TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Lokakuu 2026

Kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

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

Kybersää voi olla:  rauhallinen  huolestuttava  vakava

Kuukauden tunnuslukuja



Kyberturvallisuuskeskus julkaisi lokakuussa kuusi haavoittuvuustiedotetta. Julkaistujen haavoittuvuuksien määrä on pysynyt korkeana koko vuoden. [1]



M365-tilimurrot ja niiden yritykset ovat organisaatioille pysyvä ongelma. Lokakuussa Kyberturvallisuuskeskukselle raportoitiin edellistä kuukautta merkittävästi enemmän M365-poikkeamia.

Kybersään yleistilanne lokakuussa 2026

Suomessakin salamoivat kansainvälisesti merkittävät poikkeamat

Lokakuun merkittäviin poikkeamiin lukeutui PHP-ohjelmointikielestä löydetyt kriittiset haavoittuvuudet. PHP-ohjelmointikieli toimii maailmanlaajuisesti monien verkkosivustojen ja -palveluiden taustalla. Organisaatioiden suojaustoimenpiteet aiheuttivat laajasti käyttökatkoja verkkopalveluihin. [2]

Euroopassa tehtiin lokakuussa kyberhyökkäyksiä ruokakauppojen kylmälaitteiden säätöjärjestelmiin. Vastaavat hyökkäykset laajenivat marraskuun alussa myös Suomeen. OT-laitteiden tietoturva on ollut jo pidempään pinnalla muun muassa energia- ja vesihuoltosektoreilla tapahtuneiden hyökkäysten vuoksi. [3]

Haavoittuvuuksia julkaistiin edelleen runsaasti.

Synkkiä pilviä tekoälyn hyödyntämisen lisääntyessä huijauksissa

Kyberturvallisuuskeskuksen vastaanottamissa ilmoituksissa ovat yleistyneet videopuheluhuijaukset, joissa esiinnytään poliisina tai pankkien työntekijöinä. Deepfake- eli syväväärennösteknologiaa epäillään hyödynnettävän huijauksissa. Tavoitteena on saada haltuun pankkitunnuksia, maksukorttitietoja ja muita henkilötietoja. [4]

Huijauksissa korostui lokakuussa myös hotelli- ja majoituspalveluiden nimissä lähetetyt huijausviestit. Niissä hyödynnettiin oikeita varausten tietoja, jotka ovat voineet vuotaa majoituspalvelun tai varausjärjestelmän kautta. [5]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen



Lokakuu oli Euroopan kyberturvallisuuskuukausi. EU:n kampanjan tavoitteena on lisätä kansalaisten ja organisaatioiden kyberturvallisuustietoisuutta. Kyberturvallisuuskeskus osallistui kampanjaan jakamalla sosiaalisessa mediassa Nyt valppaana -verkoston kaikille suunnattuja vinkkejä tietoturvaan. [6]



Tekstiviestihuijausten toteuttamista vaikeutettiin Traficomin määräyksellä. Operaattoreiden on 2.11.2026 alkaen muutettava viestin lähettäjätunnus muotoon "Roskaposti" tai estettävä tekstiviesti, jos viestin lähettäjällä ei ole vahvistettua käyttöoikeutta lähettäjätunnukseen. [7]



IoT- ja OT-laitteiden suojaamisen tärkeys on ollut pinnalla etenkin viime kuukausina. Julkaisimme kattavan artikkelin, jossa käydään läpi suojaamisen periaatteita ja viimeaikaisia poikkeamia. [8]

Kuukauden raekuuro
PHP-ohjelmointikielen kriittiset haavoittuvuudet

PHP-haavoittuvuudet muodostivat kansainvälisesti merkittävän poikkeaman

Erittäin laajalti käytössä olevasta verkkopalvelujen toteuttamiseen käytetystä PHP-ohjelmointikielestä löydettiin kriittisiä etäkoodin suorittamisen mahdollistavia haavoittuvuuksia. Haavoittuvuuksia hyväksikäyttämällä hyökkääjä voi onnistua suorittamaan haavoittuvalla palvelimella haluamiaan komentoja ja mahdollisesti ottamaan palvelimen hallintaansa. [9]

Tieto haavoittuvuuksista tuli julki 20.10., ja korjauspäivitykset julkaistiin 21.10.[10] Haavoittuvuuksien julkitulon jälkeen maailmanlaajuisesti jopa miljoonia verkkosivuja suljettiin väliaikaisesti. Haavoittuvuuksille voidaan kehittää hyvin nopeasti hyökkäysmenetelmiä erityisesti haavoittuvuuden korjaavan ohjelmistoversion julkaisun jälkeen.

PHP-haavoittuvuuksia kohtaan esiintyi merkittävää skannausta ja hyväksikäyttöyrityksiä. Ensimmäisiä varmennettuja onnistuneita haavoittuvuuksien hyväksikäyttötapauksia havaittiin maailmalla nopeasti.

Kyberturvallisuuskeskuksella ei ole tiedossa hyväksikäyttötapauksia tai tietomurtoja, jotka olisi tehty Suomessa PHP-haavoittuvuuksia käyttäen. Haavoittuvuuksien hallinta aiheutti kuitenkin käyttökatkoja moniin palveluihin, kun haavoittuvia palveluita suljettiin tai rajoitettiin varotoimenpiteenä.

Haavoittuvuudet muodostivat kansainvälisesti merkittävän poikkeaman, ja niiden potentiaalinen vaikutusalue oli erittäin laaja. PHP:tä käytetään maailmanlaajuisesti lukuisissa verkkopalveluissa, joten haavoittuvuudet koskevat potentiaalisesti monenlaisia organisaatioita ja palveluntarjoajia. Riskipotentiaalia laajentaa se, että PHP:tä voidaan käyttää myös kolmansien osapuolten ohjelmistoissa ja laitteissa. [11]

Kybersään ilmiöt

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä.

Kybersää
lokakuu 2026

1 kk

Tietomurrot- ja vuodot

Tietomurtoilmoitukset lisääntyivät selvästi lokakuussa. WordPress-haavoittuvuuksia hyödynnettiin ClickFix-sisällön levittämiseen, mikä korostaa päivitysten tärkeyttä. Microsoft 365 -tilien tietomurrot lisääntyivät voimakkaasti.

Haittaohjelmat

Lokakuun aikana haittaohjelmia ja niiden levitystä on havaittu muun muassa yksittäisten sähköpostien liitteinä ja ClickFix-tekniikalla murretuilla verkkosivustoilla.

Haavoittuvuudet

Lokakuussa julkaistiin kuusi haavoiituvuustiedotetta.

Haavoittuvuuksien määrän kasvu jatkui ja lokakuun aikana myönnettiin yli 17 000 uutta CVE-tunnistetta, kun lokakuussa 2025 luku oli 4 273.

Huijaukset ja kalastelut

Majoitusvarauspalveluiden, viranomaisten ja pankkien nimissä tehtävien huijausten määrä lisääntyi.

Taistelu tekstiviestihuijauksia vastaan tehostui: rekisteröimättömän lähettäjän nimen paikalla lukee nyt "Roskaposti".

Automaatio ja IoT

Euroopassa kylmälaitteisiin tehdyt kyberhyökkäykset aiheuttivat merkittävää tuotehävikkiä ja taloudellisia tappioita.

Hyökkäykset paljastivat haavoittuvien etäohjattavien laitteiden riskit, jotka koskevat kaikkia julkiseen verkkoon näkyviä ratkaisuja.

Verkkojen toimivuus

Lokakuu oli palvelunestohyökkäysten suhteen tavanomainen. Palvelunestohyökkäyksiä on näkynyt ja niillä on ollut ajoittaisia, rajattuja vaikutuksia palvelujen saatavuuteen.

Kybersää
lokakuu 2026 1/2

1 kk

Tietomurrot ja -vuodot

- Tietomurtoilmoitusten määrä kasvoi selvästi syyskuusta, vaikkakin muutoin kuukausi oli hyvin tavanomainen.
- Ohjelmistohaavoittuvuuksia hyödynnettiin laajasti osassa ilmoitettuja tietomurtoja. Valtaosassa tapauksista WordPress-haavoittuvuuksia käytettiin ClickFix-sisällön lisäämiseen verkkosivuille. WordPress-sivustojen päivittämiseen ja haavoittuvuuksien hallintaan kannattaa panostaa. [12, 13]
- Microsoft 365 -tilien tietomurtojen määrä kasvoi voimakkaasti lokakuussa. Eniten tapauksia ilmoitettiin kiinteistö- ja rakennusalan pienissä organisaatioissa.

Haittaohjelmat

- Tarkastelujakson aikana haittaohjelmia ja näiden levitystä on havaittu erityisesti ClickFix-tekniikkaa hyödyntäen. Esimerkiksi WordPress-sivustojen tietomurrot ovat usein johtaneet haitallisen sisällön lataamiseen murretulle verkkosivulle ja sitä kautta jatkohyödynnetty haittaohjelmien levityksessä.
- Kyberturvallisuuskeskukselle on ilmoitettu tapauksesta, jossa organisaatiolle oli asiakkaan toimesta toimitettu USB-tikku, joka oli sisältänyt haittaohjelman. Haitallinen ohjelma tunnistettiin ennen kuin se ehti aiheuttaa vaikutuksia.

Haavoittuvuudet

- Lokakuussa eniten keskustelua herättivät PHP-haavoittuvuudet CVE-2026-109618 ja CVE-2026-109619 (PHP2Shell). [14]
- Haavoittuvuuksia hyväksikäyttämällä hyökkääjä voi mahdollisesti suorittaa etänä mielivaltaisia komentoja palvelimella ja ottaa sen täysin hallintaansa.
- Useat organisaatiot kuten Valtori ajoivat alas palveluitaan ennen haavoittuvuuksien korjauksen julkaisua.
- Suomessa kyseisten PHP-haavoittuvuuksien hyväksikäyttöä ei ole toistaiseksi havaittu.

Kybersää
lokakuu 2026 2/2

1 kk

Huijaukset ja kalastelut

- Lokakuu oli Euroopan kyberturvallisuuskuukausi. Viranomaiset, koulutusorganisaatiot ja järjestöt jakoivat käytännön vinkkejä turvalliseen digiarkeen Nyt valppaana -verkostossa. Verkoston kyberneuvonta jatkuu edelleen marraskuussa. [15]
- Majoitusvarauspalveluiden, viranomaisten ja pankkien nimissä tehtävien huijausten määrä lisääntyi lokakuussa.
- Onneksi myös taistelu tekstiviestihuijauksia vastaan tehostui: rekisteröimättömän lähettäjän nimen tilalla lukee nyt "Roskaposti". [16]

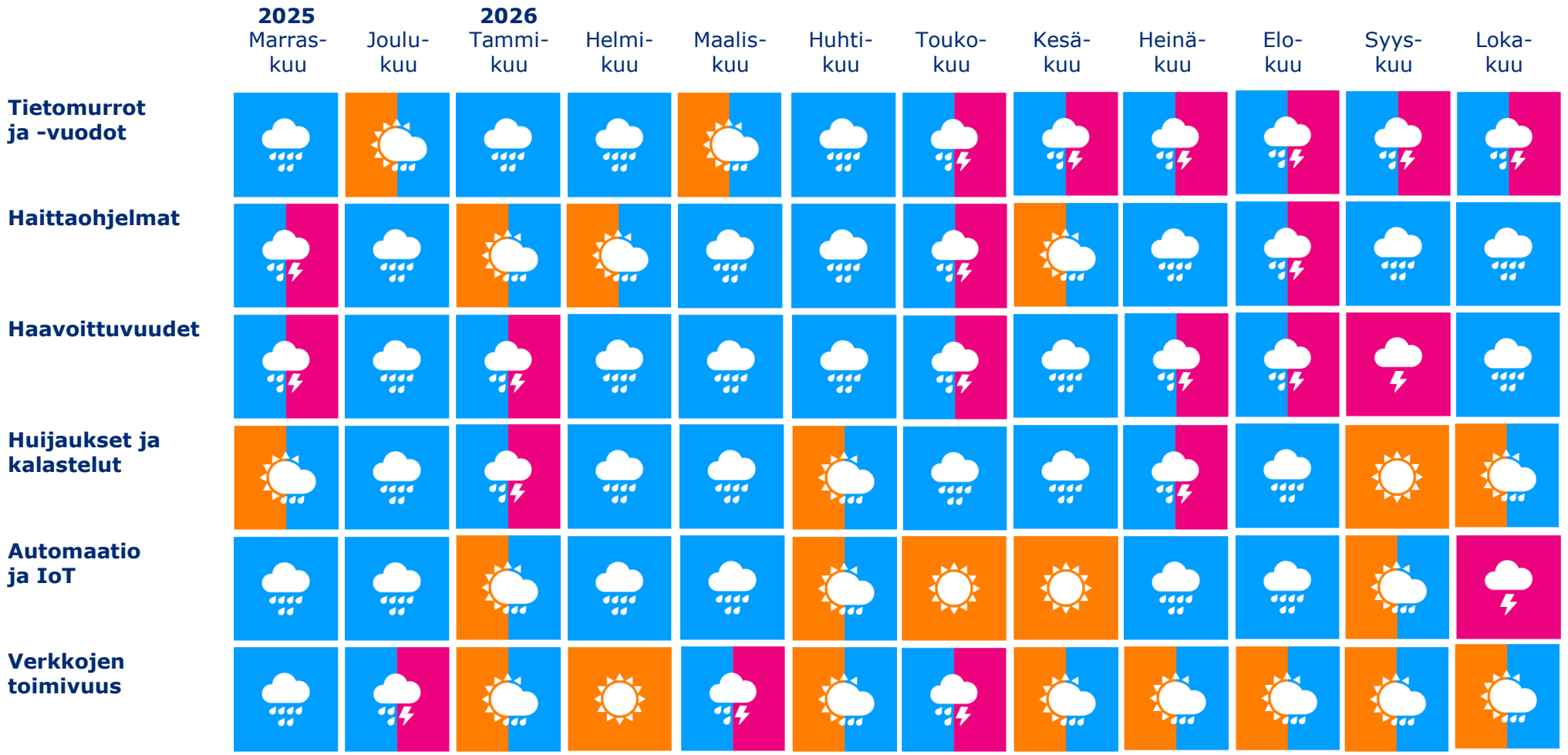
Automaatio ja IoT

- Kylmälaitteisiin Euroopassa kohdistuneet hyökkäykset osoittivat julkiverkossa olevien etäohjausratkaisujen riskit käytännössä. Hyökkäyksiä havaittiin myös Suomessa. [17]
- Ranska attribuoi maan kylmälaitteisiin kohdistuneet hyökkäykset Iraniin. Muihin maihin kohdistuneiden hyökkäysten tekijöistä ei ole vielä tietoa. [18]
- Tapahtunut korostaa riskienhallinnan ja kyberturvallisuuden merkitystä fyysiseen maailmaan vaikuttavissa ratkaisuissa. IoT- ja OT-laitteita ei pidä altistaa suoraan julkiselle internetille, jos siihen ei ole välttämätöntä tarvetta.

Verkkojen toimivuus

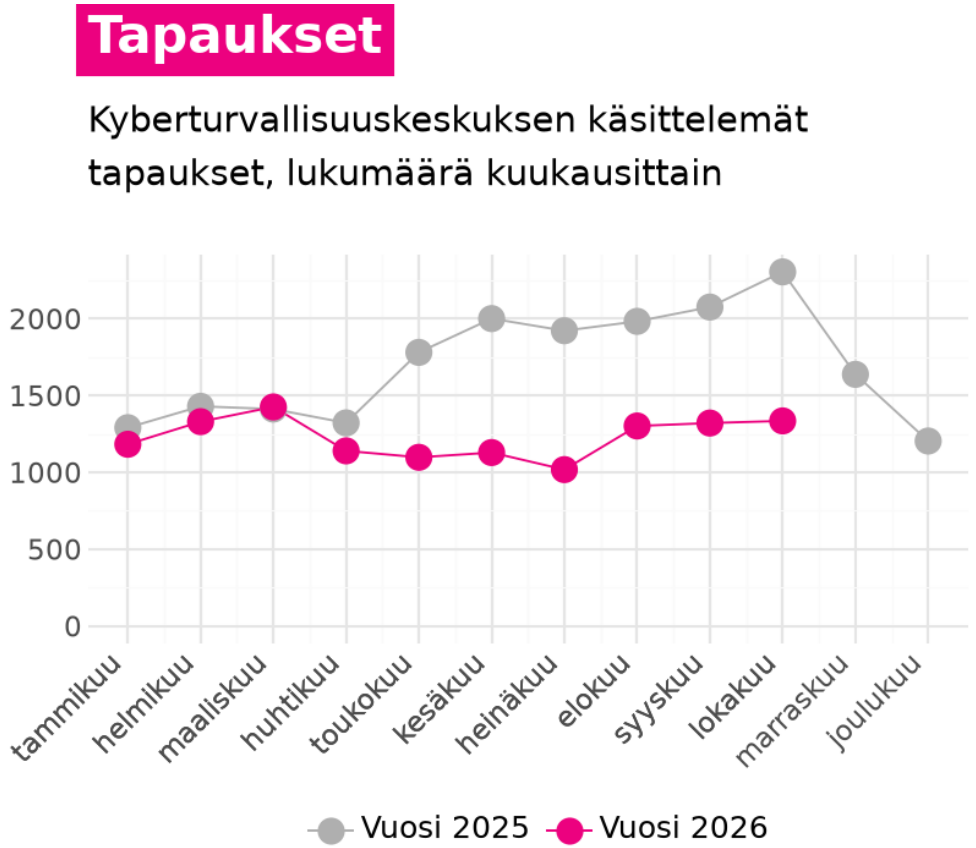
- Palvelunestohyökkäyksiä voidaan toteuttaa puhtaasti liikennemäärän lisäksi esimerkiksi ohjelmistohaavoittuvuuksia tai ohjelmistojen heikkouksia hyväksikäyttämällä.
- Määräys teletoiminnan häiriötilanteista päivitettiin ja on annettu 15.10. Määräys vaikuttaa sekä kuluttajille että Traficomille tehtäviin teleyritysten häiriöilmoituksiin. Määräys astuu voimaan 1.1.2027. [19]

Kybersään ilmiöt
kulunut 12 kk



Tapaukset

- Kyberturvallisuuskeskus käsitteli lokakuussa 1335 tapausta. Tapausmäärät eivät itsessään kerro tilanteesta kaikkea. Ilmoitusten määrä on hieman pienempi vuoden takaiseen tasoon ja 12 kuukauden keskiarvoon nähden noin 6 % pienempi.
- Lokakuuta ei kuitenkaan voida pitää rauhallisena, vaikka ilmoitetut tapausmäärät ovat olleet vähäisempiä. Laajat haavoittuvuuskokonaisuudet, kuten PHP2Shell ja Citrix NetScaleriin kohdistuneet haavoittuvuudet ovat aiheuttaneet laajoja kartoitus- ja suojaamistoimenpiteitä.
- Lisäksi haavoittuvuudet ovat aiheuttaneet merkittäviä tietomurtotapauksia. Näiden selvitykset ovat kestäneet pitkään ja vaatineet laajoja resursseja niin organisaatioilta kuin Kyberturvallisuuskeskukselta.



Kybersääennuste

Kybersääennuste on aiempiin havaintoihin perustuva yhteenveto ja suuntaa-antava arvio lähikuukausien kyberuhista ja niiden kehityskuluista.

Osiossa käsitellään myös puolivuosittain ilmiöiden pitkän aikavälin kehitysnäkymiä ja lähitulevaisuuden top 5 kyberuhat.

Kybersääennuste
Kyberuhat pysyvät tavanomaisina

1 kk

Sanonta, ettei kyberturvallisuus tunne valtioiden rajoja, on etenkin lokakuussa näkynyt kansalaisille saakka, ja tullee näkymään myös jatkossa. On odotettavissa, että moneen valtioon samanaikaisesti vaikuttavat kybervaikuttamis-kampanjat ja kriittisistä haavoittuvuuksista johtuvat poikkeamat jatkuvat.

M365-tilimurtojen aallot jatkuvat todennäköisesti myös loppuvuoden ajan.

Organisaation varautuminen

- Organisaatioiden kannattaa panostaa kouluttamiseen, jotta käyttäjät osaavat tunnistaa M365-tunnustenkalastelu-yritykset ja ilmoittaa niistä IT:tuelle.
- Organisaatioiden on syytä edelleen varautua nopeisiin päivittämisiin, kun kriittisiä haavoittuvuuksia julkaistaan tiiviiseen tahtiin.
- Organisaatioissa kannattaa ottaa käyttöön kehittyneitä turvallisuus-ominaisuuksia, kuten ehdollisen pääsyn (conditional access) käytäntöjä, riskiperusteinen tunnistautuminen (risk-based authentication) ja jatkuva pääsyn arviointi (continuous access evaluation).



Huolestuttava

Kyberuhkien määrä ja vakavuus ovat tavanomaisella tasolla.

Kybersääennuste on aiempiin havaintoihin perustuva yhteenveto ja suuntaa-antava arvio kyberuhkien tilasta. Arviota ei tule käyttää sellaisenaan kyberuhkiin varautumisessa, vaan sen tukena on käytettävä organisaatiokohtaista tietoa ja analyysiä. Kyberuhat voivat muuttua nopeasti, myös negatiiviseen suuntaan.

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
Päivitetty määräys teletoiminnan häiriötilanteista tulee voimaan 1.1.2027

- Liikenne- ja viestintävirasto Traficomin 15.10.2026 antama määräys teletoiminnan häiriötilanteista tulee voimaan 1.1.2027.
- Määräyksellä ajantasaistetaan 1.1.2020 voimaan tullut määräys teletoiminnan häiriötilanteista.
- Yksi määräyksen keskeisimmistä muutoksista on, että päivitetyssä määräyksessä tarkennetaan sähköisen viestinnän palveluista annetun lain 275 §:n velvoitetta, jonka mukaan teleyritysten on ilmoitettava virastolle myös toimivuuden ja tietoturvan häiriötilanteiden uhista. Näin ollen teleyritysten on ilmoitettava virastolle myös mahdollisista sabotaasitapauksista.
- Tietoturvan häiriötilanteita koskevia vaatimuksia on muutettu hallinnollisen taakan keventämiseksi. Teleyrityksen ei siten välttämättä tarvitse ilmoittaa samasta tapauksesta useita kertoja. Vaatimuksia on yhdenmukaistettu kyberturvallisuuslain kanssa.
- Päivityksessä on myös poistettu toimivuushäiriöiden neliportainen vakavuusluokitus A–D. Sen sijaan teleyritykset velvoitetaan ilmoittamaan häiriöistä yhden määritellyn ilmoituskynnyksen perusteella. [20]

Oikeudelliset asiat
EU:n neuvosto vahvisti kantansa Digital Omnibus -ehdotukseen

- EU:n neuvosto hyväksyi 21.10.2026 kantansa Digital Omnibus -ehdotuksesta, jonka tavoitteena on yksinkertaistaa EU:n digitaalista sääntelyä.
- Kyberpoikkeamien ilmoittamista uudistetaan merkittävästi. Tavoitteena on useiden eri säädösten mukaisten ilmoitusvelvollisuuksien yhteensovittaminen.
- Neuvosto hylkäsi komission ehdottaman EU:n yhteisen ilmoituskanavan ja esittää sen sijaan kansallisia ilmoituspisteitä, joiden kautta organisaatiot voisivat täyttää useiden EU-säädösten (esim. NIS2 ja GDPR) ilmoitusvelvoitteita.
- Neuvoston kannassa EU-tasolle ehdotetaan ilmoitustietojen käsittelyä tukevaa tietopistettä.
- Neuvoston kanta sisältää myös GDPR:n pseudonymisointia koskevia täsmennyksiä, tutkimuskäytön helpottamista sekä tiettyjä tekoälyn kehittämistä tukevia muutoksia. Lisäksi eväisteiden käyttöön ehdotetaan uusia poikkeuksia ja datan jakamiseen uusia liikesalaisuuksia suojaavia mekanismeja.
- Seuraavaksi alkavat neuvottelut Euroopan parlamentin kanssa. [21]

Oikeudelliset asiat
Tekoälysäädöksen ensimmäinen yhdenmukaistettu standardi julkaistiin EU:n virallisessa lehdessä

- Ensimmäinen EU:n tekoälysäädöstä tukeva yhdenmukaistetusta standardista julkaistiin EU:n virallisessa lehdessä lokakuussa.
- Standardi koskee tekoälysäädöksen 17 artiklan mukaisia suuririskisten tekoälyjärjestelmien tarjoajien laadunhallintajärjestelmiä.
- Komission täytäntöönpanosäädöksellä (EU) 2026/2274 standardin soveltaminen antaa olettaman vaatimustenmukaisuudesta niiden tekoälysäädöksen 17 artiklan vaatimusten osalta, jotka standardi kattaa.
- Tekoälysäädöksen standardointityössä on valmistelussa myös tekoälyjärjestelmien kyberturvallisuutta koskeva standardi (prEN 18282).
- Standardin tarkoituksena on määritellä organisatorisia ja teknisiä ratkaisuja suuririskisten tekoälyjärjestelmien kyberturvallisuuden varmistamiseksi koko niiden elinkaaren ajan. [22, 23]

Oikeudelliset asiat
Tietoturvallisuuden arviointisääntelyn muutokset tulevat voimaan 1.1.2027

- Viranomaisten tietojärjestelmien ja tietoliikenne-järjestelyjen tietoturvallisuuden arvioinnista (*arviointilaki*) ja tietoturvallisuuden arviointilaitoksista (*arviointilaitoslaki*) annettujen lakien muutokset on hyväksytty.
- Traficomin päivitettävät ja täydennettävät ohjeet viranomaisille ja valmistajille tulevat lausuttavaksi marraskuussa.

Arviointilaitoslaki

- Laitosten yritysturvallisuusselvityksestä (TL-pätevyydet, esim. Katakri) ja alihankinnasta säädetään. Uusien pätevyyksien myöntämistä joustavoitetaan. [24]

Arviointilaki

- Kotimaisille salaus-, TEMPEST- ja muiden turvallisuuskriittisten ratkaisujen valmistajille tulee oikeus hakea Traficomilta hyväksyntää julkiseen luetteloon. Ratkaisuilla suojataan kansallista, EU:n ja/tai Naton turvallisuusluokiteltua tietoa.
- Valtionhallinnon viranomaisille säädetään velvollisuus arvioida kaikki tietojärjestelmänsä. Tälle säädetään siirtymäaikoja 2-5 vuoteen ja arviointimenettelyjä lisätään nykyisestä.
- Riskiarvioinnin merkitystä ja arvioinnin tuottamaa tietoa riskinhallinnassa korostetaan.
- Traficomin rinnalle säädetään riippumaton arviointiviranomaisen tehtävä Pääesikunnan määrätylle turvallisuusviranomaiselle Puolustusvoimien järjestelmissä kansallisen tiedon käsittelyssä. [25]

Epäiletkö tietoturvaloukkausta?

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

- Sähköinen lomake www.kyberturvallisuuskeskus.fi/fi/ilmoita
- Sähköposti: cert@traficom.fi

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

Lähteet

Lähdeluettelo
1/3

1. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet
2. https://www.traficom.fi/fi/uutiset/tekoaly-nopeuttaa-haavoittuvuuksien-loytymista-kriittiset-php-haavoittuvuudet-aiheuttavat-palvelukatkoja
3. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-452026#144574-0
4. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-442026#144096-0
5. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-422026#143050-1
6. https://traficom.fi/fi/uutiset/lokakuu-euroopan-kyberturvallisuuskuukausi-vahvista-arjen-tietoturvataitojasi
7. https://traficom.fi/fi/uutiset/roskaposti-merkinta-tulee-tekstiviesteihin-ja-vaikeuttaa-huijareiden-esiintymista-tuttuna-lahettajana
8. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/iot-ja-ot-ymparistojen-tietoturva-alkaa-laitteiden-suojaamisesta
9. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-37
10. https://www.php.net/index.php#2026-10-21
11. https://www.traficom.fi/fi/uutiset/tekoaly-nopeuttaa-haavoittuvuuksien-loytymista-kriittiset-php-haavoittuvuudet-aiheuttavat-palvelukatkoja

Lähdeluettelo
2/3

12. https://kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-382026#140573-2
13. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-402026#141713-2
14. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-37
15. https://www.traficom.fi/fi/uutiset/lokakuu-euroopan-kyberturvallisuuskuukausi-vahvista-arjen-tietoturvataitojasi
16. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-442026#144096-1
17. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-452026#144574-0
18. https://www.diplomatie.gouv.fr/fr/presse-et-ressources/decouvrir-et-informer/actualites/declaration-d-attribution-a-l-iran-de-cyberattaques-visant-la-france
19. https://www.traficom.fi/fi/uutiset/teletoiminnan-hairiotilanteista-ilmoittaminen-muuttuu
20. https://www.traficom.fi/fi/uutiset/teletoiminnan-hairiotilanteista-ilmoittaminen-muuttuu
21. https://www.consilium.europa.eu/en/press/press-releases/2026/10/21/digital-rulebook-council-agrees-position-to-simplify-data-protection-privacy-and-cyber-reporting-rules/
22. https://digital-strategy.ec.europa.eu/en/library/first-harmonised-standard-supporting-ai-act-published-official-journal

Lähdeluettelo
3/3

23. https://jtc21.eu/cen-cenelec-ai-standards-catalogue/
24. https://www.finlex.fi/fi/lainsaadanto/2011/1405
25. https://www.finlex.fi/fi/lainsaadanto/2011/1406