VALTIOVARAINMINISTERIÖ

Tietoturvapoikkeamatilanteiden hallinta

13.9.2016 VAHTI-seminaari Juha Ilkka

Työryhmän kokoonpano

- Juha Ilkka, VNK
- Kirsi Janhunen, VM
- Tuija Lehtinen, MML
- Kristiina Grönroos, SYKE
- Pyry Heikkinen, Tulli
- Sami Niinikorpi, Supo
- Anssi Sahlman, Vero
- Harri Mäntylä, PLM
- Jarna Hartikainen, Viestintävirasto
- Mika Raappana, Haltik
- Paul Kinnunen, Liikennevirasto

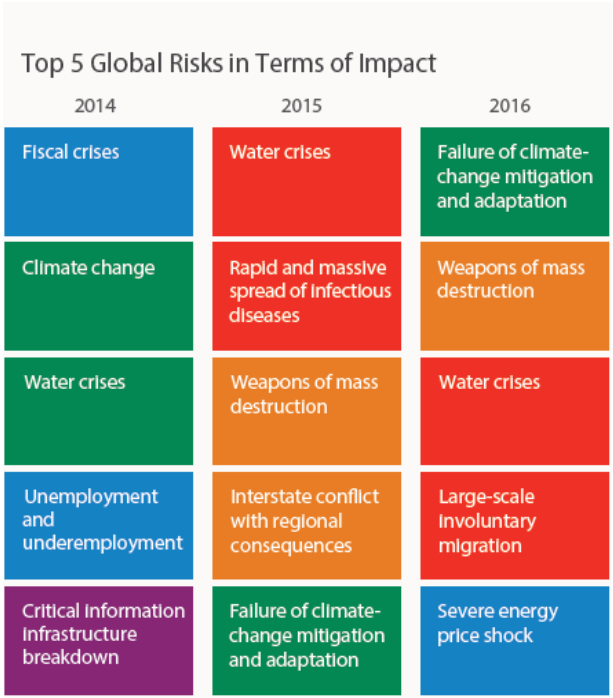
"Good evening. Today is Good Friday. There is no news.“

BBC:n uutiset 18.4.1930

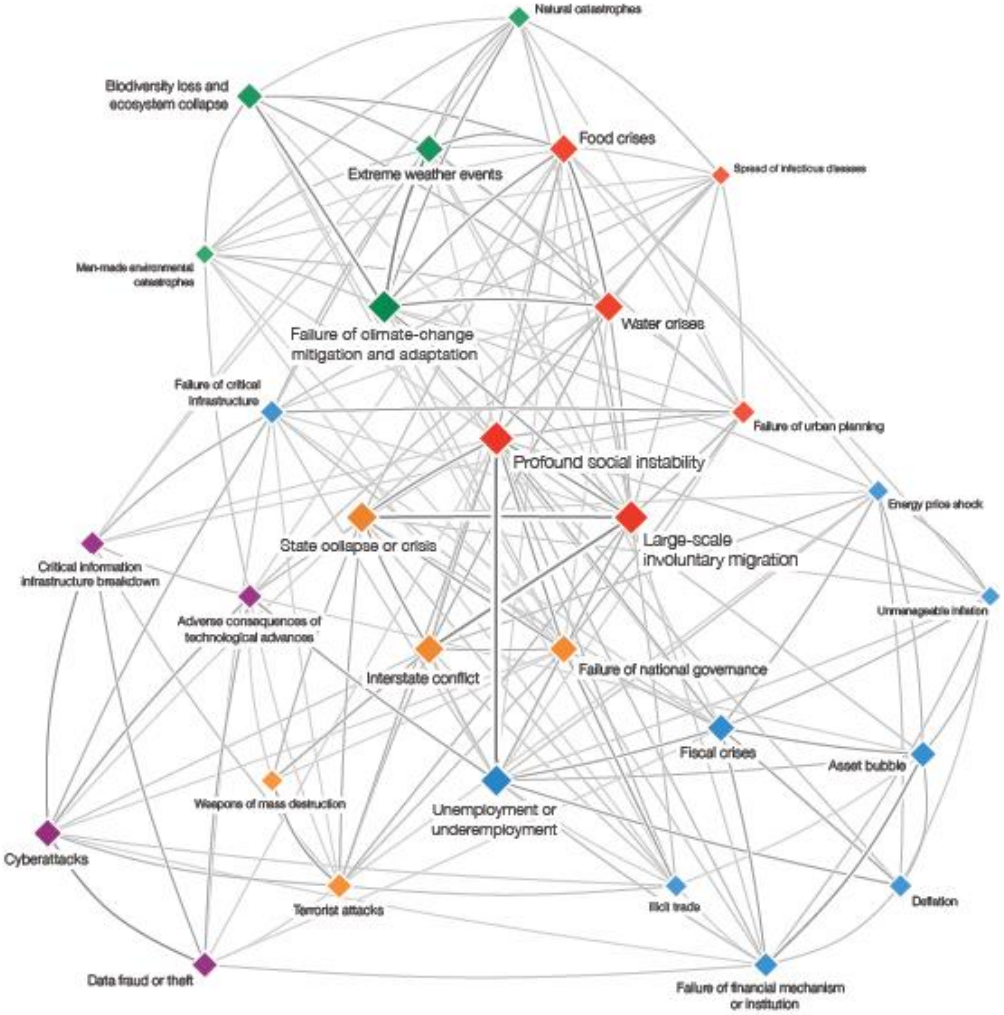
”CERT-FI:lle ilmoitetut suomalaisiin organisaatioihin kohdistetut tietomurrot eivät lisääntyneet viime vuonna.”

Viestintäviraston tietoturvakatsaus 4/2005

Tietoturvapoikkeamien vakavuudesta

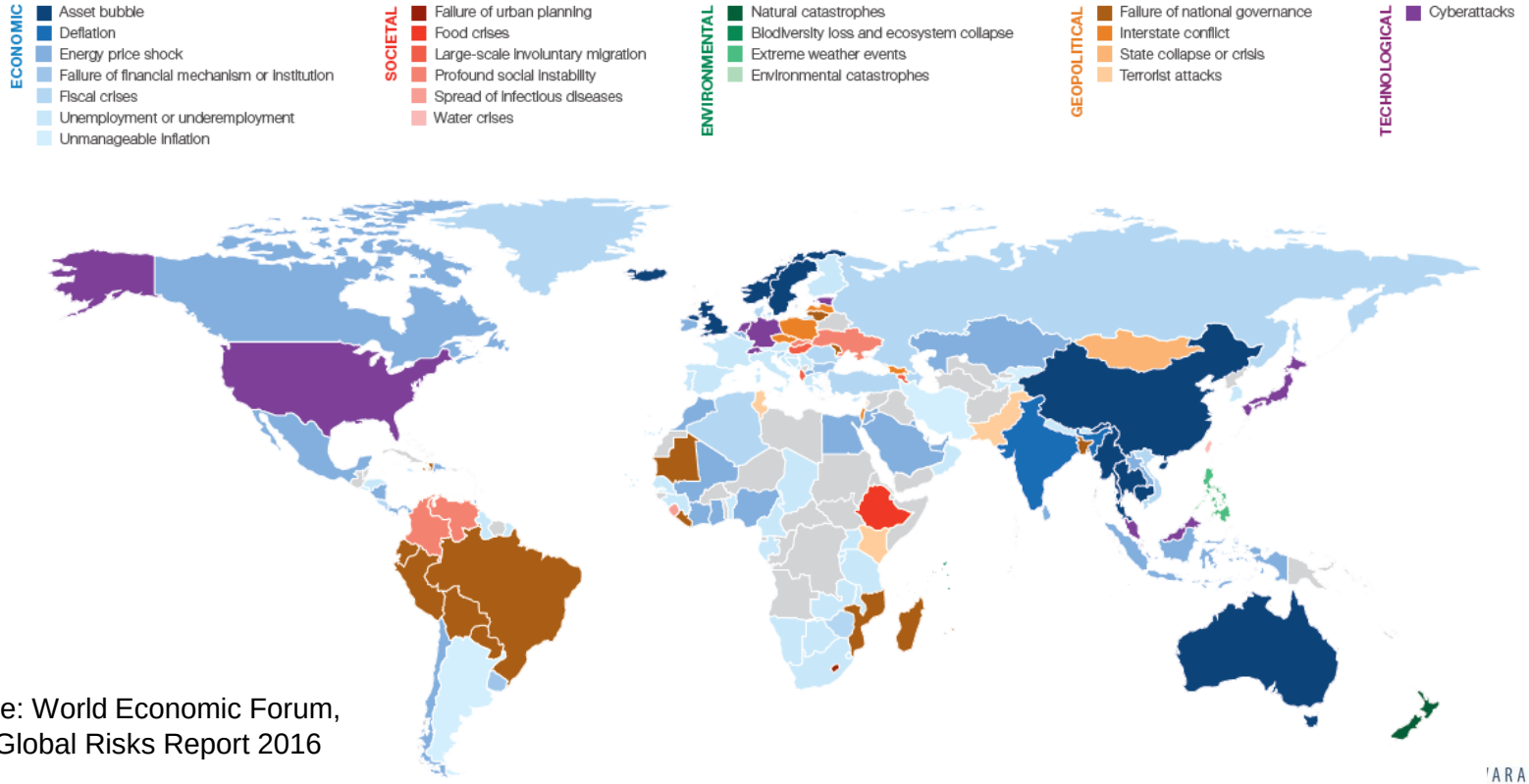


Lähde: World Economic Forum, The Global Risks Report 2016



Lähde: World Economic Forum,
The Global Risks Report 2016

Yritystoimintaan liittyvät suurimmat riskitekijät

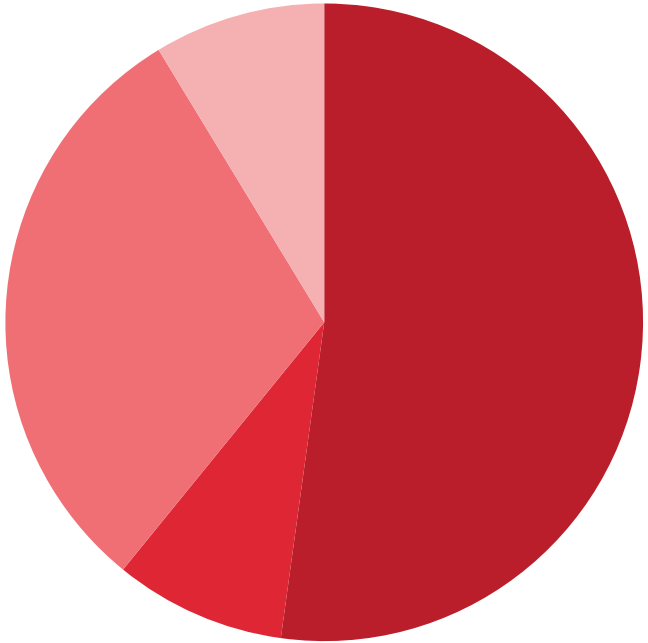


Lähde: World Economic Forum,
The Global Risks Report 2016

Ohjepäivitys

- Nykyistä ohjetta pyritty keventämään edellisestä
- Lisätty mm. tiedon jakamiseen ja yhteistyöhön liittyviä osuuksia
- Ohjeessa ei käsitellä yleisiä ICT-häiriötilanteita
- Ohje tulee lausuntopalvelun kautta 3 viikoksi lausunnolle 14.9.

Ohjeen painopisteistä



Kyberturvallisuuskeskus on ystävä

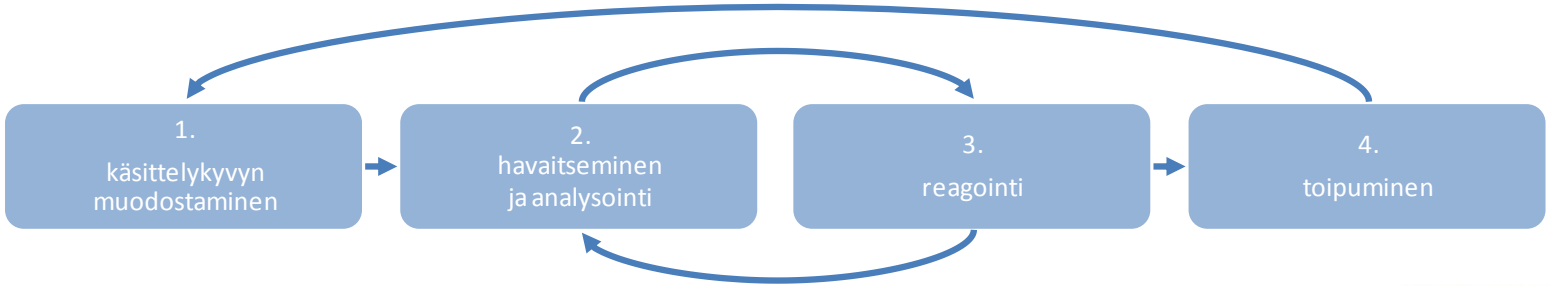
Ohjeluonnos

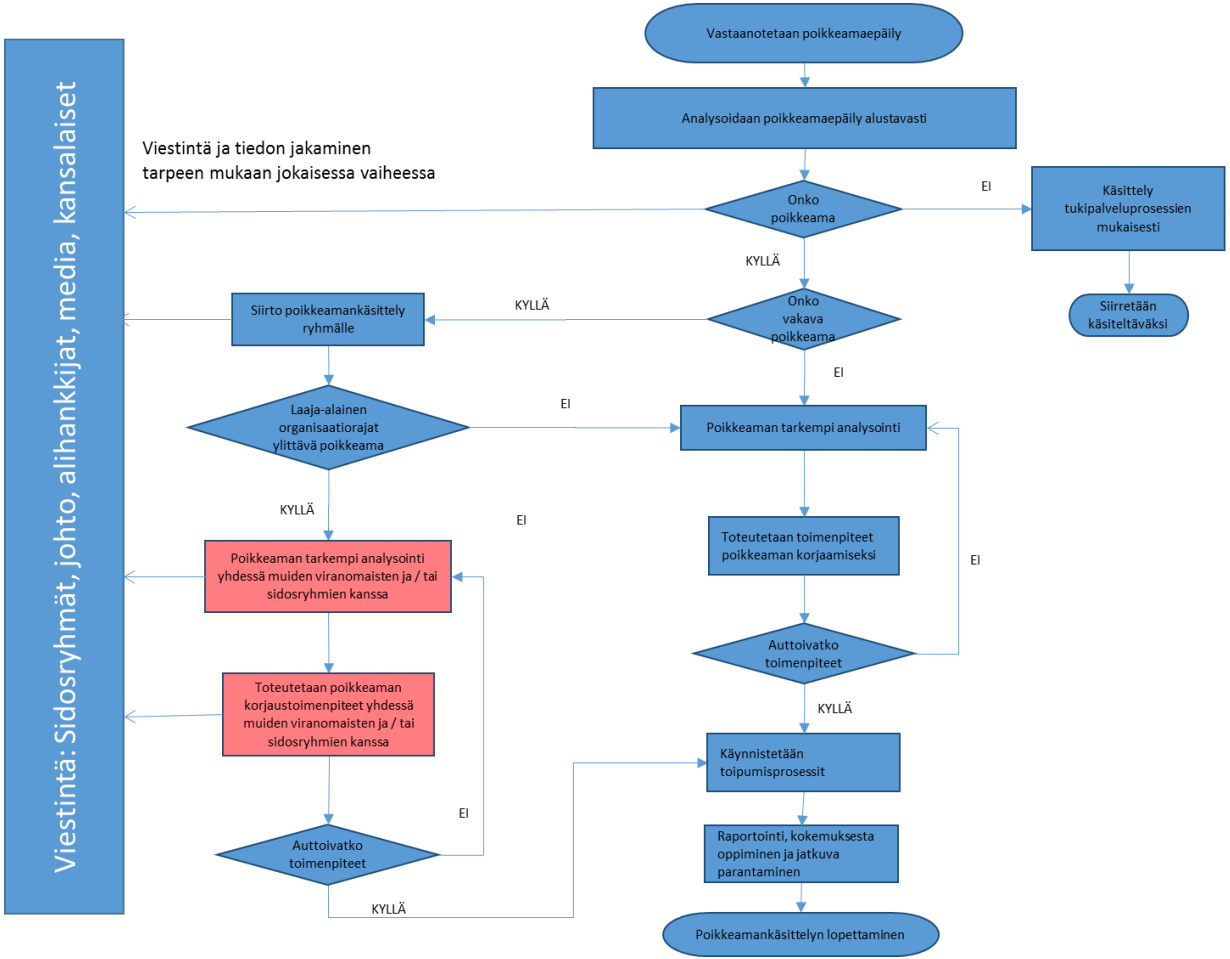
Määritelmät

- Tietoturvatapahtuma
  - Tietoturvallisuuteen liittyvä tapahtuma, jolla voi olla vahingollisia vaikutuksia organisaation toiminnalle
- Tietoturvapoikkeama
  - Tahallinen tai tahaton tapahtuma, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut

Tietoturvapoikkeamien hallintaprosessi

- Prosessin tarkoituksena on sekä varautua häiriötilanteisiin ja turvata toiminnan jatkuvuus, että toisaalta pyrkiä jatkossa estämään häiriötilanteiden muodostuminen.
- Hallintaprosessi on riippuvainen riskienhallinnan avulla määritellyistä turvakontrolleista, joiden avulla poikkeamat pyritään estämään ja tarvittaessa havaitsemaan.
- Havainnointikyky koostuu teknisten kontrollien lisäksi myös henkilöstön ja sidosryhmien havainnoista.




Viestintä: Sidosryhmät, johto, alihankkijat, media, kansalaiset
Viestintä ja tiedon jakaminen tarpeen mukaan jokaisessa vaiheessa
Vastaanotetaan poikkeamaepäily
Analysoidaan poikkeamaepäily alustavasti
Onko poikkeama
EI
Käsittely tukipalveluprosessien mukaisesti
KYLLÄ
Onko vakava poikkeama
KYLLÄ
Siirto poikkeamankäsittely ryhmälle
EI
Siirretään käsiteltäväksi
Laaja-alainen organisaatiorajat ylittävä poikkeama
EI
Poikkeaman tarkempi analysointi
KYLLÄ
EI
Poikkeaman tarkempi analysointi yhdessä muiden viranomaisten ja / tai sidosryhmien kanssa
Toteutetaan toimenpiteet poikkeaman korjaamiseksi
EI
Auttoivatko toimenpiteet
KYLLÄ
Toteutetaan poikkeaman korjaustoimenpiteet yhdessä muiden viranomaisten ja / tai sidosryhmien kanssa
Käynnistetään toipumisprosessit
EI
Auttoivatko toimenpiteet
Raportointi, kokemuksesta oppiminen ja jatkuva parantaminen
KYLLÄ
Poikkeamankäsittelyn lopettaminen

Liitteet

- Sanasto
- Traffic Light Protocol -luokittelu
- Esimerkkejä tietoturvapoikkeaman viitteistä
- Muistilista tietoturvapoikkeamista kerättävistä tiedoista
- Esimerkki tietoturvapoikkeamien viestintäsuunnitelman rungosta
- Esimerkki poikkeamatilanneohjeistuksesta
- Tietoturvapoikkeaman ilmoituslomakkeen malli
- Tapahtumapäiväkirjan malli
- Tietoturvapoikkeamien hallintaan liittyvä lainsäädäntö

Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Tietoturvapoikkeamien käsittelykyvyn muodostaminen

- Käsittää erilaiset varautumistoimet, joiden avulla poikkeamatilanteessa voidaan toimia
- Varautumistoimissa tulee huomioida mm.
  - järjestelmien ja prosessien riittävä dokumentaatio
  - päätöksenteko
  - riippuvuuksien tunnistaminen
  - omat ja yhteistyötahojen henkilöstöresurssit
  - tilannekuvan muodostaminen ja tiedon jakaminen
  - haittaohjelmien ja poikkeavan toiminnan havainnointikyvyn kehittäminen
  - sopimusmenettelyt ja harjoittelu

Tietoturvapoikkeamien käsittelykyvyn muodostaminen

1. Tietoturvapoikkeamien käsittelyn organisointi
2. Tietoturvatiedon luokittelu
3. Tietoturvatiedon jakaminen ja viestintä
4. Lokienhallinnan suunnittelu
5. Tietoturvapoikkeamien huomioiminen sopimusmenettelyissä
6. Harjoittelu

Tietoturvatiedon jakaminen ja viestintä

- Tietoturvatiedon jakamiselle tarkoitetaan asiantuntijoiden jakamaa teknistä tietoa, jonka avulla poikkeaman selvitystyötä pyritään nopeuttamaan, estämään poikkeaman leviäminen muihin organisaatioihin sekä ennaltaehkäisemään poikkeamien syntyminen.
- Viestinnällä tarkoitetaan sitä sisäistä ja ulkoista viestintää, jolla tiedotetaan henkilöstölle, sidosryhmille, medialle ja kansalaisille tapahtuneesta poikkeamasta. Viestinnän tavoitteena on mm. ehkäistä virheellisen tiedon leviäminen ja pitää tarvittavat osapuolet tietoisina poikkeaman selvitystyön etenemisestä.

Tietoturvatiedon luokittelu

Tietoturvatieto	Julkisuus	Salassapitoperuste	Suojaustaso	TLP
Haittaohjelman tunnistetiedot				TLP Green – Amber
Kohdistetun haittaohjelman tunnistetiedot	Saattaa sisältää salassa pidettävää tietoa	Julkisuuslaki 24 §:n 7 k	ST IV – II	TLP Amber - Red
Tietoturvaohjeet	Saattaa sisältää salassa pidettävää tietoa	Julkisuuslaki 24 §:n 7 k	ST IV	TLP Green - Amber
Kalasteluviestinäytteet				TLP Amber
Haittaohjelman komento- ja välityspalvelintiedot				TLP White - Red

Viranomaisyhteistyö ja ilmoitusvelvollisuus

- Harva organisaatio kykenee yksin havaitsemaan edistyneitä kohdistettuja tietoturvahyökkäyksiä tai toipumaan niistä.
- Viranomaisyhteistyön tavoitteena on lisätä turvallisuustietoisuutta, parantaa tietoturvallisuutta sekä nopeuttaa poikkeamien hallintaa.
- Tietoturvatapahtumista tulee matalalla kynnyksellä ilmoittaa Viestintävirastoon ja valtionhallinnon VIRT-ryhmälle (virtual incident security response team) sekä tarvittaessa tehdä rikosilmoitus.
- Viestintäviraston kyberturvallisuuskeskuksesta voi kysyä tietoja valtionhallinnon yhteistyöverkostoista

Ilmoitusvelvollisuus

Tieto	Kenelle ilmoitetaan	Aika	Peruste
Kansainväliseen turvaluokiteltuun tietoon kohdistunut väärinkäytös	Kansallinen turvallisuusviranomainen (UM/NSA)	24 h sisällä	Neuvoston turvallisuusmääräys
Henkilötietoihin kohdistunut väärinkäytös	Kansallinen valvontaviranomainen	72 h sisällä	EU:n tietosuoja-asetus
Varoihin tai omaisuuteen kohdistunut väärinkäytös	Valtiontalouden tarkastusvirasto	Viipymättä	Laki (676/2000) 16 §
Vakoilun tai törkeän vakoilun ilmoittaminen	Poliisi tai uhan kohde	Viipymättä	Rikoslaki 15 luku, 10 §

Tietoturvapoikkeamien havaitseminen ja analysointi

Tietoturvapoikkeaman havaitseminen ja analysointi

- *Tietoturvapoikkeaman havaitseminen ja analysointi* käsittää normaalista poikkeavan toiminnan havaitsemisen ja analysoinnin, minkä tavoitteena on selvittää mitä on tapahtunut ja miksi.
- Analysoinnin tuloksena voidaan todeta onko, kyseessä tietoturvapoikkeama tai esim. ICT-häiriötilanne.

Tietoturvapoikkeaman havaitseminen ja analysointi

1. Tietoturvapoikkeaman havaitseminen
2. Poikkeamatietojen kerääminen
3. Poikkeaman analysointi

Tietoturvapoikkeamatiedon lähteitä

- järjestelmälokit (esim. keskitetty lokienhallintajärjestelmä tai SIEM)
- hyökkäyksen havainnointi- ja estojärjestelmät (IDS/IPS)
- tietoverkon aktiivilaitteet (mm. kytkimet, reitittimet ja palomuurit)
- haittaohjelmien ja roskapostin suodatusjärjestelmät
- päätelaitteet
- palvelutoimittajan tai tietoliikenneoperaattorin järjestelmä
- ulkopuoliselta taholta hankittavat seuranta- tai valvontapalvelut
- muiden organisaatioiden tietoturvayksiköt (esimerkiksi Viestintäviraston GovCert-palvelu)
- rikosilmoitin-, kulunvalvonta- ja kameravalvontajärjestelmät
- yleisesti saatavilla olevat tietolähteet, kuten julkiset haavoittuvuustiedotteet
- Valtorin tietoturvapoikkeamien valvomo (SSOC, Security and Service Operations Center)
- valtionhallinnon tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä GovHAVARO
- käyttäjien ja asiakkaiden palvelupyynnöt ja yhteydenotot

Poikkeamatietojen kerääminen

- Poikkeamatiedon kokoamiseen ja analysointiin osallistuvat henkilöt on perehdytettävä aineiston keräämiseen ja tallettamiseen liittyviin ohjeisiin ja lainsäädäntöön
- Kerättävää tietoa saatetaan tarvita selvitystyön ja raportoinnin lisäksi juridisiin tarkoituksiin
- Kerättäviä tietoja on listattu ohjeen liitteeseen

Analysointi

- Analysoinnin alkuvaiheessa arvioidaan poikkeaman tyyppi ja syyt
  - poikkeaman nykyinen ja potentiaalinen vaikutus järjestelmiin ja muuhun tietojenkäsittely-ympäristöön
  - poikkeaman mahdolliset seurannaisvaikutukset organisaation toimintaan
  - poikkeaman ja siihen reagoimisen taloudelliset seuraukset
  - poikkeaman vaikutus organisaation julkisuuskuvaan sekä sidosryhmiin sekä
  - uhattuna olevien tietojen merkitys organisaatiolle ja sidosryhmille.

Poikkeaman luokitteluesimerkki

Vakavuusaste	Kuvaus
Vähäinen	Poikkeaman vaikutus organisaation toimintaan on vähäinen. Vähäisten tietoturvapoikkeamien hoitaminen on osa organisaation normaalia toimintaa. Poikkeamasta voi harkinnan mukaan ilmoittaa Viestintäviraston Kyberturvallisuuskeskukseen.
Vakava	Poikkeamalla on merkittävä vaikutus organisaation toimintaan ja tietoturvapoikkeamien käsittelyryhmä kutsutaan koolle. Poikkeamasta tehdään ilmoitus Viestintäviraston Kyberturvallisuuskeskukseen.
Kriisitilanne	Kyseessä on laaja-alainen tai jopa organisaatiorajat ylittävä poikkeama. Organisaation sisäiset kriisinhallintatoimenpiteet käynnistetään ja poikkeamasta tehdään ilmoitus Viestintäviraston Kyberturvallisuuskeskukseen. Kyberturvallisuus ja kohdeorganisaatiot arvioivat, kutsutaanko koolle VIRT-koordinointikokous. Koolle kutsuminen voidaan tehdä myös toimivaltaisen viranomaisen toimesta.

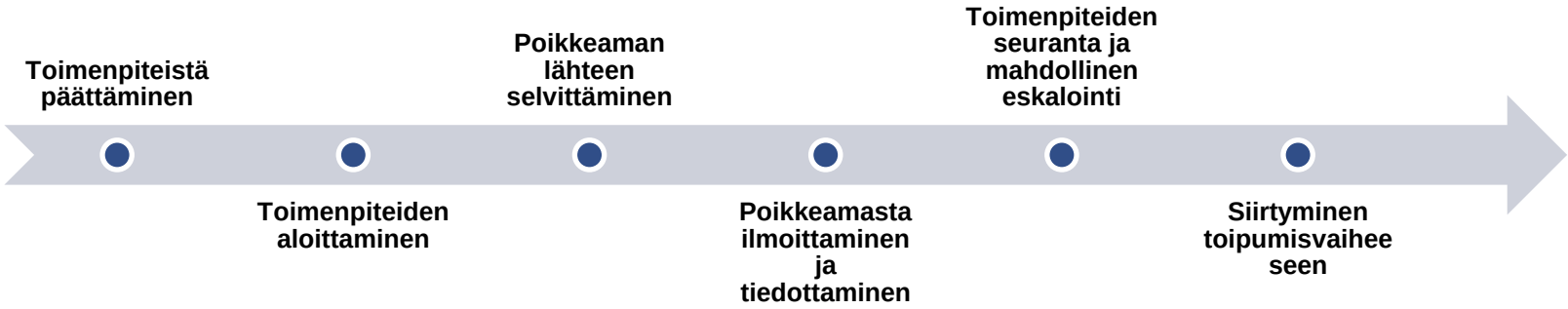
Tietoturvapoikkeamaan reagointi

Tietoturvapoikkeamaan reagointiin

- *Tietoturvapoikkeamaan reagointiin* liittyvät toimenpiteet, joiden avulla
  - mahdolliset vahingot minimoidaan,
  - poikkeamasta informoidaan muita viranomaisia ja sidosryhmiä
  - käynnistetään toimenpiteet poikkeaman korjaamiseksi.

Tietoturvapoikkeamaan reagointi

1. Tietoturvapoikkeaman käsittely
2. Todistusaineiston turvaaminen
3. Tietoturvatiedon jakaminen ja viestintä



Esimerkkejä erilaisista poikkeamatilanteista

- Epäilyttävää tiedonsiirtoa ulkopuoliseen kohteeseen
- Palvelunestohyökkäys
- Järjestelmässä on tunkeutuja
- Oman henkilökunnan tekemät tietoturvaloukkaukset
- Haittaohjelmatilanteet
- Kohdistetut hyökkäykset
- Tietojen kalastelu
- Pääsynhallinnan kriittinen poikkeama
- Sensitiivisen tiedon laajamittainen väärä käsittely

Toipuminen tietoturvapoikkeamasta

Toipuminen tietoturvapoikkeamasta

- *Toipumisvaiheessa* organisaation ja palveluiden toiminta palautetaan normaalitilaan.
- Poikkeamasta laaditaan raportti, jonka havaintojen perusteella kehitetään käsittelykykyä ja varautumista, jotta poikkeaman toistuminen voitaisiin jatkossa estää.
- Edellytyksiä onnistuneelle toipumiselle ovat mm. ajan tasalla oleva järjestelmädokumentointi, joka sisältää kaiken toipumisessa tarvittavan tiedon tietoverkoista ja yhteyksistä.
- Osana toipumista tulee huomioida mahdolliset muutostyöt poikkeaman toistumisen estämiseksi.

Toipuminen tietoturvapoikkeamasta

1. Tekniset toipumistoimenpiteet
2. Viestintä
3. Raportointi ja tapauksesta oppiminen
4. Päätöksenteko

Vaatimukset

Vaatimukset

- Poikkeamien hallintaan yhteensä 80 vaatimusta
  - 39 uutta vaatimusta
  - 51 aikaisempaa vaatimusta
- perus, korotettu vai korkea taso
- Suositus, vahva suositus vai pakollinen vaatimus
- Vaatimukset luovutetaan VAHTIn rakennetyöryhmälle jatkotyöstöä varten

Esimerkkejä vaatimuksista

Vaatimus	Perustaso	Korotettu taso	Korkea taso
Organisaatiolla on menettely järjestelmien eristämiseen verkosta	Vahva suositus	Pakollinen	Pakollinen
Rikosepäilyissä organisaatio tekee rikosilmoituksen poliisille	Suositus	Suositus	Suositus
Organisaatiossa ylläpidetään tapahtumapäiväkirjaa tietoturvapoikkeamatilanteissa	Pakollinen	Pakollinen	Pakollinen
Organisaatiolla on käytössään palvelu verkkoliikenteen suodattamiseen palvelunesto-liikenteeltä	Vahva suositus	Vahva suositus	Vahva suositus

Lisätietoja

Juha Ilkka
Tietoturvallisuuspäällikkö
Valtioneuvoston kanslia
valmiusyksikkö