TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Heinäkuu 2025

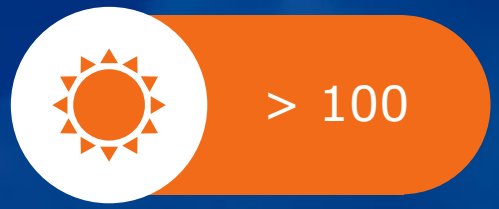
#kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

Tämä tuote on suunnattu ensisijaisesti eri tasoilla organisaatioiden tietoturvallisuuden parissa työskenteleville. Lukija saa nopean kokonaiskuvan, mitä kyberturvallisuuskentällä on tapahtunut ja mitä on tulossa.

Kybersää voi olla:  rauhallinen  huolestuttava  vakava

Kuukauden tunnuslukuja



Poliisi tiedotti heinäkuussa osallistuneensa kansainväliseen operaatioon, joka kohdistui palvelunestohyökkäyksistä tunnettuun NoName057(16)-hakkeriryhmään. Europolin mukaan operaatio Eastwoodin yhteydessä lamautettiin yli 100 haitallista palvelinta eri puolilla maailmaa. [1, 2]

BadBox 2.0 -haittaohjelmaa koskevat havainnot laskivat noin 50 % kesäkuun huippulukemista. Muihin haittaohjelmiin nähden BadBox-havaintoja tehdään edelleen paljon.

Heinäkuun aikana KTK:lle ilmoitettiin kaksi kiristyshaittaohjelmatapausta, joista toinen jäi yritykseksi. Onnistuneessa tapauksessa hyödynnettiin vanhaa SonicWall-haavoittuvuutta.

Kybersää heinäkuu 2025

Tietomurrot ja -vuodot

- Tietomurtojen määrä väheni hieman tarkastelujaksolla, mutta tietomurtoyritykset lisääntyivät.
- 70–80 % raportoiduista tapauksista liittyi SharePoint-haavoittuvuuteen. Tapaus on osoitus järjestelmien säännöllisen ylläpidon ja päivittämisen tärkeydestä.
- Onnistuneissa murtotapauksissa tietovuotojen määrä kasvoi.
- Useissa tietomurtoyritystapauksissa tietoturvatoimet estivät tietomurron onnistumisen.

Huijaukset ja kalastelut

- Traficomin ja KRP:n nimissä läheteltiin huijausviestejä, joissa uhattiin sakoilla ja lapsipornosyytteillä. Huijauksilla kalasteltiin pankkitunnuksia.
- Ärhäkkä sähköpostihuijaus kiristi bitcoin -virtuaalirahaa ja uhkasi paljastaa arkaluonteisia kuvia uhrista. Kaikki viestin väitteet ovat huijausta, ja kiristäjä on lähettänyt saman uhkauksen tuhansille vastaanottajille. Väitettyjä kuvia ei ole olemassakaan.

Haittaohjelmat ja haavoittuvuudet

- Microsoft SharePoint -tuotteeseen kohdistunut haavoittuvuus CVE-2025-53770, jota on hyväksikäytetty laajalti globaalisti.
- Citrix NetScaler -tuotteissa olevien haavoittuvuuksien CVE-2025-5777 ja CVE-2025-5349 hyväksikäyttöä on havaittu edelleen maailmalla.
- Android.BadBox2 -haittaohjelmaa havaitaan edelleen Suomen verkkoliikenteessä. Haittaohjelma vaikuttaa Android-pohjaisiin älylaitteisiin ja liittää laitteita osaksi bottiverkkoa.

Automaatio ja IoT

- Radiolaitedirektiivin (RED) helmikuussa 2022 voimaan astuneen kybersäädöksen soveltaminen alkoi 1.8.2025.
- Säädös asettaa ensimmäiset pakolliset kyberturvallisuusvaatimukset verkkoon liitettäville langattomille laitteille EU:ssa. Vaatimustenvastaiset tuotteet voidaan vetää markkinoilta.
- Traficom vastaa säädöksen markkinavalvonnasta Suomessa.

Verkkojen toimivuus

- Venäjämielistä NoName057(16)-haktivistiryhmää vastaan toteutettiin kansainvälinen poliisioperaatio, jossa tehtiin pidätysmääräyksiä, etsintöjä ja takavarikoita sekä suljettiin rikollista IT-infrastruktuuria. [1]
- Onnistuneesta operaatiosta huolimatta NoName057(16) on jatkanut toimintaansa heinäkuun aikana.

Vakoilu

- SharePointin haavoittuvuuksia on hyödynnetty myös Suomessa tietomurroissa ja niiden yrityksissä.
- Microsoftin mukaan sekä APT-toimijat että rikolliset ovat hyödyntäneet haavoittuvuutta.
- Britannia on asettanut pakotteita Venäjän sotilastiedusteluun yhdistetyille tahoille. Myös EU ja NATO ovat tuominneet Venäjän toimet.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Euroopan turvallisuus- ja yhteistyöjärjestön (ETYJ) Helsinki +50 -juhlakonferenssi järjestettiin 31.7. Finlandiatalolla. [3] Kyberturvallisuuskeskus seurasi kyberturvallisuustilannetta tapahtuman ajan. Konferenssipäivä ja sitä edeltänyt viikko olivat rauhallisia, eikä merkittäviä poikkeamia havaittu.

Suomessa tehtiin heinäkuun lopulla useita havaintoja aggressiivisesta kiristysviestikampanjasta. Pornokiristysteemaisia viestejä on lähetetty yksityishenkilöille ja organisaatioille, ja niissä vaaditaan maksua bitcoineissa. Viestin otsikkona on usein ”yhteistyötarjous” ja lähettäjän sähköpostiosoitteeksi on väärennetty vastaanottajan sähköpostiosoite. [4] Kyseessä on huijaus, eikä hyökkääjällä ole pääsyä laitteelle.

Microsoft SharePoint-palvelussa on havaittu vakava haavoittuvuus, joka vaikuttaa paikallisiin SharePoint Server -tuotteisiin. Haavoittuvuutta on hyväksikäytetty maailmanlaajuisesti. [5]

Heinäkuun kyberturvallisuuden yleiskuva

Heinäkuu alkoi kyberturvallisuuden kannalta rauhallisesti, säätilanteen heikentyessä kuun loppua kohden:

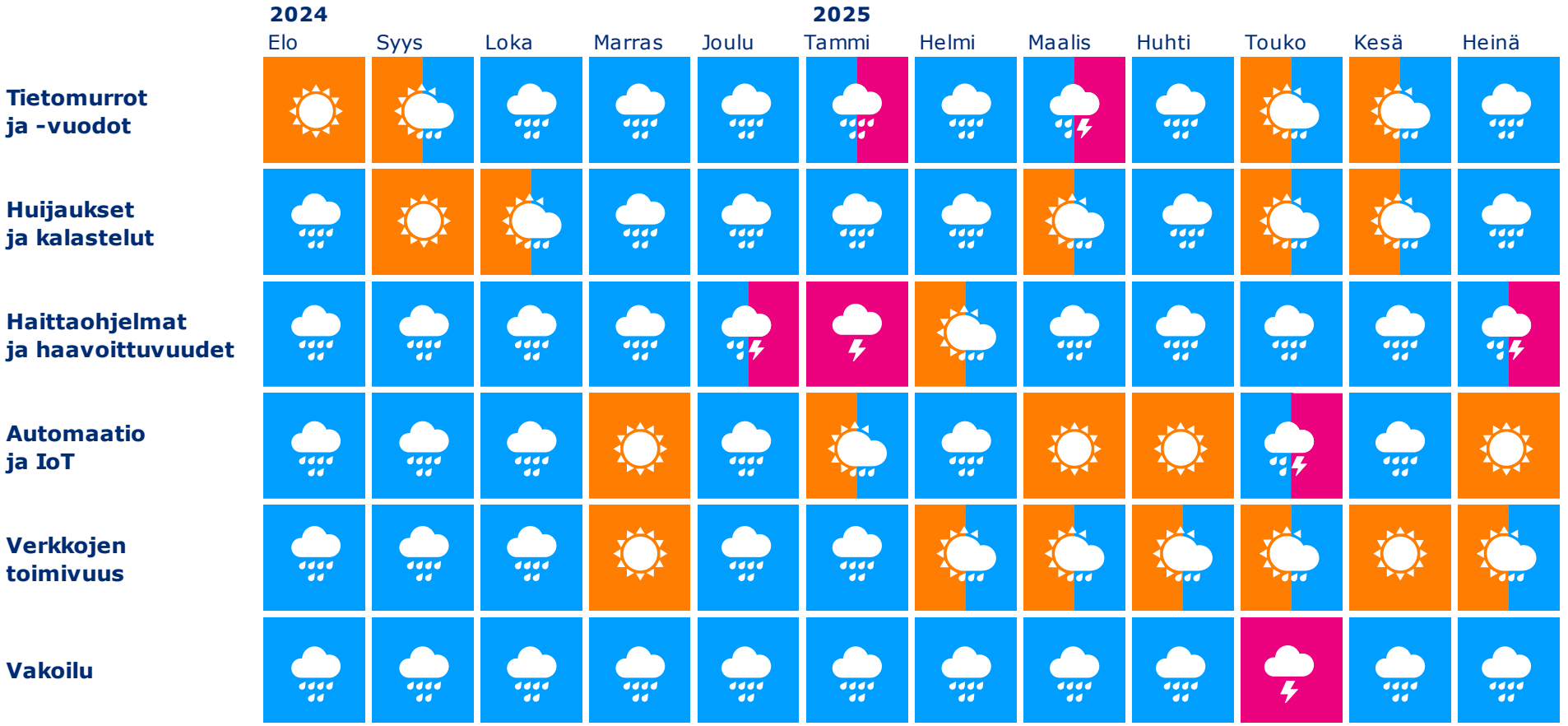
- Kuukauden aikana havaittiin tietomurtoja, jotka heikensivät kyberturvallisuuden yleiskuvaa aiempiin kesäkuukausiin nähden.
  - Suomessa tietomurtoja kohdistui muutamiin eri sektoreilla toimiviin yrityksiin. Murtojen yhteydessä onnistuttiin anastamaan henkilötietoihin lukeutuvaa dataa. Valtaosassa tapauksista dataan ei kuitenkaan ole sisältänyt kaikkein arkaluontoisimpia tietoja, kuten henkilötunnuksia.
- Vakavat globaalit haavoittuvuudet edesauttoivat erilaisia kyberhyökkäyksiä.
  - Heinäkuun aikana Microsoftin SharePoint-palvelussa havaittiin vakava haavoittuvuus, jota on hyväksikäytetty maailmanlaajuisesti. Haavoittuvuus koskettaa paikallisesti toimivia SharePoint Server-palvelua, eikä vaikuta pilvipohjaiseen versioon. [6]
  - Haavoittuvuutta on hyväksikäytetty merkittävissä tietomurroissa ympäri maailman. Haavoittuvuuden hyväksikäyttö näkyy myös noin 70-80 % osassa heinäkuun kansallisia tietomurtotapauksia.
- Hyökkääjät käyttävät Microsoft 365:n Direct Send -ominaisuutta lähettääkseen viestejä, jotka näyttävät tulevan organisaation sisältä. Menetelmä mahdollistaa sähköpostin roskapostisuodattimen ja sääntöjen kiertämisen. Suosituksena on tarkistaa Reject Direct Send -toiminnon asetukset, ja käyttää tiukkoja SPF/DMARC-määrityksiä sekä monivaiheista tunnistautumista.
- Haittaohjelmiin liittyvät havainnot tasoittuivat hieman kesäkuuhun verrattuna.
  - BadBox 2.0-haittaohjelmahavainnot tasoittuivat kesäkuun jälkeen. Haittaohjelman muodostama uhka ei ole kuitenkaan poistunut, sillä Googlen mukaan haittaohjelma on saastuttanut jopa 10 miljoonaa laitetta maailmanlaajuisesti.

Ilmiöiden ja toimialojen trendit

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä eri aikaväleillä. Toimialakohtaisissa nostoissa on esitelty eri toimialojen tilannetta yleistasolla.

Kyberturvallisuuden trendit
kulunut 12 kk

1 kk



Pitkä aikaväli ja lähitulevaisuus

Osiossa on esitelty pitkän aikavälin ja lähitulevaisuuden kyberturvallisuuden ilmiöitä. Seuraamiemme pitkän aikavälin ilmiöiden joukosta analysoidaan kuukausittain yksi ilmiö. Top 5 –kyberuhkat kertovat puolestaan lähitulevaisuuden uhkista.

Pitkän aikavälin (5v+) kybersää: ilmiöt joita seuraamme

Pitkän aikavälin kybersää: Infrastruktuurin kyberfyysinen turvallisuus

Infrastruktuurin kyberfyysinen turvallisuus säilyy merkittävänä kokonaisuutena myös tulevaisuudessa.

- Tietoliikenteen kannalta merkittäviä fyysisiä poikkeamia on tapahtunut viimeisen kahden vuoden aikana useita. Suomen merenalaiseen tietoliikenneinfrastruktuuriin kohdistuneet vauriotapaukset korostuivat talvella ja vuodenvaihteessa, mutta laivojen aiheuttamat kaapelivauriot ovat tauonneet tammikuun jälkeen. Suomea koskettavia merkittäviä tapauksia ei ole sattunut kevään tai kesän aikana.
  - Suomen ja Ruotsin aktiivinen puuttuminen vauriotapauksiin, yhdistettynä Naton tammikuussa käynnistämään valvontaoperaatioon, ovat saattaneet edesauttaa tapausten hiipumista. [7]
  - Viranomaisten kyky puuttua poikkeamiin on ollut hyvä, ja tapauksiin liittyen on nostettu myös rikossyyteitä. [8]
  - Raskaamman ja hankalasti saavutettavan infrastruktuurin korjaaminen on usein hankalaa ja kallista: Eagle S -aluksen aiheuttamien kaapelivaurioiden korjaaminen kesti kuukausia ja maksoi arviolta 60 miljoonaa euroa. [9]
- Erilaiset vahingot ja sään ääri-ilmiöt aiheuttavat myös haittaa tiedonsiirrolle. Maa-alueilla tietoliikennekaapeleita katkeaa tyypillisimmin juuri luonnonilmiön, tai maanrakennuksen yhteydessä tapahtuneen vahingon seurauksena.
- Infrastruktuurin turvaaminen on korostunut Euroopassa ja muualla maailmassa. Kriittiseen infrastruktuuriin lukeutuvat tietoliikenne- ja teleyhteydet ovat myös valtiollisten toimijoiden jatkuvan kiinnostuksen kohteena.
- Harmittomammatkin ilmiöt saattavat aiheuttaa merkittävää haittaa:
  - Ajattelemattomat tempaukset ja sosiaalisen median haasteet saattavat tietoliikenteen häiritsemisen lisäksi aiheuttaa vaaraa ihmisille. Esimerkiksi muuntamoihin murtautuminen tai telemastoihin kiipeäminen voi olla hengenvaarallista. Tapausten turvallinen ratkaiseminen saattaa edellyttää järjestelmien sammuttamista, mikä ilmenee paikallisina palvelukatkoksina.

Top 5 uhat lähitulevaisuudessa (6kk–2v)

1.

Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

Haavoittuvuuden korjaavan päivityksen asentamisen lisäksi on usein tarpeen tutkia, onko haavoittuvuutta hyödynnetty jo ennen päivityksen asentamista.

2.

Toimitus- ja palveluketjujen tietoturva ja jatkuvuus ovat yhä kriittisempiä.

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.

3.

Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa.

Organisaatioiden olisi hyvä tunnistaa tekoälyn tuomia haasteita, ja varautua niihin esimerkiksi kouluttamalla henkilöstöään.

Symbolit

Uusi

Päivitetty

4.

Kiristyshaittaohjelmat -Merkittävä uhka organisaatioille

Viimeisen vuoden aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi, ja niiden määrä kasvaa jatkuvasti myös globaalisti.

5.

Tietoliikenneinfran suojaamisen tärkeys korostuu

Tietoliikenne- ja tietojärjestelmäinfran suojaaminen maailmalla ja kotimaassa on tärkeää, sekä siihen kohdistuvien vahinkojen ja luonnonilmiöiden että ulkopuolisten aiheuttamien tahallisten häiriöiden takia.

1. Vakavia haavoittuvuuksia hyödynnetään yhä nopeammin

- **Voimassa oleva kyberkestävyyssäädös (Cyber Resilience Act, CRA) asettaa sovellusalaan lukeutuville toimijoille velvoitteita haavoittuvuuksien hallintaan. Vaatimuksia tullaan tarkentamaan parhaillaan työn alla olevassa harmonisoidussa standardissa ja niiden soveltaminen alkaa 30.8.2026.** [10]
- Verkon reunalaitteet muodostavat merkittävän rajapinnan hyökkäyksille. Reunalaitteiden kirjo on laaja, ja niihin lukeutuvat muun muassa palomuurit ja VPN-laitteet. Organisaatioiden tulisi parhaansa mukaan pysyä selvillä käyttämänsä järjestelmäkokonaisuuden osista ja niiden päivitystarpeista. Hyökkääjät etsivät aktiivisesti haavoittuvuuksia esimerkiksi ohjelmistopäivitysten muistioista, mikä altistaa päivittämättömiä laitteita hyökkäyksille.
- Uhkien hallinnassa korostuvat sekä havainnointi että reagointikyky. Järjestelmäympäristön valvonta edistää hyökkäysten rajoittamista, mutta organisaatioilla tulee myös olla suunnitelma hyökkäyksestä ja sen vaikutuksista palautumiseen.
- Monien merkittävien laitevalmistajien verkon reunalaitteissa, kuten VPN-yhdyskäytävissä, on havaittu vakavia ja helposti hyödynnettäviä haavoittuvuuksia viimeisen vuoden aikana.
- Rikolliset pyrkivät hyväksikäyttämään haavoittuvuuksia jo ennen kuin niitä on ehditty korjata. Haavoittuvuuden aktiivinen hyväksikäyttö saattaa usein tapahtua jo ensimmäisen vuorokauden sisällä siitä, kun haavoittuvuudesta on tullut julkinen.
  - Järjestelmien nopea päivittäminen on erityisen tärkeää ja valmius päivittämiseen on syytä ylläpitää jatkuvasti, myös yleisinä loma-aikoina.
- Haavoittuvuuksien hallinta on haastavaa, mikäli organisaatio ei tunne ympäristöään. Järjestelmien kartoitus ja dokumentointi on syytä tehdä säännöllisesti.
  - Haavoittuvia palveluita näkyy monesti myös julkisesti verkkoon. Organisaatioiden olisikin hyvä myös tarkastella omia palveluitaan säännöllisesti ja varmistaa, että mahdollisuuksien mukaan palveluita ei olisi näkyvissä julkisesti verkkoon.

2. Toimitus- ja palveluketjujen tietoturva ja jatkuvuus on yhä kriittisempää

- Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista.
  - Toimitusketjuihin liittyvä uhka ei kohdistu pelkästään komponentteihin, vaan saattaa myös konkretisoitua esimerkiksi ohjelmistojen ja ohjelmointikirjastojen kautta.
  - Maailmalla uutisoidaan jatkuvasti toimitusketjuihin kohdistuvista kyberuhista sekä niissä havaituista heikkouksista. **Viimeisimpänä lisäyksenä trendiin voidaan pitää kesäkuussa Suomessakin yleistynyttä BadBox 2.0 -haittaohjelmaa, jota on esiasennettu tuntemattomien valmistajien halpoihin laitteisiin.**
- Kyberturvallisuuskeskukselle ilmoitetuissa tapauksissa vaikuttaa usein siltä, että alihankintaketjuihin liittyvät vastuut ovat organisaatioille epäselviä. Vastuut olisikin hyvä määritellä aina siten, että poikkeamatilanteessa olisi selvää, mitä vastuunjaoista on sovittu.
  - Toimintakulttuurilla ja prosesseilla on suuri merkitys uhkien havaitsemisessa, tunnistamisessa ja tiedon jakamisessa.
- Organisaatioiden on keskeistä ymmärtää omat alihankkijaketjunsa ja olla tietoisia sopimusyksityiskohdista palveluntarjoajien kanssa. On tärkeä selvittää kolmannen osapuolen tietoturvan taso ja ulottaa tietoturvallisuuden hallinta myös palveluihin, kattaen esimerkiksi:
  - Konsultit ja heidän organisaatioidensa sisäiset järjestelmät.
  - Laitteistot ja palvelut, joita voidaan käyttää joko osana omaa tuotetta, palvelukokonaisuutena tai ostettuna palveluna.
  - Organisaation tulee ymmärtää koko alihankintaketju, koska myös organisaation alihankkija voi hankkia tuotteen/palvelun seuraavalta ketjussa olevalta palveluntarjoajalta.

3. Tekoälyn tuomiin haasteisiin on hyvä varautua organisaatioissa

- **Erilaiset tekoälysovellukset saattavat aiheuttaa uusia ja yllättäviä tietoturvauhkia organisaatioille. Osin automaattisesti toimivat sovellukset ja avustajat saattavat esimerkiksi videoneuvottelun yhteydessä käsitellä dataa, jonka käyttöä kaikki osallistujat eivät ole hyväksyneet. Sovelluksilla saattaa myös olla laaja pääsy organisaation dataan. Riskit korostuvat, jos sovellus säilyttää tai käsittelee dataa organisaation ulkopuolisella palvelimella.** [11]
- **Viimeaikainen kehitys viittaa siihen, että uhkatoimijat käyttävät yhä aktiivisemmin tekoälypalveluita haittaohjelmien ja hyökkäysten jalostamiseen. Tekoälyä voidaan hyödyntää esimerkiksi kalasteluviestien laatimiseen, tai haittaohjelmakoodin tulkittavuuden hankaloittamiseen (obfuscation).**
- Organisaatioiden on hyvä ottaa huomioon erityisesti tietosuoja- ja salassapitonäkökulmat tekoälyn mahdollisessa käytössä, ja pohtia näihin liittyviä linjauksia organisaation sisällä.
  - Tekoälyn käyttöön tulisi laatia organisaation sisäinen käyttöpolitiikka ja ohjeistus henkilöstölle siitä, miten tekoälyä voi sallitulla tavalla hyödyntää työssä.
  - Iso-Britanniassa laaditun selvityksen mukaan noin viidesosassa paikallisista yrityksistä on paljastunut mahdollisesti sensitiivisen tiedon vaarantuneen henkilöstön tekoälyn käytön seurauksena.
- Syväväärennöksien eli ns. deepfake-tekniikan käytöstä osana kyberrikoksia on puhuttu kansainvälisessä uutisoinnissa.
  - Syväväärennösten tekeminen voi näyttäytyä rikollisille houkuttelevana tapana huijata organisaation työntekijöitä tai aiheuttaa mainehaittaa.
  - Kyberturvallisuuskeskukselle tehtyjen yksittäisten ilmoitusten valossa suomenkielisien syväväärennöksien käyttö ei kuitenkaan vaikuta olevan vielä kovinkaan yleistä.

4. Kiristyshaittaohjelmat - Merkittävä uhka organisaatioille

- **Kiristyshaittaohjelmien määrä kasvaa jatkuvasti globaalisti, ja ilmiö ja siihen liittyvä palvelutuotanto on jatkuvassa kehityksessä.**
  - Akira on viimeiset kaksi vuotta ollut Kyberturvallisuuskeskukselle eniten ilmoitettu kiristyshaittaohjelma. Sen lisäksi on raportoitu useita kiristyshaittaohjelmia, joita ei ole ennen havaittu Suomessa.
- **Kiristysluontoisissa hyökkäyksissä salaavia haittaohjelmia on tavattu aiempaa vähemmän. Viimeaikoina kansainvälisesti kiristyshyökkäyksissä on korostunut tiedostojen salaamisen sijaan datan nopea varastaminen kohdejärjestelmästä, jolloin kiristäjä lupaa lunnaita vastaan hävittää varastetun aineiston, tai jättää sen julkaisematta. Tietoturvayhtiö Sophoksen tutkimuksen mukaan vuonna 2025 tiedostoja on salattu vain 50 prosentissa tapauksista [12].**
- Kiristyshaittaohjelmien muodostama uhka on säilynyt ennallaan, vaikka KTK:lle ilmoitetut tapausmäärät ovat olleet viime vuosina laskusuunnassa. Kiristyshaittaohjelma saattaa pahimmassa tapauksessa lopettaa organisaation toiminnan kokonaan. Hyökkäys voi kohdistua myös toimitusketjuun ja levitä sitä kautta nopeasti useisiin organisaatioihin samalla kertaa. Varsinkin huoltovarmuuskriittisten organisaatioiden joutuessa uhriksi voivat yhteiskunnan elintärkeät toiminnot vaarantua.
- Organisaatioiden tulee ottaa kiristyshaittaohjelmahyökkäykset ja niistä palautuminen huomioon varautumisessa ja harjoitustoiminnassa.
- Kiristyshaittaohjelma tartutetaan usein kalasteluviestin, vuotaneiden käyttäjätunnusten tai päivittämättömien haavoittuvuuksien kautta. Erityisesti verkon reunalaitteiden päivityksistä ja käyttäjätunnusten monivaiheisesta tunnistautumisesta on syytä pitää huolta. Tiedostojen salaus ja muut hyökkääjän tekemät toimenpiteet saatetaan toteuttaa viipymättä sisäänpääsyn jälkeen, joten ennaltaehkäisy, havainnointi ja nopea reagointi ovat avainasemassa.
- Osa kiristyshaittaohjelmista pyrkii etsimään ja tuhoamaan myös kohteensa varmuuskopiot, joten ainakin yksi varmuuskopio tulee säilyttää poissa verkosta. Kyberturvallisuuskeskuksen tiedossa olevista kiristyshaittaohjelmasta palautuneista organisaatioista suurin osa palautui varmuuskopioiden avulla.

5. Tietoliikenneinfrastruktuurin suojaamisen tärkeys korostuu

- Sekä Suomessa että maailmalla on vuoden mittaan tapahtunut tietoliikenneinfrastruktuuriin kohdistuneita vahinkoja ja luonnonilmiöitä, sekä ulkopuolisten tekijöiden aiheuttamia tahallisia häiriöitä.
- Kaikkien tietoliikenne- ja tietojärjestelmäinfrastruktuurin omistajien kannattaa huolehtia siitä, että viestintäverkon tai -palvelun komponentit on suojattu fyysisesti siten, etteivät asiattomat pääse niihin helposti käsiksi.
  - Suomessa julkinen sektori on varautunut vastaaviin häiriötilanteisiin.
  - Yksityisen sektorin toimijoiden on syytä pohtia häiriötilanteisiin varautumista. Häiriönsietoa voidaan parantaa esimerkiksi kahdentamalla kriittisiä järjestelmiä ja yhteyksiä, sekä varmistamalla niiden sähkönsaanti lyhyen sähkökatkoksen varalta.
- Yleisen teletoiminnan osalta Liikenne- ja viestintävirasto Traficomin määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista asettaa vaatimukset laitetilojen ja siirtoteiden suojaamiselle yleisen viestintäverkon ja palvelujen komponenttien tärkeysluokkien perusteella. Tärkeysluokitus perustuu viestintäpalvelun tyyppiin sekä maantieteelliseen alueeseen tai käyttäjämäärään, johon viestintäverkon tai -palvelun komponentti vaikuttaa.
  - Fyysisen suojauksen lisäksi tärkeää on myös se, että itse laitetilojen rakenne täyttää määräyksen velvoitteet, ja että niissä on vaadittava ajantasainen kulunvalvonta, ja että niistä saadaan asianmukaiset hälytykset valvontahenkilöstölle.
- Pelkkä vahinkojen korjaaminen ei riitä. Häiriöiden ja niistä kerätyn informaation perusteella on tarpeen miettiä myös toimenpiteitä, joilla voidaan parantaa suojaustasoa.
  - Suojaustason parantamiseksi Traficom sekä teleoperaattorit tekevät yhteistyötä, jotta esimerkiksi kotimaassa tapahtuneiden vahinkojen ja muiden häiriöiden määrää voitaisiin edelleen vähentää.

Tietoturva-alan kehitys, sääntely ja standardit

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.

Oikeudelliset asiat

Hallituksen esitys eduskunnalle sähköisestä tunnistamisesta, luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä annettua EU:n asetusta täydentäväksi lainsäädännöksi [13]

- Euroopan parlamentti ja neuvosto antoivat 11.4.2024 asetuksen (EU) 2024/1183 (n. eIDAS-muutosasetus). eIDAS-muutosasetus on sellaisenaan jäsenvaltioissa sovellettavaa oikeutta, mutta jättää myös jäsenvaltioille kansallista liikkumavaraa.
- Tavoitteena on varmistaa oikeus digitaaliseen identiteettiin, joka on käyttäjän yksinomaisessa määräysvallassa. Tarkoituksena on varmistaa, että jäsenvaltioiden rajat ylittäviin asiointitilanteisiin on saatavilla turvallisia ja luotettavia sähköisiä identiteettiratkaisuja, niin käyttäjien kuin asiointipalvelujen näkökulmasta. Tavoitteena on myös vähentää riskejä ja kustannuksia omaksumalla yhdenmukaisempi lähestymistapa sähköiseen tunnistamiseen. Luottamuspalvelujen osalta tavoitteena on varmistaa yhtäläiset edellytykset luottamuspalvelujen tarjoamiseen ja niiden hyväksymiseen jäsenvaltioissa.
- Velvoitteina jäsenvaltioille on digitaalisen identiteetin lompakon tarjoaminen, kansallisen valvontaelimen ja kansallisen yhteyspisteen nimeäminen, jotka edellyttävät kansallista täydentävää lainsäädäntöä.
- Esityksessä ehdotetaan lisäksi muun muassa lompakon kanssa ensimmäisen yhteensopivan sähköisen todistuksen toteuttamista Suomessa, joka olisi poliisin tuottama digitaalinen henkilöllisyystodistus.
- Hallituksen esityksen lisäksi on laadittu kuvaus kansallisesta eurooppalaisen digitaalisen identiteetin lompakoiden ekosysteemistä. Kuvauksen tarkoituksena on antaa käytännönläheinen yleiskuva lompakon ympärille syntyvistä tehtävistä ja rooleista sekä hyödyntämisen edellytyksistä ja eduista.
- Lausunnot pyydetään antamaan viimeistään 29.8.2025.
- Linkki: **https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=7d7e6aee-7801-4bba-961f-35e7ddc98b83**

Oikeudelliset asiat

Euroopan komissio on julkaissut EU:n avaruusasetusehdotuksen (EU Space Act) [14]

- Asetuksen tarkoituksena on yhtenäistää eurooppalainen avaruussääntely, lisätä toiminnan turvallisuutta avaruudessa, lisätä avaruustoiminnan resilienssiä ja kyberturvallisuutta sekä luoda yhtenäinen tapa arvioida avaruustoiminnan ympäristövaikutuksia.
- Asetusehdotusta voi kommentoida kahdeksan viikon ajan siitä, kun käännökset siitä ovat valmistuneet. [15]

- **Euroopan unionin virallisessa lehdessä on 30.7.2025 julkaistu seitsemän kesäkuussa hyväksyttyä komission täytäntöönpanoasetusta liittyen eIDAS-asetuksen täytäntöönpanoon.** [16]
  - Asetukset liittyvät pääosin luottamuspalveluihin. Asetukset tulevat voimaan 19.8.2025, tosin osalla on siirtymäaikaa 4 kk, 12 kk sekä 24 kk ja soveltaminen alkaa siten myöhemmin. Loput kesäkuussa hyväksytyistä 13 täytäntöönpanoasetuksesta julkaistaan syyskuun aikana.
  - Asetukset antavat tarkempia ohjeita liittyen mm. valvontaelinten toimintaan, luottamuspalvelujen ilmoittamiseen, vertaisarviointeihin ja teknisiin yksityiskohtiin.

Oikeudelliset asiat

Liikenne- ja viestintäviraston verkkotunnusmääräys M68 on päivitetty. Määräys astuu voimaan 18.8.2025. [17]

- Liikenne- ja viestintävirasto Traficom on antanut päivitetyn verkkotunnusmääräyksen M 68, joka korvaa vuoden 2016 määräyksen. Uudistuksen taustalla on muuttunut lainsäädäntö ja toimintaympäristö, erityisesti NIS 2 -direktiivi.
- Verkkotunnusjärjestelmä on tunnistettu kriittiseksi infrastruktuuriksi, jonka ylläpitäminen ja säilyttäminen luotettavana, häiriönsietokykyisenä ja turvallisena on keskeistä internetin eheyden säilymisen kannalta ja olennaisen tärkeää internetin jatkuvalle ja vakaalle toiminnalle.
- Määräyksen merkittävimmät muutokset liittyvät verkkotunnusvälittäjien lisääntyviin tiedonantovelvollisuuksiin sekä verkkotunnusten käyttäjien tietojen oikeellisuuden varmistukseen. Muutosten myötä valvovan viranomaisen ja käyttäjien tiedonsaanti parantuu. Määräysmuutoksen myötä virheellisten tietojen määrä verkkotunnusrekisterissä arvioidaan vähenevän.
- Linkki:

Oikeudelliset asiat

EU:n radiolaitedirektiivi asettaa vaatimukset erilaisille langattomasti radiotaajuuksilla toimiville laitteille. [18, 19]

- Uusi asetus 2022/30 koskien RED:n artikloja 3(3)(d/e/f) on annettu. Asetuksessa tietyille RED:n soveltamisalaan kuuluville laitteille, kuten internetiin liitettäville laitteille, leluille, lastenhoitoon liittyville laitteille ja päälle puettaville laitteille, asetetaan tietoturvallisuusvaatimuksia.
- Uusilla vaatimuksilla suojataan verkkoja, parannetaan käyttäjien yksityisyyden suojaa ja pienennetään sellaisten taloudellisten petosten riskiä, joissa hyödynnetään verkkoon liitettyjä laitteita.
- Asetuksessa on annettu siirtymäaika laitevalmistajille. Tietoturvavaatimusten soveltamisen aiottu aloitusaika oli 1.8.2024. Euroopan komissio on nyt siirtänyt soveltamisen määräpäivää vuodella, jotta tietoturvavaatimusten teknisten standardien valmisteluun saadaan enemmän aikaa.
- EU-markkinoille saatettavien radiolaitteiden tulee olla tietoturvavaatimusten mukaisia 1.8.2025 alkaen.

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

Lähdeluettelo

1) Poliisi mukana kansainvälisessä lainvalvontaviranomaisten NoName057(16)-hakkeriryhmään kohdistuvassa yhteisoperaatiossa https://poliisi.fi/-/poliisi-mukana-kansainvalisessa-lainvalvontaviranomaisten-noname057-16-hakkeriryhmaan-kohdistuvassa-yhteisoperaatiossa
2) Global operation targets NoName057(16) pro-Russian cybercrime network https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network
3) Helsinki+50-konferenssi korostaa kansalaisyhteiskunnan roolia https://um.fi/ajankohtaista/-/asset_publisher/gc654PySnjTX/content/helsinki-50-konferenssi-korostaa-kansalaisyhteiskunnan-roolia
4) Aggressiivinen kiristysviestikampanja käynnissä https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/aggressiivinen-kiristysviestikampanja-kaynnissa
5) Kyberturvallisuuskeskuksen viikkokatsaus - 30/2025 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-302025#88813-0
6) Joint Statement on SharePoint vulnerabilities - Assessment and advice on recovery and mitigating actions https://www.enisa.europa.eu/news/joint-statement-on-sharepoint-vulnerabilities-assessment-and-advice-on-recovery-and-mitigating-actions
7) NATO launches 'Baltic Sentry' to increase critical infrastructure security https://www.nato.int/cps/en/natohq/news_232122.htm
8) Eagle S:n kapteenia ja perämiehiä syytetään rikoksista: tästä on kyse https://yle.fi/a/74-20176846
9) Eagle S:n kapteenia ja perämiehiä syytetään törkeistä rikoksista – Suomelle miljoonavahingot https://www.is.fi/kotimaa/art-2000011420227.html
10) Kyberkestävyyssäädös (Cyber Resilience Act, CRA) https://kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra
11) Ole valppaana tekoälyn kanssa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ole-valppaana-tekoalyn-kanssa
12) Sphos - The state of Ransomware 2025https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2025.pdf
13) Luonnos hallituksen esityksestä eduskunnalle sähköisestä tunnistamisesta, luottamuspalveluista ja eurooppalaisesta digitaalisesta identiteetistä annettua EU:n asetusta täydentäväksi lainsäädännöksi https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=7d7e6aee-7801-4bba-961f-35e7ddc98b83
14) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the safety, resilience and sustainability of space activities in the Union https://defence-industry-space.ec.europa.eu/document/download/0adeee10-af7a-4ac1-aa47-6a5e90cbe288_en?filename=Proposal-for-a-Regulation.pdf
15) EU Space Act – new rules for safe, resilient and sustainable space activities https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13971-EU-Space-Act-new-rules-for-safe-resilient-and-sustainable-space-activities_en
16) Official Journal L series daily view, 30 July 2025 https://eur-lex.europa.eu/oj/daily-view/L-series/default.html?&ojDate=30072025
17) Verkkotunnusmääräys M 68 https://www.finlex.fi/fi/viranomaiset/maarayskokoelmat/traficom-viestinta/2025/51219
18) KOMISSION DELEGOITU ASETUS (EU) 2022/30 https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32022R0030&from=EN
19) KOMISSION DELEGOITU ASETUS (EU) 2023/2444 https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:L_202302444&qid=1699450603394