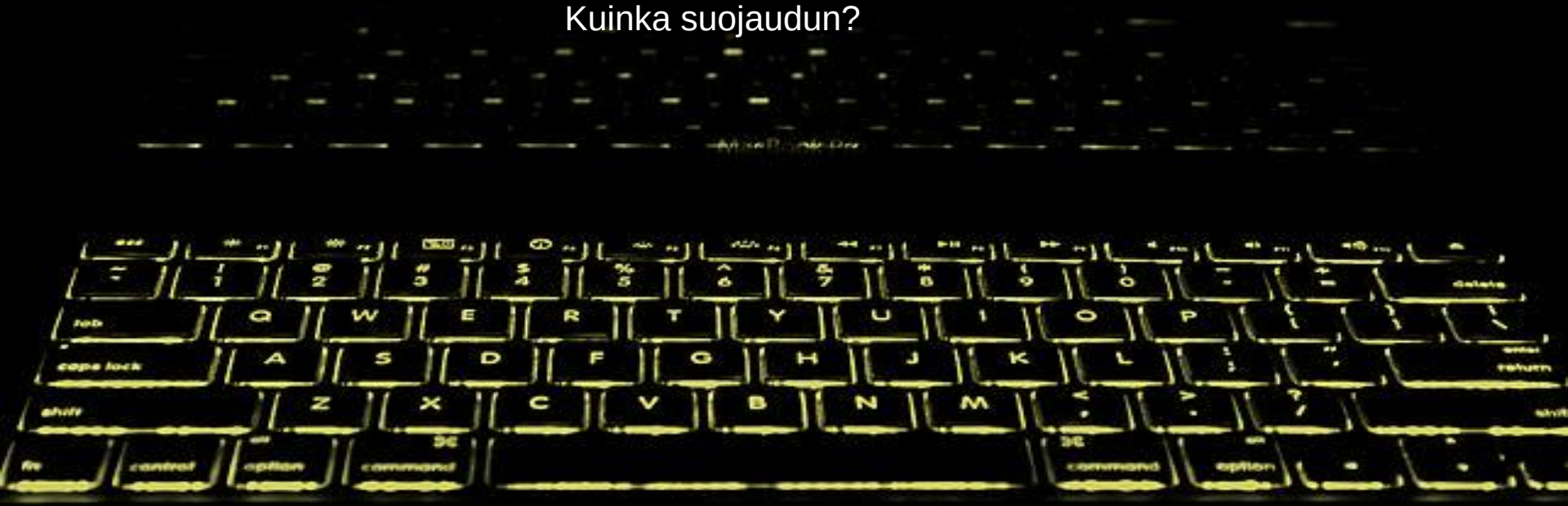
Tietomurron vaiheet

1. Tiedustelu
   - tunkeutumisväylät/mahdollisuudet ja työkalut
2. Tunkeutuminen
   - Tunnuksilla, haittaohjelmalla
3. Kartoitus
   - Admin-oikeudet, tietoturvamekanismien sulkeminen
4. Takaportit
   - Pitempikestoinen pääsy tietoverkkoon
5. Toiminnan valmistelu
   - Varmuuskopioinnin estäminen, tiedon pakkaaminen
6. Toteutus
   - Varastettavien tietojen siirtäminen tai tietojärjestelmän lamauttaminen

Kyberturvallisuuskeskus.fi

POLIISI
LOUNAIS-SUOMI

Kuinka suojaudun?



Kuinka suojaudun

- Huomioi käsittelemäsi tiedon luonne
- Huolehdi salasanaturvallisuus
- Ylläpidä ohjelmistot ja laitteet ajantasaisina
  - ohjelmistopäivitykset, varmuuskopiot,
  - oletussalasanat, virustorjunta
- Varmista kirjautumissivuston oikeellisuus
- Vältä kirjautumista julkisissa verkoissa
  / tunneloi yhteys VPN
- Ilmoita viranomaisille
  poliisi; kyberturvallisuuskeskus; tietosuojavaltuutettu

POLIISI
LOUNAIS-SUOMI

Ilmoitanko poliisille?

- Maksutonta
- Hyväksyttävyys
- Viranomaisten toiminta ja rikosten ennalta estäminen
- Rikosten sarjoittaminen
- Selvittäminen
- Vastuullisuus
- Omien virheiden peittäminen?
- Hyödyt vs. haitat

POLIISI
LOUNAIS-SUOMI

HENKILÖTIEDOT RIKOLLISILLE – MITEN ESTÄN VÄÄRINKÄYTÖKSET?

Henkilökohtainen luottokielto	Yhteystietojen luovutuskiellot	Muuttoilmoituksen estot	Rekisteröintikielto
• Suomen asiakastieto • Bisnode	• Digi- ja väestötietovirasto • Teleoperaattori	• Digi- ja väestötietovirasto • Posti	• PRH:n kauppa-, yhdistys- ja säätiörekisterit

POLIISI
LOUNAIS-SUOMI

Organisaatiotason varautuminen

- Tietoturvallisuus on osa prosesseja ja päätöksentekoa
  - Käyttöoikeuksien hallinta
  - Tietoturvallisuus on ajatusmalli
- Perusasiat kuntoon
  - Toimintaympäristön tunnistaminen
  - Keskinäisriippuvuuksien tunnistaminen
- Vastuuta ei voi ulkoistaa!
  - Organisaatio vastaa itse tietoturvasta
  - Ulkoinen toimija ei vapauta vastuusta

dia- Marko Leponen

POLIISI
LOUNAIS-SUOMI

TIETOMURRON TORJUNTA

Estäminen

- Käyttäjäoikeudet
- Laite/ palvelinhallinta
- Tietoverkon hallinta
- Tiedon hallinta

Havaitseminen

- Tietoturvaratkaisut
- Tietoturvakontrollit
- Lokitietojen kattavuus
- Lokien hallinta
- Valvontatoiminto

Tutkinta

- Valmistelu
- Eristäminen
- Karkotus
- Varmistaminen

POLIISI
LOUNAIS-SUOMI

Miten suojaan työni?

Tietoverkkoympäristö

- Yhdistää
  - CAAS – Crime as a service”
  - Virtuaalivaluutat
  - IoT + uudet tekotavat
- Häivyttää
  - Darknet, proxy-palvelut,
  - suojatut yhteydet, VPN:n
  - levy- ja tiedostosalaukset

Viranomaiset
Toimivaltuudet
Lait
Resurssit
Toiminnot
Syytefoorumi

POLIISI
LOUNAIS-SUOMI

RIKOSPROSESSI

Lähde: Kyberrikos on poliisiasia - Opas yrityksille kyberrikostutkinnan kulusta (polamk.fi)

1. Esitutkinta
2. Syyteharkinta
3. Oikeudenkäynti
4. Rangaistuksen täytäntöönpano

POLIISI
LOUNAIS-SUOMI

POLIISI
LOUNAIS-SUOMI

Varaudunko vai vastustanko?

POLIISI
LOUNAIS-SUOMI

Varaudunko vai vastustanko?

Tietoverkkojen ja tietojärjestelmien kehitys

Suojautuminen on velvollisuus

Kiitos

POLIISI
LOUNAIS-SUOMI