



Kuinka toimin erilaisissa häiriötilanteissa?

Julkisen hallinnon digitaalisen turvallisuuden teemaviikko

Erja Kinnunen, Verohallinto

2.10.2017

Sisältö

- Miksi palveluiden toimivuus ja jatkuvuus on tärkeää?
- Mikä on häiriö?
- Miten toimin yksilönä?
- Miten organisaation tulisi toimia?
- Miten voimme varautua?
- Mitä odotamme sopimuskumppanilta / palvelutoimittajalta?
- Mitä häiriön jälkeen?

Miksi palveluiden toimivuus ja jatkuvuus on tärkeää?

- Koko julkishallinnon toiminta on erittäin riippuvaista tiedoista ja tietojärjestelmistä
- Manuaaliset työvaiheet ja työvälineet poistuvat asteittain kokonaan
- Miten työpäiväsi sujuisi jos esim. sähköposti tai organisaatiosi tietoliikenneverkko olisi päivän poissa toiminnasta?

Häiriö (VAHTI tietoturvasanasto 8/2008)

1. tilanne tai tapahtuma, jonka vuoksi järjestelmä ei toimi normaalisti
 2. toiminnan jonkin osatekijän haitallinen vaihtelu, jonka puitteissa toiminta voi silti pääosin jatkua
- Ks. tietoturvapoikkeama = haitallinen tapahtuma, tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyydestä on tai saattaa olla vaarantunut
 - Käytännössä meillä tapahtuu tietoturvapoikkeamia todella harvoin verrattuna ICT-palvelutuotantoon tai muuhun digitaalisessa toimintaympäristössä tapahtuviin teknisiin häiriöihin – joista osa saattaa johtua esimerkiksi luonnonilmiöistä

Häiriö

- ketä koskee?
 - yksi käyttäjä / useita käyttäjiä
- miten ilmenee?
 - palvelu ei toimi
 - työväline ei toimi
 - työasema/-väline toimii kummallisesti
 - en osaa käyttää palvelua / järjestelmää / työvälinettä

Miten toimin yksilönä?

- Mikä on roolisi organisaatiossa?
- Johtaja / päällikkö?
- Tietoturva- / turvallisuusvastaava?
- Prosessista / palvelusta vastaava?
- Tekninen henkilö, esim. järjestelmävastaava?
- Loppukäyttäjä / palvelun hyödyntäjä?

Miten toimin yksilönä?

- Ota selvää oman organisaatiosi käytännöistä!
 - löytyykö ohjeet Intranetistä?
- Seuraa organisaatiosi vikailmoitussivua tai vastaavaa!
- Minne ilmoitan?
 - jos jokin palvelu ei toimi
 - jos oma työväline ei toimi
 - jos epäilet tietoturvaongelmaa
 - jos haluat neuvoja
- Usein yksi kontaktipiste
 - helpdesk, service desk tms.
 - puhelinnumero, sähköpostiosoite, intranet-lomake, helpdesk-sovellus tms.

**Ilmoita, jos
huomaat häiriön!**

Miten organisaation tulisi toimia?

- Kuvatut käytännöt / prosessit täytyy olla olemassa
- Häiriönhallintaprosessi
 - mitä tehdään, kuka osallistuu
 - vastuunjako organisaation ja palvelutoimittajien kesken
 - milloin tietoturvakatastrofa otetaan mukaan selvittelyyn
- Tietoturvakatastrofien hallintaprosessi
 - organisaation oma ja valtionhallinnon yhteinen CERT-/VIRT-toiminta
 - CERT.FI
 - milloin otetaan yhteyttä poliisiin tai muihin viranomaisiin
- Viestintä pitää olla mietittynä ja kuvattuna
 - sisäinen ja ulkoinen

Miten voimme varautua?

- Mistä häiriöt johtuvat?
 - riskiarviointi; skenaariot, todennäköisyydet, vaikutukset
 - ylläpidä riskirekisteriä jatkuvasti / säännöllisesti
- Mihin pitää varautua?
 - riskiskenaariot
 - todennäköisimmät?
 - ne joihin on helppo varautua?
 - ne joista aiheutuvat suurimmat menetykset?
- **Jatkuvuussuunnittelu!**

Varautuminen ja jatkuvuus

- Jatkuvuussuunnittelu
 - Toiminnan / prosessin jatkuvuus
 - yleiset skenaariot; ihmiset, tilat, työvälineet, tietojärjestelmät eivät ole käytettävissä
 - Vaihtoehtoiset toimintatavat
- Toipumissuunnittelu
 - tietojärjestelmän tai palvelun elvyttäminen häiriötilanteissa
 - kuvaa tekniset toimintatavat
- Valmiussuunnittelu
 - miten toimitaan poikkeusoloissa
- Kaikissa tärkeitä roolit, vastuut, toimenpiteet, varamenettelyt, yhteystiedot ja **viestintä**

Sopimuskumppanit / palvelutoimittajat

- Mikään organisaatio ei toimi yksin
- Sovellus-, käyttöpalvelu-, tietoliikennetoimittajat
- Palvelutoimittajien kanssa sopimukset
 - mitä edellytämme?
 - Tietoturvavaatimukset
 - SLAt, sanktiot
 - jatkuvuus- / toipumissuunnitelmat

Tilanteen jälkeen

- Jälkikäteisanalysointi
 - mitä tapahtui?
 - miksi tapahtui?
 - miten toimittiin?
 - mitä siitä seurasi?
 - voidaanko jatkossa toimia paremmin?
- Mahdollista / helpompaa kun toimenpiteistä pidetään kirjaa häiriön aikana
- Ohjeiden ja prosessien päivittäminen!
- Tiedottaminen ja viestintä

Kaksi vaihtoehtoista toimintatapaa

- Kun organisaatio kohtaa jonkin häiriön ensimmäistä kertaa
 1. organisaatiolla ei ole suunnitelmia toiminnasta häiriötilanteessa
 2. organisaatio on laatinut tarvittavat suunnitelmat, kouluttanut suunnitelmat sekä harjoitellut niiden mukaista toimintaa
 - jo pienimuotoinen harjoittelu auttaa häiriötilanteisiin varautumista
 - jos tarvittavat asiantuntijat, esimiehet ja viestintä mieltivät yhdessä pöydän ääressä (ns. pöytä-/paperiharjoitus) todennäköisimpiä toimintaan vaikuttavia häiriötilanteita, se auttaa varautumaan myös muun tyyppisiin häiriöihin

**Harjoitus tekee mestarin –
mestaritkin harjoittelevat!**

Hyödyllistä lisätietoa

- www.vahtiohje.fi
- **erityisesti**
- [VAHTI 2/2016 Toiminnan jatkuvuuden hallinta](#)
- [VAHTI 8/2017 Tietoturvapoikkeamatilanteiden hallinta](#)
- [VAHTI 22/2017 Ohje riskienhallintaan](#)