TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Toukokuu 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

Viime vuoden kesäkuun alkuun mennessä olimme julkaisseet 10 haavatiedotetta ja tänä vuonna luku on 15, joka vastaa 50 % kasvua julkaistujen tiedotteiden määrässä.

Kyberkestävyyslaki tuli voimaan 1.6.2026 ja se täydentää EU:n säädöstä sekä määrittelee toimintatavat Suomessa. Tuoreen kyberkestävyyslain ja EU:n kyberkestävyyssäädöksen (Cyber Resilience Act, CRA) tavoitteena on parantaa markkinoilla olevien tuotteiden kyberturvallisuutta.

Euroopan komission Horisontti Eurooppa -ohjelmassa on tarjolla jopa 100 % rahoitusta ohjelmistojen, laitteistojen ja tekoälyn kyberturvallisuuden tutkimus-, kehittämis- ja innovaatiotoiminnan edistämiseen erilaisia kyberuhkia ja -hyökkäyksiä vastaan, kehittyvät kryptoteknologiat soveltuvasti huomioiden. Rahoitusta voi hakea 15.9. asti. [1]

Kybersään yleistilanne toukokuussa 2026

Toukokuu jatkui epävakaana pitkälti haavoittuvuuksien takia

Toukokuun kybersää näyttäytyi vaihtelevana ja paikoin epävakaana. Kuukauden aikana nähtiin toistuvia ja laaja-alaisia huijauskampanjoita, joissa rikolliset esiintyivät mm. lasten, viranomaisten, pankkien ja palveluiden nimissä.

Samalla havaittiin, että kalastelu kehittyi teknisesti, sillä Microsoft 365 -tileihin kohdistui tekoälyavusteista kohdentamista, mikä teki viesteistä entistä uskottavampia. Huhtikuussa ennustimme M365-tilimurtojen seurauksena jatkokalasteluista, mikä toteutui mm. vaikeammin havaittavana device-code –kalasteluna. Varoitimme toukokuussa myös koko alkuvuoden jatkuneesta pikaviestitilien kaappauksista ja ohjeistimme ilmiöltä suojautumiseen. Kuukauden aikana julkaistiin useita kriittisiä haavoittuvuuksia, joista osa oli jo aktiivisen hyväksikäytön kohteena.

Ajoittaista aurinkoa kybersäähän toivat uudistuneet Kyberturvallisuuskeskuksen Hyöky-palvelu [2] , joka otettiin entistä laajempaan käyttöön sekä tuotantokäyttöön otettu FINMISP-palvelu [3] , joka tehostaa teknisen kyberuhkatiedon jakamista huoltovarmuuskriittisille organisaatioille ja viranomaisille.

Tietoturvallisuus ei lomaile kesällä

Kesälomien aikaan erityisesti toimitusjohtaja-huijaukset ja muut rahaliikenteeseen kohdistuvat petokset lisääntyvät, kun organisaatioiden normaali arki hidastuu ja avainhenkilöitä on poissa.

Lomakaudella riskit kasvavat erityisesti silloin, kun tehtäviä hoitavat sijaiset tai kesätyöntekijät, jotka eivät vielä tunne organisaation käytäntöjä, minkä vuoksi perehdytyksellä ja selkeillä toimintamalleilla on suuri merkitys.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Microsoft on käynnistänyt yhden viime vuosien tärkeimmistä tietoturvapäivityksistä: Windowsin Secure Boot -varmenteiden (certificate) uusimisen. Muutos liittyy erityisesti siihen, että osa käytössä olevista Secure Boot -varmenteista saavuttaa elinkaarensa lopun. Vuonna 2011 käyttöön otetut juurivarmenteet alkavat vanhentua kesästä 2026 lähtien. Muutos koskee käytännössä lähes kaikkia Windows-laitteita, jotka on valmistettu vuoden 2012 jälkeen. Microsoft arvioi kuitenkin, että suurin osa moderneista Windows 11 -laitteista saa päivitykset automaattisesti Windows Updaten kautta. [4]

M365-tietojenkalastelussa on havaittu uusi aalto: tekoälyavusteinen laitekoodin kalastelukampanja. Kampanja kohdistuu organisaatioihin ja yksittäisiin käyttäjiin. Hyökkäyksen tavoitteena on saada luvaton pääsy tileihin sekä yritysten resursseihin. Uuden tyylisellä M365 Device Code -kalastelulla tehtyä tietomurtoa ei havaita perinteisten Microsoftin kalasteluhyökkäysten varoituksilla. Tämän vuoksi hyökkääjillä on mahdollisuus tehdä kaikessa hiljaisuudessa esimerkiksi laskutuspetoksia. Organisaatioita suositellaankin tarkistamaan kyselyllä tehdyt Device Code -tietomurrot sekä rajoittamaan Device Code Flow -toiminnon käyttöä ehdollisilla pääsynhallintasäännöillä (Conditional Access). Verkkosivuillamme kerromme lisää, miten organisaatiot ja yksityiset henkilöt voivat suojautua ilmiöltä ja artikkelista löydät myös ohjeet hakukyselyn tekemiseen. [5]

Kybersään ilmiöt

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä.

Kybersää
toukokuu 2026

1 kk

Tietomurrot- ja vuodot

Tietomurtojen määrä kasvoi 24 % huhtikuusta. Kasvua selittää M365-tilimurtojen aalto. Saimme kaksi kiristyshaittaohjelmailmoitusta. Vakavilta vaikutuksilta vältyttiin.

Haittaohjelmat

Kuukauden aikana Kyberturvallisuuskeskukselle ilmoitettiin useista haittaohjelmahavainnoista. Haittaohjelmia on jaettu organisaatioille ja yksityisille henkilöille kalasteluviestien liitteinä, rekrytointihuijausten ohessa sekä murrettujen verkkosivujen kautta.

Haavoittuvuudet

Uusia haavoittuvuuksia raportoitiin myös toukokuussa suuri määrä ja sama trendi näyttäisi jatkuvan koko loppuvuoden.

Huijaukset ja kalastelut

Äitienpäivänä esiintyi "Hei äiti"-huijauksia. Huijauksia laaditaan yhä enemmän tekoälytyökaluilla.

Toimitusjohtajahuijaukset lisääntyvät lomakaudella. Kesälomasijaisia yritetään huijata johtajan nimissä.

Automaatio ja IoT

EU:n kyberkestävyyssäädös CRA:ta täydentävä kansallinen kyberturvallisuuslaki astui voimaan maanantaina 1.6.2026.

Verkkojen toimivuus

Palvelunestohyökkäykset eivät aiheuttaneet merkittäviä häiriöitä Suomessa.

Verkkojen toimivuushäiriöt korostuivat toukokuussa.

Kybersää
toukokuu 2026 1/2

1 kk

Tietomurrot ja -vuodot

- Toukokuussa julkaistut haavoittuvuudet johtivat tietomurtoihin organisaatioissa. Vakavilta vaikutuksilta kuitenkin vältyttiin.
- Hiljaisen alkuvuoden jälkeen saimme ilmoituksia kiristyshaittaohjelmista. Yritysten varautuminen on parantunut ja kiristyshaittaohjelmista palaudutaan yleensä hyvin. Yhdessä tapauksessa hyökkäys havaittiin niin nopeasti, että hyökkääjän toimintaa voitiin seurata reaaliaikaisesti ja estää pääsy yrityksen ympäristöön.
- Useita M365-tilimurtoja tehtiin uhrien hyväksyttyä vahingossa hyökkääjän laitteen omilla M365-tunnuksillaan. Murtojen avulla hyökkääjät yrittivät tehdä laskutuspetoksia.

Haittaohjelmat

- Toukokuun aikana haittaohjelmien jakaminen ja näiden välityksellä tehdyt tietovuodot ovat olleet merkittävä haitta.
- Rekrytointihuijausten muodossa on onnistuttu jakamaan troijalaisia työasemille, mikä on johtanut työasemien tietojen vuotamiseen hyökkääjälle.
- Kansainväliseen yritykseen kohdistuneen toimitusketjuhyökkäyksen välityksellä on pystytty toukokuun aikana levittämään haitallisia ohjelmia eri organisaatioille, jotka ovat käyttäneet yrityksen tuotteita ja palveluita.
- ClickFix-tekniikalla on jaettu toukokuun aikana haittaohjelmia murrettujen verkkosivujen kautta.

Haavoittuvuudet

- Toukokuussa haavoittuvuusilmoituksia tehtiin viisi kappaletta.
- Haavoittuvuudet osuivat Drupal Coreen (CVE-2026-9028), Cisco Catalyst SD-WAN -tuotteeseen (CVE-2026-20182), cPanel- ja WHM -hallintaohjelmistoon (CVE-2026-29201, CVE-2026-29202, CVE-2026-29203), Ivanti EPMM -tuotteeseen (CVE-2026-5786, CVE-2026-5787, CVE-2026-5788, CVE-2026-7821, CVE-2026-6973) sekä Palo Alto PAN-OS-ohjelmiston User-ID Authentication Portal -palveluun (CVE-2026-0300)
- Osaa haavoittuvuuksia on käytetty aktiivisesti hyväksi.

Kybersää
toukokuu 2026 2/2

1 kk

Huijaukset ja kalastelut

- Toukokuisena äitienpäivänä rikolliset yrittivät saada vanhemmat luulemaan, että heidän lapsellaan on uusi puhelin. Huijausviestillä yritettiin saada äiti lähettämään rahaa.
- Traficomia on käytetty huijausten verukkeena. Kalasteluviesteissä vedotaan maksamattoman sakon erääntymiseen ja kalastellaan sen avulla pankkitunnuksia.
- Lomakauden lähestyessä myös toimitusjohtajahuijaukset lisääntyvät. Kesälomasijaisia yritetään huijata johtajan nimiin väärennetyillä viesteillä hyväksymään maksusuorituksia rikollisen tilille.

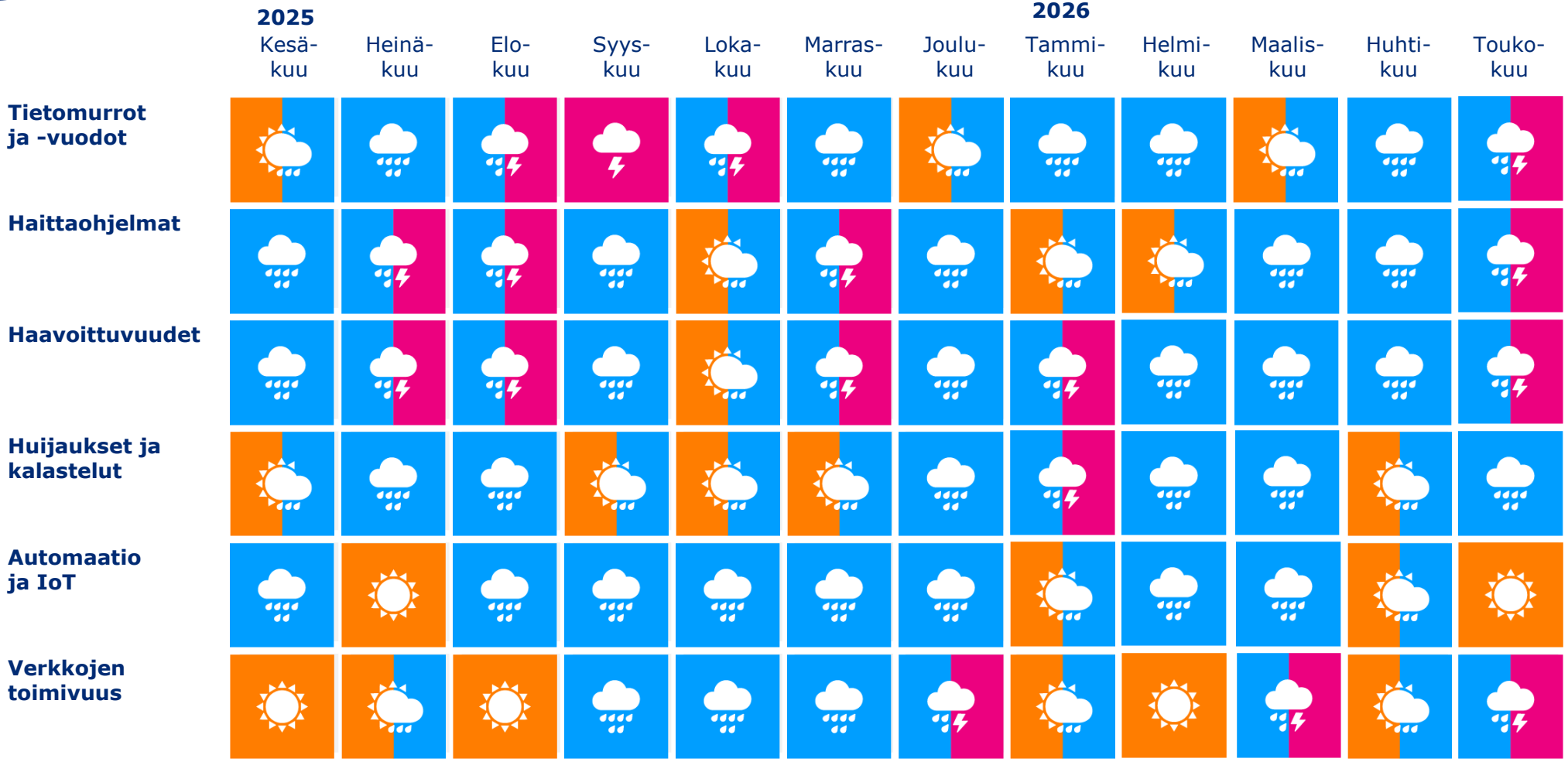
Automaatio ja IoT

- Kansallinen CRA:ta täydentävä laki eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista astui voimaan 1.6.2026. Laki käsittelee markkinavalvontaa, ilmoitettujen laitosten ilmoittamista ja hallinnollisia seurauksia. Lisäksi sillä täydennetään kansallista sääntelyä EU:n kyberturvallisuussertifioinneista. Näistä tehtävistä vastaa keskitetysti Liikenne- ja viestintävirasto Traficom.
- Ilmoitettuja laitoksia koskevia säädöksiä aletaan soveltaa 11.6.2026, mistä lähtien Traficomilta voi hakea ilmoittamista CRA:n mukaisiin arviointitehtäviin.

Verkkojen toimivuus

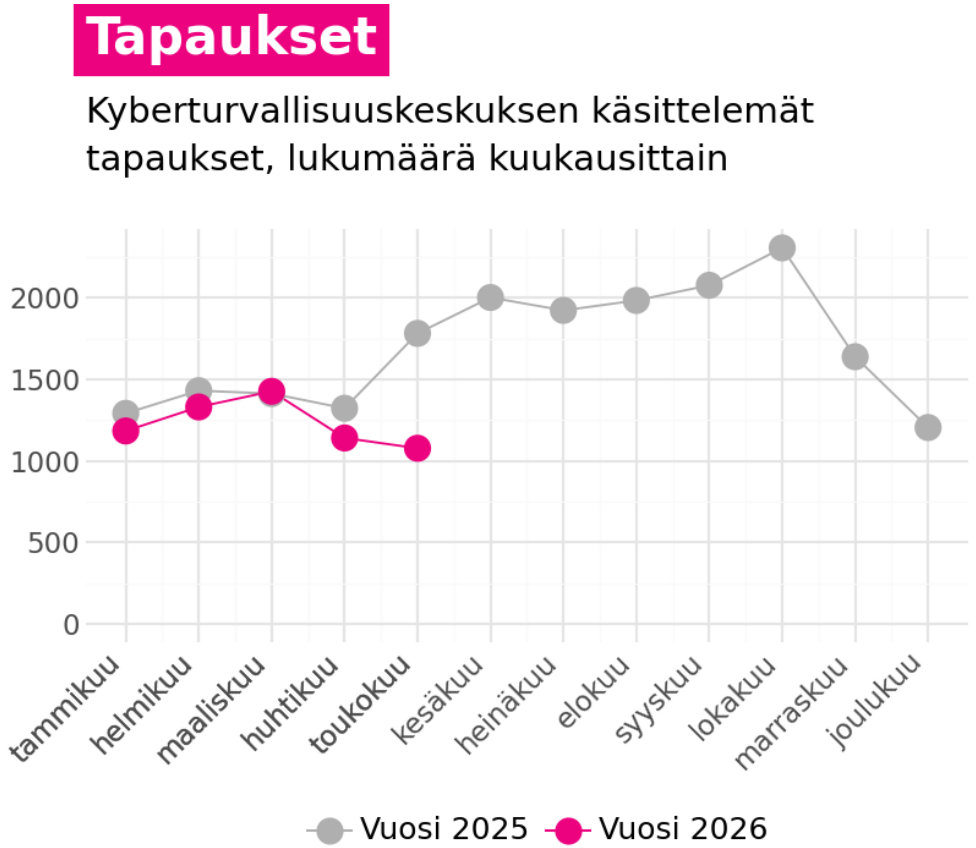
- Palvelunestohyökkäykset ovat internetin arkipäivää ja siksi verkossa tarjottavat palvelut tulee suojata. Vaikka hyökkäyksiä ei voida kokonaan estää, niitä voidaan torjua ja niiden vaikutukset minimoida.
- Verkkojen vakavien toimivuushäiriöiden määrä oli poikkeuksellisella tasolla toukokuussa.

Kybersään ilmiöt
kulunut 12 kk



Tapaukset

- Kyberturvallisuuskeskus käsitteli toukokuussa 1077 tapausta.
- Ilmoitusten määrä on 12 kuukauden keskiarvoon verrattuna huomattavasti vähäisempi.
- Kyberturvallisuuskeskukselle ilmoitettujen poikkeamien vakavuus kuitenkin korostui. Toukokuuta leimasivat erilaiset haavoittuvuudet, kiristyshaittaohjelmahyökkäykset sekä useat tietomurrot. Tietomurrot kohdistuivat laajasti sekä organisaatioihin että yksittäisiin käyttäjiin.
- Vaikka ilmoituksia siis tehtiin tavanomaista vähemmän, niiden sisältö oli merkitykseltään poikkeuksellisen vakavaa.



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

Kesäkuun kybersäähän ei ole nähtävissä erityisiä muutoksia. Tietomurrot ja haavoittuvuudet todennäköisesti jatkuvat samalla tasolla. Kesäkuussa alkavat näkyä kesälomakauden vaikutukset kyberturvallisuuteen erilaisten huijausten muodossa, joita ovat esimerkiksi toimitusjohtajahuijaukset sekä erilaiset matkusteluun liittyvät kalastelut.

Organisaation varautuminen

- Organisaatioiden varautuminen ja valmius ei saa riippua tietoturvahenkilöstön lomista.
- Ennen lomalle lähtöä kannattaa varmistaa, että käytössä olevat laitteet ja sovellukset ovat ajan tasalla ja päivittää ne.

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
Kyberkestävyyslaki voimaan 1.6.2026

- Kyberkestävyyslain ja EU:n kyberkestävyyssäädöksen (Cyber Resilience Act, CRA) tavoitteena on parantaa markkinoilla olevien tuotteiden kyberturvallisuutta.
- Valmistajien on suunniteltava ja tehtävä tuotteet kyberturvallisiksi sekä ilmoitettava haavoittuvuuksista ja vakavista tietoturvapoikkeamista. Vaatimuksia on myös maahantuojille, jälleenmyyjille ja avoimen lähdekoodin ohjelmistovastaaville.
- Valmistajien tulee ilmoittaa haavoittuvuuksista Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle 11.9.2026 alkaen ja kaikkien markkinoille tuotavien tuotteiden tulee noudattaa kyberkestävyyssäädöstä 11.12.2027 alkaen.
- Markkinavalvontaa sekä ilmoitettujen laitosten nimeämistä ja valvontaa koskevat viranomaistehtävät järjestetään keskitetysti Traficomin Kyberturvallisuuskeskuksessa. Suuririskisiä tekoälyjärjestelmiä valvovat kuitenkin samat viranomaiset, jotka valvovat tekoälyasetuksen vaatimuksia toimialan mukaan.
- Tuotteiden vaatimuksenmukaisuutta arvioivat laitokset voivat hakea Suomessa ilmoittamista kyberkestävyyssäädöksen mukaisiin arviointitehtäviin 11.6.2026 alkaen Traficomin Kyberturvallisuuskeskukselta. [6] [7]
- Lisäksi komissio on julkaissut delegoidun asetuksen (EU) 2026/339, jolla kumotaan 11.12.2027 alkaen radiolaitteiden kyberturvallisuusvaatimuksia koskeva delegoitu asetus (EU) 2022/30.
- Nykyisiä radiolaitteiden kyberturvallisuusvaatimuksia sovelletaan siihen asti, että kyberkestävyyssäädöstä aletaan sovelletaan täysimääräisesti. Tavoitteena on välttää päällekkäistä sääntelyä.

Oikeudelliset asiat
Arviointisääntelyn päivittäminen eteni eduskuntaan

- Muutoksia esitetään lakiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) ja lakiin tietoturvallisuuden arviointilaitoksista (1405/2011). [8]
- Tietoturvallisuuden arviointilaitoksen arviointipätevyyden osoittamisen menettelyjä joustavoitettaisiin. Säädettäisiin alihankinnasta ja säädettäisiin yritysturvallisuusselvityksestä turvallisuusluokitellun tiedon käsittelyn arviointipätevyyksissä.
- Salaus-, hajasäteilysuojaus- ja muiden turvallisuuskriittisten Suomessa valmistettujen ratkaisujen Suomeen sijoittautuneet valmistajat voisivat hakea Traficomilta hyväksyntää julkiseen luetteloon.
- Valtionhallinnon viranomaisille tulisi velvollisuus tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointiin.
  - Arviointimenettely ja arvioinnin tekijä määräytyisi riskiarvion ja turvallisuusluokan perusteella.
- Traficomin arviointiviranomaisen yleisen tehtävän rinnalle säädettäisiin Pääesikunnan määrätylle turvallisuusviranomaiselle Puolustusvoimia koskeva riippumaton arviointiviranomaisen tehtävä.
  - Kansainvälisten tietoturvallisuusvelvoitteiden edellyttämät arvioinnit ovat jatkossakin Traficomin tehtävä.

Oikeudelliset asiat
Maanalaisen verkkoinfrastruktuurin sijaintitietoja koskevan lain valmistelu lopetetaan

- Liikenne- ja viestintäministeriö lopettaa maanalaisen verkkoinfrastruktuurin sijaintitietoja koskevan hallituksen esityksen valmistelun. [9]
- Lain tarkoituksena oli mahdollistaa maanalaisen verkkoinfrastruktuurin sijaintitietojen parempi selvittäminen. Lailla olisi luotu lainsäädäntöpohja sijaintitietopalvelun toteuttamiselle. Sääntelyllä olisi pyritty suojaamaan verkkotietoja ja varmistamaan käsittelyn tietoturvallisuus.
- Hallituksen esityksen valmistelussa tuli esiin lukuisia haasteita. Myös hankkeen kustannukset olisivat suuremmat kuin hankkeesta odotetut hyödyt.
- Valtionhallinnon tiukentuneen taloustilanteen vuoksi ministeriö ei näe mahdollisena sijaintitietopalvelun jatkokehitystä.
- Sijaintitietojen nykytilassa tunnistettuihin haasteisiin haetaan ratkaisuja ensisijaisesti olemassa olevan lainsäädännön ja määräysten kautta.
- Nykyinen sijaintitietopalvelua koskeva sääntely on yhteisrakentamislaissa. Sääntely kumotaan sijaintitietopalvelua koskevilta osilta soveltuvan lakihankkeen yhteydessä.

Oikeudelliset asiat
Valtioneuvosto hyväksyi kriittisten toimijoiden häiriönsietokykyä koskevan suunnitelman

- Valtioneuvosto hyväksyi 21.5.2026 kriittisten toimijoiden häiriönsietokykyä koskevan valtakunnallisen suunnitelman (ns. CER-strategia). [10]
- Suunnitelman tavoitteena on kriittisten toimijoiden häiriönsietokyvyn parantaminen ja se ohjaa kriittisiksi määrättyjen toimijoiden häiriönsietokyvyn kehittämistä kaikilla CER-lain määrittämillä toimialoilla.
- Suunnitelmassa muun muassa kuvataan kriittisten toimijoiden häiriönsietokyvyn parantamista koskevat tavoitteet, painopisteet ja toimenpiteet sekä kerrotaan, miten kriittiset toimijat määritetään ja mitkä viranomaiset ovat toiminnassa mukana. [11]
- Suunnitelma on voimassa enintään neljä vuotta kerrallaan.
- Suunnitelman laatiminen liittyy yhteiskunnan kriittisen infrastruktuurin suojaamista ja häiriönsietokyvyn parantamista koskevaan lakiin. Lailla toimeenpannaan kansallisesti EU:n CER-direktiivi, joka velvoittaa jäsenvaltioita parantamaan kriittisten toimijoiden häiriönsietokykyä ja varautumista. Laki tuli voimaan 1. heinäkuuta 2025.

Oikeudelliset asiat
Päivitetty Kyberturvallisuussanasto selkeyttämään kyberturvallisuustermien käyttöä

- Liikenne- ja viestintäministeriöön sijoitettu valtion kyberturvallisuusjohtajan toimisto ja Sanastokeskus julkaisivat 11.5.2026 Kyberturvallisuussanaston. [12]
- Ensimmäinen Kyberturvallisuussanasto laadittiin vuonna 2018. Nyt sanasto on päivitetty vastaamaan muuttuneen toimintaympäristön käsitteitä.
- Päivitetyssä sanastossa on noin 60 keskeistä kyberturvallisuuden käsitettä määritelmineen. Termeille annetaan myös vastineet ruotsin ja englannin kielillä.
- Kyberturvallisuussanaston tavoitteena on kyberturvallisuuteen liittyvien peruskäsitteiden määrittely, suositeltavien termien valinta ja termien käytön selkeyttäminen. Käsitteet pyritään määrittelemään siten, että niitä voidaan käyttää yhdenmukaisesti eri yhteyksissä.
- Sanasto on tarkoitettu työvälineeksi kaikille kyberturvallisuuden parissa työskenteleville. Se edistää julkisen hallinnon tietojen yhteen toimivuutta.

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
- 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 osoitteesta www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot.

Lähteet

Lähdeluettelo
1/1

1. https://kyberturvallisuuskeskus.fi/fi/uutiset/jopa-100-eu-rahoitusta-ohjelmistojen-laitteistojen-ja-tekoalyn-kyber-ja-kvanttiturvallisuuden-parantamiseksi
2. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/hyoky
3. https://kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/liity-finmisp-palveluun
4. https://kyberturvallisuuskeskus.fi/fi/uutiset/windowsin-secure-bootin-varmenteet-vanhenevat-kesakuusta-2026-alkaen-mita-se-tarkoittaa-organisaatioille-ja-kayttajille
5. https://kyberturvallisuuskeskus.fi/fi/uutiset/uusi-aalto-m365-tietojenkalastelussa-ai-avusteinen-laitekoodin-kalastelukampanja
6. https://traficom.fi/fi/uutiset/uusi-kyberkestavyyslaki-voimaan-16-haavoittuvuuksista-ilmoitettava-traficomille-syksysta-alkaen
7. https://valtioneuvosto.fi/hanke?tunnus=LVM014:00/2024
8. https://www.eduskunta.fi/asiat-ja-aanestykset/valtiopaivaasiat/HE%2085%2F2026%20vp
9. https://lvm.fi/-/maanalaisen-verkkoinfrastruktuurin-sijaintitietoja-koskevan-lain-valmistelu-lopetetaan
10. https://valtioneuvosto.fi/-/1410869/valtioneuvosto-hyvaksyi-kriittisten-toimijoiden-hairionsietokykya-koskevan-suunnitelman
11. https://julkaisut.valtioneuvosto.fi/items/600194c6-75fa-4a44-bcd9-2f9c836a7bd6
12. https://lvm.fi/-/paivitetty-kyberturvallisuussanasto-selkeyttamaan-kyberturvallisuustermien-kayttoa