TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Joulukuu 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

Kybersää uudistuu 2026

Kybersään ulkoasu ja sisältö päivittyy tammikuun 2026 julkaisusta alkaen. Muutoksilla tavoitellaan aiempaa saavutettavampaa, tasalaatuisempaa ja samalla informatiivisempaa julkaisua.

Asiakaspalaute huomioitiin kehitystyön yhteydessä ja olemme säilyttäneet Kybersään parhaat palat. Näiden ohella luvassa on myös uutta sisältöä ja ennakoivuutta.

Jatkossa julkaisemme laajemmat analyysikalvot, kuten Top 5 -uhkat, osana maaliskuun ja syyskuun Kybersää-julkaisuja.

Kuukauden tunnuslukuja

300 TB

Spotify-musiikkipalveluun kohdistui joulukuussa tietomurto, jonka yhteydessä varastettiin suuri määrä äänitiedostoja. Hyökkääjien mukaan palvelusta olisi anastettu jopa 300 terabittiä dataa, mikä käsittäisi lähes koko palvelun tietokannan. [1]

3

Haavoittuvuuksia raportoitiin joulukuun aikana kohtalaisen paljon. Kyberturvallisuuskeskus julkaisi kuukauden aikana kolme tiedotetta kriittisistä haavoittuvuuksista. Näiden hyväksikäytöstä tehtiin Suomessa joitakin havaintoja. [2]

25

MITRE julkaisi Top 25 -listauksen vuoden 2025 merkittävimmistä ohjelmistoheikkouksista. Listan kärjessä oli edellisvuoden tapaan Cross-site Scripting. [3]

Kybersää joulukuu 2025

Tietomurrot ja -vuodot

- Joulukuu oli rauhallinen tietomurtojen ja -vuotojen suhteen. Marraskuuhun verrattuna ilmoituksia tuli lähes 30 % vähemmän.
- Tietomurroissa näkyivät Ciscon sähköpostiturvatuotteiden ja Reactin React Server Components haavoittuvuuksien hyväksikäytöt.

Huijaukset ja kalastelut

- Majoitusliikkeiltä ja majoituspalveluiden asiakkailta on joulukuun lomakaudella kalasteltu runsaasti. Rikolliset kalastelevat majoituspalvelun tunnukset, joiden avulla kalastellaan maksukorttitietoja.
- Pikaviestipalveluiden tilejä on kaapattu aiempaa enemmän. Tilejä pommitetaan jatkuvilla kirjautumisyrityksillä, tai uhrin numerolle yritetään luoda uusi tili. Vahvistusviestejä ei pidä hyväksyä ja niiden linkkejä ei pidä avata. Omat tilit on syytä suojata kytkemällä päälle monivaiheinen kirjautuminen.

Haittaohjelmat ja haavoittuvuudet

- Kriittinen haavoittuvuus Reactin React Server Components – toiminnallisuudessa (CVE-2025-55182)
- TOTOLINK X5000R -kotireitittimestä löytynyt haavoittuvuus, joka mahdollistaa tietyissä olosuhteissa laitteen kaappaamisen. Haavoittuvuuteen ei ole olemassa korjausta (CVE-2025-13184)
- Kriittinen haavoittuvuus Cisco Secure Email Gateway ja Secure Email and Web Manager –tuotteissa (CVE-2025-20393)

Automaatio ja IoT

- Havaintojemme perusteella OT-järjestelmien etähallintayhteyksiä on toteutettu Suomessa tietoturvattomasti. Syynä ovat mm. etäyhteysratkaisuissa käytettyjen reunalaitteiden oletusasetukset, jotka eivät sovi OT-ympäristöön, koska ne mahdollistavat rajoittamattoman liikenteen Internetin suuntaan.

Verkkojen toimivuus

- Jouluviikolla Venäjä-mielinen NoName kohdisti jälleen palvelunestohyökkäyksiään suomalaisiin kohteisiin. Merkittäviltä vaikutuksilta säästyttiin, mutta hyökkäysten torjunta aiheutti lisätöitä.
- Yhdysvaltojen oikeusministeriö on asettanut NoName-ryhmään yhdistetyn henkilön syytteeseen. Syytteen julkaisussa NoName-ryhmän kerrotaan saaneen rahallista tukea Venäjän valtiolta. [4]
- Suomenlahdella havaitut kaapelivauriot eivät aiheuttaneet merkittäviä vaikutuksia Suomen tietoliikenneyhteyksiin.
- Hannes-myrsky aiheutti useita toimivuushäiriöitä ympäri Suomea.

Vakoilu

- Yhdysvaltojen mukaan Venäjän valtio on länsimaissa kyberhyökkäyksiä ja -häirintää toteuttaneiden Cyber Army of Russia Reborn (CARR)-/Z-Pentest- ja NoName057(16)-haktivistiryhmien taustalla. Myös useat muut maat osallistuivat julkilausumaan. CARR/Z-Pentest yhdistetään Venäjän GRU:hun.
- Myös Tanska ja Saksa ovat syyttäneet julkisesti Venäjää kyberhyökkäyksistä. Palvelunestohyökkäysten lisäksi Tanskassa hyökättiin vesihuoltolaitokseen. Saksassa puolestaan hyökättiin lennonjohtojärjestelmää vastaan sekä yritettiin häiritä vaaleja.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Liikenne- ja viestintävirasto Traficom on uudistanut viestintäverkon kriittisistä osista antamansa määräyksen. Uudistettu määräys laajentaa sääntelyn koskemaan tietyiltä osin myös 5G-verkon tukiasemia. [5]

Pilvipalveluiden pääkäyttäjätunnusten hallinta on tärkeä osa pilvipalveluiden turvallisuutta. Tietoturva Nyt! -artikkelissa *”Pilvipalveluiden pääkäyttäjätunnusten hallinta – parhaat käytännöt”* käymme läpi kolme yleisintä pilvipalvelua – Amazon Web Services (AWS), Microsoft Azure ja Google Cloud Platform (GCP) – ja kerromme, miten niiden pääkäyttäjätunnuksia tulisi suojata ja ylläpitää. [6]

Joulun jäljiltä useissa talouksissa saattaa olla uusia reitittimiä ja muita verkkolaitteita, joiden asetukset on syytä tarkistaa turvallisuuden parantamiseksi. Voit lukea ohjeita reitittimen asetuksista ja turvallisesta kytkennästä ohjeestamme *”Kotiverkon ja reitittimen tietoturva”.* [7]

Joulukuun kyberturvallisuuden yleiskuva

Joulukuu alkoi kyberturvallisuuden näkökulmasta verrattain rauhallisesti, tilanteen kuitenkin heikentyessä hieman kuukauden loppua kohden.

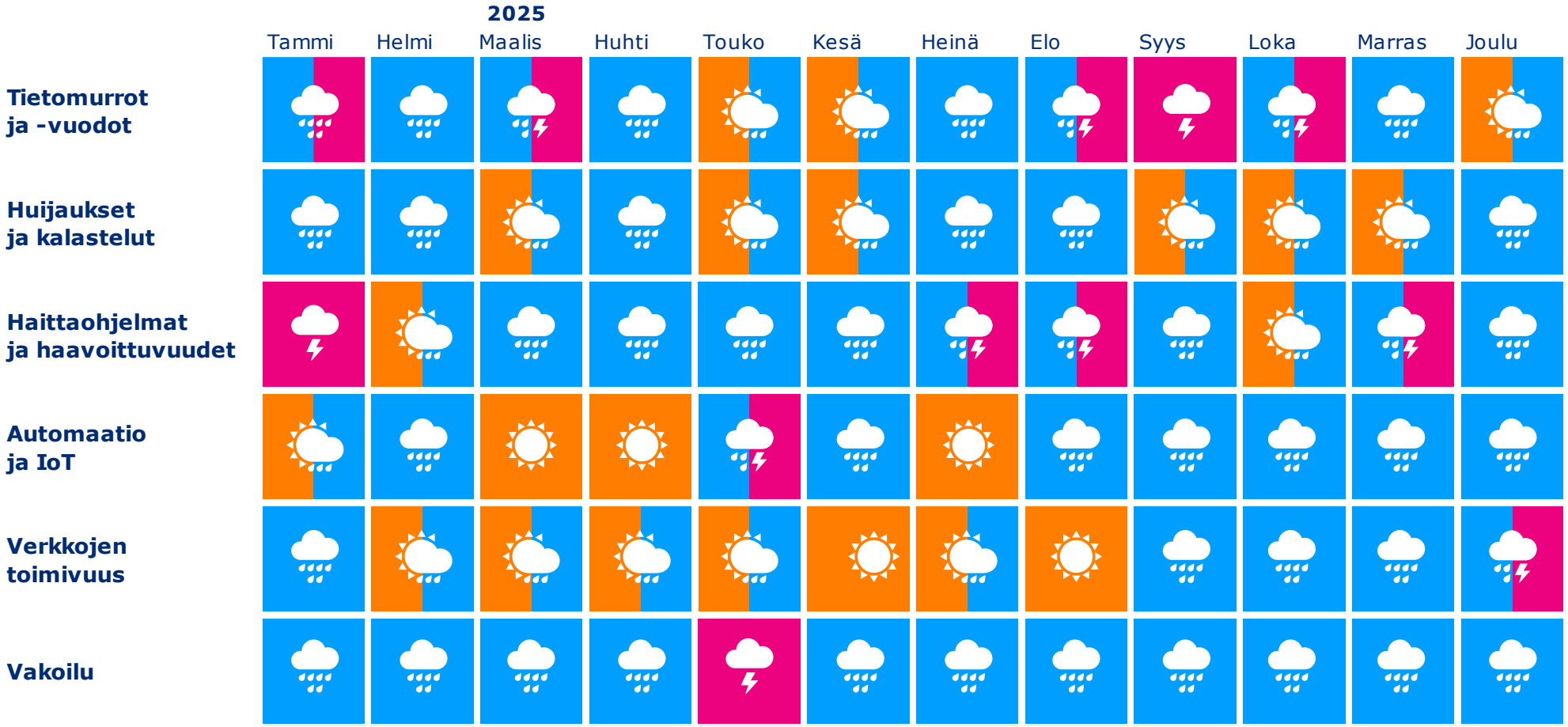
- Kuukauden alussa tehtiin useita ilmoituksia Topline.com -verkkosivulle luoduista valeprofiileista, joiden yhteydessä epäiltiin identiteettivarkauksia. Sivustolle on kopioitu merkittävä määrä LinkedIn-käyttäjäprofiilien tietoja. [8]
- Kriittisiä haavoittuvuuksia raportoitiin kohtalainen määrä. Näistä Ciscon sähköpostiturvatuotteiden haavoittuvuudet ja Reactin React Server Components-toiminnallisuuden haavoittuvuus CVE-2025-55182, eli niin kutsuttu React2Shell, korostuivat kuukauden alkupuolella. [9, 10]
- Uudenvuoden aattona nähtiin jälleen Suomen ja Viron väliseen tiedonsiirtokaapeliin kohdistunut vauriotapaus, jonka seurauksena Fitburg-nimiselle alukselle kohdistettiin moniviranomaisoperaatio. Aluksen epäillään vaurioittaneen ankkurillaan Elisan kaapelia. [11] Tapauksesta ei kuitenkaan aiheutunut merkittäviä vaikutuksia tiedonsiirrolle. [12]
- Vuoden loppupuolen merkittävimpien tapausten joukkoon nousi hieman yllättäen Hannes-myrsky, joka aiheutti sähkökatkoja eri puolilla maata. Ilmatieteen laitoksen mukaan myrsky oli yksi vuosikymmenten pahimmista ja aiheutti sähkökatkoja samanaikaisesti jopa 180 000 asiakkaalle. [13]
  - Voimakkailla luonnonilmiöillä sekä niiden aiheuttamilla katkoksilla ja fyysisillä tuhoilla oli merkittäviä välillisiä vaikutuksia tiedonsiirtoon.

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: Teollisuusautomaation kyberturvallisuus

Teollisuusautomaatioon liittyy keskeisesti OT-järjestelmät (Operational Technology), joilla tarkoitetaan tuotannon fyysisten prosessien reaaliaikaiseen ohjaukseen ja valvontaan käytettäviä laitteita, järjestelmiä ja ohjelmistoja. Häiriöt näissä järjestelmissä voivat pahimmillaan aiheuttaa yhteiskunnan toimintakyvyn vaarantavia, vakavia ja laaja-alaisia poikkeamatilanteita. Viimeaikaisten havaintojen perusteella kolme vakavinta OT-järjestelmiin kohdistuvaa kyberuhkaa ovat haktivismi, vakoilu ja sabotaasi [14]:

- Haktivistien tavoitteena on kohteiden häirintä sekä kerättyjen tietojen hyödyntäminen informaatiovaikuttamisessa.
- Vakoilua voi tapahtua kilpailuedun saavuttamiseksi tai poliittisen tiedonhankinnan tukena.
- Sabotaasin motiviina voi olla taloudellinen hyöty tai valtiollinen vaikuttaminen.

Teollisuusautomaatiota käyttävien sektorien toimintakentät muuttuvat kiihtyvällä tahdilla. Digitalisaatio, tekoälyn hyödyntäminen [15] sekä IT/OT-konvergenssi lisääntyvät ja automaatiojärjestelmät, etähallinta, monitorointi ja tarvittava tieto hajaantuvat entistä enemmän ns. perinteisistä laitosympäristöistä yhä useampiin sijanteihin. Riskinä on, että teollisuusautomaatioympäristöissä ei pysytä kyberturvallisuuden kehityksen perässä ja resurssit [16] eivät ole riittäviä verrattuna IT-maailmaan.

Tiedon määrän, tarvittavien suojattujen ja toimintavarmojen yhteyksien, toimitusketjujen pituuden ja monimutkaisuuden, ympäristöjen kompleksisuuden sekä hyökkäyspinta-ala kasvamisen myötä varautumiseen tulee uudenlaisia haasteita.

- Varautumiseen ja tuotantoympäristöjen turvaamiseen kuitenkin panostetaan entistä enemmän, sääntely ja vaatimukset lisääntyvät, standardeja tulee lisää ja niissä on mietitty alusta asti myös tietoturva-aspekteja.
- EU:n kyberkestävyyssäädös CRA velvoittaa valmistajia laatimaan tuotteille ohjelmistojen materiaaliluettelon eli SBOM:n, jonka käyttöä on edistetty kansainvälisesti. [17] Tämä tulee helpottamaan mm. haavoittuvuuksienhallintaa.

Kyberturvallisuuskeskus tekee yhteistyötä teollisuusautomaation parissa kotimaisissa ja kansainvälisissä verkostoissa, tarjoaa ohjeita ja tukea poikkeamiin sekä kartoittaa Internetiin näkyviä suojaamattomia automaatiojärjestelmiä, kirjautumisikkunoita ja näiden hallintapaneeleita.

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.

Traficomin uudistetulla määräyksellä torjutaan organisaatioiden nimissä lähetettäviä huijausviestejä[18]

- Numeron väärentäminen tekstiviestiä lähetettäessä sekä harhaanjohtavien lähettäjätunnisteiden käyttö on ollut rikollisten laajasti hyödyntämä tekniikka ja merkittävä yhteiskunnallinen ongelma.
- Liikenne- ja viestintävirasto Traficom on uudistanut määräyksensä (28 L/2025 M) viestintäverkkojen ja -palveluiden yhteentoimivuudesta. Uudistettu määräys velvoittaa nyt teleyritykset huolehtimaan viestien lähettäjätietojen oikeellisuudesta ja tunnistamaan lähettäjät luotettavasti. Velvoitteilla ehkäistään kansalaisten riskiä joutua rikoksen uhriksi.
- Uudistettu määräys tulee voimaan 4.5.2026.
- Jotta suomalaisella puhelinnumerolla tai nimimuotoisella tunnuksella lähetetty viestiliikenne voi jatkua, on organisaation uuden määräyksen mukaan luvitettava käyttämänsä numerot ja tunnukset. Määräyksen voimaantulon jälkeen kaikki luvittamattomat viestit joko estyvät tai niiden lähettäjätunnus muutetaan seuraavasti:
  - 4.5.2026 alkaen lähettäjätunnisteeksi muutetaan "Tuntematon”
  - 2.11.2026 alkaen tunnisteeksi muutetaan "Roskaposti".

Traficomin uudistetulla määräyksellä vahvistetaan viestintäverkkojen kriittisten osien turvallisuutta [19]

- Liikenne- ja viestintävirasto Traficom on uudistanut viestintäverkon kriittisistä osista antamansa määräyksen. Viestintäverkon kriittisinä osina pidetään verkon keskeisiä toimintoja ja toimenpiteitä, joilla kontrolloidaan tai ohjataan olennaisella tavalla verkkoon pääsyä ja verkossa kulkevaa liikennettä.
- Verkon kriittisissä osissa ei saa käyttää viestintäverkkolaitetta, jos on painavia perusteita epäillä, että laitteen käyttäminen vaarantaisi kansallista turvallisuutta tai maanpuolustusta. Jos tällaisia perusteita ilmenee, Traficom yhdessä muiden turvallisuusviranomaisten kanssa arvioi asian, ja virasto voi päätöksellään velvoittaa lopettamaan laitteen käytön ja poistamaan sen verkosta, ellei mahdollista uhkaa voida poistaa muilla keinoilla.
- Määräyksessä asetetaan velvoitteita tunnistaa ja dokumentoida viestintäverkkojen kriittiset osat ja niissä käytetyt komponentit. Velvoitteet koskevat teleyritysten yleisten viestintäverkkojen lisäksi myös kriittisiä erillisverkkoja kuten ydinvoimaloiden, satamien sekä lentokenttien ja muiden yhteiskunnalle elintärkeiden toimijoiden yleiseen viestintäverkkoon liitettyjä verkkoja.
- Uudistettu määräys laajentaa sääntelyn koskemaan tietyiltä osin myös 5G-verkon tukiasemia. Teleyritysten on jatkossa tunnistettava 5G-verkon kriittiset osat, kuten tukiasemat, arvioitava niiden keskeisyys ja merkittävyys, sekä dokumentoitava arviot.
- Uusi määräys tulee voimaan 19.12.2026 ja korvaa toukokuussa 2021 annetun aiemman määräyksen.

Euroopan komissio antoi X:lle 120 miljoonan euron sakot digipalveluasetuksen noudattamatta jättämisestä [20]

- Päätös on ensimmäinen, jonka komissio on antanut digipalveluasetuksen (DSA) noudattamatta jättämisestä, ja X:n on korjattava menettelynsä määräajan kuluessa.
- Komissio totesi muun muassa, että X:n käyttämä ns. "blue checkmark" on harhaanjohtava. Käyttäjä voi saada merkistä sellaisen mielikuvan, että sen käyttäjä on varmennettu ja aito, vaikka merkin hankkiminen ei sitä takaakaan. Tämä saattaa mahdollistaa käyttäjien huijaukset siten, että "blue checkmark" käyttäjä tekeytyy joksikin muuksi henkilöksi ja huijaa toisia käyttäjiä esim. sijoituspetoksiin.
- Lisäksi komission päätöksen mukaan X ei anna digipalveluasetuksen mukaista riittävää pääsyä ulkopuolisille tahoille sen mainosvarastoihin. Tutkijoiden tai kansalaisjärjestöjen pääsyllä alustan mainosvarastoihin voidaan edesauttaa esimerkiksi näkyvyyttä siihen, ketkä ovat todellisuudessa mainosten julkaisijoita, ovatko ne niitä tahoja, joiden nimissä mainos väitetään esitettävän vai joku valheellinen taho.
- Digipalveluasetus (DSA) turvaa digipalveluiden, kuten erilaisten verkkoyhteisöjen ja markkinapaikkojen käyttäjän asemaa. Digipalveluasetus parantaa verkon käyttäjien oikeuksia ja tekee verkkoalustojen, kuten somepalvelujen, käytöstä aikaisempaa reilumpaa ja turvallisempaa.

Euroopan komissio on laatinut Kyberkestävyyssäädöstä täsmentävän delegoidun asetuksen, joka tarkentaa jäsenmaiden CSIRT-yksiköiden välisiin haavoittuvuusilmoituksiin liittyviä ehtoja

- Euroopan Unionin Kyberkestävyyssäädöksellä (Cyber Resilience Act, CRA) asetetaan kyberturvallisuuden vähimmäisvaatimukset digitaalisen elementin sisältäville laitteille ja ohjelmistoille, jotka ovat suoraan tai epäsuorasti liitettävissä toiseen laitteeseen tai verkkoon.
- Säädöksen tavoitteena on parantaa EU:n markkinoille saatettujen tuotteiden tietoturvaa niin, että tuotteissa on vähemmän haavoittuvuuksia.
- Säädöksen mukaan EU:n markkina-alueelle asetettujen tuotteiden valmistajien on ilmoitettava tuotteeseen sisältyvistä aktiivisesti hyödynnetyistä haavoittuvuuksista CSIRT-yksikölle ja ENISA:lle 11.9.2026 lähtien.
- Euroopan komissio on 11.12.2025 hyväksynyt delegoidun asetuksen, jossa tarkennetaan puolestaan eri jäsenmaiden CSIRT-yksiköiden välisiin haavoittuvuusilmoituksiin liittyviä ehtoja. Tällaista ilmoittamista voidaan tietyissä tapauksissa lykätä, mikäli se aiheuttaisi tuotteen valmistajalle esimerkiksi tietojen arkaluonteisuuden vuoksi kyberturvallisuusriskin. [21]
- Delegoitu asetus on parhaillaan Euroopan parlamentin ja neuvoston hyväksyttävänä.
- Kyberkestävyyssäädöksen kaikkia tuotteita koskevista horisontaalistandardeista on myös tullut lausuttavaksi haavoittuvuuksienhallintaa käsittelevä osa. Standardista on mahdollista antaa lausunto 12.2. mennessä. [22]

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) Hacktivists claim near-total Spotify music scrape https://www.malwarebytes.com/blog/news/2025/12/hacktivists-claim-near-total-spotify-music-scrape
2) Haavoittuvuudet https://kyberturvallisuuskeskus.fi/fi/haavoittuvuudet?limit=20&offset=0&query=&sort=updated
3) MITRE shares 2025's top 25 most dangerous software weaknesses https://www.bleepingcomputer.com/news/security/mitre-shares-2025s-top-25-most-dangerous-software-weaknesses/
4) Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups https://www.justice.gov/opa/pr/justice-department-announces-actions-combat-two-russian-state-sponsored-cyber-criminal
5) Viestintäverkkojen turvallisuutta vahvistetaan - 5G-tukiasemat sääntelyn piiriin https://www.traficom.fi/fi/ajankohtaista/viestintaverkkojen-turvallisuutta-vahvistetaan-5g-tukiasemat-saantelyn-piiriin
6) Pilvipalveluiden pääkäyttäjätunnusten hallinta – parhaat käytännöt https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/pilvipalveluiden-paakayttajatunnusten-hallinta-parhaat-kaytannot
7) Kotiverkon ja reitittimen tietoturva https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-yksityishenkiloille/kotiverkon-ja-reitittimen
8) Poliisi varoittaa identiteettivarkauksista ja valheellisista myynti-ilmoituksista https://poliisi.fi/-/poliisi-varoittaa-identiteettivarkauksista-ja-valheellisista-myynti-ilmoituksista
9) Kriittinen haavoittuvuus Reactin React Server Components -toiminnallisuudessa https://kyberturvallisuuskeskus.fi/fi/haavoittuvuus_23/2025
10) Kriittinen haavoittuvuus Cisco Secure Email Gateway ja Secure Email and Web Manager –tuotteissa https://kyberturvallisuuskeskus.fi/fi/haavoittuvuus_25/2025
11) Poliisi kuulustellut kaapelirikosta epäillyn Fitburgin miehistöä: ”Kaikilla sellainen rooli tai asema aluksella, joka kytkeytyy vaurioihin” https://yle.fi/a/74-20202336
12) Häiriö Elisan merikaapeliyhteydessä Suomenlahdella https://elisa.fi/asiakastiedotteet/tiedote/h%C3%A4iri%C3%B6-elisan-merikaapeliyhteydess%C3%A4-suomenlahdella/32466413597296/?tag=elisa.fi%3Adisturbance
13) Hannes-myrsky oli vaikutuksiltaan yksi viime vuosikymmenten pahimmista https://www.ilmatieteenlaitos.fi/tiedote/y1raPHX8OP5JXFp48VI4t
14) Kyberturvallisuus OT-järjestelmissä https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/ot_operational%20technology%20ohje.pdf
15) CISA, Australia, and Partners Author Joint Guidance on Securely Integrating Artificial Intelligence in Operational Technology https://www.cisa.gov/news-events/alerts/2025/12/03/cisa-australia-and-partners-author-joint-guidance-securely-integrating-artificial-intelligence
16) OT-ympäristöjen kyberuhkiin varautumisen kehittämisen esiselvitys https://teknologiateollisuus.fi/digipooli/wp-content/uploads/sites/12/2025/02/OT-ymparistojen-kyberuhkiin-varautumisen-esiselvitys.pdf
17) A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity https://www.cisa.gov/resources-tools/resources/shared-vision-software-bill-materials-sbom-cybersecurity
18) Organisaatioiden nimissä lähetettäviä huijausviestejä torjutaan uusilla keinoilla https://www.traficom.fi/fi/ajankohtaista/organisaatioiden-nimissa-lahetettavia-huijausviesteja-torjutaan-uusilla-keinoilla
19) Viestintäverkkojen turvallisuutta vahvistetaan - 5G-tukiasemat sääntelyn piiriin https://www.traficom.fi/fi/ajankohtaista/viestintaverkkojen-turvallisuutta-vahvistetaan-5g-tukiasemat-saantelyn-piiriin
20) Commission fines X €120 million under the Digital Services Act https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934
21) Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/2847 täydentämisestä määrittelemällä ehdot kyberturvallisuuteen liittyvien syiden soveltamiselle lykättäessä ilmoitusten välittämistä https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282025%298407&qid=1765524819538
22) Cybersecurity requirements for products with digital elements. Part 1-3: Vulnerability Handling https://lausunto.sfs.fi/Home/Details/22096