Kyber-turvallisuus Suomessa

Traficomin julkaisuja
8/2025

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuus Suomessa on Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen julkaisu, jossa pureudumme kyberturvallisuuden ajankohtaisiin ilmiöihin, haasteisiin ja ratkaisuihin, jotta voimme yhdessä rakentaa turvallisempaa digitaalista tulevaisuutta.

Esittelemme yhteistyökumppaneitamme ja myös sidosryhmämme saavat puheenvuoron.

Julkaisua ovat olleet tekemässä Liikenne- ja viestintäministeriö, Huoltovarmuuskeskus, Kyberala ry, Teknologiateollisuus sekä iso joukko Traficomin ja Kyberturvallisuuskeskuksen asiantuntijoita.

Tämä julkaisu on tiivis, kuvitettu käsikirja tämän päivän kyberturvallisuuteen. Visualisoinnit auttavat havainnollistamaan monimutkaisia ja teknisiä ilmiöitä sekä hahmottamaan asioiden mittakaavaa.

Tutustu julkaisun aiheisiin perusteellisemmin Kyberturvallisuuden vuosi 2024 -verkkojulkaisussa.

Kyberturvallisuus tehdään yhdessä.

Traficomin julkaisuja 8/2025

ISBN 978-952-311-969-7
ISSN 2669-8757 (verkkojulkaisu)
ISSN 2669-8749 (painettu)

Kyberturvallisuuden vuosi 2024 julkaisun löydät verkkosivuiltamme:
https://vuosiraportit.traficom.fi/fi/kyberturvallisuus/kyberturvallisuuden-vuosi-2024

Digitaalinen yhteiskuntamme perustuu toimiviin ja turvallisiin tietoverkkoihin sekä sähköisiin palveluihin

Vuosi 2024 muistetaan isoista kybertapauksista, kuten Helsingin kaupungin tietomurrosta, kaapelivaurioista, Nordeaan kohdistuneista palvelunesto-hyökkäyksistä sekä Valion kohdistuneesta kiristyshaittaohjelma-hyökkäyksestä. Rikolliset kohdistivat toimintansa myös kansalaisiin.

Kyberuhkien torjunta on joukkuepeliä. Autamme yrityksiä, viranomaisia ja kansalaisia varautumaan ja tunnistamaan tämän hetken ja tulevaisuuden kyberuhkia sekä vastaamaan uhkiin. Toiminnan ytimessä on yhteistoiminta elinkeinoelämän ja viranomaisten kanssa.

Kybertoimintaympäristön aktiviteettitaso pysyi myös vuonna 2024 edelleen korkeana ja turvallisuustilanteessa ei ole näköpiirissä paranemisen merkkejä.

Vuoden 2024 lopussa julkaistu kyberturvallisuusstrategia ja sen toimeenpanosuunnitelma antavat erinomaiset strategiset suuntaviivat kyberturvallisuuden kansalliseen kehittämiseen. Toimeenpano-ohjelmassa on osoitettu useita kehittämistehtäviä myös Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle.

Turvallisuusviranomaisena Kyberturvallisuuskeskus auttaa yrityksiä, viranomaisia ja kansalaisia varautumaan ja tunnistamaan tämän hetken ja tulevaisuuden kyberuhkia.

Ollaan valppaina ja jatketaan yhdessä digitaalisen yhteiskuntamme suojelemista.

Anssi Kärkkäinen
Ylijohtaja
Kyberturvallisuuskeskus

Lue Anssin kirjoitus kokonaisuudessaan Kyberturvallisuuden vuosi -raportista

Kybervuosi 2024

SUOMESSA

M365-tilimurrot uhkasivat jälleen lisääntyä organisaatioissa, mutta ne saatiin kuriin ennaltaehkäisevällä tiedonvaihdolla.

Kuntien sivustoja oli palvelunesto-hyökkäysten kohteina.

Kyberturvallisuuskeskus oli mukana varmistamassa, että presidentin- ja EU-parlamenttivaalit sujuivat rauhallisesti

Helsingin kaupunkiin kohdistui yksi Suomen suurimmista tietomurroista.

Liikkeellä oli paljon kalasteluviestejä eri organisaatioiden ja viranomaisten nimissä.

Pankkialan toimijoihin kohdistui pitkäkestoisia palvelunestohyökkäyksiä.

Itämeren pohjassa kulkevia kansainvälisiä tietoliikenne- ja sähkökaapeleita vaurioitui.

SUOMESSA

01 02 03 04 05 06 07 08 09 10 11 12

MAAILMALLA

Lähes jokaisessa Linux-käyttöjärjestelmässä käytössä olevaan XZ Utils-työkaluun oli pitkä-jänteisellä operaatiolla rakennettu vaarallinen takaportti. Se huomattiin sattumalta juuri ennen kuin haitallinen päivitys pääsi leviämään.

Hankalasti korjattava Palo Alton VPN-tuotteiden haavoittuvuus altisti organisaatiot tietomurroille useita viikkoja. Annoimme vakavan varoituksen 18.4.2025.

Ivanti-valmistajan VPN-tuotteista paljastui paljon haavoittuvuuksia. Organisaatiot kiirehtivät päivittämään vaarantuneita laitteitaan myös Suomessa.

Viallinen CrowdStrike-tietoturvaohjelmiston päivitys seisautti kokonaisia toimitusketjuja ja aiheutti globaaleja häiriöitä.

MAAILMALLA

Selitteet

- Tietojenkalastelu, tieto- ja tilimurrot sekä tietovuodot
- Palvelunesto-hyökkäykset
- Haavoittuvuudet
- Muut kybermaailman tapahtumat

Uudistettu kyberturvallisuus-strategia rakentuu yhteistyölle

Kyberturvallisuus on erottamaton osa Suomen kokonaisturvallisuutta. Kyberturvallisuus koskettaa kaikkia meitä.

Suomen kyberturvallisuusstrategia uudistettiin hallitusohjelman mukaisesti vastaamaan Suomen muuttunutta toimintaympäristöä lokakuussa 2024. Edellisen kyberturvallisuusstrategian julkaisemisen jälkeen esimerkiksi koronapandemia, Venäjän aloittama hyökkäyssota Ukrainassa ja Suomen Nato-jäsenyys ovat vaikuttaneet Suomen toimintaympäristöön.

Strategia on valmisteltu laajassa yhteistyössä. Mukana olivat kaikki keskeiset ministeriöt sekä noin sata organisaatiota julkiselta ja yksityiseltä sektorilta, tiedeyhteisöistä ja kansalaisjärjestöistä.

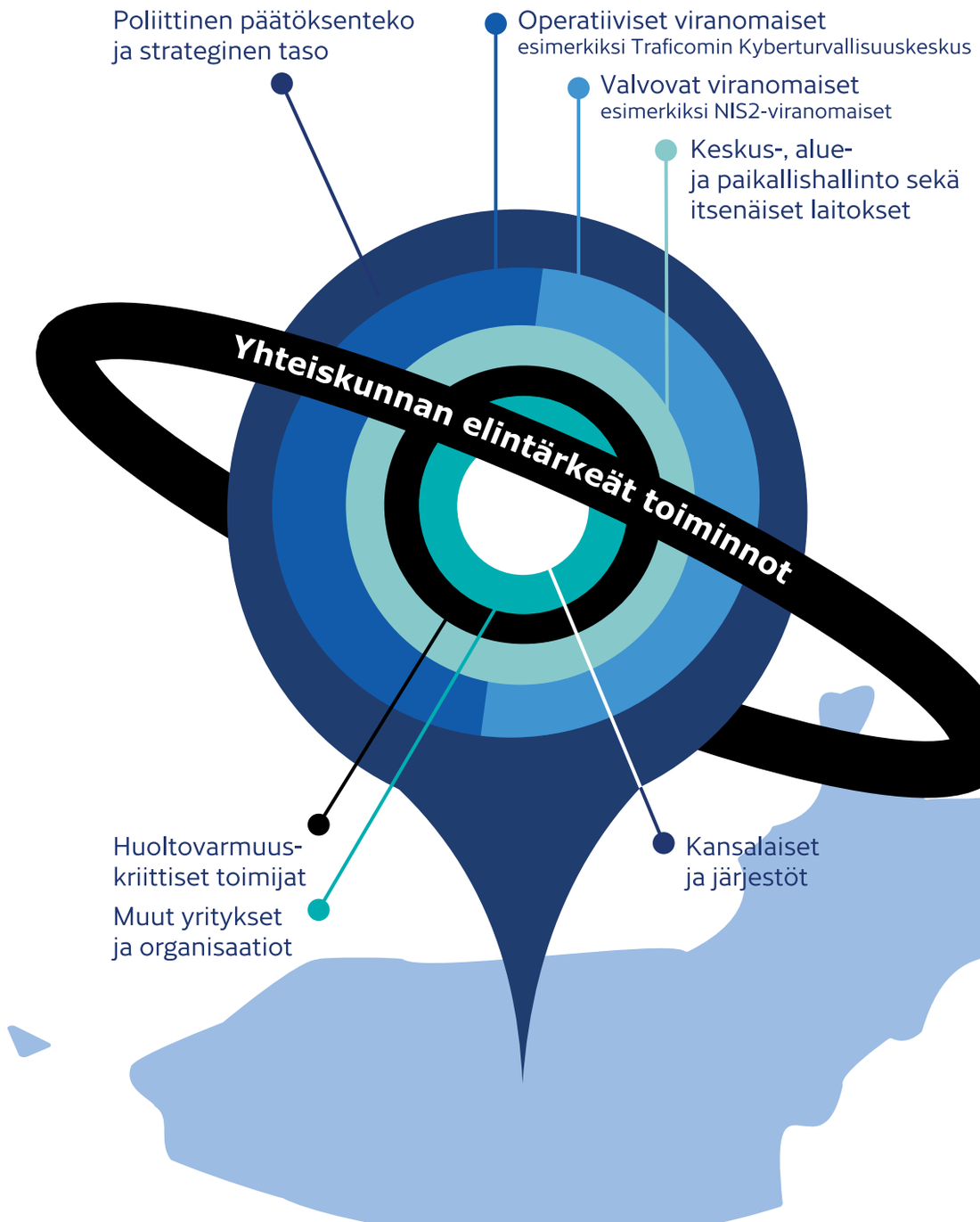
Kyberturvallissuusstrategian toimeenpanosuunnitelmassa määritellään konkreettiset toimenpiteet strategian tavoitteiden saavuttamiseksi. Näistä osa voidaan toteuttaa nopeasti, mutta osa ulottuu pitkälle tulevaisuuteen, vuoteen 2035 saakka.

Rauli Paananen
Valtion kyberturvallisuusjohtaja
Liikenne- ja viestintäministeriö

Suomen kyberturvallisuus-strategia 2024–2035

Kyberturvallisuuden vuosi

Yhteiskunnan toimijat kansallisen kyberturvallisuuden varmistamisessa



Kyberturvallisuus kuuluu kaikille

Digitaalinen turvallisuus on osa kokonaisturvallisuutta ja erityisasemassa koko yhteiskunnan kriisinsietokyvyn kannalta, sillä kaikki yhteiskunnan osa-alueet ja talouden sektorit ovat riippuvaisia erilaisten digitaalisten sovellusten toiminnasta. Huoltovarmuuskeskuksen vuoden 2024 strategiassa digitaalinen turvallisuus on yksi painopistealueista.

Digitaalisesti verkottuneessa yhteiskunnassa kyberhäiriöt muodostavat merkittävän uhkatekijän yritysten ja yhteiskunnan toiminnalle. Varautumisessa ja jatkuvuudenhallinnassa on siirryttävä yksittäisistä järjestelmistä kokonaisten toimintoketjujen ja prosessien suojaamiseen, ja siihen tarvitaan yhä tiiviimpää yhteistyötä yritysten ja viranomaisten välillä, sillä monia yhteiskunnan kriittisiä palveluita tuottavat yritykset.

Huoltovarmuuskeskus edistää digitaalista turvallisuutta **Digitaalinen turvallisuus 2030 -ohjelman** kautta, toteuttaen kyber- ja informaatioturvallisuutta vahvistavia projekteja yhdessä eri kumppaneiden kanssa.

Kyberturvallisuuskeskuksen kanssa toteutettuja projekteja vuonna 2024:

- HAVARO-palvelun kehitys
- Ohjelmistoturvallisuuden kehittäminen -hanke
- Satelliittilaajakaistojen hyödyntäminen varautumisessa
- ISAC-harjoituskonsepti
- Hack the Networks, 5G-verkkojen tietoturvan hakkerointitapahtuma
- Toimialavastaavien rahoitus Kyberturvallisuuskeskuksessa

Juha Ilkka
Johtava varautumisasiantuntija
Huoltovarmuuskeskus

Kyberturvallisuusala murroksessa

Vuonna 2024 suomalainen teollisuus ja kyberturvallisuusala sen osana kohtasi edelleen nopeasti muuttuvan toimintaympäristön, jossa keskeisiä elementtejä olivat uhkaympäristön jatkuva muutos, tietojärjestelmien teknishallinnollinen “korjausvelka”, sääntely, kansalliset kehittämispyrkimykset sekä kansainvälinen kauppa ja politiikka.

Yritykset pitivät kyberturvallisuutta yhtenä suurimmista riskeistä. Yritys- ja toimialakohtaisesti kyberturvallisuuden hallinnan taso vaihtelee kuitenkin merkittävästi. Ohjelmistohaavoittuvuuksien ja kiristyshaittaohjelmien torjunta sekä teollisuusympäristöjen suojaaminen edellyttävät ajantasaisia menetelmiä ja ratkaisuja, sillä keskeisintä ovat tieto-omaisuuden ja -järjestelmien teknishallinnolliset suojauskeinot.

Kyberturvallisuuskeskus osallistui riskienhallinnan kehittämiseen tarjoamalla tukea yrityksille riskienhallintakeinojen käyttöönottoon. Alustavat tulokset ovat hyvin rohkaisevia ja yrityksiä tulisikin tukea jatkossa aiempaa voimakkaammin. Samalla markkinoilla ei ole riittävästi kyberturvallisuuden hallinnan ammattilaisia riskienhallinnan tarpeisiin nähden.

Digitaalista hallintoa ja palveluita tarjoavien yritysten näkökulmasta olennaisimpia uusia lakeja olivat data-asetus, ekosuunnitteluasetus, huolellisuusvelvoitedirektiivi, NIS2-direktiivi, tekoälyasetus ja kyberkestävyyssäädös.

Kansainvälistyminen on kyberturvallisuusalan yritysten kannattavuuden ja innovaatioiden edellytys. Suomessa kehittyy kansainvälisesti arvostettu osaamiskeskittymä, jolla on merkittävä vientipotentiaali.

Peter Sund
Toimitusjohtaja
Kyberala ry
Teknologiateollisuus ry

Kyberturvallisuuskeskus pähkinänkuoressa

Digitaalinen yhteiskuntamme perustuu toimiviin ja turvallisiin tietoverkkoihin sekä sähköisiin palveluihin. Seuraamme Traficomissa jatkuvasti digitaalisen yhteiskunnan ja kyberturvallisuuden ilmiöitä. Kansallisena turvallisuusviranomaisena autamme yrityksiä, organisaatioita, viranomaisia ja kansalaisia varautumaan ja tunnistamaan tämän hetken ja tulevaisuuden kyberuhkia. Vaikutamme myös teknologiseen kehitykseen.

Kyberturvallisuudesta huolehtiminen on valtaosin perusasioiden kunnossapitoa, esimerkiksi riskien, pääsyn ja haavoittuvuuksien hallintaa. Haavoittuvuuksia käytetään hyväksi kiihtyvällä tahdilla ja jokainen meistä tai edustamamme organisaatio voi joutua hyökkäyksen uhriksi. Autamme uhkiin varautumisessa ja vastaamisessa.

Tarjoamme koko yhteiskunnalle palveluita, joita on kehitetty yhdessä esimerkiksi Huoltovarmuuskeskuksen kanssa. Lisäksi koostamme ja tuotamme joka päivä kellon ympäri kyberturvallisuuden tilannekuvaa ja -analyysia, jota hyödynnetään yhteiskunnan eri sektoreilla aina ylimmän valtionjohdon päätöksentekoa myöten. Toiminnan ytimessä on yhteistoiminta elinkeinoelämän ja viranomaisten kanssa. Kyberuhkien torjunta on joukkuepeliä.

Kyberturvallisuuskeskus:

- ylläpitää kansallisen kyberturvallisuuden **tilannekuvaa**.
- selvittää suomalaisiin tietojärjestelmiin **kohdistuvia tietoturvaloukkauksia ja niiden uhkia**.
- tukee **tietoturvallisuuden, varautumisen ja yksityisyyden suojan** toteutumista viestintäverkoissa ja sähköisessä viestinnässä.
- toimii **julkisesti säännellyn satelliittipalvelun** (Galileo PRS) vastuuviranomaisena.
- **arvioi ja hyväksyy** tietojärjestelmiä ja salaustuotteita sekä jakelee salausteknistä materiaalia.
- toimii Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen mukaisena kansallisena **koordinointikeskuksena**.

Tilannekuva- ja verkostopalvelut auttavat kehittämään tietoturvaa nopeasti muuttuvassa maailmassa

Kyberturvallisuuskeskus tuottaa ajantasaista tilannekuvaa kyberuhkista ja riskeistä yhteistyössä kansallisten ja kansainvälisten viranomaisten sekä muiden sidosryhmien kanssa. Tämä tieto tukee päätöksentekoa aina ylimpään valtionjohtoon saakka ja auttaa kohdentamaan resursseja tehokkaasti.

Tilannekuvan avulla yhteiskunta voi ennakoida ja torjua kyberuhkia sekä reagoida nopeasti mahdollisiin häiriöihin. Keskuksen julkaisemat viikkokatsaukset ja kuukausittainen Kybersää tarjoavat analyysiä kyberturvallisuustilanteesta organisaatioille ja kansalaisille. Lisäksi Tietoturva Nyt! -uutiset käsittelevät ajankohtaisia tietoturva-aiheita.

Tilannekuvatuotteilla on keskeinen rooli kyberturvallisuuden kehittämisessä ja varautumisessa. Vuonna 2024 tehdyn kyselyn mukaan niiden arvioitiin olevan **erittäin laadukkaita (4,6/5)**.

Yritykset, organisaatiot ja yksityishenkilöt voivat ilmoittaa tietoturvaloukkauksista Kyberturvallisuuskeskukselle. Jokainen ilmoitus on tärkeä kyberturvallisuuden vahvistamiseksi.

Vuonna 2024 Kyberturvallisuuskeskus vastaanotti yli 18 000 kyberpoikkeamailmoitusta. Automaattisesti käsiteltyjä ilmoituksia kertyi noin 185 000. Luvut ovat linjassa aiempien vuosien lukujen kanssa.

Tiedoista tilannekuvaan

Tilannekeskus
seuraa signaaleja

Tilannekuva
yksityiskohdista ymmärrykseen

- Organisaatioiden ja kansalaisten tietoturvapoikkeamailmoitukset
- Uutisseuranta
- Havainto-järjestelmät
- Lakisääteiset ilmoitukset
- Data-analyysi

- Näkökulmat eri toimintaympäristöihin
- Tilannekeskuksen keräämä tieto
- Muu Kyberturvallisuuskeskuksen keräämä tieto

Kotimainen ja kansainvälinen viranomais- ja muu sidosryhmäyhteistyö mahdollistavat nopean tilannekuvan luomisen.

Verkostojen tilannekuva

Yhteistyöryhmät luovat edellytykset tiedon turvalliselle käsittelylle ja jakamiselle

ISAC-tiedonvaihtoryhmät (Information Sharing and Analysis Centre) ovat toimialakohtaisia kyberturvallisuuden yhteistyöelimiä. Ryhmien tarkoitus on mahdollistaa tietoturva-asioiden luottamuksellinen käsittely ja tiedonjako osallistujien kesken.

Toiminnassa jaettava tieto on olennainen osa kansallista kyberturvallisuuden kokonaistilannekuvaa. ISAC-tiedonvaihtoryhmät muodostavat laajan kansallisen verkoston, jolla on tärkeä rooli myös kyberturvallisuuteen liittyvien laajojen häiriötilanteiden hallinnassa ja näihin liittyvässä tiedonvaihdossa. Yhteistyötä häiriötilanteissa harjoitellaan myös säännöllisesti.

Kyberuhkiin vastaamisessa on erityisen tärkeässä roolissa avoin ja mahdollisimman nopea tiedonvaihto.

Tämän mahdollistamiseksi Kyberturvallisuuskeskuksella on käytössään verkostojen sekä muiden yhteistyökumppaneiden kanssa tehtävään tiedonvaihtoon erilaisia ratkaisuja ja alustoja, jotka mahdollistavat reaaliaikaisen tiedonvaihdon sekä teknisen tiedon jakamisen käyttäjien välillä.

ISAC-tiedonvaihtoryhmiä toimii tällä hetkellä 17 toimialalla. Yhteensä ryhmiä on 24, joissa on useita satoja osallistujia. Osallistujaorganisaatiot ovat pääasiassa yhteiskunnan toiminnan kannalta keskeisiä huoltovarmuuskriittisiä organisaatioista, julkishallinnon toimijoita ja turvallisuusviranomaisia.

Uusimmat ISAC-tiedonvaihtoryhmät ovat kiinteistö- ja rakennusalan KIRA-ISAC -tiedonvaihtoryhmä sekä puolustusjärjestelmätoimijoiden MIL-ISAC. Vuonna 2025 toimintansa aloittaa korkean teknologian HITECH-ISAC.

ISAC-verkosto (Information Sharing and Analysis Centre) koostuu noin 300 organisaatiosta. ISAC-toiminta perustuu vapaaehtoisuuteen ja **luottamukselliseen tiedonvaihtoon**.

Kyberpalveluilla tietoa kyberturvallisuuden tasosta

Kyberturvallisuuskeskus tuottaa ja tarjoaa palveluita organisaatioille niiden tieto- ja kyberturvallisuuden parantamiseksi. Palveluilla organisaatiot saavat arvokasta tietoa omasta kyberturvallisuuden kypsyystasostaan sekä parantavat kansallista kyberturvallisuuden tilannekuvaa. Tieto havainnoista auttaa organisaatiota suojaamaan toimintakykyään sekä tarjottavien palveluiden turvallisuutta ja toimintavarmuutta.

Palvelumme ovat pääsääntöisesti maksuttomia ja kuuluvat kaikille. Osa palveluista on suunnattu tukemaan valtionhallinnon ja huoltovarmuuskriittisten organisaatioiden kyberturvallisuutta.

Palveluita on kehitetty yhdessä esimerkiksi Huoltovarmuuskeskuksen kanssa. Toiminnan ytimessä on yhteistoiminta elinkeinoelämän ja viranomaisten kanssa. Kyberuhkien torjunta on joukkuepeliä.

Kybermittari

Kybermittari vastaa tarpeisiin johtaa kyberturvallisuutta perustuen tietoon nykyisestä kyberturvallisuuden kypsyystasosta ja kuinka organisaatio nykyisillä kyvykkyyksillä pystyy vastaamaan toimintaympäristönsä muuttuviin uhkiin.

HAVARO

HAVARO havainnoi suomalaisiin yrityksiin kohdistuvia vakavia tietoturvauhkia ja varoittaa niistä. HAVAROn kehittäminen on jatkunut voimakkaana, jotta se pysyy teknologian kehittämisen tahdissa.

Hyöky

Hyöky on Kyberturvallisuuskeskuksen tuottama kansallinen hyökkäyspintakartoitus kyberturvallisuuden parantamiseksi huoltovarmuuskriittisissä organisaatioissa sekä kunnissa. Hyöky on maksuton ja helppokäyttöinen palvelu, joka kartoittaa organisaation hyökkäyspinnan julkisissa tietoverkoissa.

Kyberharjoituksissa koetellaan organisaation toiminta- ja toipumiskykyä kyberhäiriön osuessa omalle kohdalle

Kyberhäiriö voi osua mihin tahansa organisaatioon sen koosta tai toimialasta riippumatta. Kyberharjoitukset tarjoavat turvallisen alustan arvioida ja kehittää toimintatapoja haastavissa kriisi- ja häiriötilanteissa sekä niistä toipumisessa turvallisessa harjoitteluympäristössä.

Kyberuhka voi myös kohdistua palvelukumppaniin ja heijastua sitä kautta omaan toimintaan. Harjoituksissa on hyvä tarkastella myös toimialojen sisäisiä toimitusketjuja sekä toimialojen välisiä riippuvuuksia ja yhteistä tilannekuvaa.

Häiriöillä voi olla vakavia vaikutuksia organisaation toimintaan ja maineeseen. Harjoittelun avulla organisaatio voi parantaa toimintavalmiuksiaan, pienentää varsinaisten kyberhyökkäysten vaikutuksia ja jopa tunnistaa uusia potentiaalisia uhkia etukäteen.

Harjoitukset tarjoavat verkostoitumisen lisäksi arvokasta tietoa organisaatioiden operatiivisen toiminnan, johtamisen, viestinnän ja tilannekuvatoiminnan kehittämiseen. Näillä keinoilla voidaan vaikuttaa organisaation kyvykkyyteen toipua kyberhäiriötilanteista nopeammin. Toimintakyvyn varmistaminen laajoissa kyberhäiriötilanteissa edellyttää ajantasaisen suunnittelun lisäksi myös säännöllistä harjoittelua sekä oppien jalkauttamista organisaatioon.

Kyberturvallisuuskeskuksen verkkosivuilta saat apua kyberharjoituksen suunnitteluun, skenaarioiden valitsemiseen kuin harjoituspalveluja tarjoaviin yrityksiin.

Traficomin Kyberturvallisuuskeskuksen harjoitustoiminto tukee yhteiskunnalle kriittistä harjoittelua.

Kyberharjoitukset

Ohjelmistovirheet tekevät organisaatioista haavoittuvia

Haavoittuvuuksia ja ohjelmistovirheitä esiintyy kaikessa teknologiassa. Koska haavoittuvuudet voivat altistaa vakavillekin tietoturvahäiriöille, on tärkeää, että ohjelmistovirheet saadaan nopeasti ja luottamuksellisesti ohjelmistovalmistajan ja järjestelmätoimittajan tietoon. Näin ne voivat tarjota ohjelmistovirheelle korjauksen tai lievennyskeinot ennen kuin rikolliset ehtivät hyödyntää haavoittuvuutta. Tärkeää on myös saada tietoa haavoittuneen tuotteen tai palvelun käyttäjille.

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio avustaa haavoittuvuuden tai vakavan ohjelmistovirheen löytäjää tekemään yhteistyötä ohjelmistovalmistajien ja -toimittajien kanssa. Julkaisemme päivittäin haavoittuvuuskoosteen. Lisäksi julkaisemme merkittävistä haavoittuvuuksista haavoittuvuustiedotteen.

Haavoittuvuuksien löytämiseksi organisaatiot ja yritykset voivat järjestää bug bounty -ohjelmia, jotka palkitsevat virheen löytäjän. Ohjelmistovirheitä ja heikkouksia etsitään myös hakkereille järjestetyissä hakkerointitapahtumissa. Ne ovatkin turvallinen ja suositeltava tapa harrastaa hakkerointia. Muista hakkeroidessasi hakkeroinnin eettiset periaatteet!

Haavoittuvuuskoordinaatio

HAAVOITTUVUUKSIA KÄYTETÄÄN HYVÄKSI KIIHTYVÄLLÄ TAHDILLA

Jokainen meistä voi joutua hyökkäyksen uhriksi. Nopea reagointi haavoittuvuuksiin on tärkeää.

Kyberturvallisuuskeskus on mukana rakentamassa maailman turvallisinta ja toimivinta digitaalista yhteiskuntaa

Kansallinen kyberturvallisuuden tilannekuva

Suomalaisiin tietojärjestelmiin kohdistuvien tietoturvaloukkausten ja uhkien selvittäminen

Tuki varautumisen, tietoturvallisuuden sekä yksityisyyden suojan toteutumiseen viestintäverkoissa ja sähköisessä viestinnässä

Julkisesti säännellyn satelliittipalvelun (Galileo PRS) vastuuviranomainen

Tietojärjestelmien ja salaustuotteiden arviointi ja hyväksyntä sekä salausteknisen materiaalin jakelu

Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamis-keskuksen kansallinen koordinointikeskus

ohjaus • valvonta • tuotteet • havainnointi • varoitukset
arviointi • rahoitus • osaaminen • verkostot

ilmoitukset ja uhkatieto

Turvaamme yhteiskunnan elintärkeitä toimintoja

Siviiliyhteiskunta

Organisaatiot
Kansalaiset
Viestintäverkot
Muu kriittinen infrastruktuuri

Yhteiskunnan kyberturvallisuus

Maanpuolustus

Perustettu
2014

Budjetti noin
26 M€

Henkilöstö noin
190

Tarkastuksia*
40

Verkosto-tapaamisia*
440

Julkaistuja tiedotteita*
150

Automaattisesti käsiteltyjä tapahtumia*
200 000

Käsiteltyjä tietoturvapoikkeamia*
19 000

*Keskimäärin vuosittain, likimäärä.

Suomessa viestintäverkot toimivat luotettavasti

Vuonna 2024 viestintäverkkojen toiminta jatkui Suomessa edelleen vakaana. Toimivuushäiriöiden kokonaismäärä kasvoi noin kymmenellä prosentilla, mutta vakavimpien toimivuushäiriöiden määrä pysyi samalla tasolla edellisvuoteen verrattuna.

Häiriöt aiheuttivat katkoksia alueellisiin palveluihin tai hätäliikenteeseen hetkellisesti, ja yli kahdeksan tunnin katkokset olivat edelleen melko harvinaisia. Myrskyjen määrä vuonna 2024 jatkoi edelleen kasvuaan, mikä näkyi myös sähkökatkosten määrän ja niistä aiheutuneiden katkosten syyn huomattavana kasvuna.

Pitkällä aikavälillä tarkasteltuna yleisten viestintäpalveluiden toimivuushäiriöiden, ja erityisesti kaikkein vakavimpien vikatilanteiden määrä jatkaa lievää laskuaan, vaikkakin edellisvuoteen verrattuna toimivuushäiriöiden lukumäärä kokonaisuudessaan hieman kasvoikin. Viranomaiset jatkavat tiivistä yhteistyötä suomalaisten teleyritysten kanssa verkkojen toiminnan luotettavuuden korkean tason ylläpitämiseksi.

Häiriöihin on varauduttu pitkäjänteisesti

Suomesta on useita merikaapeleita muualle Eurooppaan ja maailmaan tietoliikenteen toiminnan varmistamiseksi. Manner-Suomen sisällä kaapeleita on tuhansia.

Tärkeimmät järjestelmät ovat kahdennettuja ja reittivarmistettuja. Laitteistojen tai yhteyksien vikaantuessa tai huoltotöiden yhteydessä liikenne siirtyy automaattisesti varayhteydelle ja toimii normaalisti.

Internetin käyttö ei riipu yhdestä kaapelista tai edes sen varayhteydestä. Järjestelmä kokonaisuutena kestää useita samanaikaisia häiriöitä.

Varautumisella on Suomessa pitkät perinteet

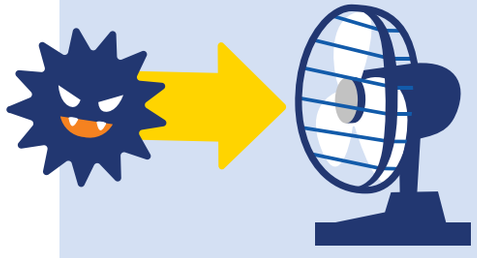
Kyberuhkiin varaudutaan monin tavoin ja jokainen voi omalla toiminnallaan vaikuttaa digitaalisen yhteiskuntamme varautumiseen.

Ohjeita ja linkkejä:

- Kyberturvallisuuskeskuksen ohjeet

Yhteistyössä toteutettuja ohjeita:

- Kyberuhkien lieventäminen rajallisilla resursseilla
- Häiriö- ja kriisitilanteisiin varautumisen opas
- Tietovuoto-opas kansalaisille
- Tietomurto-opas organisaatiolle



VARAUTUMINEN JA ENNALTAEHKÄISY VAATIVAT RESURSSEJA

Varautumiseen panostaminen on kuitenkin yleensä huomattavasti halvempaa kuin jo tapahtuneen kyberpoikkeaman selvittäminen.

EU:n uusi kyberturvallisuus-sääntely vaatii ennakoivaa riskienhallintaa

Liikenne- ja viestintäviraston uudistama teletoiminnan tietoturvamääräys astui voimaan 1. syyskuuta 2024. Uudistuksessa huomioidaan viestintäverkkojen ja -palvelujen kehittyminen sekä vastataan uusiin, tietoturvaa uhkaaviin ilmiöihin.

NIS2-direktiivin (kyberturvallisuusdirektiivi) kansallinen täytäntöönpano on loppusuoralla. NIS2-direktiivi korvaa aiemman EU:n verkko- ja tietoturvadirektiivin. NIS2:n tavoitteena on vahvistaa sekä EU:n yhteistä että jäsenvaltioiden kansallista kyberturvallisuuden tasoa tiettyjen kriittisten sektoreiden osalta.

Direktiivissä osoitetaan yhteiskunnan kriittisille sektoreille kyberturvallisuutta vahvistavia riskienhallintavelvoitteita ja raportointivelvoitteet merkittävistä poikkeamista.

Kyberkestävyyssäädöksellä (CRA) asetetaan kyberturvallisuuden vähimmäisvaatimukset digitaalisen elementin sisältäville laitteille ja ohjelmistoille, jotka ovat suoraan tai epäsuorasti liitettävissä toiseen laitteeseen tai verkkoon. Tavoitteena on luoda puitteet turvallisten tuotteiden ja ohjelmistojen kehittämiselle, vähentää haavoittuvuuksien määrää ja parantaa tuotteiden turvallisuuden tasoa koko tuotteen elinkaaren ajan.

Toisena tavoitteena on parantaa kuluttajien tietoisuutta markkinoilla olevien laitteiden ja ohjelmistojen kyberturvallisuusnäkökohdista.

Kyberkestävyyssäädöksen tavoitteita täydentää osaltaan radiolaitedirektiivi ja sen tietoturvavaatimukset, jotka markkinoille saatettavien laitteiden on täytettävä 1.8.2024 lähtien.

Muita ajankohtaisia sääntelyaihioita ovat kybersolidarisuuden säädösehdotus, EU:n tekoälyasetus sekä EU:n viestintäverkkojen turvallisuus.

Luottamuspalvelut ja sähköinen tunnistaminen – turvallisen digitaalisen asioinnin kulmakivet

Suomessa vahvaa sähköistä tunnistusta ja hyväksyttyjä luottamuspalveluita valvoo Traficom. Nämä palvelut auditoidaan määräajoin. Virasto valvoo palvelujen kohdalla lainmukaisuutta ja määräysten noudattamista. Sääntelyn tavoitteena on muun muassa varmistaa palvelujen jatkuva turvallinen toiminta, myös loppukäyttäjän näkökulmasta. Kansalaisten käyttämät tunnistusmenetelmät kuuluvat jatkuvan arvioinnin piiriin. Vahvoja sähköisiä tunnistuspalveluja tarjoavat pankit, teleoperaattorit ja tunnistuksen välityspalvelut. Ajantasaisen listan löydät viraston sivuilta.

Tunnistuspalvelurekisteri

Luottamuspalvelut ovat osa turvallista sähköistä infrastruktuuria. Niitä voidaan käyttää osana sähköisiä asiointiprosesseja. Henkilökortilla oleva kansalaisvarmenne mahdollistaa esim. korkean tason tunnistuksen asiointipalveluihin. Kansalaisvarmenteeseen liitetyn salaisen avaimen avulla voidaan luoda hyväksyttyjä sähköisiä allekirjoituksia. Hyväksytty sähköinen allekirjoitus vastaa käsin tehtyä allekirjoitusta. Luottamuspalvelutyyppejä ovat muun muassa varmenteet (esim. kansalaisvarmenne), leimavarmenteet (oikeushenkilölle), aikaleimat, verkkosivujen todentamisvarmenteet, allekirjoitusten ja leimojen validointipalvelut ja rekisteröidyt säilytyspalvelut. Suomeen rekisteröidyt hyväksytyt luottamuspalvelut löydät EU-komission luotetusta listasta.

Luottamuspalvelut

EU-sääntelyllä varaudutaan toimintaympäristön muutoksiin

NIS2
Kyberturvallisuusdirektiivi
Yhdenmukaistaa ja vahvistaa yhteiskunnan tärkeiden sektoreiden kyberturvallisuuden tasoa

2022–2023
julkaisu, lausuntokierros, jatkovalmistelu

5/2024
NIS2-HE eduskunnalle

Q1/2025
Kansallinen NIS2-lainsäädäntö voimaan

CSOA
Kybersolidaarisuussäädös
Varautuminen ja reagointi kyberpoikkeamiin

H1/2024
neuvotteluissa sopuun

Q4/2024
parlamentin ja neuvoston äänestykset, asetus annetaan

Q1/2025
CSOA voimaan

H1/2026
EU:n laajuinen kyberturvallisuus-reservi

CSA
Kyberturvallisuusasetus
Tuotteiden, palveluiden ja prosessien sekä tietoturva-palvelujen sertifiointi

2019
asetus voimaan

2/2024
EUCC-täytäntöönpano-asetus voimaan

vaatimuksenmukaisuuden arviointilaitoksia koskevia säädöksiä aletaan soveltaa

Valmistelu:
EUCS, EU5G ja EUDIW

Q1/2025
CSA muutettu kattamaan myös tietoturvapalvelut

2/2025
EUCC-täytäntöönpano-asetusta aletaan soveltaa

AI Act
Vaatimuksia korkean riskin AI-järjestelmille

CRA
Kyberkestävyyssäädös
Vaatimuksia laitteille ja ohjelmistoille

2022–2023
ehdotus, neuvottelut

12/2024
CRA voimaan

6/2026
ilmoitettuja laitoksia koskevat säädökset

9/2026
haavoittuvuuksien raportointia koskevat säädökset

12/2027
tuotteiden olennaiset kyberturvallisuusvaatimukset

RED
Radiolaitedirektiivi

~ Q1/2025
vaatimusten harmonisoidut standardit julkaistaan

8/2025
tietoturvavaatimuksia aletaan soveltaa

2024

2025

2026

2027

EU- ja Nato-hyväksyntöjen tavoittelu kiinnostaa laajasti kotimaista yrityskenttää

Kyberturvallisuuskeskuksen turvallisuusviranomaistehtäviin kuuluu salaustuotteiden ja turvallisuuskriittisten tuotteiden hyväksyntä EU- ja Nato-turvallisuusluokitellun tiedon suojaamiseen ja käsittelyyn. Julkisia hyväksyntöjä myönnetään tuotteille, jotka täyttävät kansainvälisen turvallisuusluokitellun tiedon suojaamiseen vaaditut turvallisuusominaisuudet.

EU- ja Nato-hyväksyntöjen tavoittelu kiinnostaa tällä hetkellä laajasti kotimaista yrityskenttää. Kiinnostusta ovat kasvattaneet Nato-jäsenyyden ja muuttuneen turvallisuustilanteen myötä auenneet liiketoimintamahdollisuudet sekä teknologian nopea kehittyminen. Tämä näkyy Kyberturvallisuuskeskuksessa moninkertaistuneena arviointipyyntöjen määränä. Eturintamassa tuotteiden arviointipyyntöjen osalta ovat olleet erilaiset salauslaitteet ja yhdyskäytävätuotteet.

Ensimmäinen Traficomin tekemä salaustuotehyväksyntä Naton turvallisuusluokitellun tiedon suojaamiseksi valmistui kesäkuussa.

Nato- ja EU-kriteeristöt ja niiden tuotteille asettamat turvallisuusvaatimukset ovat tuotteiden valmistajille usein uusia, samoin kuin hyväksynnän menettelyt. Tapauskohtainen neuvonta, ohjeet ja infotilaisuudet ovat tärkeä osa Kyberturvallisuuskeskuksen elinkeinoelämää ja toisia turvallisuusviranomaisia tukevaa työtä.

Kvantinkestävä kyberturvallisuus

Kyberturvallisuuden tulevaisuuden uhkista yksi on kvanttikoneiden kehityksen myötä kehittyvä kyky purkaa tietoliikenteen ja tiedostojen salauksia. Tämän uhan arvioidaan toteutuvan seuraavan 10–15 vuoden aikana.

Vuonna 2024 NIST (National Institute of Standards and Technology) julkaisi ensimmäiset hyväksytyt kvanttiturvalliset algoritmit. Kyberturvallisuuskeskus päivitti Suomen kansalliset kryptografiset vahvuusvaatimukset niiden mukaiseksi.

Kvanttiuhkaa torjumaan sekä julkisten organisaatioiden että yksityisten yritysten on otettava käyttöön kvantinkestävät salausratkaisut. Ohjelmistojen ja salausta toteuttavien laitteiden valmistajien on siirryttävä valmistamaan niitä. Kvanttisiirtymä tulee tehdä mahdollisimman pian kartoittamalla tällä hetkellä käytössä olevat palvelut, suunnittelemalla siirtymä ja turvattomiksi jäävien palveluiden suojaaminen muilla tavoilla ja toteuttamalla suunnitellut toimenpiteet. Kyberturvallisuuskeskuksen lisäksi vastaavaa ohjeistusta Suomessa ovat julkaisseet muun muassa Huoltovarmuuskeskus huoltovarmuuskriittisten toimijoiden osalta ja kansainvälisesti sekä Euroopan Unioni että useat valtiot.

Kryptografiset vahvuusvaatimukset

Kvanttisiirtymän toteuttaminen organisaatioille

Verkostoitumismahdollisuuksia, tietoa ja rahoitustukea kyberturvallisuuskentälle

Euroopan kyberturvallisuuden osaamiskeskuksen Suomen kansallinen koordinointikeskus (NCC-FI) toimii Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksessa. Toiminnalla vahvistetaan kyberturvallisuuden tutkimus-, kehitys- ja innovaatiotoimintaa Suomessa ja Euroopassa.

NCC-FI myönsi vuonna 2024 mikro- ja pk-yrityksille 1,5 miljoonaa euroa rahoitustukea tietoturvaratkaisujen parantamiseen. Se tarjoaa koulutusta EU-rahoitushakemuksien laatimiseen sekä järjestää erilaisia tapahtumia.

Osaamisyhteisön jäsenmäärä ylitti sadan toimijan rajan vuonna 2024. Osaamisyhteisön toimijoiden välisen yhteistyön edistäminen on keskeisessä roolissa kyberturvallisuuden tutkimuksen, kehittämisen ja innovoinnin edistämisessä Suomessa ja EU:ssa, joten tavoitteemme on myös tulevina vuosina vahvistaa tätä yhteistyötä ja tarjota ajankohtaista tietoa sekä työkaluja kyberturvallisuusalan kehittämiseen.

Kyberturvallisuusalan kehittäminen

Kyberturvallisuuskeskuksen yhteydessä aloitti toimintansa EU:n kansallisen kyberturvallisuuden sertifiointiviranomainen

Vuonna 2024 julkaistiin ensimmäinen kyberturvallisuusasetuksen (Cybersecurity Act, CSA) mukainen EU:n kyberturvallisuuden sertifiointijärjestelmä, EUCC (Common Criteria based European candidate Cybersecurity Certification Scheme). EUCC-järjestelmän avulla ICT-tuotteille voidaan hankkia kyberturvallisuussertifikaatti, joka hyväksytään kaikkialla EU:ssa.

Kyberturvallisuuskeskus toimii Suomessa kansallisena kyberturvallisuussertifioinnin viranomaisena, vastaten kyberturvallisuussertifiointien valvonnasta ja korkean varmuustason sertifikaattien myöntämisestä. Keskus on valmistautunut tuleviin kyberturvallisuussertifiointeihin vuoden 2024 aikana kehittämällä valvontakäytäntöjä ja jakamalla tietoa kyberturvallisuussertifiointeihin liittyen. Keskus on myös osallistunut aktiivisesti EU:n kyberturvallisuussertifiointijärjestelmien säädösvalmisteluun.

Pilvipalveluita ja 5G-verkkoja koskevien sertifiointijärjestelmien osalta valmistelutyö jatkuu vuonna 2025.

Kyberturvallisuussertifiointi

Kansallinen kyberturvallisuussertifioinnin viranomainen valvoo EU:n kyberturvallisuusasetuksen ja sertifiointijärjestelmien vaatimusten noudattamista Suomessa.

Kova tarve kyberturvallisuus-viestinnälle

Kyberturvallisuuskeskus on aktiivisesti mukana useilla kyberturvallisuuden viestintä- ja keskustelufoorumeilla: verkossa, tapahtumissa ja mediassa.

Vuosi 2024 oli Kyberturvallisuuskeskuksen viestinnässä vilkas. Uusia alkuja olivat muun muassa pelitapahtumiin osallistuminen, koko väestölle suunnattuun Häiriö- ja kriisitilanteisiin varautumisen oppaan tuotantoon osallistuminen sekä Nyt valppaana! –kampanja, jonka tavoitteena on tarjota jokaiselle keinoja onnistua digitaalisten palvelujen käyttäjänä.

Yhteistyö tiedotusvälineiden ja Kyberturvallisuuskeskuksen välillä oli kaikkien aikojen vilkkain. Myös kansainvälinen mediakiinnostus kasvoi merkittävästi vuonna 2024. Vastaamme tarpeeseen tuoda kyberturvallisuuteen vaikuttavat asiat nopeasti, luotettavasti ja ymmärrettävästi kaikkien saataville. Mediat ovat tässä korvaamaton voimavara.

Tapasimme tuhansia kyberturvallisuudesta kiinnostuneita tapahtumissamme ja messuilla ja tavoitimme vielä paljon lisää ihmisiä verkossa.

Myös viestintäkumppaneiden kirjo on monipuolistunut, teemme yhteistyötä niin viranomaisten, oppilaitosten kuin kansalaisjärjestöjen kanssa, jotta mahdollisimman moni saisi ajankohtaista tietoa kyberturvallisuudesta.

Traficom medialle

Nyt valppaana!

KYBERTURVALLISUUSKESKUKSEN TAPAHTUMIA

Vuoden päätapahtuma oli yhdessä Huoltovarmuuskeskuksen kanssa järjestetty **Tietoturva 2024** -seminaari 13.3.2024. Se keräsi paikan päälle ja verkkoon yhteensä yli 3 000 katsojaa. Huoltovarmuuskeskuksen ja Kyberala ry:n kanssa järjestettiin myös neljä **Kyberala murroksessa** -webinaaria, joiden yhteenlaskettu osallistujamäärä oli noin 2200.

Kyberturvallisuutta yli rajojen

Kyberturvallisuuskeskus on tiivistänyt kahdenvälisiä suhteita usean maan kanssa. Olemme aktiivisesti mukana monessa kansainvälisessä tiedonvaihtoverkostossa.

Tiivis kansainvälinen tiedonvaihto on muun muassa mahdollistanut useiden tietoturvaloukkausten havaitsemisen ajoissa tai jopa kokonaan ennalta ehkäisemisen. Myös toimialakohtainen kansainvälinen tiedonvaihto on ollut aiempaa aktiivisempaa ja siten hyödyttänyt huoltovarmuuskriittisten toimialojen kyberturvallisuutta.

Kyberturvallisuuskeskus julkaisi toukokuussa ensimmäistä kertaa kansainvälisten kumppaneiden kanssa yhteisesti laaditun ohjeen, joka käsitteli kyberuhkien lieventämisestä rajallisilla resursseilla.

Suomi osallistui useisiin kansainvälisiin kyberharjoituksiin. Esimerkiksi EU-johtoiseen Cyber Europe -harjoitukseen osallistui yli 5000 henkilöä ympäri Eurooppaa. Suomesta oli mukana Kyberturvallisuuskeskuksen lisäksi kriittisen infrastruktuurin toimijoita.

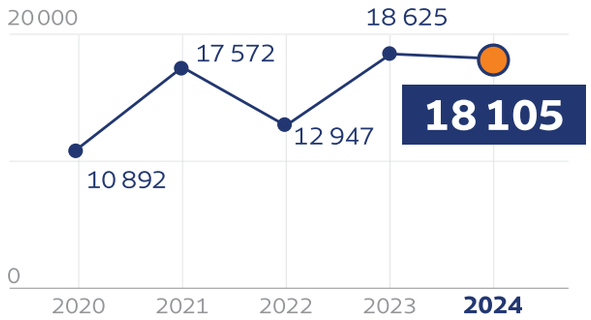
Kyberturvallisuuskeskus koordinoi kyberturvallisuuteen liittyviä EU-rahoitushankkeita Suomessa. Euroopan unionin Digital Europe -hankkeessa jaettiin noin 1,9 miljoonaa euroa suomalaisille yrityksille tietoturvan parantamiseen vuosina 2023-2024. Kyberturvallisuuskeskus myös esimerkiksi järjesti EU-rahoitushakuihin keskittyvän matchmaking-tapahtuman Helsingissä, johon tuli osallistujia kaikista Pohjoismaista ja Baltian maista.

KYBERTURVALLISUUSKESKUS OSALLISTUU TIIVIISTI KANSAINVÄLISEEN TIEDONVAIHTOON

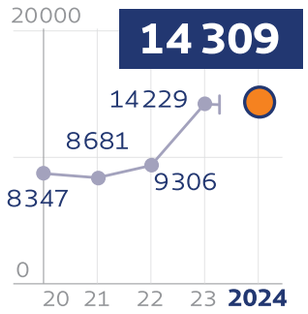
- Valtioiden kansallisten kyberturvallisuusviranomaisten väliset luottamusverkostot
- Kansainväliset viranomaisyhteistyökumppanit
- EU ja Nato
- Kansainvälinen tietoturvayhteisö

2024 lukuina

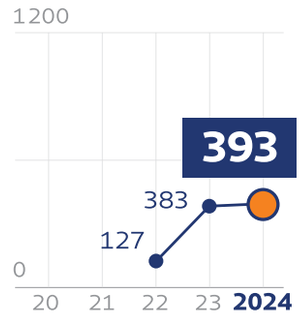
TIETOTURVAPOIKKEAMA-ILMOITUKSET YHTEENSÄ



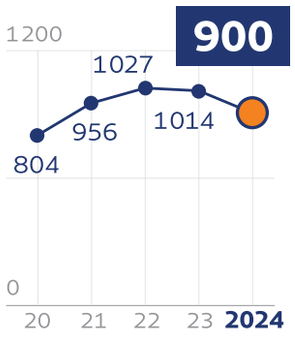
HUIJAUKSET JA KALASTELUT [1]



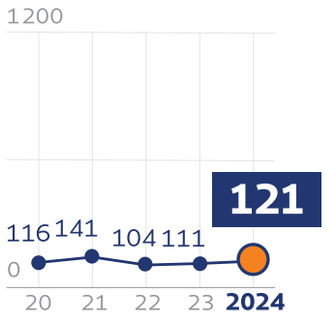
TIETOMURRON YRITYKSET [2]



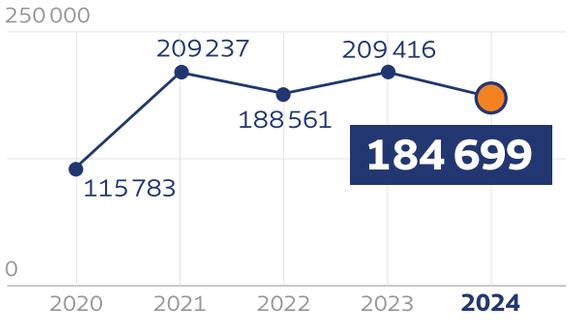
TIETOMURROT [3]



TIETOVUODOT



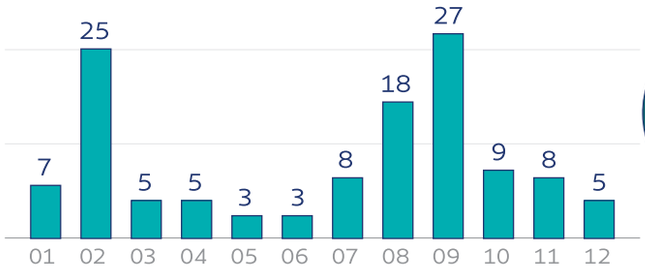
AUTOMAATTISESTI KÄSITELLYT AUTOREPORTER-HAVAINNOT



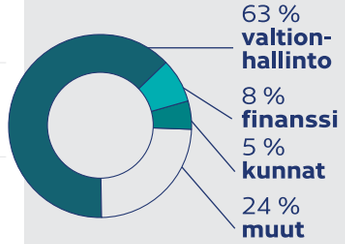
[1] Huijausten ja kalastelujen tilastointi on muuttunut vuoden 2024 aikana, joten eri vuosien luvut eivät ole keskenään täysin vertailukelpoisia.
[2] Tietomurtojen yrityksiä on tilastoitu vasta 2022 alkaen.
[3] Sisältää myös ilmoitetut kansalaisten sometilien murrot.

PALVELUNESTOHYÖKKÄYKSET

Ilmoitetut tapaukset kuukausittain



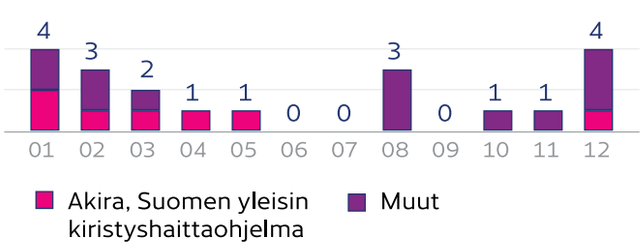
Hyökkäyksistä ilmoittaneet



Eri puolilla suomalaista yhteiskuntaa kohdataan ja torjutaan vuosittain yli 10 000 palvelunestohyökkäystä. Suurin osa palvelunestohyökkäyksistä pystytään torjumaan nopeasti, eikä niistä aiheudu vaikutuksia käyttäjille. Siksi vain murto-osasta tehdään ilmoitus Kyberturvallisuuskeskukselle.

KIRISTYSHAITTAOHJELMAT

Ilmoitetut tapaukset kuukausittain



Kohteet

Suomessa kiristyshaittaohjelmia on havaittu muun muassa ICT-, tietoturva- ja elintarvikealalla sekä teollisuusyrityksissä.

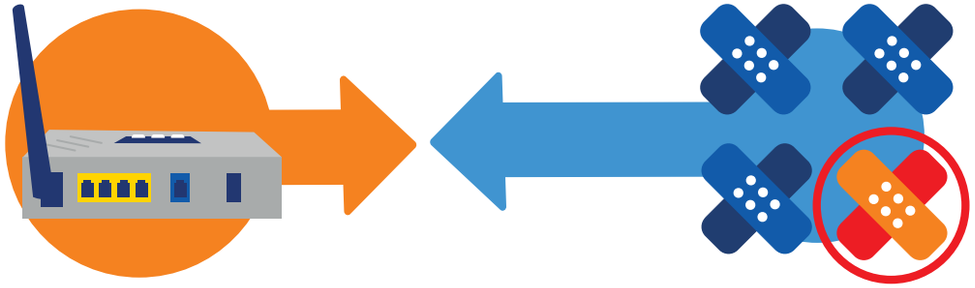
HAAVOITTUVUUS-KOORDINAATIO

Otimme vuoden aikana ennalta-ehkäisevästi yhteyttä yli tuhannen haavoittuvan VPN-laitteen omistaja-organisaatioihin. Julkaisimme yhteensä 26 haavoittuvuustiedotetta.

VAROITUKSET

Annoimme vuoden ainoan varoituksen 18.4.2024.
Vakava varoitus koski Palo Alton laitteiden haavoittuvuuksia, jotka olivat ehtineet johtaa maailmalla ja Suomessa tietomurtoihin ennen vian korjaavaa päivitystä. Varoitus poistettiin 7.5.2024.

Kansalaisten yleiset kyberuhat

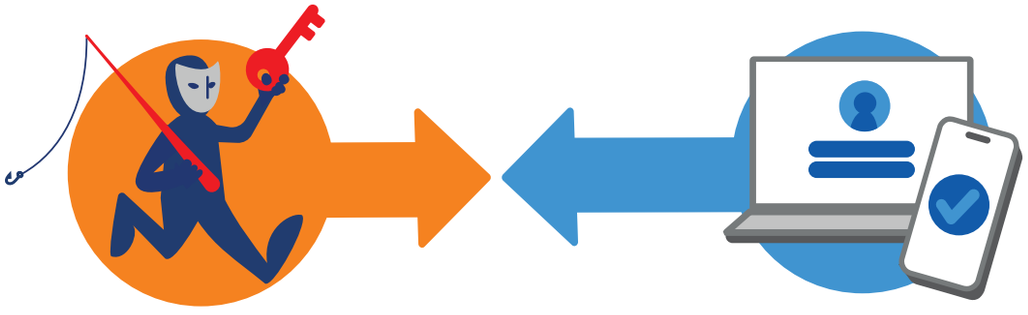


HUONOSTI SUOJATTU LAITE

Päivittämättä jäänyt tai suojaamaton laite on kuin avoin ovi rikollisille.

PÄIVITÄ AHKERASTI

- Pidä laitteesi ja ohjelmistosi ajan tasalla.
- Ota käyttöön automaattiset päivitykset.
- Varmuuskopioi.
- Käytä vahvoja salasanoja.



KAAPATUT TUNNUKSET

Tietojenkalastelulla rikolliset yrittävät saada haltuunsa käyttäjätunnuksia, salasanoja, pankkitunnuksia tai luottokorttitietoja.

MONIVAIHEINEN TUNNISTAUTUMINEN (MFA)

Huijari ei pääse tilillesi huomaamatta, jos kirjautuminen täytyy hyväksyä vielä erikseen.

Huijaukset

Huijaus voi olla esimerkiksi

- ohittamaton tarjous,
- viranomaisen viesti,
- uusi ihastus,
- hakukonetulos, joka vie valesivulle,
- avuntarjous pyytämättä,
- avunpyyntö tai
- muka maksamatta jäänyt lasku.

OLE VALPPAANA!

- Selvitä viestin aitous.
- Älä klikkaa tuntemattomia linkkejä.
- Kirjaudu vain palvelun virallisten verkkosivujen kautta tai käytä sovellusta.
- Suhtaudu varauksella uusiin nettituttavuuksiin.
- Älä anna rahaa tai tunnuksia tuntemattomalle verkossa tai puhelimessa.
- Huijausviesteissä lietsotaan usein akuutin kiireen tuntua.

JOS TULET HUIJATUKSI

Virheitä sattuu kaikille, eikä sitä tarvitse hävetä. Jos epäilet tulleesi huijatuksi, on hyvä toimia **heti**.

- Ilmoita pankkiin.
- Tee rikosilmoitus poliisille.
- Ilmoita Kyberturvallisuuskeskukselle.
- Hae apua Rikosuhripäivystyksestä.
- Kerro läheiselle.

Tietovuoto-opas kansalaisille

Lähitulevaisuuden kyberilmiöitä

TOIMITUSKETJUJEN SUOJAAMINEN

Ohjelmisto- ja laitteisto-toimitusketjujen suojaamisen merkitys kasvaa.

TEKOÄLYYN LIITTYVÄT RISKIT KONKRETISOITUVAT

Tekoälyjärjestelmien yleistyminen ja halpeneminen konkretisoi niihin liittyviä riskejä.

- Kehittyneet toimitusketju-hyökkäykset voivat yleistyä. Näitä ovat muun muassa haitalliset koodinlisäykset sekä kolmannen osapuolen kirjastojen haavoittuvuuksien löytäminen ja hyväksikäyttö.
- Generoitua ääntä ja videota aletaan käyttää huijauksissa rutiininomaisesti.
- Tekoälyn hallinta organisaatiossa vaikeutuu. Moniin palveluihin tulee yllättäviä tekoälytoiminnallisuuksia. Palveluita saatetaan ottaa innokkaasti käyttöön myös turvallisuusprosessien ohi.

ASIANTUNTIJAPULA JATKUU

- Kyberasiantuntijat sijoittuvat korkeampaa asiantuntemusta vaativiin tehtäviin.
- Automaation, tekoälyn ja koneoppimisen hyödyntäminen tietoturvan toistuvissa rutiini-tehtävissä saattaa helpottaa asiantuntijapulaa.

KVANTTILASKENTA

Kvanttilaskennan edistysaskelien uskotaan jatkuvan vauhdikkaina.

KYBERHYÖKKÄYKSET KEHITTYVÄT

Kyberturvallisuuden puolustajien ja rikollisten kilpajuoksu jatkuu, muun muassa kiristyshaitta-ohjelma- ja palvelunesto-hyökkäysten kehittyessä.

KYBERHYGIENIA PARANEE

Uusien teknologioiden käyttöönotto parantaa kyberhygieniaa. Tähän vaikuttaa etunenässä Passkeys- ja Zero trust -tekniikoiden käyttöönoton yleistyminen.

Kyberturvallisuuskeskus palvelee koko yhteiskuntaa

OHJEET, OPPAAT JA VINKIT

Organisaatioille, yksityishenkilöille ja palveluiden ylläpitäjille

Ohjeet ja oppaat

PALVELUT

Tukea yrityksille ja organisaatioille varautumisen kaikissa vaiheissa

Palvelut

AJANKOHTAISTA TIETOA SUOMEN KYBERTURVALLISUUSTILANTEESTA

- Tietoturva Nyt! – aina kun tapahtuu
- Viikkokatsaus joka perjantai
- Kybersää joka kuukauden toinen torstai

Tilannekuvatuotteet

Ilmoita Kyberturvallisuuskeskukselle

Mahdollisimman tarkat tiedot ovat tärkeitä johtolankoja.

- Ruutukaappauksia havainnoistasi
- Huijausviestit yhteystietoineen
- Epäilyttävät linkit
- Lokitiedot

kyberturvallisuuskeskus.fi/fi/ilmoita

Kartoitamme, mitä kybermaailmassa tapahtuu

- Jaamme tietoa tilanteesta kansalaisille, organisaatioille ja valtionjohdolle,
- autamme ja neuvomme,
- ennaltaehkäisemme,
- ajamme alas rikollisten verkkosivuja,
- ... ja paljon muuta!