TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Helmikuu 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

Microsoft 365 -käyttäjätilien murrot lisääntyivät jälleen. Murtoja ilmoitettiin Kyberturvallisuuskeskukselle 67 % enemmän kuin tammikuussa.

Kyberturvallisuuskeskus julkaisi helmikuussa yhden haavoittuvuustiedotteen, joka käsitteli Cisco Catalyst SD-WAN -tuotteissa olleita kahta kriittistä haavoittuvuutta. [1]

Neljä ministeriä tutustui kansalliseen kyberturvallisuusharjoitukseen (KYHA) 10.2.2026 vierailullaan Jyväskylässä. Kuntien ja kriittisen infrastruktuurin kansallisessa kyberharjoituksessa vahvistettiin tänä vuonna erityisesti logistiikkatoimialaan liittyvää kyberosaamista. [2]

Kybersään yleistilanne helmikuussa 2026

Helmikuu jatkui sateisena

Hyistä tihkua tuli useammasta suunnasta: Kyberturvallisuuskeskukselle raportoitujen tapausten perusteella rikolliset hyödynsivät monikanavaisia keinoja, kuten kiristysviestejä, pankkien ja viranomaisten nimissä soiteltuja huijauspuheita, robottipuheluita, laadukkaita tietojenkalasteluviestejä sekä sijoitus- ja kryptohuijauksia.

M365-tilimurrot jatkuivat edelleen ja AiTM-hyökkäysten kyky ohittaa monivaiheinen tunnistautuminen korosti tarvetta vahvemmille suojausmekanismeille.

Helmikuun aikana raportoitiin useita kriittisiä haavoittuvuuksia laajasti käytetyissä ohjelmistoissa ja palveluissa. Vaikka haavoittuvuudet ovat teknisesti merkittäviä ja mahdollistaisivat pahimmillaan järjestelmien haltuunoton tai tietojen luvattoman käytön, niiden kansalliset vaikutukset ovat toistaiseksi jääneet vähäisiksi.

Tästä huolimatta tilannekuvaa seurataan tiiviisti, sillä haavoittuvuuksien hyväksikäyttöyrityksiä on havaittu eri ympäristöissä.

Useat havaitut haavoittuvuudet ovat saaneet korkean CVSS-pisteytyksen, mikä korostaa päivittämisen ja suojaustoimien ajantasaisuuden merkitystä.

Huomioitavaa haavoittuvuuksiin liittyen

- Organisaatioita kehotetaan varmistamaan, että kriittiset järjestelmät on päivitetty ja että loki- ja valvontamekanismit ovat kunnossa mahdollisten hyödyntämisyritysten tunnistamiseksi.
- Lisäksi on tärkeää huomioida, että haavoittuvuuksia hyödynnetään usein pian niiden julkaisun jälkeen, joten reagoinnin nopeus on keskeistä riskien hallinnassa.

Kuukauden raekuuro
Kyberulottuvuus mukana Yhdysvaltojen ja Israelin hyökkäyksessä Iraniin

Yhdysvallat ja Israel hyökkäsivät Iraniin 28.2.2026. Hyökkäyksen ensipäivinä kineettisten iskujen rinnalla nähtiin myös kyberoperaatioita.

- Iranilaisia verkkopalveluita ja sovelluksia häirittiin ja useat haktivistiryhmät käynnistivät vastavuoroisesti palvelunesto- ja verkkosivujen häirintäoperaatioita.
- Erityistä huomiota herätti iranilaisten rukoussovelluksen kaappaus, jossa sovelluksen sisältö muutettiin Iranin hallintoa vastustavaksi.
- Iranin kansallinen internetyhteys putosi noin neljään prosenttiin normaalista Iranin suljettua laajasti verkkoyhteyksiään maassa. [3]
- Useampi valtio on julkaissut arvioita Iranin tilanteen vaikutuksista kyberturvallisuuteen. [4]
- Arvioiden mukaan Iranilla ja Iraniin kytköksissä olevilla toimijoilla arvioidaan kuitenkin edelleen olevan kykyä toteuttaa kyberoperaatioita, mikä lisää välillisen kyberuhan riskiä erityisesti organisaatioille, joilla on toimintaa tai toimitusketjuja Lähi-idässä. [5]
- Suomeen ei ole toistaiseksi kohdistunut merkittäviä kyberturvallisuusvaikutuksia Iranin tilanteen seurauksena.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kyberturvallisuuskeskus on julkaissut ohjesivuston, jossa käsitellään kvanttitietokoneiden kehittymisen aiheuttamaa uhkaa nykyisille salausmenetelmille. Kvanttiuhka koskee erityisesti tietoja, joiden on säilyttävä luottamuksellisina pitkälle tulevaisuuteen. Tällaisia ovat esimerkiksi henkilötiedot, terveystiedot, liikesalaisuudet sekä viranomaisten salassa pidettävät tiedot. [6]

Selainten lisäosat voivat parantaa toiminnallisuutta, mutta niihin liittyy merkittäviä tietoturvariskejä, koska ne saavat usein laajat oikeudet selaimen sisältöihin. Riskiä voi vähentää pitämällä lisäosien määrän pienenä, poistamalla tarpeettomat lisäosat sekä asentamalla uusia vain virallisista lähteistä ja arvioimalla kehittäjän luotettavuuden sekä pyydetyt käyttöoikeudet. [7]

Digi- ja väestötietoviraston uusi "Harjoitusten vaikutusten varmistaminen ja kehitystoimien vieminen käytäntöön" -opas korostaa, että harjoituksista saadaan hyötyä vain, jos opit ja kehityskohteet dokumentoidaan, analysoidaan ja juurrutetaan organisaation toimintaan. Siksi harjoituksille tulee luoda selkeä prosessi, jossa palaute, dokumentointi ja kehitystoimien seuranta tukevat jatkuvaa varautumisen ja kyberturvallisuuden kehittämistä. [8]

Kybersään ilmiöt

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä.

Kybersää
helmikuu 2026

1 kk

Tietomurrot- ja vuodot

Helmikuu oli huomattavasti aktiivisempi kuin tammikuu. Esiintyi yksi merkittävä tietomurto, jossa hyödynnettiin ohjelmiston nollapäivähaavoittuvuutta.

Microsoft 365 -tietomurtoja ilmoitettiin 67 % enemmän kuin tammikuussa.

Haittaohjelmat

Helmikuu näyttäytyi haittaohjelmien osalta rauhallisena kansallisesti. Kyberturvallisuuskeskukselle ilmoitettiin kuitenkin muutamia tapauksia haittaohjelmien levityksestä ClickFix-tekniikkaa käyttämällä.

Haavoittuvuudet

Helmikuun aikana raportoitiin paljon haavoittuvuuksia. Muutamia poikkeuksia lukuun ottamatta vaikutukset Suomen osalta olivat pääosin rajallisia.

Huijaukset ja kalastelut

Pankkien ja viranomaisten nimissä soitettiin huijauspuheluita.

Sähköpostissa lähetettiin väärennettyjä huijauslaskuja.

Automaatio ja IoT

Automaatiojärjestelmiin kohdistunut uhkatoiminta muuttui vakavammaksi vuonna 2025.

Tekoälyn avustamana tehdyt löydökset paransivat robotti-imurijärjestelmän tietoturvaa.

Verkkojen toimivuus

Palvelunestohyökkäykset eivät aiheuttaneet merkittäviä häiriöitä Suomessa.

Palvelunestohyökkäyksiin käytettäviä bottiverkkoja hyödynnetään myös muussa rikollisuudessa.

Kybersää
helmikuu 2026 1/2

1 kk

Tietomurrot ja -vuodot

- Valtorin mobiililaitehallinta-järjestelmään kohdistui vakava tietomurto, jossa hyödynnettiin ohjelmiston aiemmin tuntematonta nollapäivähaavoittuvuutta.
- Verkkosivustoihin on kohdistunut tietomurtoja, joissa on hyödynnetty erilaisia haavoittuvuuksia sekä heikkoja salasanoja.
- Yrityksen verkkoon murtauduttiin VPN-palvelun kautta kiristyshaittaohjelmahyökkäyksessä.
- Microsoft 365 -tilimurtoon liittynyt BEC-huijausyritys havaittiin ajoissa ja pysäytettiin.

Haittaohjelmat

- Kyberturvallisuuskeskukselle ilmoitettiin muutamista verkkosivuista, joissa levitettiin haittaohjelmaa ClickFix-tekniikkaa käyttämällä.
- Kalastelun yhteydessä on havaittu myös Docusign-teemalla levitettävän haittaohjelmaa, jossa käyttäjää pyydetään klikkaamaan linkistä, jonka seurauksena käyttäjän laitteelle asentuu haittaohjelma.

Haavoittuvuudet

- Cisco Catalyst SD-WAN –tuotteissa on ollut kriittisiä haavoittuvuuksia. Tuotteita käyttävien tahojen on syytä tunnistaa haavoittuvat laitteet verkkoympäristöstään, kerätä riittävät tiedot ja snapshotit haavoittuvista laitteista, päivittää laitteet uusimpaan versioon sekä suorittaa uhkametsästystä hyväksikäytön varalta (CVE-2026-20127 ja CVE-2026-20129).
- Ivanti EPMM haavoittuvuuksien (CVE-2026-1281 ja CVE-2026-1340) hyväksikäyttöä ja hyväksikäytön yrityksiä näkyi myös aktiivisesti helmikuussa.

Kybersää
helmikuu 2026 2/2

1 kk

Huijaukset ja kalastelut

- Huijauspuheluiden soittajat ovat puhelimessa esiintyneet pankin tai viranomaisen edustajana.
- Puhelinliittymän haltijoiden puhelinnumeroilla on avattu tilejä pikaviestipalveluihin, kuten Telegram ja WhatsApp. Useissa tapauksissa on epäilty, että rekisteröintiin on hyödynnetty liittymään kuuluvaa vastaajapalvelua.
- Sähköpostitse on lähetetty väärennettyjä laskuja, joissa saajan tilinumeron tilalle on väärennetty huijarin hallussa oleva pankkitili.

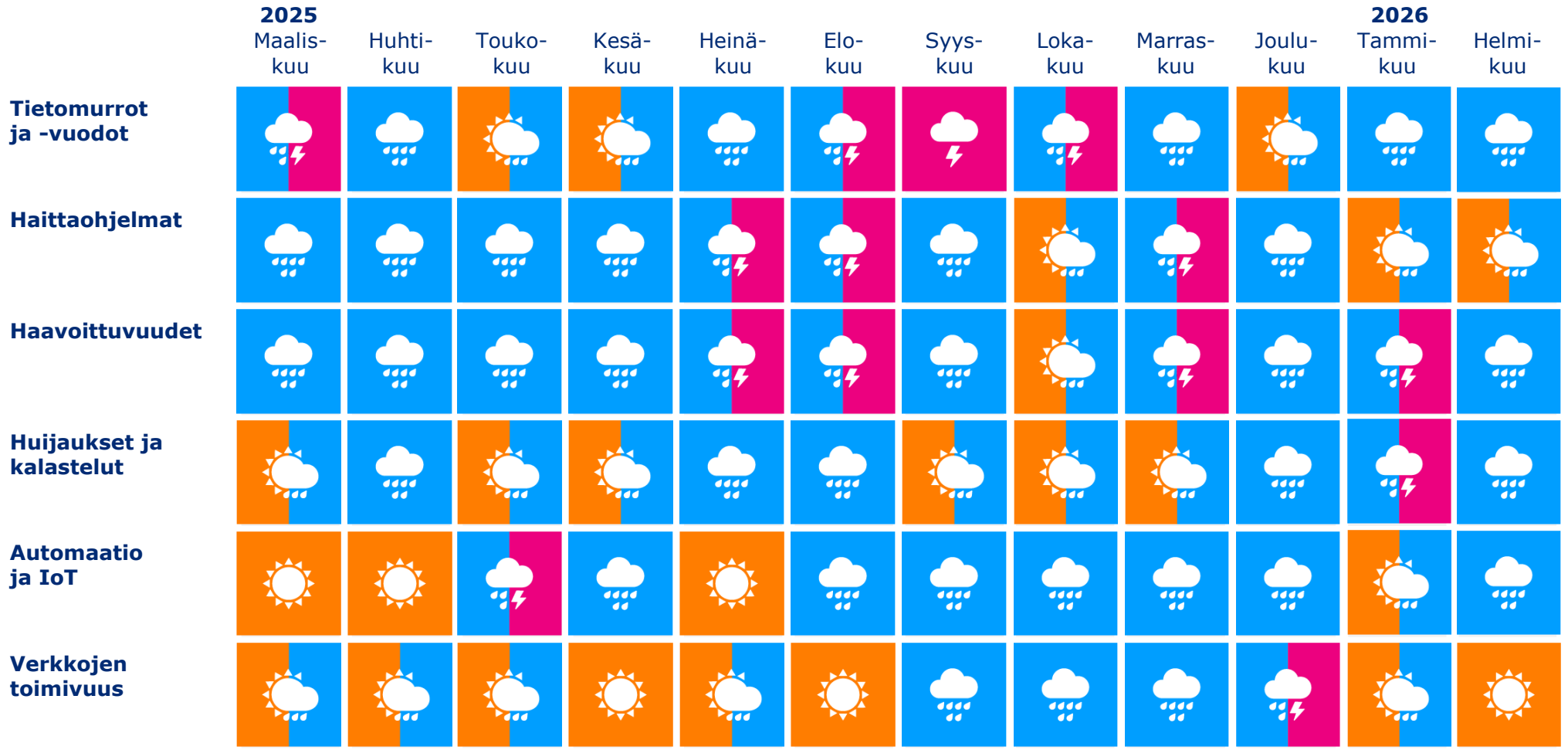
Automaatio ja IoT

- Teollisuusautomaatiojärjestelmiin erikoistunut tietoturvayhtiö Dragos julkaisi vuosikatsauksensa. [9] Keskeisiä havaintoja olivat joidenkin uhkatoimijoiden siirtyminen jalansijojen hankinnasta aktiiviseen vahingontekoon ja järjestelmien haltijoiden jatkuvat vaikeudet havainnoida uhkatoimintaa.
- Robotti-imurijärjestelmästä paljastui suojauspuutteita, [10] jotka mahdollistivat pääsyn 7000 imuriin 24 maassa. Tapaus osoittaa, miten AI-työkaluja voidaan hyödyntää haavoittuvuuksien löytämisessä. Se korostaa myös riippumattomien tietoturva-auditointien, toimivien haavoittuvuusraportointikanavien ja CRA:n edellyttämien perustason suojausten tärkeyttä.

Verkkojen toimivuus

- Suomessa havaittujen palvelunestohyökkäysten vaikutukset rajautuivat väliaikaisiin häiriöihin.
- Haittaohjelmia, joilla verkkolaitteita liitetään osaksi bottiverkkoja, käytetään myös muuhun kyberrikollisuuteen, kuten mainospetoksiin ja tiedonkeruuseen.
- Helmikuussa yleisissä viestintäverkoissa ei havaittu vakavia toimivuushäiriöitä.

Kybersää
kulunut 12 kk

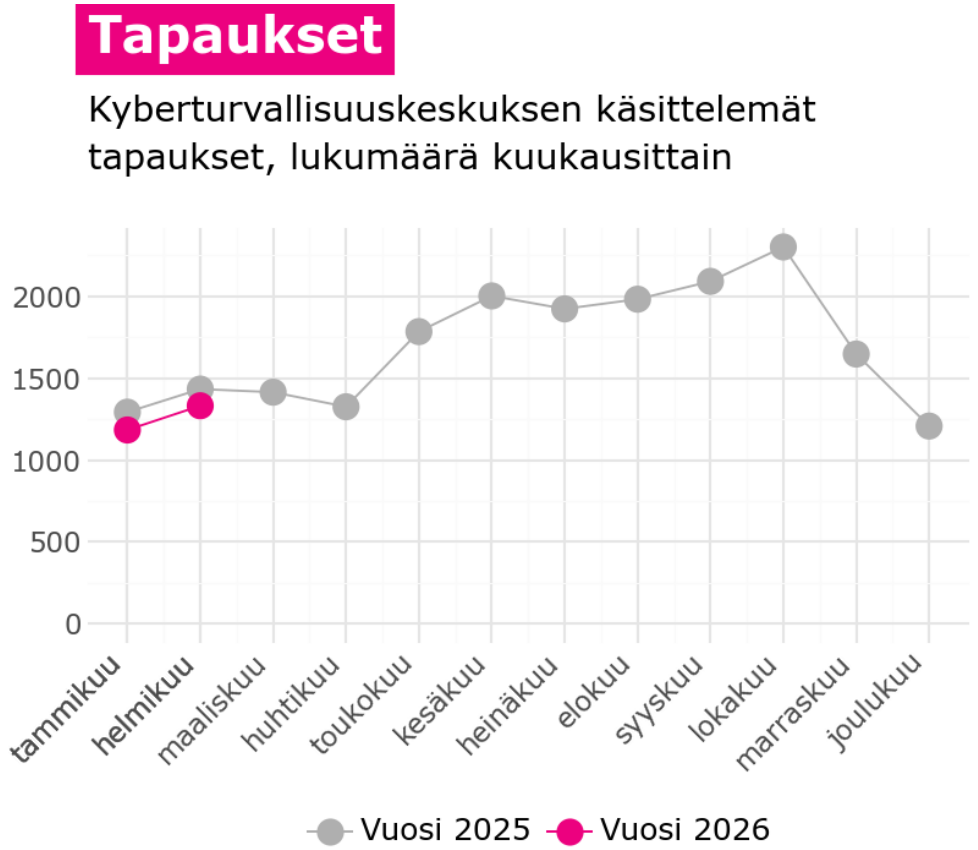


Kybersää lukuina

Tässä osiossa kerromme
Kyberturvallisuuskeskuksen käsittelemien tapausten
lukumääriä ja havaintoja kuluneelta kuukaudelta.

Tapaukset

- Kyberturvallisuuskeskus käsitteli helmikuussa 1 332 tapausta. Tämä on noin 20 % vähemmän kuluneen 12 kuukauden keskiarvoon nähden.
- Helmikuun aikana raportoitiin useita kriittisiä haavoittuvuuksia laajasti käytetyissä ohjelmistoissa ja palveluissa. Vaikka haavoittuvuudet ovat olleet vakavia ja mahdollistaisivat pahimmillaan järjestelmien haltuunoton tai tietojen luvattoman käytön, niiden vaikutukset ovat toistaiseksi jääneet vähäisiksi Suomessa. Haavoittuvuuksien hyväksikäyttöyrityksiä kuitenkin havaitaan jatkuvasti ja näihin on organisaatioiden tärkeää varautua.
- Helmikuun aikana on havaittu myös kasvua M365-tilimurroissa ja -kalasteluissa. Vaikka tapausten määrä ei ole vielä yltänyt edellisen vuoden syksyn tasolle, kasvu on huolestuttava ilmiö.



Kybersääennuste
Kyberuhat pysyvät tavanomaisina

Edellisen sääennusteen arvio haavoittuvuuksien ja tilimurtojen hyväksikäyttöjen kerrannaisvaikutuksista toteutui helmikuussa. Sama kehitys jatkuu edelleen: on odotettavissa, että runsastuneet M365- ja muiden käyttäjätilien murrot johtavat esimerkiksi laskutuspetoksiin, kuten toimitusjohtajahuijauksiin. Murretuilta tileiltä lähetetään myös jatkokalasteluviestejä.

Lähi-idän nopeasti muuttuvalla tilanteella voi olla odottamattomia kerrannaisvaikutuksia Suomeen esimerkiksi monimutkaisten toimitusketjujen kautta.

Organisaation varautuminen

- Valistaminen ja monivaiheinen tunnistautuminen (MFA) eivät riitä suojaamaan työntekijöitä kehittyneiltä tilimurtoyrityksiltä, kuten AiTM-tekniikkaa käyttävältä kalastelulta.
- Organisaatioissa kannattaa ottaa käyttöön kehittyneitä turvallisuusominaisuuksia, kuten ehdollisen pääsyn (conditional access) käytäntöjä, riskipohjainen tunnistautuminen (risk-based authentication) ja jatkuva pääsyn arviointi (continue access evaluation).

Huolestuttava

Kyberuhkien määrä ja vakavuus ovat tavanomaisella tasolla.

Kyberuhat voivat kuitenkin muuttua nopeasti, myös negatiiviseen suuntaan.

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.

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
EU hyväksyi työkalupakin ICT-toimitusketjun turvallisuuden vahvistamiseksi

- EU:n NIS-yhteystyöryhmä hyväksyi uuden työkalupakin ICT-toimitusketjun turvallisuuden vahvistamiseksi (ICT Supply Chain Security Toolbox). [11]
- Jäsenmaat ovat kehittäneet työkalupakin yhteistyössä Euroopan komission ja EU:n kyberturvallisuusvirasto ENISA:n kanssa. Työkalupakin laatimisen taustalla ovat EU-neuvoston ICT-toimitusketjun turvallisuutta koskevat päätelmät vuodelta 2022.
- Työkalupakki tarjoaa EU-maille yhteisen lähestymistavan ICT-toimitusketjujen kyberturvallisuusriskien tunnistamiseen, arviointiin ja lieventämiseen. Työkalupakissa suositellaan, että EU-maat rajoittavat korkean riskin toimijoiden käyttöä prioriteettisektoreilla.
- Työkalupakki auttaa jäsenmaita sekä julkisen ja yksityisen sektorin toimijoita vahvistamaan ICT-toimitusketjujen turvallisuutta komission kyberturvallisuusasetuksen uudistamista koskevan ehdotuksen (CSA2) mukaisesti. [12]
- Työkalupakin suositukset ovat ei-sitovia, mutta päivitetyn kyberturvallisuusasetuksen vaatimukset olisivat oikeudellisesti sitovia.

Oikeudelliset asiat
EU julkaisi työkalupakin merikaapeliturvallisuuden vahvistamiseksi

- Euroopan komissio julkaisi raportin, joka sisältää merikaapeliturvallisuuden työkalupakin (Submarine Cable Security Toolbox) sekä Euroopan kannalta merkittävät merikaapelihankkeet (CPEI). Samanaikaisesti julkaistiin 347 miljoonan euron rahoituspaketti strategisiin merikaapelihankkeisiin. [13]
- Julkaisu on osa 21.2.2025 hyväksyttyä EU:n kaapeliturvallisuutta koskevaa toimintasuunnitelmaa, jonka tavoitteena on kasvattaa Euroopan merikaapeleiden turvallisuutta ja resilienssiä. Raportti on jatkoa komission 23.10.2025 julkaisemalle EU:n merikaapeli-infrastruktuurien turvallisuutta ja resilienssiä koskevalle raportille. [14]
- Työkalupakki sisältää EU:n laajuisia suosituksia keinoista, joilla pyritään lieventämään lokakuussa julkaistussa raportissa tunnistettuja riskejä. Työkalupakki sisältää suosituksia fyysisistä ja kyberturvallisuustoimenpiteistä sekä riippuvuuden vähentämisestä EU:n ulkopuolisista toimijoista.
- Työkalupakin suositukset ovat ei-sitovia, mutta samanlaisia oikeudellisesti sitovia vaatimuksia voisi tulla sovellettavaksi komission 20.1.2026 ehdottaman uuden kybertuvallisuussääntelyn myötä.

Oikeudelliset asiat
Hallitus esittää, että jammereiden luvattomasta hallussapidosta tulisi rangaistavaa

- Hallitus antoi eduskunnalle lakiesityksen 19.2.2026 koskien radiohäirintään tarkoitettujen radiolaitteiden eli nk. jammereita koskevan lainsäädännön muuttamista. Muutokset tehtäisiin sähköisen viestinnän palveluista annettuun lakiin.
- Esityksessä ehdotetaan muutoksia sääntelyyn, joka koskee radiotaajuista viestintää häiritseviä tai väärentäviä laitteita. Radiotaajuista viestintää käyttävät esimerkiksi matkaviestinverkot ja satelliittipaikannusjärjestelmät, kuten GPS.
- Tällä hetkellä jammereita pidetään radiolähettiminä, joiden hallussapito on luvanvaraista. Esityksellä luotaisiin jammereille radiolähettimistä erillinen määritelmä, joka mahdollistaisi radiolähettimiä tiukemman sääntelyn.
- Jammereiden oikeudeton hallussapito kriminalisoitaisiin, mikä mahdollistaisi laitteiden takavarikoinnin. Oikeudettoman hallussapidon kriminalisointi parantaisi muun muassa viranomaisten mahdollisuuksia puuttua laitteiden maahantuontiin.
- Muutos asettaisi selkeämmät ehdot laitteiden käytöstä ja hallussapidosta viranomaisille ja muille oikeutetuille tahoille. [15]

Oikeudelliset asiat
Lakiesitys maanalaisen verkkoinfran sijaintitiedoista

- Liikenne- ja viestintäministeriössä valmisteltu lakiesitys maanalaisen verkkoinfrastruktuurin sijaintitiedoista mahdollistaisi sijaintiselvityspalvelun. Hallituksen esitysluonnos on ollut lausuntokierroksella 12.3.2026 saakka. Lakiesitys on tarkoitus antaa eduskunnalle keväällä 2026, ja tavoitteena on saada laki voimaan 1.1.2027.
- Tällä hetkellä maanalaisten verkkojen verkkotietoja hallinnoivat hajanaisesti eri toimijat. Myös sijaintitietoja hallinnoivien palveluiden turvallisuus vaihtelee.
- Laki mahdollistaisi sijaintiselvityspalvelun toteuttamisen. Verkkotietojen selvittäminen olisi mahdollista alueidenkäytön suunnittelua sekä maan- ja vesistönrakennusta harjoittaville toimijoille yhden sähköisen tietopisteen kautta. Tavoitteena on parantaa verkkoinfrastruktuuria koskevien sijaintitietojen hallinnointia ja turvallisuutta sekä vähentää maanalaiseen rakentamiseen liittyviä kaivuuvahinkoja.
- Palvelussa verkkotoimija voisi valita, toimiiko se keskitetyssä vai hajautetussa järjestelmässä. Keskitetyssä järjestelmässä verkkotoimijat toimittaisivat verkkotietonsa järjestelmään etukäteen. Liikenne- ja viestintävirasto Traficom käsittelisi sijaintiselvityspyynnöt ja -vastaukset ja valvoisi niitä. Hajautetussa järjestelmässä toimittajat hallinnoisivat omia verkkotietojaan.
- Laki sisältäisi useita uusia turvallisuuteen liittyviä vaatimuksia. Myös verkkotietojärjestelmiä hallinnoivien yritysten ja verkkotietoja käyttävien yritysten turvallisuussääntelyä yhdenmukaistettaisiin ja vahvistettaisiin. Sijaintiselvitysvastauksissa ei jaettaisi tietoa kriittisestä infrastruktuurista. [16]

Oikeudelliset asiat
CRA:n soveltamisohjeet kommentoitavana

- Komissio on laatinut ohjeluonnoksen EU:n kyberkestävyyssäädöksen (Cyber Resilience Act, CRA) soveltamiseen.
- Ohjeistus antaa sääntelyn kohteille käytännön tukea CRA:n vaatimusten tulkintaan ja toimeenpanoon.
- Sidosryhmiltä toivotaan palautetta ohjeistukseen 31.3.2026 mennessä.
- Ohjeistus on luettavissa ja kommentoitavissa EU-komission verkkosivuilla. [17]

Lähteet

Lähdeluettelo
1/2

1. https://www.kyberturvallisuuskeskus.fi/fi/kriittisia-haavoittuvuuksia-cisco-catalyst-sd-wan-tuotteissa
2. https://www.epressi.com/tiedotteet/koulutus/kansallinen-kyberharjoitus-vahvisti-kunta-ja-logistiikkatoimijoiden-kyberosaamista.html
3. https://www.forbes.com/sites/daveywinder/2026/02/28/iran-plunges-into-near-total-internet-blackout-as-epic-fury-strikes-begin/
4. https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026
5. https://www.ncsc.gov.uk/news/ncsc-advises-uk-organisations-take-action-following-conflict-in-middle-east
6. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/kvanttiturvallinen
7. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-072026
8. https://kehittajille.suomi.fi/palvelut/digiturva/jatkuvuuden-hallinta-ja-varautuminen/harjoitustoiminta/harjoitusten-vaikutusten-varmistaminen-ja-kehitystoimien-vieminen-kaytantoon
9. https://www.dragos.com/ot-cybersecurity-year-in-review
10. https://www.malwarebytes.com/blog/news/2026/02/hobby-coder-accidentally-creates-vacuum-robot-army

Lähdeluettelo
2/2

11. https://digital-strategy.ec.europa.eu/en/news/ict-supply-chain-security-eu-adopts-toolbox-mitigate-risks
12. https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security
13. https://digital-strategy.ec.europa.eu/en/news/commission-increases-submarine-cable-security-eu347-million-investment-and-new-toolbox
14. https://digital-strategy.ec.europa.eu/en/library/submarine-cable-security-toolbox-and-cable-projects-european-interest
15. https://lvm.fi/-/hallitus-esittaa-etta-jammereiden-luvattomasta-hallussapidosta-tulisi-rangaistavaa
16. https://lvm.fi/-/lausuntokierros-lakiesitys-maanalaisen-verkkoinfran-sijaintitiedoista-mahdollistaa-sijaintiselvityspalvelun
17. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16959-Draft-Commission-guidance-on-the-Cyber-Resilience-Act_en