TLP:CLEAR

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuuskeskuksen rooli Suomen kriittisen infrastruktuurin ja digitaalisen yhteiskunnan tukena

Jere Finne
Erityisasiantuntija
Kyberturvallisuuskeskus

TLP:CLEAR

Mikä ihmeen Kyberturvallisuuskeskus?

Mitä Kyberturvallisuuskeskus tekee?

Miksi meille kannattaa ilmoittaa tietoturvaloukkauksista ja -poikkeamista ja mitä apua tarjoamme organisaatioille?

Miten ilmoitusten avulla muodostettava tilannekuva auttaa Kyberturvallisuuskeskusta viestimään asioista ja palvelee koko yhteiskunnan kyberturvallisuutta?

TLP:CLEAR

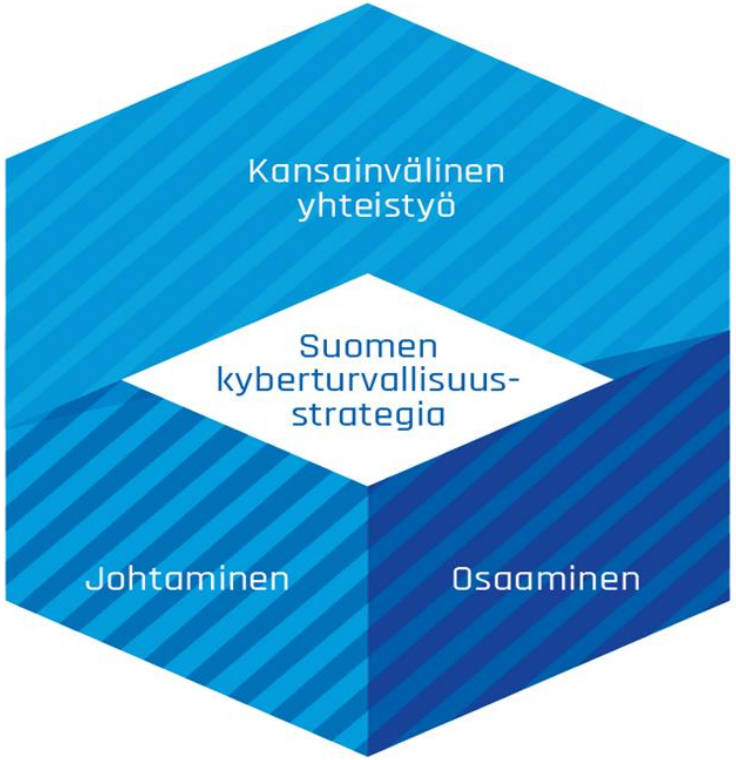
Kyberturvallisuuskeskus tukee Suomen kriittistä infrastruktuuria havainnoimalla uhkia sekä ylläpitämällä luottamuksellisia tiedonjakoryhmiä ja kansallista kyberturvallisuuden tilannekuvaa.

TRAFICOM

TLP:CLEAR

Kyberturvallisuusstrategia 2019

Kyberturvallisuuden **johtamisen**, **suunnittelun** ja **varautumisen** parempi koordinaatio



Kansainvälisen yhteistyön kehittäminen – kybertoimintaympäristön rajatonta turvaamista

Kyberturvallisuuden osaamisen kehittäminen – arkiosaaminen ja huipputaitajat kyberturvallisuuden varmistajina

Laki Liikenne- ja viestintävirastosta (935/2018)

”Liikenne- ja viestintäviraston kyberturvallisuuskeskus, jäljempänä Kyberturvallisuuskeskus, ***tukee****,* ***ohjaa*** *ja* ***valvoo tietoturvallisuutta*** *ja* ***yksityisyyden suojan toteutumista sähköisessä viestinnässä****. Se* ***ylläpitää kansallisen kyberturvallisuuden tilannekuvaa****. Kyberturvallisuuskeskuksen toiminta* ***edistää*** *ja* ***varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta****. Kyberturvallisuuskeskus toimii julkisesti säännellyn* ***satelliittipalvelun vastuuviranomaisena*** *ja* ***Euroopan kyberturvallisuuden*** *teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2021/887 6 artiklan mukaisena* ***kansallisena koordinointikeskuksena****. Lisäksi Kyberturvallisuuskeskus* ***huolehtii viestintätoimialan varautumisesta normaaliolojen häiriötilanteisiin ja poikkeusoloihin****,* ***edistää*** *ja* ***valvoo sähköisen viestinnän toimintavarmuutta*** *sekä* ***tukee toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin****.” (3§)*

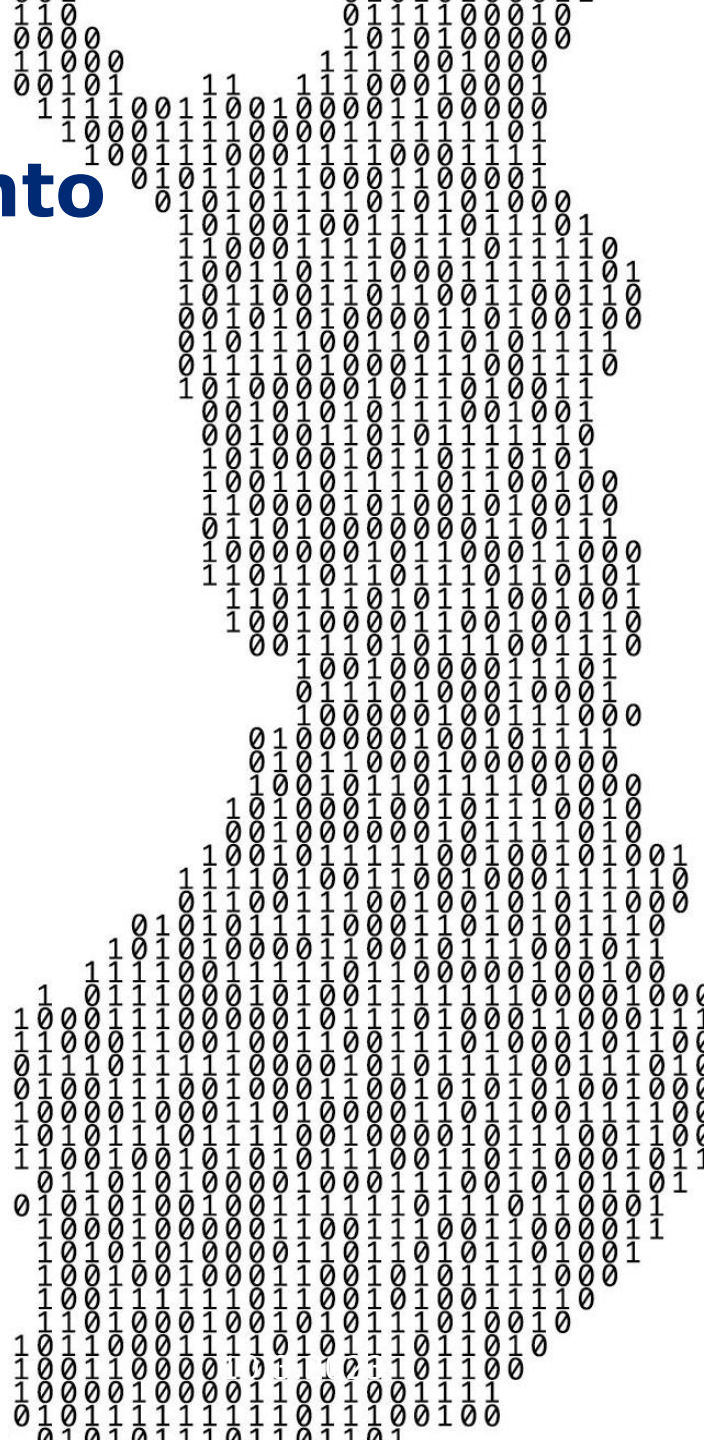
Kyberturvallisuuskeskus

- Tukee, ohjaa ja valvoo tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä
- Ylläpitää kansallisen kyberturvallisuuden tilannekuvaa ja tukee organisaatioiden päätöksentekoa ja tiedolla johtamisen tarpeita
- Edistää ja valvoo sähköisen viestinnän toimintavarmuutta
- Tukee yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin
- Tarkastaa, sertifioi ja arvioi tietojärjestelmiä ja tuotteita sekä akkreditoi näitä arvioivia toimijoita
- Tarjoaa kansalaisille ajankohtaista ja luotettavaa tietoa kyberturvallisuudesta
- Toimii Suomen kansallisena kyberturvallisuuden koordinointikeskuksena osana EU:n koordinointikeskusten verkostoa
- Toimii eurooppalaiseen Galileo-paikannusjärjestelmään liittyvän julkisesti säännellyn satelliittipalvelun (PRS) vastuuviranomaisena
- Toimii yhteistyössä eri viranomaisten, yritysten, järjestöjen ja kansainvälisten kumppanien ja oppilaitosten kanssa

TLP:CLEAR

Kyberturvallisuuskeskuksen CERT-toiminto

- Computer Emergency Response Team
- CERT-toiminnon tehtävänä on
  - ennaltaehkäistä tietoturvaloukkauksia ja niiden uhkia
  - ylläpitää tilannekuvaa
  - tiedottaa tietoturva-asioista.
- CERT-toiminnan tavoitteena on
  - yleisten viestintäverkkojen ja viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistaminen
  - yhteiskunnan elintärkeiden toimintojen turvaaminen.
- CERT-palvelustamme saat apua tietoturva-asioissa. Yleisen tietoturvatietouden lisäksi voimme auttaa vakavien tietoturvaloukkausten teknisessä selvityksessä.
- Yhteydenotot kerryttävät tilannekuvaa, jonka perusteella voidaan tehdä viestintää ja pyrkiä estämään vastaavat vahingot muualla



TLP:CLEAR

Koordinointi ja avunanto tietoturvaloukkauksissa

- Tarjoamme apua tietoturvaloukkauksen selvittämiseksi ja tutkimiseksi sekä koordinoimme tarvittavia toimenpiteitä
- Käsittelemme kaikki tapaukset luottamuksellisesti
- Toimenpiteet voivat pitää sisällään
  - tiedon jakamista
  - yhteistyökumppanien ja -verkostojen kontaktointia
  - teknistä analyysiä
  - lainopillista neuvontaa.
- Jokainen ilmoitus parantaa mahdollisuuksiamme auttaa koko yhteiskuntaa
- Ilmoita meille tietoturvaloukkauksesta:
  - www.kyberturvallisuuskeskus.fi/fi/ilmoita
  - cert@traficom.fi

Kyberturvallisuuskeskuksen palvelut poikkeaman ilmoittajalle

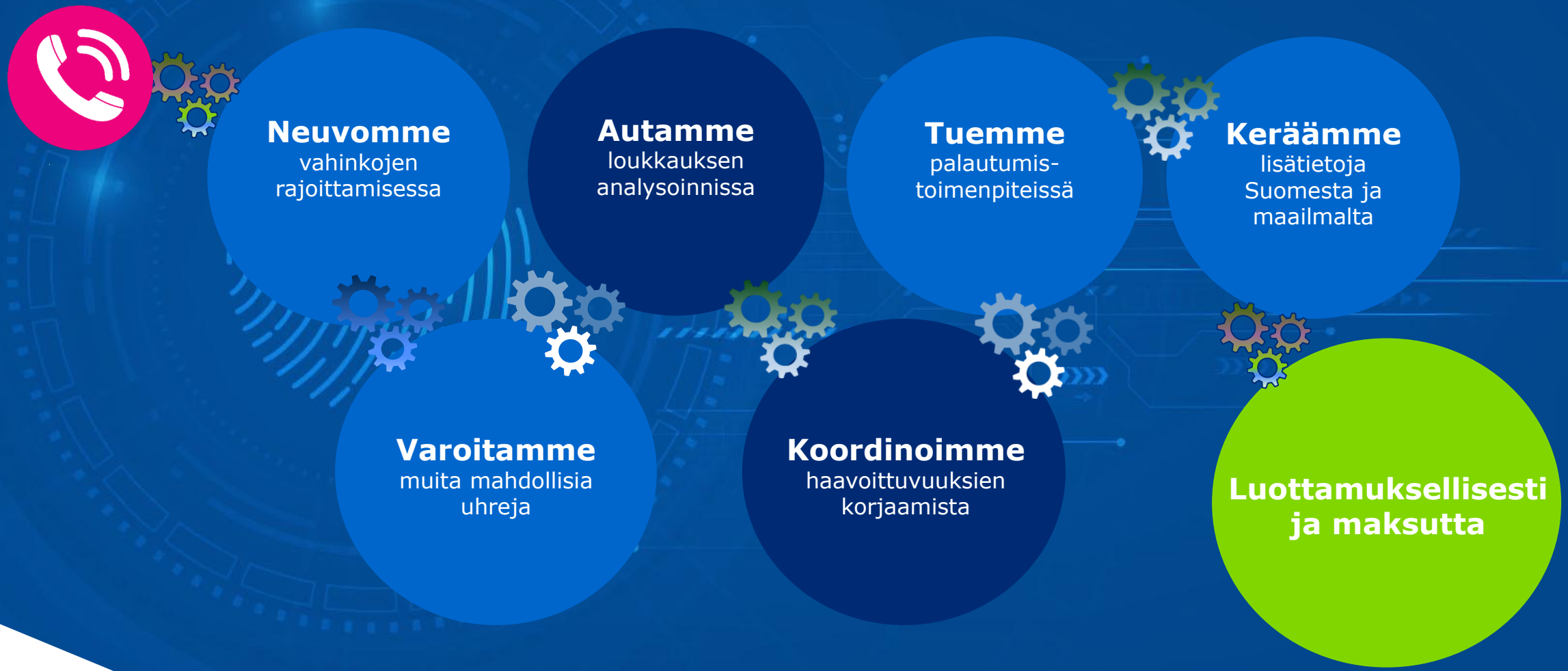
Kyberturvallisuuskeskus tekee:

- Neuvonta tilanteen ja tarvittavien toimenpiteiden hahmottamiseksi
- Koordinointi poikkeaman hallintaan osallistuvien tahojen kesken
- Tuki ja neuvonta tilanteen palauttamiseksi normaaliksi
- Niiden tahojen varoittaminen, joita tilanne uhkaa
- Tilanteen tekninen analysointi
- Haavoittuvuuskoordinaatio
- Haitallisen internet-sisällön poistopyynnöt

Kyberturvallisuuskeskus ei tee:

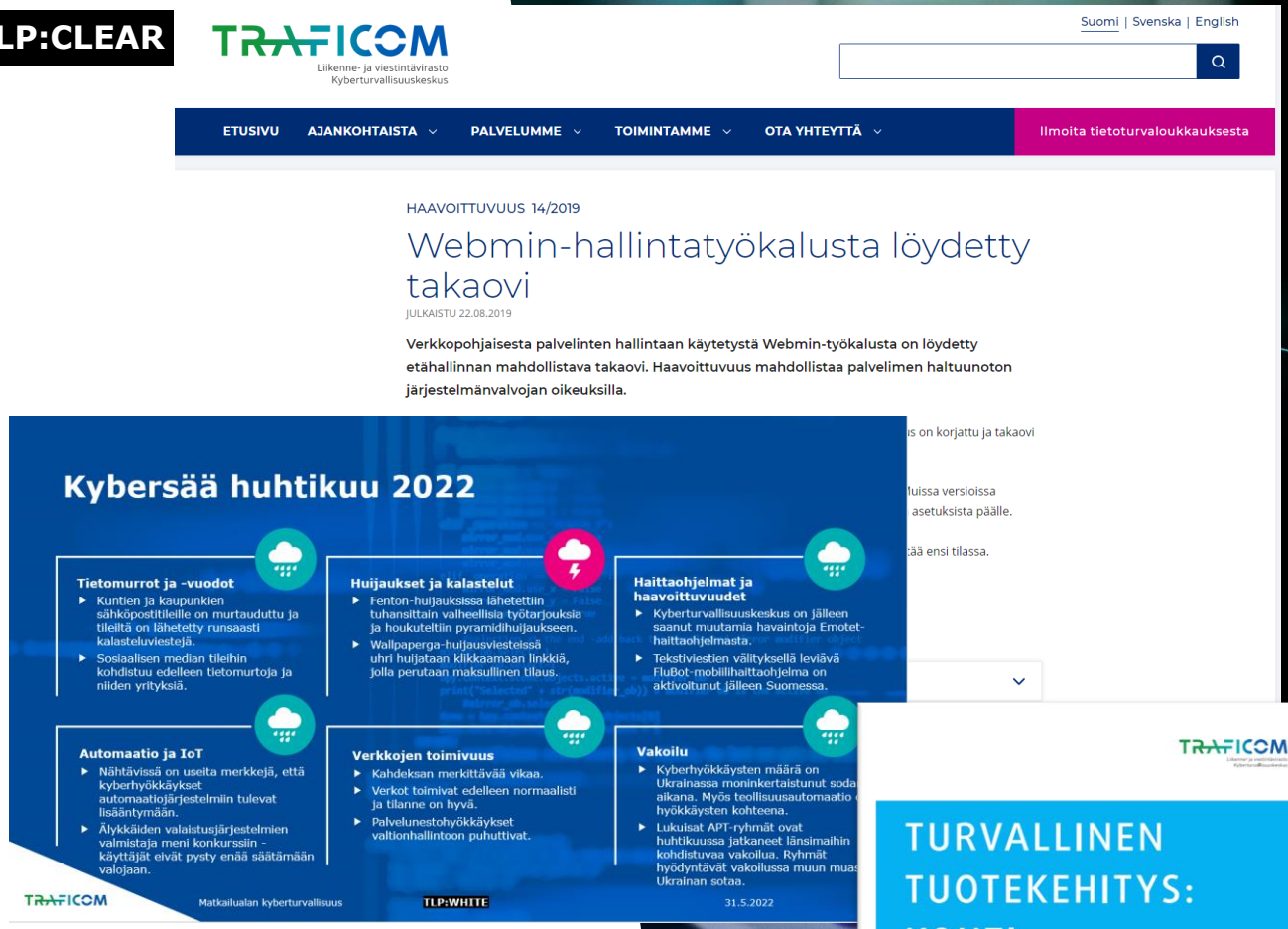
- Ilmoittajan paljastaminen muille tahoille ilman ilmoittajan lupaa
  - Paitsi tietyissä lain sallimissa tilanteissa tietyille viranomaisille
- Tietojärjestelmien korjaaminen
- Syyllisen selvittäminen

Palvelulupaus tietoturvaloukkauksissa



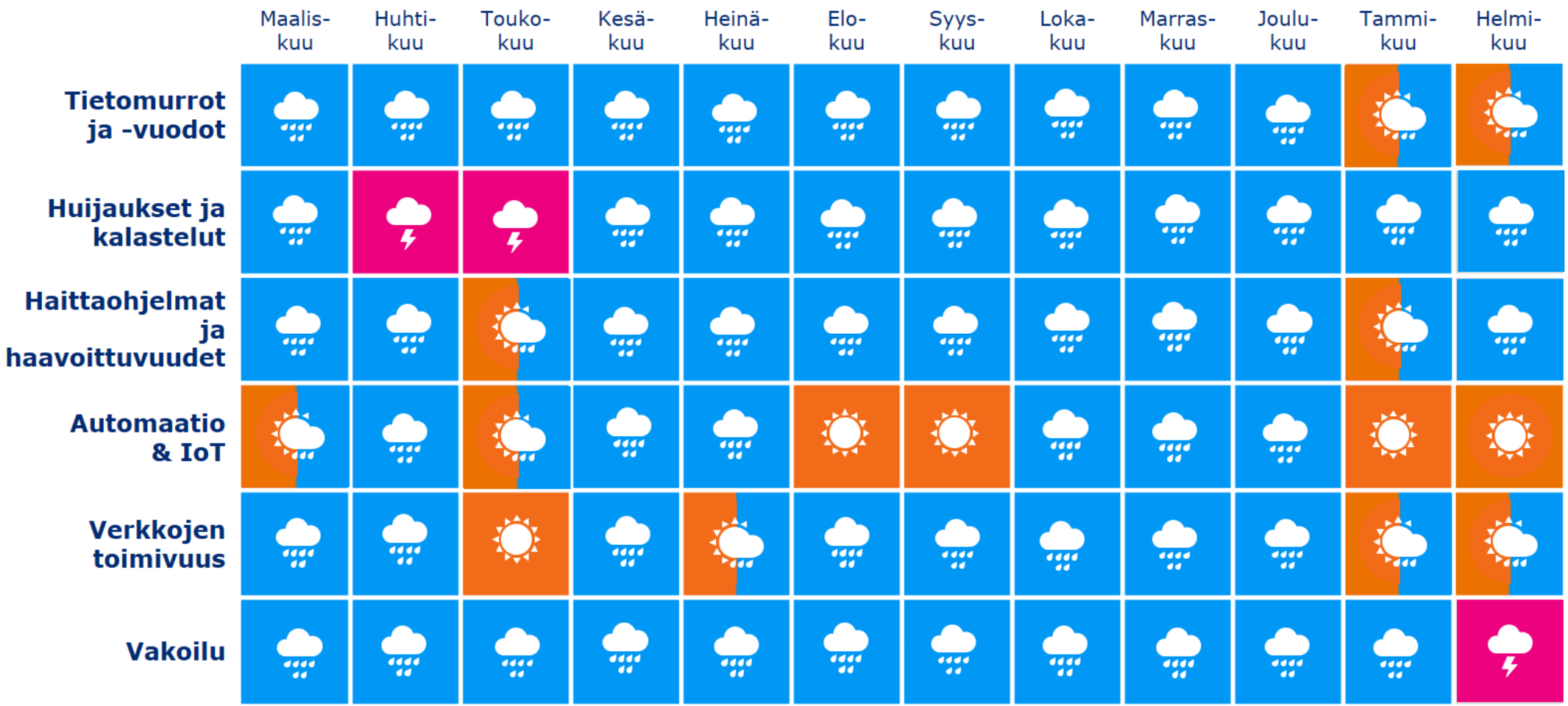
Tilannekuvatuotteita

- Haavoittuvuustiedotteet
- Haavoittuvuuskooste
- Kybersää
- News-uutiskirje
- Tietoturva Nyt! –julkaisut
- Toimialakohtainen tilannekuva ja tiedotteet
- Varoitukset
- Viikkoraportti
- Tietoturvan vuosi
- Osa ei-julkisia



- Saat tuotteet käyttöösi liittymällä toimialakohtaisille sähköpostilistoille.
  - Laita viestiä osoitteeseen kyberturvallisuuskeskus@traficom.fi
- Uutiskirjeen ja haavoittuvuuskoosteen voit tilata internet-sivuiltamme osoitteesta
  - www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

Kyberturvallisuuden trendit
kulunut 12 kk



Ohjeet ja suositukset

- Julkaisemme tietoturva-aiheisia ohjeita, oppaita ja vinkkejä niin organisaatioille, yksityishenkilöille kuin palveluiden ylläpitäjille.
  - Kyberturvallisuus ja yrityksen hallituksen vastuu
  - Toiminta kiristyshaittaohjelmatapauksissa – johdon ohje
  - Suojautuminen Microsoft Office 365 –tunnusten kalastelulta ja tietomurroilta
  - Toimintaohjeita kyberhyökkäystilanteista toipumiseen
  - Kyberharjoitusohje ja kyberharjoitusskenaariot
  - ... ja monia muita!
- Tutustu ohjeisiin ja oppaisiin osoitteessa
  - www.kyberturvallisuuskeskus.fi/fi/ohjeet

Kyberturvallisuuden uhkakuvia

Kyberrikollisuutta eivät hidasta maantieteelliset rajat

Kyberrikollisuus on nopeaa ja opportunistista toimintaa

Mistä kyberuhka rakentuu?

Kyberrikollisuus...

- on kansainvälistä ja tilaisuuteen tarttuvaa toimintaa, joka **uhkaa jokaista organisaatiota sen toimialasta tai koosta riippumatta**.

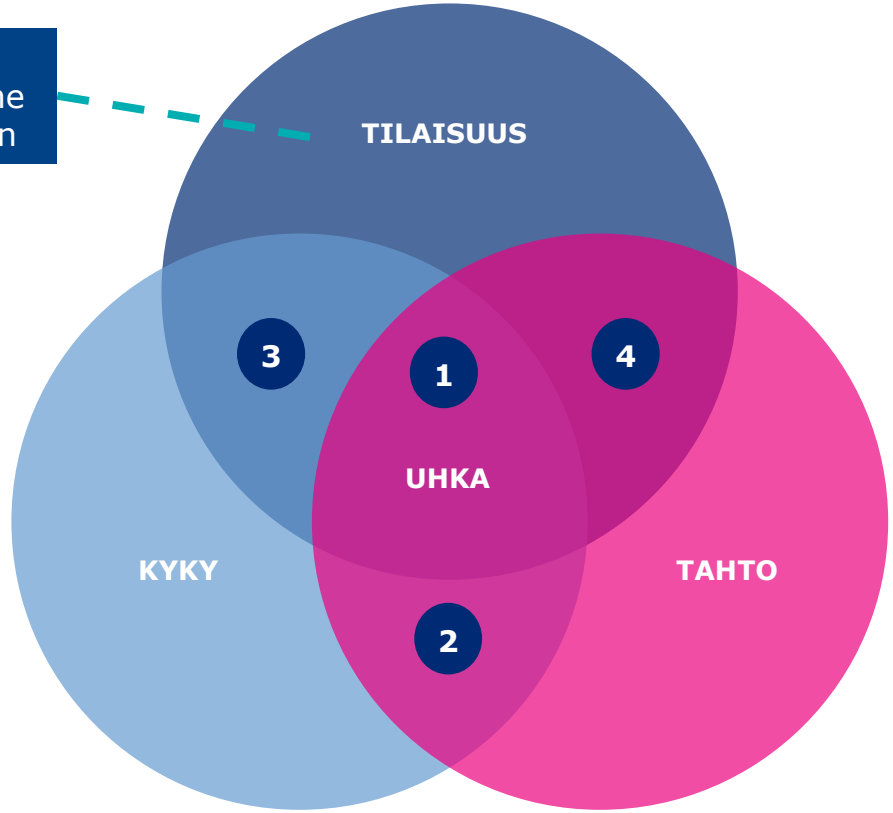
- muodostaa organisaatioille **merkittävän liiketoimintariskin**.

Murtovaras tulee kauimmillaan Suomen lähialueelta pakettiautollaan. Organisaation tiedot varastava ja salakirjoittava kyberrikollinen voi toimia toiselta mantereeltakin.

Kyberuhkan rakennuselementit

Organisaation kyberturvallisuuden kivijalka rakennetaan arkisilla kyberturvallisuuden toiminnoilla, kuten ohjelmistopäivityksillä, hyvillä salasanakäytänteillä ja tietoturvakulttuurilla. Näillä toimilla voidaan pienentää uhkatoimijoiden tilaisuuksia toteuttaa onnistuneita kyberhyökkäyksiä.

Ulkoisen uhkan tapauksessa voimme vaikuttaa vain tähän

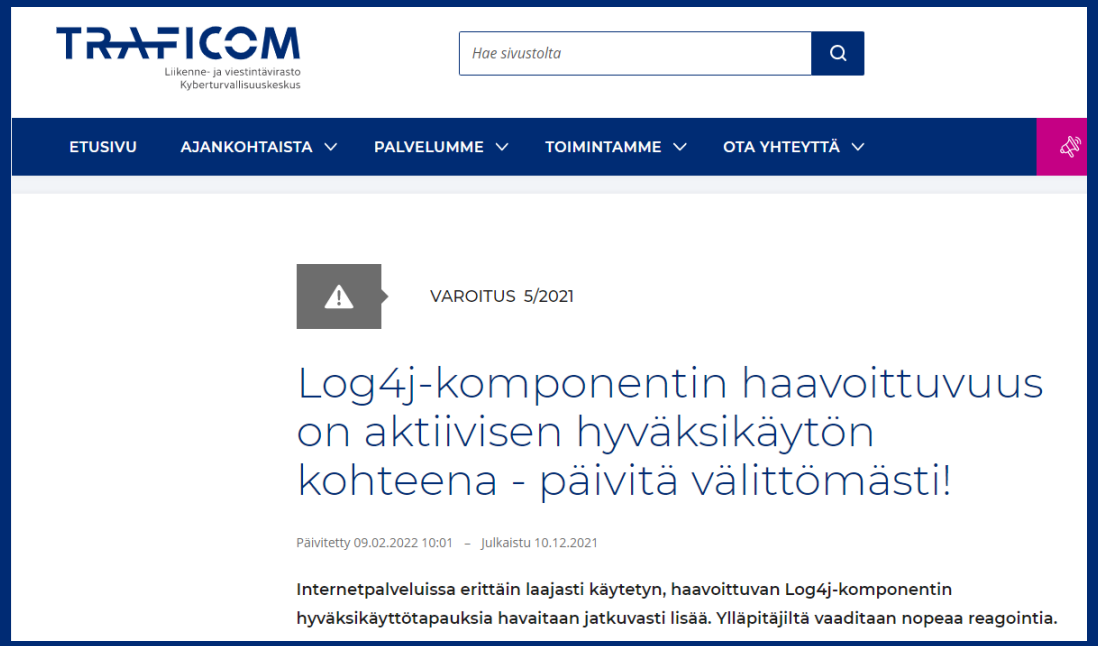


Uhkan vakavuus

1. **Aktiivinen uhka**
   Kyberriski voi todella realisoitua
2. **Tilaisuuttaan vaaniva uhka**
3. **Tarvittaessa aktivoitavissa oleva uhka**
4. **Tällä hetkellä vaaraton uhka**

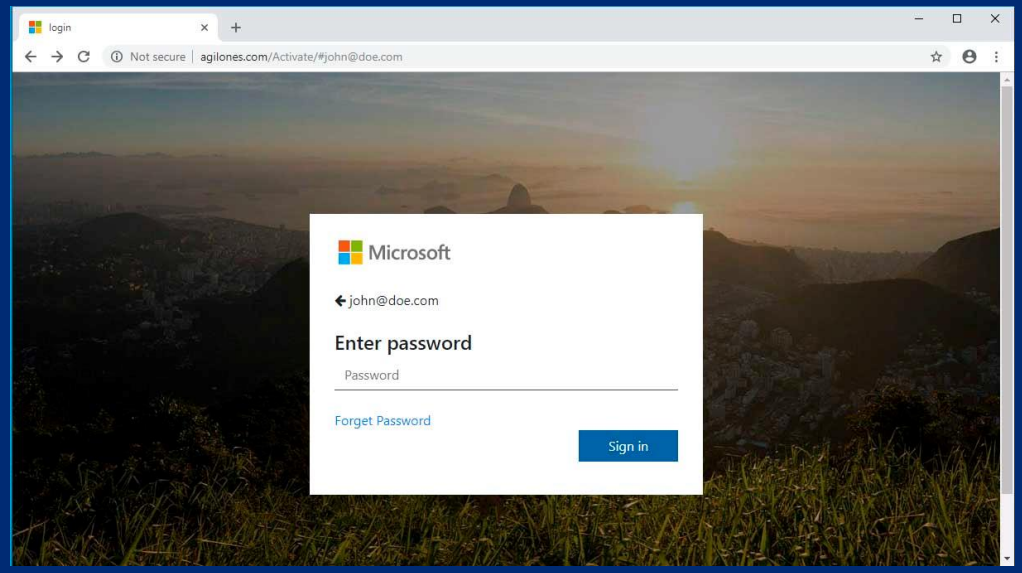
Ohjelmistohaavoittuvuudet

- Päivittämättömät ohjelmistohaavoittuvuudet avaavat rikollisille reitin organisaatioon
- Aikajänne ohjelmistohaavoittuvuuden julkisuuteen tulosta aktiiviseen hyväksikäyttöön lyhimmillään alle kaksi tuntia
- Globaalia, automatisoitua ja sattumanvarausta
- Säännöllinen ja nopea päivitysten asentaminen auttaa torjumaan kyberhyökkäyksiä



Käyttäjätunnusten ”kalastelu”

- Moni kyberonnettomuus käynnistyy tietojen kalastelulla.
- Tunnuskalastelua tehdään monella eri tavalla ja eri laitteiden kautta. Sitä kohdistetaan organisaatioihin kuin yksityishenkilöihin. Se on helppoa ja yksinkertaista, ja sillä voidaan saada merkittävää hyötyä.
- Tunnuksia pyritään myös arvaamaan koneellisesti tai hyödyntämään erilaisia salasanatietovuotoja.
- Kalastelun lopputuloksena voi myös olla kiristyshaittaohjelma eli lunnastroijalainen.
- Kaksi- tai monivaiheinen tunnistautuminen on tehokas keino torjua tilimurtoja ja estää kalastelujen onnistuminen.



Kiristyshaittaohjelmat

- Erityisen merkittävä uhka organisaatioille on kiristyshaittaohjelmahyökkäykset, joiden kohteeksi voi joutua kuka tahansa pienestä konepajasta kansainväliseen teknologiajättiin.
- Hyökkäyksessä kohdetta kiristetään tietojen salaamisella ja salauksen purkamisesta vaaditaan lunnasmaksu.
- Lisäksi voidaan kiristää hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.
- Lunnaiden maksu ei kuitenkaan ole suositeltavaa, koska hyökkäys ja sitä kautta kiristäminen voi jatkua siitä huolimatta.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse.
- Varmuuskopiot ja päivitykset ovat tehokas keino estää ja rajata hyökkäyksen vaikutuksia.

Hyökkääjän toiminta kiristyshaittaohjelmatapauksissa

Kiristyshaittaohjelma eli lunnastroijalainen

- **Rikolliset** pyrkivät salaamaan organisaation datan salausalgoritmilla ja **vaativat lunnaita** tietojen palauttamista vastaan.
- Rikolliset saattavat myös varastaa salaamansa tiedot ja **kiristää organisaatiota tietovuodolla**.

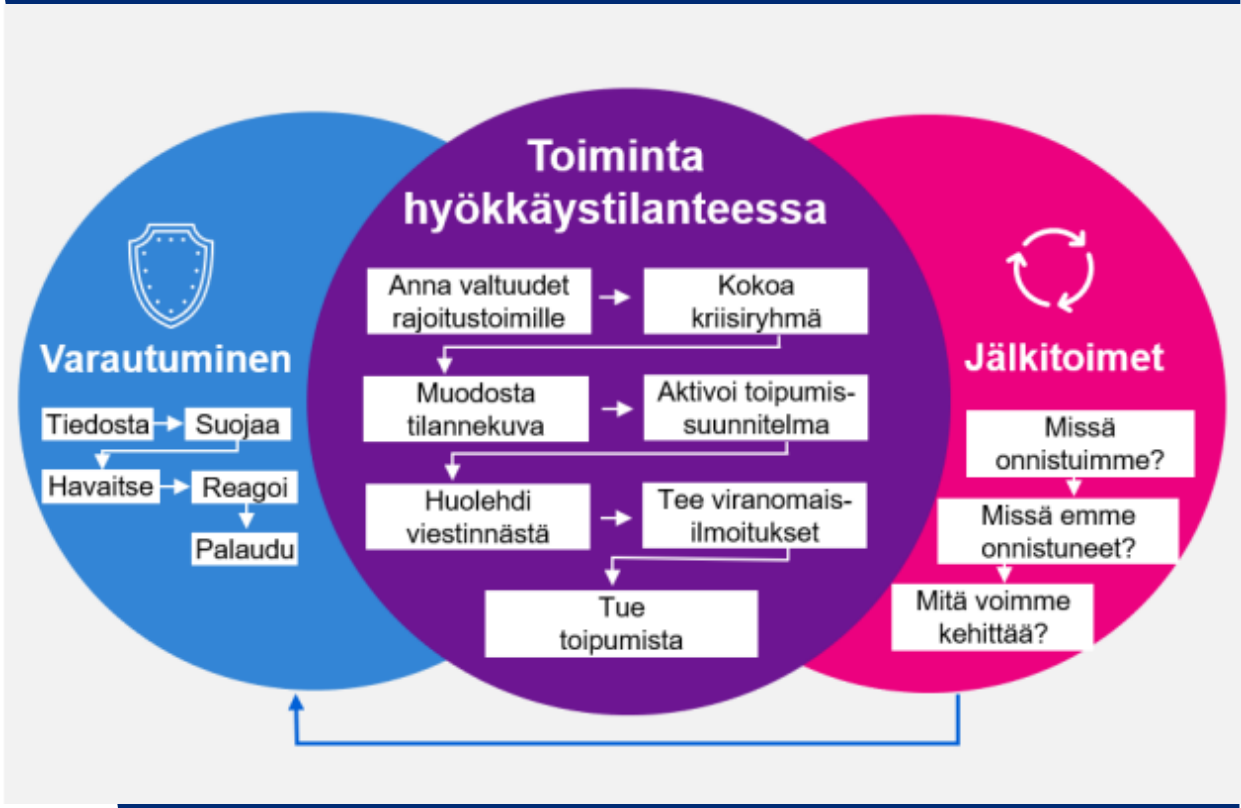
  ”Te saatatte vuottaa asiakkaidenne luottamuksellisia tietoja.”

  ”Teidän liikesalaisuuksianne vuotaa.”
- Hyökkäysten **motiivi on yleensä taloudellinen** - kiristyshaittaohjelmat ovat osoittautuneet rikollisille tehokkaaksi tavaksi yrittää ansaita taloudellista hyötyä.

10 https://attack.mitre.org/

Kiristyshaittaohjelma-hyökkäykseen varautuminen ja hallinta

- Hyökkäyksiin on syytä varautua etukäteen. Ennalta tehdyt kyberturvallisuutta parantavat toimet ovat kustannustehokkain ja vaikuttavin keino varautua hyökkäyksiin.
- Sataprosenttista kyberturvallisuutta on kuitenkin mahdoton saavuttaa, joten toimintaan mahdollisessa hyökkäystilanteessa on syytä varautua ja harjoitella.
- Hyökkäystilanteen jälkeen on tärkeää käydä läpi hyökkäyksen kulku ja analysoida:
  - Missä onnistuimme?
  - Missä emme onnistuneet?
  - Mitä voimme kehittää?



Toiminta tietoturvaloukkauksissa

Toimivaltaiset viranomaiset ja tietoturvaloukkauksista ilmoittaminen

Ensitoimenpiteet kohdatessasi kyberturvallisuuden poikkeaman

1. Aloita sisäinen selvitys ja poikkeamanhallinta. Varmista henkilöresurssit.
2. Tee välittömät ilmoitukset, joista olet mahdollisesti sopinut yhteistyökumppaneidesi kanssa.
   - Esimerkiksi Puolustusvoimien kanssa tehdyn turvallisuussopimuksen velvoitteet
3. Apua, emme hallitse tilannetta yksin! Tai uhka koskee muitakin organisaatioita eikä tietoa uhkasta ole julkisesti saatavilla.
   ➔ Tee vapaaehtoinen ilmoitus Kyberturvallisuuskeskukselle.
4. Epäiletkö poikkeaman johtuvan rikoksesta?
   ➔ Tee rikosilmoitus poliisille. Suojaa todistusaineisto.
5. Tee muut ilmoitukset, joihin laki tai sopimukset sinua mahdollisesti velvoittavat.
   - Onko sinulla lain mukaan velvollisuus ilmoittaa toimivaltaiselle viranomaiselle? Esim. NIS-direktiivi?
   - Koskeeko poikkeama henkilötietoja? ➔ Tee ilmoitus tietosuojavaltuutetulle.
6. Jos poikkeama edellyttää teknistä tutkintaa, hanki osaava kyberturvallisuuden palveluntarjoaja tekemään sitä

- Päivitä tekemiäsi ilmoituksia sitä mukaa, kun saat uutta tietoa tapahtumasta ja tilanteesta.
- Pidä aloite tiedottamisessa. Muista aina myös sisäinen tiedottaminen.

TLP:CLEAR

Toimivaltaiset viranomaiset

Palveluntarjoajat
Hyödyntäkää palveluntarjoajien erityisosaamista heti alusta alkaen

Verkostot
Älkää jääkö asian kanssa yksin, vaan ottakaa verkostot avuksi ja jakakaa tietoa

Muistakaa lisäksi

Poliisi

Toimivaltainen viranomainen rikosten selvittämisessä, esitutkinnan toteuttamisessa, syyteharkintaan saattamisessa, rikosten ennaltaehkäisemisessä ja paljastamisessa.

Kyberturvallisuuskeskus

Kansallinen tietoturvaviranomainen, joka kerää tietoa tietoturvaloukkauksista ja niiden uhkista, käsittelee tapaukset luottamuksella, auttaa tarvittaessa selvittämisessä, tutkinnassa ja koordinoinnissa.

Tietosuojavaltuutetun toimisto

Tietosuojalainsäädännön toimeenpanosta vastaava kansallinen valvontaviranomainen, joka käsittelee henkilötietojen tietoturvaloukkaukset.

Huoltovarmuuskeskus ja poolit

Toimivat työ- ja elinkeinoministeriön alaisuudessa ja tehtävänä on huolehtia maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvästä suunnittelusta ja operatiivisesta toiminnasta.

Suojelupoliisi

Sisäministeriön alaisuudessa toimiva siviilitiedusteluorganisaatio, joka tiedustelee ja estää ennalta kansalliseen turvallisuuteen kohdistuvia uhkia, myös kybertoimintaympäristössä.

Puolustusvoimat

Vastaa maan sotilaallisesta puolustamisesta, valvoo maa- ja vesialuetta sekä ilmatilaa. Tehtävänä turvata maan sotilaallinen koskemattomuus ja itsenäisyyden säilyminen.

TRAFICOM

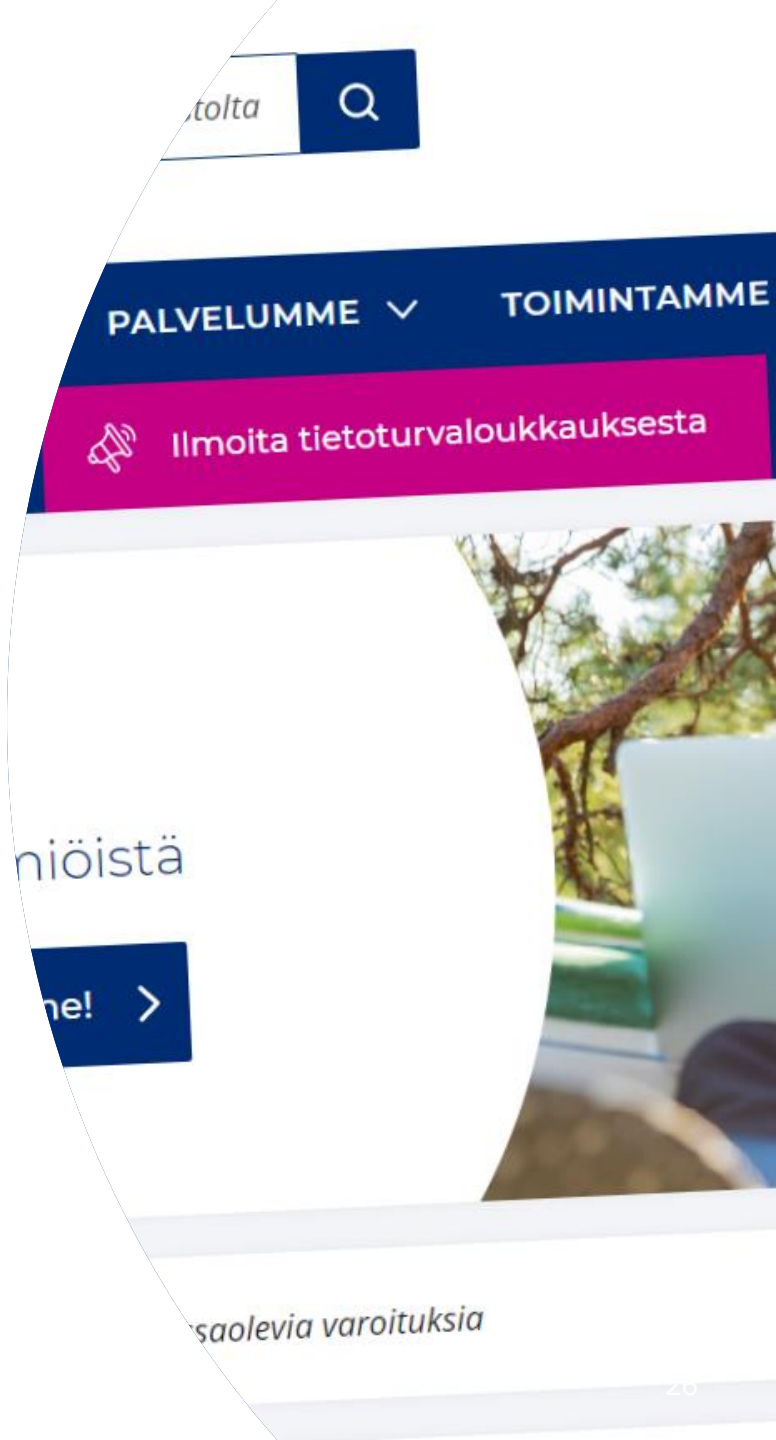
TLP:CLEAR

Viranomaisille ilmoittaminen

Poliisi	Ilmoita rikosepäilyistä poliisille matalalla kynnyksellä. https://poliisi.fi/tee-rikosilmoitus
Kyberturvallisuuskeskus	Ilmoita tietoturvaloukkauksista Kyberturvallisuuskeskukselle. Yhteydenotot käsitellään luottamuksellisesti. https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
Tietosuojavaltuutetun toimisto	Henkilötietojen tietoturvaloukkaukset tulee dokumentoida ja niistä ilmoittaa Tietosuojavaltuutetun toimistolle 72 tunnin kuluessa tapauksen huomaamisesta ilman aiheetonta viivytystä. https://tietosuoja.fi/tietoturvaloukkaukset
NIS-valvontaviranomainen	NIS-direktiivin mukaisilla yhteiskunnan kriittisen infrastruktuurin tarjoajien ja toimijoiden tulee lisäksi ilmoittaa havaitsemistaan tietoturvauhkista ja -loukkauksista toimialan valvontaviranomaiselle. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/nis-koordinointi-ja-viranomaisyhteistyo

Kyberturvallisuuskeskukselle ilmoittajan tarkastuslista

- ❑ Tilanteen kuvaus ja tapahtumien aikajana
- ❑ Vaikutukset oman organisaation toimintaan
- ❑ Tehdyt toimenpiteet ja tiedossa olevat ratkaisumenetelmät
- ❑ Tiedossa olevat uhkan tunnistetiedot
- ❑ Tiedon hyödynnettävyys
  - ▶ Saako Kyberturvallisuuskeskus keskustella tapauksesta suoraan ilmoittajan ICT-palveluntarjoajan tai asiakkaiden kanssa?
  - ▶ Onko rikosilmoitus tehty? Saako Kyberturvallisuuskeskus keskustella tapauksesta suoraan Poliisin kanssa?



Epäiletkö tietoturvaloukkausta?

Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä meihin.

- Sähköinen lomake: https://www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi
- Puhelin: 0295 345 630 (arkisin klo 9-15)

Muissa asioissa voitte olla meihin yhteydessä osoitteessa kyberturvallisuuskeskus@traficom.fi

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallinen yhteiskunta rakennetaan yhdessä – älkää jääkö yksin!

Ota yhteyttä:
kyberturvallisuuskeskus@traficom.fi