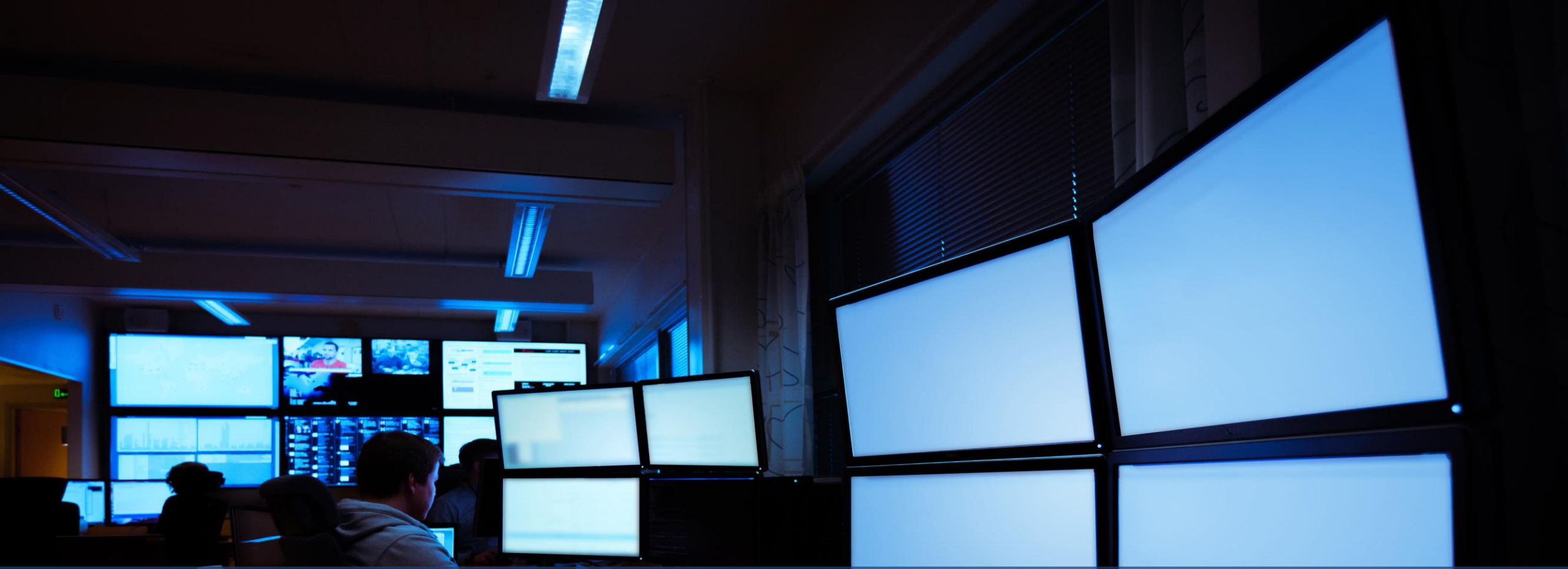


Viestintäviraston Kyberturvallisuuskeskuksen palvelut tietoturvaloukkaustilanteissa

Kauto Huopio

Mikä on Viestintäviraston Kyberturvallisuuskeskus?

- Kyberturvallisuuskeskus on Kansallinen tietoturvaviranomainen, joka kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta.
  - » Kyberturvallisuuskeskus on osa Viestintävirastoa
  - » N. 70 työntekijää
- Kyberturvallisuusstrategia 2013

- Kyberturvallisuuskeskuksen keskeisimmät toiminnot
  - » Kootaan ja ylläpidetään tilannekuvaa
  - » Tietoturvaloukkausten ilmoituspiste
  - » Tietoturvaloukkausten havainnointi (HAVARO)
  - » Yhteistyöverkostot
  - » Haavoittuvuuskoordinointi
  - » Järjestelmäturvallisuus
  - » Salaustuotteiden hyväksynnät
  - » Turvallisuussääntely
  - » Suojatut satelliittien aika- ja paikkasignaalit
  - » Harjoitustoiminta

Yhteistyö valtiovarainministeriön kanssa

- Kyberturvallisuuskeskus toteuttaa VM:n rahoituksen turvin palveluita valtionhallinnon toimijoiden käyttöön
- Tavoitteena edesauttaa valtionhallinnon toimijoiden varautumista kyberuhkiin sekä varmistaa toiminnan nopea palautuminen häiriötilanteissa
- Palvelut pääsääntöisesti käyttäjilleen maksuttomia

Valtionhallinnon toimijoille kohdennetut palvelut

Tilannekuva ja verkostojohtaminen

- **Tilannekuva**
- Ohjeet ja suositukset
- Haavoittuvuuskoordinaatio
- **Yhteistyöverkostot**
- **Harjoitustoiminta**

Havainnointi ja avunanto

- **Koordinointi ja avunanto**
- **Vakavien tietoturvaloukkausten havainnointi**
- Autoreporter

Muut viranomaispalvelut

- Arvioinnit ja hyväksynnät
- Lainsäädännön soveltaminen
- **Tietoturvaneuvonta**

Tilannekuva

Tilannekuvatuotteet antavat ajantasaista tietoa kyberturvallisuuteen vaikuttavista tapahtumista ja ilmiöistä.

- **Varoitukset**
- **Tilannekuva ja tiedotteet**
- **Haavoittuvuustiedotteet**
- **Tietoturva Nyt -julkaisut**
- **Viikkoraportti**
- **Kybersää**

- **News-uutiskirje**
  - » Tilattavissa osoitteesta **https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/cert-fi/postituslista.html.stx**
- **Haavoittuvuuskooste**
  - » Tilattavissa osoitteesta **https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/cert-fi/postituslista.html.stx**

Tilannekuva

Tilannekuvatuotteet antavat ajantasaista tietoa kyberturvallisuuteen vaikuttavista tapahtumista ja ilmiöistä.

- Saat tuotteet liittymällä sähköpostilistalle
- Voit tiedustella listojen jäsenyyttä ja sisältöä sähköpostiosoitteesta cert@ficora.fi
- VIRT-lista valtionhallinnon toimijoille
- Julkishallinto-lista on vasta käynnistymässä

- Toimialakohtaiset sähköpostilistat
  - VIRT
  - Julkishallinto
  - Puolustusteollisuus
  - Energia-ala
  - Finanssiala
  - Teollisuusautomaatio
  - Kemia- ja prosessiteollisuus
  - Logistiikka-ala
  - Elintarvikeala
  - Terveydenhuolto
  - Teollisuusyritykset
  - Laite- ja tuotevalmistajat
  - ICT-ala
  - Media-ala
  - Tietoturvakonsultit ja -talot
  - Tietoturvatutkijat
  - CERT-toimijat

#kybersää lokakuu 2017

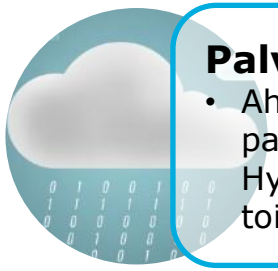
#kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tarkoituksena on antaa lukijalle nopea kokonaiskuva siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen

huolestuttava

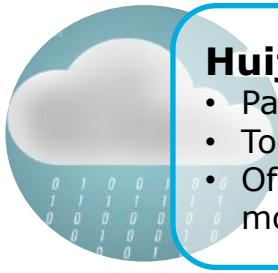
vakava

#kybersää 10/2017



Palvelunestot
- Ahvenanmaalle kohdistuneet palvelunestohyökkäykset jatkuivat lokakuussa. Hyökkäykset vaikuttivat useiden palveluiden toimintaan.

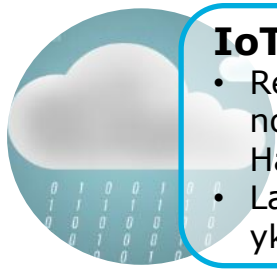
Haittaohjelmat & haavoittuvuudet
- Haittaohjelmien levitys Microsoft Officen DDE-toimintoa hyväksikäyttämällä on yleistynyt.
- Viro uusi 750 000 henkilökorttia haavoittuvuuden vuoksi



Huijaukset & kalastelut
- Pankkitunnusten kalastelu jatkuu.
- Toimitusjohtajahuijaukset jatkuvat yleisinä
- Office 365-tunnusten kalastelua käytetään monenlaisissa huijauksissa

Vakoilu
- APT28 viimeisimmät spearphishing-kampanjat on havaittu lokakuussa
- Bad Rabbit –haittaohjelmalla on mahdollisia kytköksiä valtiollisiin toimijoihin

Verkkojen toimivuus
- Lokakuussa merkittävä häiriö Lahden alueen TV-lähetyksissä parhaaseen katseluaikaan.
- Muuten edelleen suhteellisen vähän ja suhteellisen pieniä toimivuushäiriöitä.

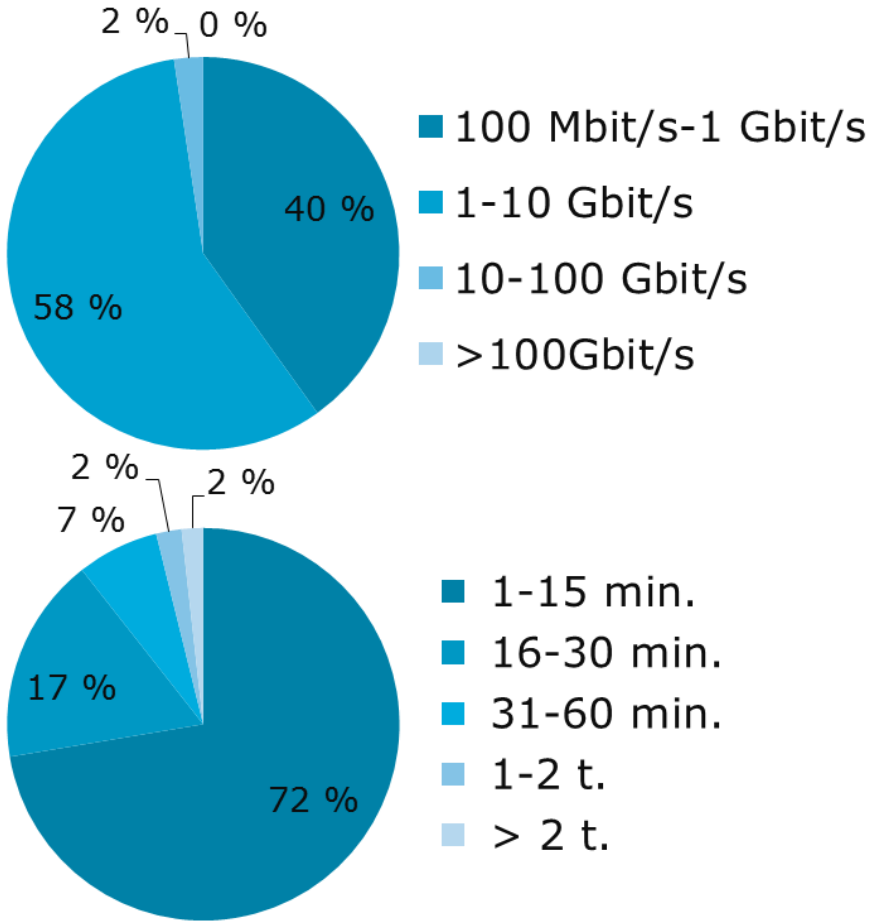


IoT
- Reaper-bottiverkko nousi tyhjästä ja levisi nopeasti , kadoten äkillisesti marraskuussa. Haavoittuvuuksiin olisi päivitykset.
- Lasten älyrannekellojen tietoturvassa ja yksityisyyden suojassa vakavia puutteita

Palvelunestot

Palvelunestohyökkäykset ja niillä uhkailu

- Ahvenanmaalle kohdistui syys- ja lokakuussa volyymiltään ja kestoltaan merkittävien palvelunestohyökkäysten sarja.
  - Hyökkäyksillä oli vaikutuksia useiden palveluiden toimintaan.
- Useita julkishallinnon toimijoita vastaan tehtiin jälleen palvelunestohyökkäyksiä, jotka aiheuttivat kuitenkin vain pieniä häiriöitä.
- Euroopassa nähty Lizard Squadin tekemäksi väitettyjä palvelunestohyökkäyksellä kiristyksiä
  - Kiristyksen yhteydessä on tehty lyhyitä palvelunestohyökkäyksiä, volyymiltään n. 5 Gbit/s.
- Suurimpia Suomessa viimeaikoina havaittuja palvelunestohyökkäyksiä:
  - 2017/Q4: n. 57 Gbit/s (kesto alle 10 min)
    - Hyökkäys jatkui 20 Gbit/s volyymillä n. 2 tuntia
  - 2016: n. 280 Gbit/s (kesto 42 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2017/Q3. Keräämme tilaston suoraan teleyrityksiltä. Lähde: Telia. Seuraava tilasto: tammikuussa 2018

Huijaukset & kalastelut

Huijaukset lokakuussa

- Uusia huijauskohteita kehitellään jatkuvasti – nyt Bitcoinit ovat suosittu teema
- Tietoja yritetään kalastella tunnettujen pankkien nimissä.
  - » Nordea, Danske Bank ja S-pankki ovat edelleen yleisiä teemoja.
  - » Myös Apple ID - ja PayPal-tunnuksia yritetään kalastella.
- Huijausviestejä on lähetetty myös verottajan nimissä
- Office 365-tunnuksien avulla rikolliset yrittävät päästä yrityksen sisäverkkoon
  - » Samalla menetelmällä urkitaan tietoja, joita käytetään laskutushuijauksiin
- Toimitusjohtajahuijaukset ovat edelleen yleisiä.
- Tilausansat käyttivät luvatta tunnettuja tuotemerkkejä, esimerkiksi Prismaa, Postia ja Finnairia.

Yhteistyöverkostot (ISAC:it)

Toimialakohtaiset tietoturva-asioiden tiedonvaihtoryhmät (ISAC, Information and Analysis Centre) ovat eri toimialoille perustettuja organisaatioiden välisiä yhteistyöelimiä

- Mahdollistaa
  - tietoturva-asioiden luottamuksellisen käsittelyn osallistujien kesken
  - organisaatioiden tietoturvaosaamisen lisäämisen
  - Kyberturvallisuuskeskuksen kokonaistilannekuvan kehittämisen
- Toiminta perustuu säännöllisiin tapaamisiin sekä määritettyihin toimintamalleihin ja osallistujiin

- ISAC-tiedonvaihtoryhmiä on perustettu seuraaville toimialoille:
  - VIRT
  - Internet-palveluntarjoajat
  - Kemia ja metsäteollisuus
  - Pankit
  - Media
  - Energia-ala
  - Elintarviketuotanto ja -jakelu
  - SOTE
  - Ohjelmistovalmistajat

Harjoitustoiminta

Harjoitustoiminnan tavoitteena on parantaa organisaatioiden toimintavalmiuksia vakavien kyberloukkaustilanteiden varalle, parantaa organisaatioiden reagointikykyä sekä lyhentää ja pienentää toteutuneiden uhkien vaikutuksia

- Tuemme kyberturvallisuuskeskus valtionhallinnon ja huoltovarmuuskriittisten yritysten kyberturvallisuuteen liittyvää harjoitustoimintaa
  - » antamalla asiantuntijatukea harjoitusten järjestämiseen
  - » osallistumalla realististen, tosielämän tietoturvaloukkauksiin perustuvien harjoitusskenaarioiden suunnitteluun.

- Harjoitustoiminnasta lisätietoa sähköpostiosoitteesta cert@ficora.fi

Tietoturvaneuvonta

Kyberturvallisuuskeskus palvelee tietoturvaneuvonnalla valtionhallinnon toimijoita ja huoltovarmuuskriittisiä organisaatioita.

- Tarkoituksena varmistaa organisaatioiden tietoisuus kybertoimintaympäristön uhkista.
- Tukea asiakkaita toimintansa ja järjestelmiensä turvallisuuden varmistamisessa.
- Neuvonnan kohde ja laajuus määritetään yhdessä asiakkaan kanssa tapauskohtaisesti.
- Kyberturvallisuuskeskus antaa tietoturvaneuvontaa kulloinkin käytettävissä olevien resurssien mahdollistamissa rajoissa.
- Lisätietoa sähköpostiosoitteesta cert@ficora.fi

Koordinointi ja avunanto tietoturvaloukkauksissa

Tarjoamme tarvittaessa apua tietoturvaloukkauksen selvittämiseksi ja tutkimiseksi sekä koordinoimme tarvittavia toimenpiteitä

- Toimenpiteet voivat pitää sisällään esimerkiksi
  - Tiedon jakamista
  - Yhteistyökumppanien ja -verkostojen kontaktointia
  - Teknistä analyysiä
  - Lainopillista neuvontaa
- Lisäksi toteutamme nk. VIRT-koordinaatiokokouksen laajoissa valtionhallinnon ICT-häiriötilanteissa

- Voit ilmoittaa meille tietoturvaloukkauksesta sähköpostitse cert@ficora.fi
- Turvaposti: https://secmail.ficora.fi/
- Asiakaspalvelu ma-pe klo 9-15 puhelimitse 0295390230
- Lisäksi Kyberturvallisuuskeskus ylläpitää valtionhallinnolle ja huoltovarmuuskriittisille toimijoille tarkoitettua 24/7 -päivystystä.
- Päivystyksen ei-julkista puhelinnumeroa voi tiedustella cert@ficora.fi

Milloin kannattaa olla yhteydessä Kyberturvallisuuskeskukseen?

- VAHTI-ohje 8/2017 esimerkit
- Erityisesti:
  - Haittaohjelmatilanteissa
    - Jos haittaohjelmatorjunta tunnistanut ja torjunut, sähköposti-ilmoitus
  - Palvelunestohyökkäystilanteissa
  - Phishing-tapauksissa
  - Pääsynhallinnan merkittävissä poikkeamissa
  - Epäiltäessä tunkeutujaa järjestelmissä
  - Tietovuototapauksissa
  - Havaittaessa epätyypillistä tiedonsiirtoa organisaation verkosta
  - Epäiltäessä APT-hyökkäystä

Kyberturvallisuuskeskuksen vahvuudet

- Kokonaistilannekuva
  - » onko näkynyt muualla
  - » muiden uhrien varoittaminen
- Vahvat yhteydet operaattoreihin ja ICT-palveluntarjoajiin
- Kansainvälinen yhteistyö
  - » CERT-toimijat, ohjelmisto- ja laitevalmistajat
- Haittaohjelma-analyysi
  - » Automatisoitu analyysiympäristö, mahdollisuus tarkempaan selvittelyyn
- APT-tapausten erityisasiantuntija-apu

Muistilista asioista

- Rauhallisuus on valttia – mutta toimi viipymättä
- Käynnistä häiriönhallintaprosessin mukainen toiminta
  - » Sisäinen koordinaatio
  - » Tapahtuman vaikutusten ja juurisyiden analyysi
  - » Yhteydet yhteistyökumppaneihin (ICT-palveluntarjoajat)
- Turvaa todistusaineisto
  - » Lokitiedot
  - » Tietojärjestelmien hallittu uudelleenasennus
- Muista viestintä – sisäinen ja ulkoinen
- Yhteydenotto Kyberturvallisuuskeskukseen ja poliisiin

Vakavien tietoturvaloukkausten havainnointi

Palvelemme huoltovarmuuskriittisiä toimijoita ja valtionhallintoa tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä HAVARO:n avulla

- Järjestelmän avulla organisaation verkkoliikenteestä havainnoidaan haitalliseksi tunnistettua tai normaalista poikkeavaa liikennettä.
- Havainnoidaan vakavia tietoturvauhkia, kuten
  - APT (Advanced Persistent Threat) -toimintaa
  - Tietoa varastavia haittaohjelmia
- HAVARO:n avulla ei ole tarkoitus havainnoida tavanomaisia tietoturvauhkia ja haittaohjelmia
- Varoitamme asiakasta havaituista tietoturvaloukkauksista.
- Koostamme asiakkaalle varoituksia muualla havaituista uhkista sekä laadimme raportteja sen omasta ja toimialan tietoturvatilanteesta.
- Lisätietoa sähköpostiosoitteesta cert@ficora.fi

Viestintävirasto
Kyberturvallisuuskeskus

cert@ficora.fi

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi