TRAFICOM
Liikenne- ja viestintävirasto

Laajamittaisten kyberturvallisuus-poikkeamien ja -kriisien hallinta Suomessa

Traficomin julkaisuja
12/2025

Sisällysluettelo

1 Johdanto

Jokaisen EU-jäsenvaltion on määritettävä NIS2-direktiivin nojalla nk. kansallinen kyberkriisinhallintakehys. Kyberkriisinhallintakehys muodostuu kyberkriisinhallintaviranomaisesta ja kyberkriisien hallintasuunnitelmasta, joista on säädetty direktiivin 9 artiklassa. Jäsenvaltion on nimettävä tai perustettava yksi tai useampi kyberkriisinhallintaviranomainen, jonka tehtävänä on vastata laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnasta. Laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelmassa tulee vahvistaa laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallinnan tavoitteet ja järjestelyt. Laajamittaisella kyberturvallisuuspoikkeamalla tarkoitetaan poikkeamaa, joka aiheuttaa niin laajan häiriön, ettei Suomella yksin ole valmiuksia hallita sitä, tai jolla on merkittävä vaikutus myös toiseen EU-jäsenvaltioon.

Suomessa NIS2-direktiivin tarkoittamana kyberkriisinhallintaviranomaisena toimii kukin viranomainen sille laissa säädettyjen tehtävien mukaisesti. Kyberkriisinhallintaviranomaisten koordinaattorina toimii Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, joka vastaa myös kansallisen NIS2-direktiivin edellyttämän kyberkriisinhallintakehyksen laatimisesta laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallitsemiseksi yhteistyössä muiden viranomaisten kanssa.

Kansallinen kyberkriisinhallintamalli kuvaa kansalliset valmiudet toimia laajamittaisessa ja vakavassa yhteiskuntaa koskettavassa kyberkriisissä ja sen, miten kriisitilanteita johdetaan, hallitaan ja koordinoidaan. Tarkat toimintamallit sekä mm. eri viranomaisten kyvykkyydet ja resurssit eivät ole julkista tietoa. Tässä asiakirjassa kuvataan siksi yleisellä tasolla kyberkriisien hallintaan liittyviä toimijoita ja toimintamalleja.

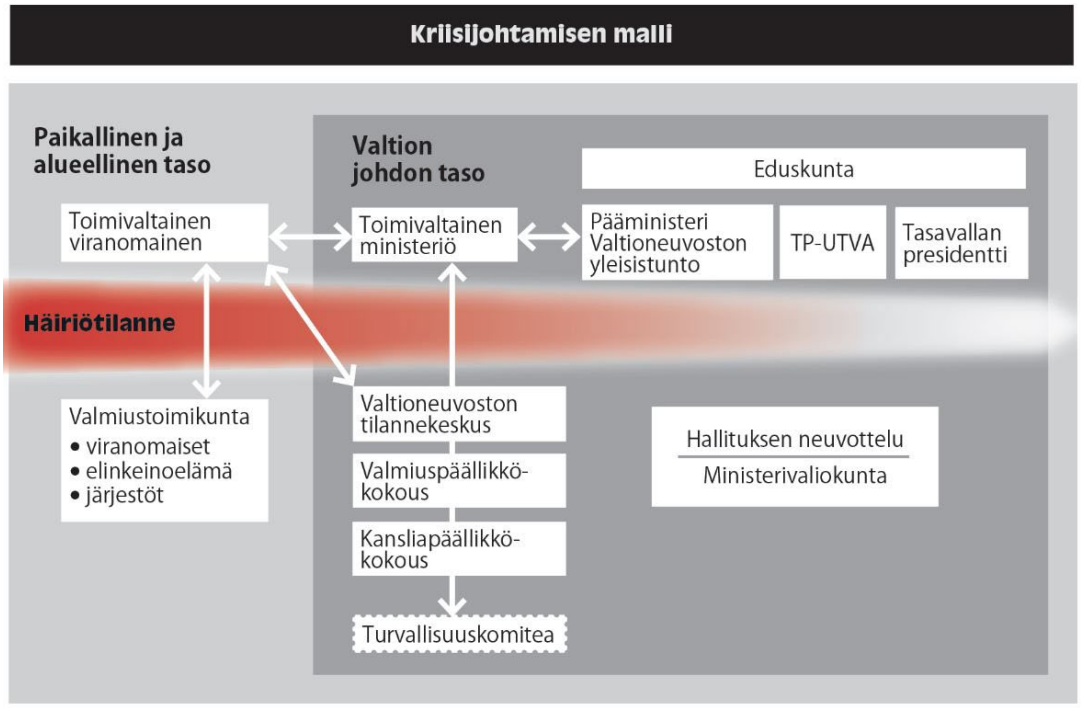
Tässä kansallisessa kyberkriisinhallintamallissa kuvataan toimijoiden roolit, tehtävät ja vastuut kyberkriisin hallinnassa, kansalliset varautumiskeinot sekä kyberturvallisuuspoikkeamien ja -kriisien hallinta Euroopan unionissa.

Mallia käytetään soveltuvin osin kuvaamaan toimintaa myös muissa sellaisissa kansallisissa vakavissa kyberpoikkeama- tai -häiriötilanteissa, jotka vaikuttavat laajamittaisesti kansallisesti merkittävän tietojärjestelmän tai tietoverkon tiedon eheyteen, luottamuksellisuuteen tai saatavuuteen. Tällaisia tilanteita voivat olla esimerkiksi yhteiskunnan elintärkeään toimintoon tai sitä ylläpitävään organisaation kohdistuvat vakavat kyberhyökkäykset. Tällaisissa tilanteissa varautumiskeinojen ja -toimien tavoitteena on turvata yhteiskunnan elintärkeiden toimintojen jatkuvuus ja palautuminen vakavissa kyberhäiriöissä.

2 Roolit, tehtävät ja vastuut kyberkriisin hallinnassa

Kansallisissa kyberturvallisuuskriiseissä noudatetaan valtioneuvoston ohjesäännön 262/2003 mukaista työjärjestystä ja toimivaltaa. Häiriötilanteessa toimivaltainen viranomainen johtaa operatiivista toimintaa ja poikkihallinnolliset yhteistyöelimet tukevat vastuuviranomaista. Toimintaa johtava taho vastaa myös kriisiviestinnästä. Muut viranomaiset, yritykset ja järjestöt osallistuvat toimintaan tilanteen hallinnan edellyttämässä laajuudessa. Vastuuviranomainen käynnistää häiriötilanteen hallintaan liittyvät toimenpiteet, tiedottaa tilanteesta tarvittavassa laajuudessa muille viranomaisille ja toimijoille sekä kytkee toimintaan muut häiriötilanteen hallinnan edellyttämät toimijat. Operatiivisten toimien ohella häiriötilanteiden hallinnan yhteydessä korostuu tiedonkulun varmistaminen toimijoiden välillä sekä valtiojohdon riittävä informointi.

Ministeriöiden välisestä yhteistyöstä säädetään valtioneuvostosta annetun lain 2 §:ssä. Pysyviä yhteistyöelimiä ovat kansliapäällikkö- ja valmiuspäällikkökokous. Kansliapäällikkökokous toimii valtioneuvoston johtamisen tukena. Häiriötilanteissa johtamisen tukena toimii myös valmiuspäällikkökokous.



Kuva 1. Valtioneuvoston yleisistunnon ja ministeriöiden päätöksentekoa ja valmistelua avustavat ministeriöiden kansliapäälliköt ja kansliapäällikkökokous. Kansliapäällikkökokous toimii valtioneuvoston johtamisen tukena. Häiriötilanteissa johtamisen tukena toimii valmiuspäällikkökokous. Turvallisuuskomitea on kokonaisturvallisuuden alalla toimiva pysyvä yhteistoimintaelin, ja häiriötilanteissa se toimii asiantuntijaelimenä. Turvallisuuskomiteassa ovat jäseninä ministeriöiden kansliapäälliköt, pelastus- ja poliisiylijohtajat, pääesikunnan ja rajavartiolaitoksen päälliköt, Tullin pääjohtaja ja Huoltovarmuuskeskuksen toimitusjohtaja. Turvallisuuskomitea avustaa valtioneuvostoa yleisen varautumisen yhteensovittamisessa. Huoltovarmuuskeskus ylläpitää yhteistyössä Turvallisuuskomitean ja muiden viranomaisten sekä yritysten ja järjestöjen kanssa ajantasaista tietoa huoltovarmuudelle kriittisestä tuotannosta, palveluista ja infrastruktuureista. (Lähde: Kohti huomisen huoltovarmuutta. Selvitys julkisen ja yksityisen sektorin yhteistyöstä, http://urn.fi/URN:ISBN:978-952-327-996-4, haettu 15.1.2025)

2.1 Laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien kansallinen menettely

Laajamittaisella kyberturvallisuuspoikkeamalla tarkoitetaan poikkeamaa, joka aiheuttaa niin laajan häiriön, ettei Suomella yksin ole valmiuksia hallita sitä, tai jolla on merkittävä vaikutus myös toiseen EU-jäsenvaltioon.

Laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintaa tuetaan toisiaan tukevilla kansallisilla kyberkriisinhallintajärjestelyillä, joita on kuvattu esimerkinomaisesti alla. Järjestelyt tukevat valtioneuvoston ohjesäännön mukaista kriisinhallintamallia. Prosessi keskittyy erityisesti viranomaisten suorittamaan yhteistyöhön tapauksen hallinnassa.

1. Ensihavainnointi

   Kyberturvallisuuspoikkeaman tai -kriisin hallintamalli käynnistyy, kun jokin taho saa ensimmäisen tiedon tai havainnon kyberturvallisuuspoikkeamasta tai -kriisistä (myöhemmin "tapahtuma"). Tällainen ensihavainnointi voi olla esimerkiksi organisaation poikkeamahavainto omassa ympäristössään, CSIRT-yksikölle vapaaehtoisen ilmoituksen kautta tuleva tiedoksianto tai CSIRT-yksikön suorittaman ennakoivan skannauksen myötä tapahtunut havainto.

2. Havainnon tiedoksituonti

   Seuraavassa vaiheessa tehty havainto tuodaan tiedoksi niille tahoille, jotka ovat oleellisia tapahtuman hallinnoimiseksi ja käsittelemiseksi. Tällaisia tahoja voivat olla eri viranomaistahot kuten Liikenne- ja viestintäviraston CSIRT-yksikkö, Poliisi, Suojelupoliisi, Puolustusvoimat tai toimivaltainen viranomainen.

3. Tapahtuman hallinnoimiseksi järjestäytyminen

   Havainnon tiedoksi tuonnista käynnistyy useampien eri tahojen suorittamia toimenpiteitä, jotka voivat toimia rinnakkain. Valtioneuvostotasoinen kyberturvallisuuden koordinaatioryhmä kokoontuu varmistamaan, että tapahtuman johtovastuut ja koordinaatio ovat selvät. Lisäksi ryhmä vastaa, että tapahtumasta on yhtenäinen ja kattava tilannekuva, joka palvelee valtionjohdon tietotarpeita.

4. Kyberturvallisuuden viranomaisyhteistyöryhmän kokoontuminen

   Tapahtuman hallinnan ja koordinoinnin tueksi voidaan kutsua kyberturvallisuuden viranomaisyhteistyöryhmä, joka edistää viranomaisten välistä kyberturvallisuuteen liittyvää yhteistoimintaa ja tiedonjakamista. Ryhmä varmistaa omalta osaltaan, että valtioneuvostotasoisella kyberturvallisuuden koordinaatioryhmällä on käytössään analysoituun tietoon perustuva tilanneymmärrys tapahtuneesta.

5. Toimivaltaisten viranomaisten toimenpiteet

Toimivaltaiset viranomaiset toimivat omien prosessiensa mukaisesti tapahtuman hallitsemiseksi, noudattaen valtioneuvoston ohjesääntöä kriisitilanteen hallitsemiseksi sekä muita kansallisia menettelytapoja ml. tämä suunnitelma.

6. Viestintävastuut

   Kansallisesta viestinnästä vastaa tilanteesta riippuen tapahtuman uhriorganisaatio yhdessä vastuuviranomaisen kanssa. Muut viranomaiset tukevat tarvittavin osin tapahtuman viestinnässä.

7. Seuranta

   Tapahtuman vaikutuksien ja korjaavien toimenpiteiden seurantaa tehdään yhteistyössä edellä mainittujen ryhmien ja vastuutahojen osalta. Seuranta on käynnissä siihen asti, kunnes todetaan tapahtuman vaikutuksien päättyneen ja korjaavien toimenpiteiden onnistuneen.

2.2 Viranomaiset kansallisessa kyberturvallisuuskriisin hallinnassa

Kansallisissa kyberhäiriötilanteissa toimivaltaiset viranomaiset johtavat häiriötilanteen hallintaa kukin tehtävänsä ja toimivaltansa puitteissa.

2.2.1 Liikenne- ja viestintäviraston Kyberturvallisuuskeskus

Liikenne ja viestintäviraston Kyberturvallisuuskeskus tukee asiantuntemuksellaan toimivaltaisia viranomaisia ja tuottaa kyberturvallisuuden tilannekuvaa. Se kerää, analysoi ja jakaa tietoa Suomessa tapahtuvista tietoturvauhkista ja -loukkauksista, sekä selvittää osaltaan Suomeen kohdistuvia teknisiä tietoturvapoikkeamia. Kyberturvallisuuskeskuksella on kansallisen kyberturvallisuuslain mukaan laajamittaisessa poikkeamassa koordinointitehtävä.

Kyberturvallisuuskeskuksessa toimii kansallinen CSIRT-yksikkö (Computer Security Incident Response Team), jonka tehtäviin kuuluu kansallisessa kyberhäiriötilanteessa:

- Tilannekuvan muodostaminen
- Ilmoitusten vastaanottaminen ja tiedonjakaminen
- Johtovastuussa olevan viranomaisen tukeminen
- Avustavat tehtävät

2.2.2 Poliisi

Tietoverkkorikosten ennalta estämisessä, selvittämisessä ja syyteharkintaan saattamisessa toimivaltaisena viranomaisena toimii poliisi.

Keskusrikospoliisi (KRP) on poliisin valtakunnallinen yksikkö, jonka toimialueena on koko Suomi. Keskusrikospoliisissa toimii tietoverkkorikosten esitutkintaan erikoistunut yksikkö, Poliisin kyberrikostorjuntakeskus, jossa tutkitaan pääasiallisesti tietoverkkoympäristöihin kohdennettuja laajoja, ennakkotapausluonteisia ja yhteiskunnallisesti merkittäviä tietoverkkorikoskokonaisuuksia.

2.2.3 Suojelupoliisi

Suojelupoliisin tehtävänä sekä havaita, estää ja paljastaa toimintaa, joka voi uhata kansallista turvallisuutta, kuten vieraiden valtioiden vakoilua tai vaikuttamista verkossa. Lisäksi Suojelupoliisin tehtävä on hankkia tietoa kansallisen turvallisuuden suojaamiseksi ylimmän valtiojohdon päätöksenteon tukemiseksi ja muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten.

2.2.4 Puolustusvoimat

Puolustusvoimat vastaa sotilaallisesta kyberpuolustuksesta, jolla tarkoitetaan niitä toimia, joilla turvataan Suomen puolustuskykyyn vaikuttavat järjestelmät ja eri sektorien toimijat erityisesti valtiollisilta uhkatoimijoilta ja niiden edustajilta puolustuskyvyn varmistamiseksi sekä turvataan Suomen suvereniteettia ja toimeenpannaan sotilaalliset kyberoperaatiot.

Sotilastiedustelun tarkoituksena on hankkia ja käsitellä tietoa Suomeen kohdistuvasta tai Suomen turvallisuusympäristön kannalta merkityksellisestä sotilaallisesta toiminnasta taikka vieraan valtion toiminnasta tai muusta sellaisesta toiminnasta, joka vaarantaa yhteiskunnan elintärkeitä toimintoja. Tietoa tuotetaan ylimmän valtiojohdon päätöksenteon tukemiseksi ja Puolustusvoimien tehtävien suorittamiseksi.

2.2.5 Valvovat viranomaiset

Sektorikohtaiset valvovat viranomaiset valvovat lain, sen nojalla annettujen määräysten sekä annettujen säädösten, eli komission täytäntöönpanosäädösten noudattamista kunkin sektorin toimijoiden osalta. Suomessa NIS2-direktiivin tarkoittamana kyberkriisinhallintaviranomaisena toimii kukin viranomainen sille laissa säädettyjen tehtävien mukaisesti.

Tarkempi kuvaus valvovien viranomaisten toimikentästä löytyy liitteestä 1.

2.2.6 Huoltovarmuuskeskus (HVK)

Huoltovarmuuskeskuksen tehtävänä on yhteistyössä huoltovarmuusorganisaation kanssa varmistaa huoltovarmuuden kannalta elintärkeiden teknisten järjestelmien toimivuus, kehittää julkishallinnon ja elinkeinoelämän yhteistoimintaa huoltovarmuusasioissa, turvata välttämätön tavara- ja palvelutuotanto sekä sotilaallista maanpuolustusta tukeva tuotanto ja ylläpitää

huoltovarmuuden tilannekuvaa. Huoltovarmuuskeskuksen hoidossa on valtion talousarvion ulkopuolinen huoltovarmuusrahasto, jota hyödynnetään tarvittaessa nopeaa rahoitusta vaativissa hankkeissa ja kriiseissä, silloin kun sillä on merkittävä vaikutus huoltovarmuuden turvaamiseen.

2.2.7 Kyberturvallisuusjohtajan toimisto

Liikenne- ja viestintäministeriöön sijoitettu valtion kyberturvallisuusjohtajan toimisto vastaa kansallisesti kyberturvallisuuden kehittämisen, suunnittelun, varautumisen ja kriittisen tieto- ja viestintäteknisen infrastruktuurin varautumisen koordinaatiosta ja yhteensovittamisesta.

2.2.8 Kyberturvallisuuden viranomaisyhteistyöryhmä

Kyberturvallisuuden viranomaisyhteistyöryhmä on valtioneuvostotason ja teknisen asiantuntijatason väliin sijoittuva yhteistyörakenne. Viranomaisyhteistyöryhmässä eri viranomaiset analysoivat omista lähteistään kerättyjä tilannetietoja ja muodostavat yhteisen tilanneymmärryksen päätöksenteon ja kulloinkin toimivaltaisten viranomaisen jatkotoimien perustaksi.

Yhteinen tilanneymmärrys parantaa edellytyksiä tunnistaa vakavia kyberuhkia ja mahdollistaa kokonaisvaltaisen tiedon välittämisen strategiselle tasolle tai muille yhteiskunnan toimijoille. Yhteistyörakenne ei korvaa viranomaisten lakisääteisiä tehtäviä eri prosesseissa, mutta varmistaa, että kussakin prosessissa on käytössä kaikki tarvittava tieto ja että tilanneymmärrys on kokonaisvaltaisempi.

Syntyvän yhteisen tilanneymmärryksen perusteella voidaan koordinoida ja arvioida tarvittavia viranomaistoimenpiteitä tai suosituksia muille toimijoille riippumatta siitä, onko kyse tietoturvatoimenpiteistä, rikosprosessiin kuuluvista asioista tai ulko- ja turvallisuuspoliittisen päätöksenteon tukemisesta.

Yhteistyöryhmä muodostuu Liikenne- ja viestintäviraston (Kyberturvallisuuskeskuksen), Suojelupoliisin, Poliisihallituksen, Keskusrikospoliisin sekä Puolustusvoimien edustajista.

2.3 Attribuutio ja kyberdiplomatia

Attribuutiolla tarkoitetaan vihamielisen kyberoperaation toteuttajan tunnistamista, paikantamista ja yksilöimistä analyyttisen, eri tietolähteitä hyödyntävän prosessin kautta. Kansallisella tasolla prosessiin kytkeytyy niin tekninen analyysi kuin viranomaisvastuut sekä ulko- ja turvallisuuspoliittinen harkinta. Attribuutio on analyysiprosessin lopputulos riippumatta siitä, onko tulos julkistettava vai ei-julkinen. Attribuutio on usein edellytys oikeudelliseen tai poliittiseen vastuuseen saattamiselle, kansainvälisten velvoitteiden mukaisille toimenpiteille (retorsio) ja sallituille vastatoimille.

2.4 Muut toimijat kansallisessa kyberkriisissä

Kansallisen kyberkriisin tapahtuessa tilanteeseen liittyy mahdollisesti useita muita toimijoita kuin viranomaistoimijoita. Tässä luvussa kuvataan yleisimmät toimijat sekä yhteistyörakenteet.

2.4.1 Kohde-/uhriorganisaatiot

Useimmiten kansallinen kyberkriisi koskettaa organisaatiota, jolla on erityisen merkittävä rooli yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta. Uhriorganisaatiolla tarkoitetaan tässä dokumentissa organisaatiota, joka on kohdannut laajamittaisen ja vakavan yhteiskuntaa koskettavan tietoturvapoikkeaman, joka vaikuttaa laajamittaisesti kansallisesti merkittävän tietojärjestelmän tai tietoverkon tiedon eheyteen, luottamuksellisuuteen tai saatavuuteen.

Uhriorganisaatioksi voi päätyä minkä kokoinen organisaatio tahansa. Eri organisaatioilla on erilaiset valmiudet vastata laajaan kansalliseen tietoturvapoikkeamaan.

Uhriorganisaatio vastaa itse havaitsemansa tietoturvatapahtuman ensivasteesta sekä rajoittamis- ja muista toimenpiteistä. Poliisin tai muiden tahojen suorittamaa tutkintaa varten organisaation tehtävänä on myös varmistaa todistusaineiston turvaaminen myöhempää mahdollista rikostutkintaa tai muuta tutkintaa varten. in

Uhriorganisaation rooliin ja tehtäviin kuuluu omien sisäisten käytäntöjen lisäksi

- Raportoida tapahtumasta oman toimialansa valvovalle viranomaiselle
- Raportoida tapahtumasta Kyberturvallisuuskeskuksen CSIRT-yksikölle
- Ilmoittaa viipymättä palveluidensa vastaanottajille, jos merkittävä poikkeama haittaa palveluiden vastaanottamista
- Tehdä rikosilmoitus poliisille, jos rikos on tapahtunut
- Tehdä tarvittaessa ilmoitus tietosuojavaltuutetulle
- Turvallisuuskriittisen toiminnan häiriintyessä tarvittaessa ilmoittaa turvallisuudesta vastaavalle valvontaviranomaiselle
- Ilmoittaa tilannekuvan luomiseksi tarvittaessa suojelupoliisille, keskusrikospolisiille, huoltovarmuuskeskukselle, pelastustoimelle, ministeriölle (VOP) ja CER -direktiivin mukaiselle valvontaviranomaiselle
- Tarvittaessa hankkia avukseen ulkopuolinen tietomurtotutkintoihin (DFIR) erikoistunut toimija avustamaan tapauksen selvittämisessä

- Tarvittaessa ilmoittaa toimialansa kyberturvallisuuden tiedonvaihtoryhmien jäsenille
- Rajat ylittävien vaikutusten osalta tarvittaessa huomioitava muiden valtioiden viranomaisille ilmoittaminen

2.4.2 Yksityiset kyberturvallisuusyritykset

Uhriorganisaatio voi tarvita tietoturvapoikkeaman hallintaan ja tutkintaan ulkopuolista apua, jota yksityiset kyberturvallisuusyritykset voivat tarjota. Uhriorganisaatio ja yksityinen kyberturvallisuusyritys vastaavat keskenään sopimusteknisistä järjestelyistä poikkeaman hallintaa ja tutkintaa koskien.

Yksityisillä kyberturvallisuusyrityksillä saattaa olla uhriorganisaation tai -organisaatioiden kyvyistä, ja tilanteen laajuudesta riippuen merkittävä rooli kyberkriisin hallinnassa ja siitä palautumisesta. Lisäksi yksityisillä kyberturvallisuusyrityksillä on merkittävä rooli tilannekuvatiedon jakamisessa ja muodostamisessa muiden yritysten ja viranomaisten kesken.

2.4.3 ISAC-tiedonvaihtoryhmät

ISAC-tiedonvaihtoryhmät (ISAC=Information Sharing and Analysis Centre) ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä. ISAC-tiedonvaihtoryhmissä käsitellään luottamuksellisesti kyberturvallisuuteen liittyviä asioita, kuten uhkia, ilmiöitä ja hyviä käytäntöjä. Ryhmät kehittävät myös edustamansa toimialan ja yhteiskunnan kyberturvallisuutta esimerkiksi toteuttamalla toimialaansa liittyviä riskianalyysejä, tutkimuksia ja ohjeistusta.

ISAC-tiedonvaihtoryhmien jäsenet muodostavat laajan kansallisen verkoston, jolla on tärkeä rooli myös häiriötilanteiden hallinnassa. Häiriötilanteessa ryhmät ja niiden jäsenet tarjoavat verkoston hyväksi asiantuntemustaan, analyysiresursseja, tietolähteitä ja kansainvälisiä yhteyksiä. Yhteistyötä häiriötilanteissa harjoitellaan myös säännöllisesti.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus vastaa ISAC-toiminnasta Suomessa.

2.5 Viestintä ja tiedonvaihto kyberkriisissä

Kansallisella tasolla viranomaisilla on käytössä useita julkisia ja ei-julkisia tiedonvaihtokanavia. Näiden lisäksi on olemassa myös muita kuin viranomaisten tiedonvaihtokanavia, joita käytetään tarvittaessa tiedonvaihtoon kansallisessa kyberkriisissä.

3 Kansalliset varautumiskeinot

Kansallisen varautumisen pohjana toimivat lukuisat erilaiset yhteistyöverkostot ja rakenteet, joita on kuvattu tarkemmin luvussa 2. Lisäksi Suomessa toimii erilaisia sektorikohtaisia yhteistyöverkostoja, joista yhtenä esimerkkinä on Kyberturvallisuuskeskuksen vetämän Häiriötilanteiden yhteistoimintaryhmä HÄTY, jonka tehtävänä on yhteistyössä teleyritysten, sähköyhtiöiden, urakoitsijoiden ja viranomaisten kesken varautua ennalta erilaisiin viestintäverkkoja koskeviin häiriötilanteisiin.

Huoltovarmuuskeskuksen tehtävänä on varautua yhdessä yrityselämän, kolmannen sektorin ja viranomaistahojen kanssa siihen, että myös kriisitilanteissa yhteiskunta toimii ja elämä jatkuu mahdollisimman häiriöttä. Huoltovarmuuskeskuksen yhteydessä toimii sektoreita ja pooleja, jotka pitävät yllä ja kehittävät huoltovarmuutta ja jatkuvuudenhallintaa oman toimialansa yritysten ja organisaatioiden verkostossa.

3.1 Kansalliset harjoitukset

3.1.1 Kansalliset kyberturvallisuusharjoitukset

Kansalliset kyberturvallisuusharjoitukset eli nk. KYHA-harjoitukset ovat merkittävimpiä valtionhallinnon kyberharjoituksia vuosittain. Valtionhallinnon siviiliviranomaisten (KYHA VH) harjoitus toteutetaan vuosittain toukokuussa, ja turvallisuusviranomaisten (KYHA TV) harjoitus syksyllä, yleensä syyskuun lopulla.

3.1.2 TAISTO-harjoitukset

Digi- ja väestötietovirasto (DVV) järjestää vuosittain Tietosuoja- ja tietoturvaloukkausten hallinnan harjoituksen (TAISTO), jossa häiriötilanteessa toimimista harjoitellaan kuvitteellisten tilanteiden kautta. Taisto on suunniteltu erityisesti julkiselle sektorille, mutta muutkin toimijat voivat osallistua harjoitukseen. Taisto tarjoaa turvallisen tilaisuuden harjoitella, testata ja kehittää organisaation digiturvan toimintamalleja kuvitteellisten häiriötilanteiden kautta. Taisto keskittyy erityisesti häiriötilanteiden hallintaan, johtamiseen ja viestintään, ja sen tapahtumat peilaavat ajankohtaisia uhkia.

3.1.3 TIETO-harjoitukset

TIETO on Suomen suurin yritysten ja viranomaisten yhteistoiminta ja tiedonvaihtoharjoitus laajojen hybridi-, kyber-, ja informaatiohäiriöiden varalta.
Se on myös yritysten jatkuvuudenhallintaa, varautumista ja kriisiviestintää laajoissa häiriötilanteissa sparraava, useiden toimialojen harjoitus.
TIETO24-harjoituksen organisoinnista vastaa huoltovarmuusorganisaation Digipooli yhteistyössä Huoltovarmuuskeskuksen, Traficomin

Kyberturvallisuuskeskuksen, Poliisin ja Puolustusvoimien kanssa. Harjoituksen järjestämisestä vastaa Huoltovarmuuskeskus.

4 Kyberturvallisuuspoikkeamien ja -kriisien hallinta Euroopan unionissa

Euroopan kyberkriisien yhteysorganisaatioiden verkosto EU-CyCLONe:n tehtävänä on tukea laajamittaisten kyberturvallisuuspoikkeamien ja kriisien koordinoitua hallintaa operatiivisella tasolla sekä varmistaa säännöllinen asiaankuuluvien tietojen vaihto jäsenvaltioiden ja unionin toimielinten, elinten, laitosten ja virastojen välillä. EU-CyCLONe koostuu jäsenvaltioiden kyberkriisinhallintaviranomaisten edustajista sekä komission edustajista, kun mahdollisella tai meneillään olevalla laajamittaisella kyberturvallisuuspoikkeamalla on tai todennäköisesti on merkittävä vaikutus direktiivin soveltamisalaan kuuluviin palveluihin ja toimintoihin. Suomea EU-CyCLONe:ssa edustaa Liikenne- ja viestintävirasto.

Suomessa kyberkriisinhallintaviranomaisena toimii kukin NIS2-direktiivissä tarkoitettu viranomainen sille laissa säädettyjen tehtävien mukaisesti. Kyberkriisinhallintaviranomaisten välisenä koordinaattorina, ja yhteyspisteenä EU-CyCLONe:en toimii Liikenne- ja viestintäviraston Kyberturvallisuuskeskus.

Unionin tason kriisinhallinnassa asianomaisten osapuolten olisi hyödynnettävä EU:n poliittisen kriisitoiminnan integroituja järjestelyjä, joista säädetään neuvoston täytäntöönpanopäätöksessä (EU) 2018/1993 (16), jäljempänä ’IPCR-järjestelyt’. Komission olisi käytettävä tähän tarkoitukseen ARGUS-järjestelmän korkean tason monialaista kriisinkoordinointiprosessia. Jos kriisiin liittyy merkittävä ulkoinen tai yhteisen turvallisuus- ja puolustuspolitiikan ulottuvuus, olisi aktivoitava Euroopan ulkosuhdehallinnon kriisinhallintamekanismi.

Liite 1 Kuvaus valvovien viranomaisten vastuualueista

Energiavirasto

Energiavirasto valvoo ja edistää energiamarkkinoita, päästöjen vähentämistä, energiatehokkuutta sekä uusiutuvan energian käyttöä.

Energiavirasto on lupa- ja valvontaviranomainen, jonka tehtävistä säädetään energiavirastosta annetussa laissa (870/2013). Lain 1 §:n mukaan sähkö- ja maakaasumarkkinoiden valvontaa ja seurantaa, sähkö- ja maakaasumarkkinoiden toimivuuden, energiatehokkuuden ja uusiutuvan energian käytön edistämistä sekä energiapolitiikan, kasvihuonekaasujen päästökaupan ja energiatehokkuuden toimeenpanotehtäviä varten on Energiavirasto. Tarkemmin sähkö- ja maakaasumarkkinoiden valvontaan liittyvistä tehtävistä säädetään siitä annetussa laissa (590/2013), jonka 2 §:n mukaan lakia sovelletaan niiden valvonta- ja seurantatehtävien hoitamiseen, jotka säädetään Energiaviraston tehtäviksi muun muassa sähkömarkkinalaissa (588/2013) ja maakaasumarkkinalaissa (587/2013). Lain tavoitteena on sähkön ja maakaasun hyvän toimitusvarmuuden, kilpailukykyisen hinnan ja kohtuullisten palveluperiaatteiden turvaamiseksi energian käyttäjille edistää tehokkaasti, varmasti ja ympäristön kannalta kestävästi toimivia kansallisia ja alueellisia sähkö- ja maakaasumarkkinoita sekä Euroopan unionin sähkön ja maakaasun sisämarkkinoita.

Sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain (590/2013) 30 §:ssä säädetään Energiaviraston tiedonsaanti- ja tarkastusoikeudesta. Lain mukaan valvottavaa toimintaa harjoittavan elinkeinonharjoittajan on annettava Energiavirastolle tässä laissa tarkoitettujen valvontatehtävien hoitamiseksi tarpeelliset tiedot ja asiakirjat. Tämän lisäksi Energiavirastolle on annettava muiden tässä laissa tarkoitettujen tehtävien hoitamiseksi tai kansainvälisten sopimusvelvoitteiden täyttämiseksi tarpeellisia tilasto- ja muita tietoja.

Ehdotetun kyberturvallisuuslain (XX/202X) mukaan Energiavirasto valvoo kyberturvallisuuslain, sen nojalla annettujen määräysten ja NIS 2-direktiivin nojalla annettujen säännösten noudattamista (valvova viranomainen) seuraavien toimialojen osalta: Sähkö, kaukolämmityksen tai kaukojäähdytyksen haltijat, kaasu (jakelu- ja siirtoverkonhaltijat ja maakaasun toimittajat) ja vedyn siirtoa harjoittavat toimijat.

Energiavirasto toimii sähköalan riskeihin varautumista koskevan EU-asetuksen (2019/941) mukaisena toimivaltaisena viranomaisena. Toimivaltaisen viranomaisen tehtäviin kuuluu muun muassa kansallisten sähkökriisiskenaarioiden määrittäminen sekä riskeihinvarautumissuunnitelmien laatiminen. Energiavirasto toimii myös asetuksen tarkoittamana kansallisena kriisikoordinaattorina, jonka tehtävänä on toimia yhteyspisteenä ja koordinoida tiedonkulkua sähkökriisin aikana.

Energiavirasto toimii myös rajat ylittävien sähkönsiirtojen kyberturvanäkökohtia koskevan komission asetuksen (EU) 2024/1366 (NCCS, kyberturvallisuusverkkosääntö) toimivaltaisena viranomaisena (ainakin toistaiseksi, kunnes verkkosäännön edellyttämä nimeäminen on tehty). Verkkosäännössä säädetään mm. kyberhyökkäysten aiheuttamien kriisien hallinnasta ja siihen liittyvästä viestinnästä.

Turvallisuus- ja kemikaalivirasto

Turvallisuus- ja kemikaalivirasto (Tukes) on lupa- ja valvontaviranomainen, jonka tehtäviin kuuluu

- laitosten ja laitteistojen turvallisuuden, urakointi- ja asennustoiminnan sekä tarkastuspalveluiden valvonta,
- valvoa ja edistää kemikaaliturvallisuutta sekä kasvinsuojeluaineiden turvallisuutta ja laatua
- jalometallituotteiden vaatimustenmukaisuuden valvonta.
- valvoo myynnissä olevien tuotteiden turvallisuutta ja teknistä luotettavuutta.
- kuluttajapalveluiden turvallisuusvalvonta

Liikenne- ja viestintävirasto Traficom

Traficom on liikenteen ja viestinnän lupa-, rekisteri- ja valvontaviranomainen. Traficom valvoo ja ohjaa viestintäverkkojen- ja palvelujen toimivuutta, varmistamista, varautumista ja häiriöiden hallintaa.

Liikennejärjestelmän osalta virasto valvoo lakisääteisesti liikennetoimijoiden kyberturvallisuutta, käsittelee NIS-tietoturvapoikkeamailmoituksia ja seuraa tilannekuvaa yli liikennemuotojen rajojen. Liikenteen turvallisuus- ja palvelut toimialla on nimetty liikennemuotokohtaiset (ilmailu, merenkulku, raideliikenne ja tieliikenne) kyberturvallisuudesta ja varautumisesta vastaavat henkilöt sekä heille varahenkilöt.

NIS2-valvonta kattaa ilmailun (kaupallisen lentoliikenteen harjoittajat, lentoaseman pitäjät ja lennonjohtopalvelun tarjoajat), raideliikenteen (rataverkon haltijat ja liikenteenohjauspalvelua tarjoavat yhtiöt, rautatieyritykset ja palvelupaikan ylläpitäjät), vesiliikenteen (sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, satamanpitäjät ja toimijat jotka huolehtivat rakenteista ja varusteista satamien alueella, ja VTS-palveluntarjoajat) sekä tieliikenteen (liikenteenhallinta ja älykkäiden liikennejärjestelmien ylläpitäjät). Lisäksi NIS2-valvontaa voidaan kohdentaa erityisestä syystä eräisiin liikennesektorin valmistusorganisaatioihin.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen Viestintäverkkojen tietoturvallisuus -yksikössä valvotaan pääosaa digitaalisen infrastruktuurin toimijoista, digitaalisen palvelun tarjoajia, hallintapalveluiden ja tietoturvapalveluiden tarjoajia sekä tutkimusorganisaatioita ja julkishallinnon toimijoita. Kyberturvallisuuskeskuksen Viestintäverkkojen tietoturvallisuus -yksikön valvomia digitaalisen infrastruktuurin toimijoita ovat internetin yhdysliikennepisteiden ylläpitäjät, aluetunnusrekisterit, pilvipalvelujen tarjoajat, datakeskuspalvelujen tarjoajat, sisällönjakeluverkkojen tarjoajat, luottamuspalvelun tarjoajat, yleisten sähköisten viestintäverkkojen tarjoajat ja yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajat.

Finanssivalvonta

Finanssivalvonta on rahoitus- ja vakuutusvalvontaviranomainen, jonka valvottavia ovat muun muassa pankit, vakuutus- ja eläkeyhtiöt sekä muut vakuutusalalla toimivat, sijoituspalveluyritykset, rahastoyhtiöt ja pörssi.

Valvira

Valvira on sosiaali- ja terveysministeriön hallinnonalan keskusvirasto. Tehtäviin kuuluu valvoa sosiaali- ja terveydenhuollon, varhaiskasvatuksen, alkoholielinkeinon sekä ympäristöterveydenhuollon asianmukaisuutta. Valvira myöntää sosiaali- ja terveydenhuollon hallinnonalan lupia ja ohjaa aluehallintovirastoja.

Lääkealan turvallisuus- ja kehittämiskeskus Fimea

Fimea on Suomen sosiaali- ja terveysministeriön alainen keskusvirasto, joka valvoo lääkkeitä, lääkinnällisiä laitteita, veri- ja kudostuotteita, biopankkeja sekä kehittää lääkealaa.

Viraston tehtäväkokonaisuuksiin kuuluvat lääkealan lupa- ja valvontatehtävät, tutkimus- ja kehittämistehtävät sekä lääketiedon tuottaminen ja välittäminen lääkehuollon ja lääkehoitojen vaikuttavuuden parantamiseksi. Fimea on osa eurooppalaista lääkevalvonnan viranomaisverkostoa ja suuntautuu aktiiviseen kansainväliseen yhteistyöhön.

Etelä-Savon ELY-keskus

Etelä-Savon ELY-keskus vastaa vesihuoltolain mukaisista valvontatehtävistä val takunnallisesti. Etelä-Savon ELY-keskus valvoo ja edistää vesihuollon (vedenjakelun ja jätevesihuollon) toimintavarmuutta ja varautumista.

Etelä-Savon ELY-keskus vastaa myös jätehuollon kyberturvallisuuden valvontatehtävistä valtakunnallisesti. ELY-keskukset valvovat aluehallintoviraston myöntämiä ympäristö- ja vesilupapäätöksiä, sekä vastaavat toimivaltaansa kuuluvista jätelain valvontatehtävistä kuten jätekuljetusten

valvonnasta Suomen rajojen sisällä.

Vuoden 2026 alusta jätehuollon osalta tehtävät siirtyvät valtion lupa- ja valvontaviranomaiselle, vesihuollon osalta elinvoimakeskukselle.

Ruokavirasto

Edistää, valvoo ja tutkii elintarvikkeiden turvallisuutta ja laatua, eläinten terveyttä ja hyvinvointia, kasvinterveyttä sekä maa- ja metsätalouden tuotantoon käytettäviä lannoitevalmisteita, rehuja ja kasvinsuojeluaineita ja lisäysaineistoja eli siemeniä ja taimiaineistoa.

Ruokaviraston valmiudesta ja varautumisesta vastaa pääjohtaja ja sen koordinaatiosta vastaa hallintojohtaja yhdessä muun johdon kanssa työjärjestyksen mukaisesti. Ruokavirastoon on asetettu valmiustoimikunta, jonka tavoitteena normaalioloissa on Ruokaviraston varautumis- ja valmiustoiminnan järjestäminen valmistelussa siten, että toimintaa kyetään johtamaan ja hallitsemaan myös häiriötilanteissa ja poikkeusoloissa.

Ruokavirasto toimii myös toimivaltaisena valvontaviranomaisena koskien NIS2-direktiivin soveltamisalaan kuuluvia elintarvikealan toimijoita, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta. NIS2-direktiivin ja sen täytäntöönpanoa koskevan kansallisen lainsäädännön mukainen valvonta on Ruokaviraston vastuulla.

Liikenne- ja viestintävirasto Traficom
PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

ISBN 978-952-311-979-6
ISSN 2669-8757 (verkkojulkaisu)

TRAFICOM
Liikenne- ja viestintävirasto