TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Huhtikuu 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

Keväällä 2026 satelliittinavigoinnin (GNSS) ja matkaviestinverkkojen häiriöt sekä Traficomin tekemät häirintähavainnot ovat lisääntyneet. GNSS-häiriöitä havaitaan erityisesti ilmailussa eteläisen ja keskisen Suomen alueella kaikkina vuorokauden aikoina.[1]

Tekstiviestien lähettäjien tunnistaminen tiukentui 4.5.2026, kun viestien lähettäjien tunnistaminen ja lähettäjätunnusten käyttöoikeuden varmistaminen tuli pakolliseksi organisaatioille, jotka lähettävät tekstiviestejä kansalaisille. Uudistetun määräyksen tavoitteena on estää organisaatioiden nimissä lähetettäviä huijausviestejä.[2]

EU käynnistää tekoälyyn, drooneihin, robotiikkaan ja kvanttiteknologiaan perustuvan AGILE-ohjelman nopeuttamaan Euroopan puolustusteknologian kehitystä. Ohjelman 115 miljoonan euron pilottivaiheen rahoitus suunnataan erityisesti startupeille ja pk-yrityksille. Ohjelmalla varmistetaan nopea rahoitusprosessi sekä mahdollisuus siirtyä kenttätestaukseen 1–3 vuodessa.[3, 4]

Kybersään yleistilanne huhtikuussa 2026

Huhtikuu ei tuonut mukanaan merkittävää muutosta kybersäähän

Lämpenevää kevätsäätä viilensivät erityisesti M365-tilimurrot, joita ilmoitettiin Kyberturvallisuuskeskukselle edellistä kuukautta enemmän. Kuukauden aikana maahan ropisi myös sadepisaroita useissa eri tuotteissa julkaistujen haavoittuvuuksien vuoksi.

Tekoälypohjaisten ratkaisujen hyödyntäminen haavoittuvuuksien kartoittamisessa ja hyväksikäytössä nousi kuukauden puheenaiheeksi.

Tekoälyn hyväksikäytön on havaittu yleistyneen myös petoksissa.

- Kyberturvallisuuskeskuksen tiedossa on toistaiseksi vain yksittäisiä tapauksia, joissa on käytetty tekoälyllä tuotettua ääntä ja kuvaa esimerkiksi toimitusjohtajahuijauksissa ja sijoituspetoksissa.

Traficom julkaisi vuoteen 2035 sijoittuvat kyberturvallisuuden skenaariot, jotka kuvaavat neljää vaihtoehtoista tulevaisuutta

Kyberturvallisuuden näkökulmasta ratkaiseviksi kysymyksiksi nousevat kaikissa skenaarioissa tekoäly, toimitusketjut, informaatioympäristön luotettavuus sekä kriittisen infrastruktuurin kytkeytyneisyys.

Skenaariot tukevat varautumista, päätöksentekoa ja strategista keskustelua tilanteessa, jossa tulevaisuuden digitaalisen yhteiskunnan turvallisuus rakentuu yhä monimutkaisempien riippuvuuksien varaan. [5, 6]

Traficomin verkkosivuja uudistettiin

Olemme uudistaneet Kyberturvallisuuskeskuksen verkkosivuja osana Traficomin verkkosivualustan uudistusta. Muutos parantaa sivustojen toimivuutta ja mahdollistaa niiden kehittämisen jatkossa. Sivustoilla voi esiintyä yksittäisiä puutteita, kuten rikkinäisiä linkkejä. Korjaamme niitä jatkuvasti. Pahoittelemme uudistuksesta koituneita väliaikaisia häiriöitä. [7]

Kuukauden raekuuro
AI-pohjainen haavoittuvuusskannaus muuttaa pelikenttää

AI-pohjainen haavoittuvuusskannaus nousi laajaksi puheenaiheeksi huhtikuussa sen tarjoamien kyvykkyyksien vuoksi.

Kehittyneiden AI-ratkaisujen on arvioitu tehostavan pahantahtoista haavoittuvuuksien kartoitusta ja lisäävän hyväksikäytettävien haavoittuvuuksien määrää. Tekoälyn avulla voidaan löytää uusia ennalta tuntemattomia haavoittuvuuksia ja tekoäly pystyy käyttämään niitä itsenäisesti hyväksi.

AI-ratkaisuissa hyökkäyspolkujen mallinnus (attack path analysis) helpottuu myös huomattavasti. AI-ratkaisuja hyödyntämällä hyökkääjän on mahdollista löytää ja ketjuttaa erilaisia haavoittuvuuksien hyväksikäytön mahdollistavia tekijöitä, kuten tunnistus-, konfiguraatio- ja logiikkavirheitä kohteena olevassa verkkoympäristössä.

Tämä haastaa perinteisiä skannausmenetelmiä, jotka eivät välttämättä tunnista löydettyjen haavoittuvuuksien kokonaisriskiä.

Kehittyneiden AI-ratkaisujen ei kuitenkaan uskota täysin korvaavan perinteistä tunnisteisiin pohjaavaa haavoittuvuusskannausta, vaan ne muuttavat toiminnan luonnetta itsenäisemmäksi, nopeammaksi sekä kokonaisvaltaisemmin uhkia ja riskitekijöitä huomioivaksi suorituskyvyksi.

AI-pohjaiset sovellukset ovat siten samalla mahdollisuus organisaatioiden riskienhallinnan ja kyberturvallisuuden parantamiseksi. Esimerkiksi joidenkin ennusteiden mukaan tekoälysovelluksilla voidaan peräti kattaa puolet nykyisistä kyberhyökkäysten suojaus- ja torjuntatoimista vuoteen 2028 mennessä.[8]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Ilmoittaudu mukaan Traficomin, liikenne- ja viestintäministeriön sekä Kyberala ry:n 3. kesäkuuta järjestämään EU:n kyberkestävyyssäädöksen (CRA) voimaantuloa koskevan infotilaisuuteen. Tapahtumassa EU-komission, kansallisten viranomaisten ja yritysten edustajat tuovat esiin näkökulmia sääntelyn sisältöön, velvoitteisiin ja sen kansalliseen toimeenpanoon. [9]

Organisaatioita kannustetaan siirtymään tietojenkalasteluille resistentteihin menetelmiin, kuten FIDO2/WebAuthn tai varmennepohjaiseen tunnistautumiseen. Perinteinen monivaiheinen tunnistautuminen (MFA) kyetään yhä useammin ohittamaan Adversary-in-the-Middle (AiTM) -hyökkäyksillä, OAuth-väärinkäytöillä ja istuntotunnisteiden varastamisella. [10, 11]

FINMISP-palvelu on julkaistu! FINMISP on Kyberturvallisuuskeskuksen tarjoama kansallinen kyberuhkatiedon jakopalvelu, joka perustuu MISP-alustaan (Malware Information Sharing Platform). Palvelun avulla tehostetaan teknisen uhkatiedon jakamista kansallisesti ja kansainvälisesti havaituista tietoturvapoikkeamista. Kyberturvallisuuskeskus toimii verkoston keskuksena ja jakaa tietoa palvelun asiakkaille. [12]

Kybersään ilmiöt

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä.

Kybersää
huhtikuu 2026

1 kk

Tietomurrot- ja vuodot

Tietomurtoja ilmoitettiin 14 % enemmän kuin maaliskuussa. Tietovuotoja raportoitiin kuitenkin huhtikuussa vähemmän. Useiden raportoitujen tietovuototapausten taustalla oli virheellinen konfiguraatio.

Haittaohjelmat

Kuukausi oli aktiivinen haittaohjelmahavaintojen osalta. Kyberturvallisuuskeskus sai ilmoituksia mm. ClickFix-tekniikalla levitetyistä haittaohjelmista, yksittäisistä Magecart- ja infostealer-haittaohjelmista.

Haavoittuvuudet

Julkaistujen haavoittuvuuksien määrä pysyi korkeana myös huhtikuussa. Verkkoon näkyvien laitteiden ja palveluiden nopea päivittäminen korostuu edelleen haavoittuvuuksien hyväksikäyttömahdollisuuksien vähentämiseksi.

Huijaukset ja kalastelut

Viranomaisviestintä siirrettiin huhtikuussa kokonaan suomi.fi-palveluun. Huijarit seuraavat tilannetta ja lähettävät linkkejä väärennettyihin palveluihin.

Hotelli- ja matkavarauspalveluhuijaukset yleistyvät lomakauden lähestyessä.

Automaatio ja IoT

Yhdysvaltain viranomaiset julkaisivat ohjeen nollaluottamusperiaatteiden soveltamisesta OT-järjestelmiin.

IoT-laitteet ja kuluttajatason verkkolaitteet ovat kiinnostavia hyökkäyksen kohteita myös valtiollisille toimijoille.

Verkkojen toimivuus

Tekoälypalveluita organisaation ulkopuolelle tarjotessa tulee huomioida mahdollisuudet niiden kuormittamiseen.

Tekoälyn hyödyntämisen myötä kasvavat määrät ohjelmistohaavoittuvuuksia voivat näkyä palvelunestohyökkäyksiin käytettävien bottiverkkojen kasvuna.

Kybersää
huhtikuu 2026 1/2

1 kk

Tietomurrot ja -vuodot

- Huhtikuussa ilmoitettiin selvästi edellistä kuukautta enemmän murrettuja M365-tilejä. Suurin osa tunnuksista kalasteltiin AiTM-tekniikalla, joten pelkkä MFA-suojaus ei enää riitä estämään tilimurtoja.
- Murretuilta tileiltä lähetettiin tuhansia jatkokalasteluviestejä, minkä arvioidaan lisäävän tietomurtoja edelleen toukokuussa.
- Useita WordPress-sivustoja murrettiin lisäosien haavoittuvuuksia hyödyntämällä. WordPressin ja lisäosien säännöllinen päivittäminen on tärkeää. Lisäksi kannattaa varmistaa, kuuluuko päivitysvastuu webhotellipalvelun tarjoajalle vai sivuston ylläpitäjälle.

Haittaohjelmat

- Magecart-haittaohjelmia havaittiin yksittäisissä verkkokaupoissa. Haittaohjelman avulla pyritään anastamaan verkkokauppaan syötettyjä henkilö- ja pankkitietoja.
- Kyberturvallisuuskeskus sai lisäksi ilmoituksia ClickFix-tekniikalla levitetyistä haittaohjelmista.
- Tietojenkalastelun ja haavoittuvuuksien avulla on pyritty levittämään myös haitallisia ohjelmistoja sekä infostealer-haittaohjelmia.
- Maaliskuussa tapahtuneet toimitusketjuhyökkäykset avoimien lähdekoodien kirjastoihin näkyvät edelleen hyökkäysvektorina haittaohjelmien levityksessä.

Haavoittuvuudet

- CVE-2026-31431 ”Copy Fail” -haavoittuvuus Linux-kernelissä, jonka avulla tavallinen käyttäjä voi saada pääkäyttäjän oikeudet.
- CVE-2026-41940 cPanel ja WHM -tuotteissa, jonka avulla autentikoimattoman hyökkääjän on mahdollista saada pääkäyttäjätason oikeudet hallintapaneeliin. Hyväksikäyttöä havaittu ja välitön päivittäminen suositeltua.
- CVE-2026-35616 FortiClient EMS haavoittuvuus, jonka avulla hyökkääjä voi ottaa haltuunsa laitteen. Haavoittuvuutta hyväksikäytetään aktiivisesti.

Kybersää
huhtikuu 2026 2/2

1 kk

Huijaukset ja kalastelut

- Viranomaisviestintä siirrettiin huhtikuussa kokonaan suomi.fi-palveluun. Huijarit seuraavat tilannetta ja lähettävät linkkejä väärennettyihin palveluihin. Verkkohuijauksen tunnistaminen helpottuu, kun ihmiset saavat tietoa huijauksista etukäteen. Tietoisuus antaa ihmisille mahdollisuuden pysähtyä ja arvioida, onko tekstiviesti, sähköposti tai puhelu aito vai huijaus. Älä seuraa tekstiviestien linkkejä vahvaan tunnistautumiseen.
- Hotelli- ja matkavarauspalveluhuijaukset yleistyvät lomakauden lähestyessä. Mieti kahdesti ja varmista palvelulta ennen kuin maksat yllättäviä ylimääräisiä maksuja.

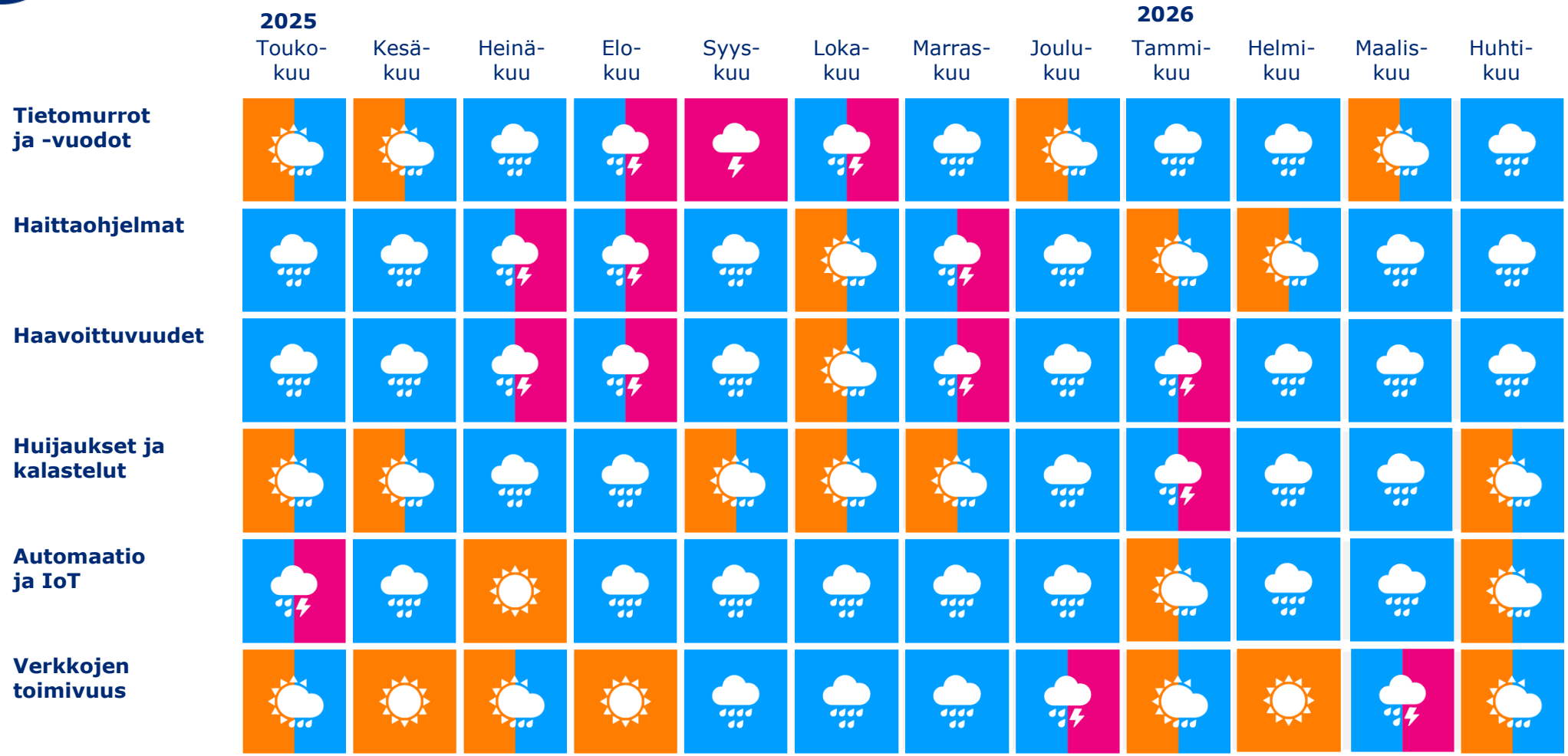
Automaatio ja IoT

- Yhdysvaltalainen viranomaistyöryhmä julkaisi dokumentin nollaluottamusperiaatteiden soveltamisesta OT-järjestelmiin ja -ympäristöihin.[13]
- Heikosti suojatut internetiin kytketyt kamerat ovat kelpo tiedonlähde myös tiedustelupalveluille. Esimerkiksi Iranin ajatolla Khamenein liikkeistä kerrotaan hankitun tietoa liikennekameroiden kuvista.[14]
- Yhdysvaltain kyberturvallisuusvirasto varoitti kiinalaisten kyberuhkatoimijoiden rakentavan peiteverkkoja murretuista IoT-laitteista.[15]

Verkkojen toimivuus

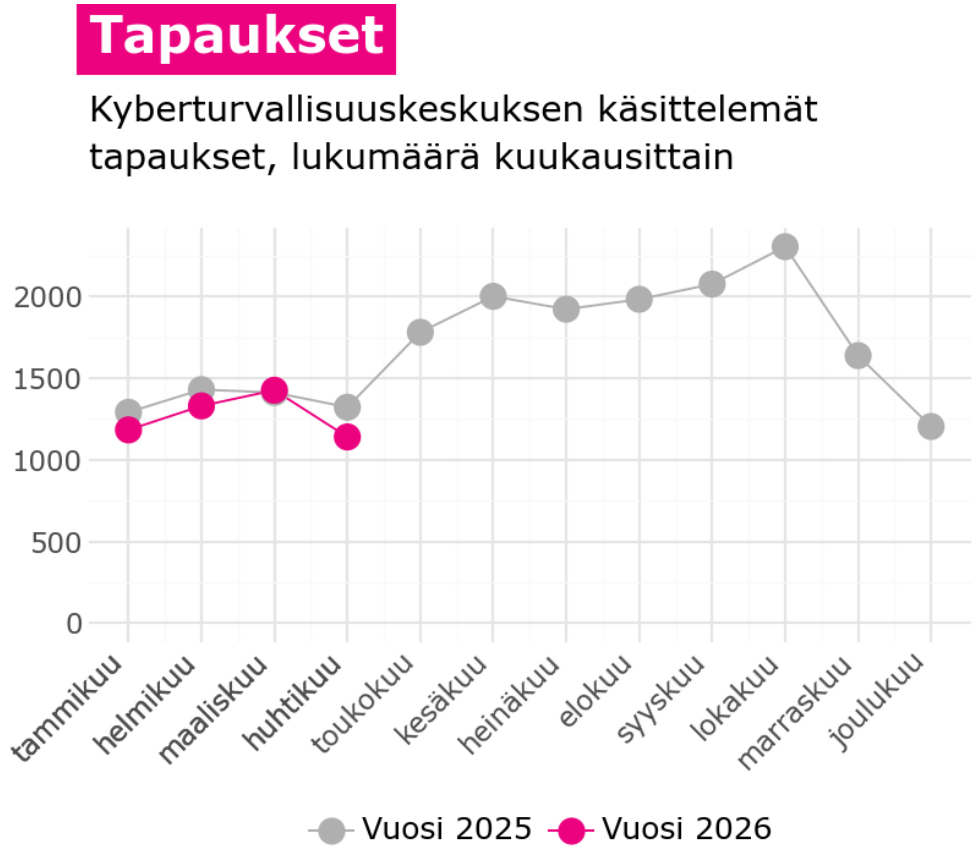
- Huhtikuussa yleisissä viestintäverkoissa ei havaittu vakavia toimivuushäiriöitä.
- Tekoälygeneroidulla sisällöllä voidaan myös ruuhkauttaa organisaation ulkopuolisille tarjoamia tekoälypohjaisia palveluita. Esimerkiksi verkkosivuilla asiakkaita avustavan chatbotin käyttöönotossa on huomioitava sen käyttämien resurssien rajoitukset.
- Palvelun ruuhkautumisen lisäksi massiiviset määrät syötteitä voivat aiheuttaa organisaatiolle ylimääräisiä kuluja.

Kybersään ilmiöt
kulunut 12 kk



Tapaukset

- Kyberturvallisuuskeskus käsitteli huhtikuussa 1140 tapausta.
- Ilmoitusten määrä oli 12 kuukauden keskiarvoon nähden vajaan kolmanneksen alhaisempi. Vaikka tapauksia ilmoitettiin määrällisesti vähemmän, ei niiden luonteessa ole havaittu merkittävää muutosta.
- Kyberturvallisuuskeskukselle ilmoitettujen tapausten osalta kuukausi oli puolipilvinen.
- M365-tilimurtoja havaittiin huhtikuussa edellistä kuukautta enemmän. Tilimurrot johtivat tietojen vaarantumiseen ja jatkokalasteluun useilla eri toimialoilla.
- Huhtikuu oli myös haavoittuvuuksien osalta erittäin aktiivinen.



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

Edelleen runsastuneet M365-tilimurrot ja murretuilta tileiltä lähetetyt jatkokalasteluviestit johtavat todennäköisesti tilimurtoihin myös toukokuussa.

Tekoälyteknologiat ja niiden soveltaminen kehittyvät nopeasti, mikä voi aiheuttaa äkillisiä muutoksia hyökkääjien toimintatavoissa. Toimintaympäristön jatkuva luotaaminen ja siihen mukautuminen on tärkeää organisaatioiden turvallisuuden kannalta.

Organisaation varautuminen

- Haavoittuvuuksienhallinnassa korostuu edelleen verkkoon näkyvien laitteiden ja palveluiden nopea päivittäminen haavoittuvuuksien hyväksikäytön vähentämiseksi.
- Tunne oma verkkoympäristösi, käyttämäsi järjestelmät ja niiden riippuvuudet, sekä korvaa elinkaarensa päähän tulevat järjestelmät ajoissa.
- Valistaminen ja monivaiheinen tunnistautuminen (MFA) eivät riitä suojaamaan työntekijöitä kehittyneiltä tilimurtoyrityksiltä, kuten AiTM-tekniikkaa käyttävältä kalastelulta.

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
Luonnos Traficomin määräykseksi teletoiminnan häiriötilanteista lausuntokierrokselle

- Liikenne- ja viestintävirasto Traficom pyytää lausuntoa luonnoksista määräykseksi teletoiminnan häiriötilanteista sekä sen perustelumuistioksi.[16]
- Määräyksellä ajantasaistetaan 1.1.2020 voimaan tullut Liikenne- ja viestintäviraston määräys teletoiminnan häiriötilanteista (66A/2019M) TRAFICOM/402245/03.04.05.00/2019.
- Määräysluonnosta on valmisteltu yhteistyössä toimialan ja eri viranomaistahojen kanssa työryhmässä vuoden 2025 ja alkuvuoden 2026 aikana.
- Määräys tarkentaa sähköisen viestinnän palveluista annetun lain (917/2014) säännöksiä, joiden mukaan teleyrityksen on ilmoitettava viipymättä tilaajalle ja käyttäjälle, sekä Liikenne- ja viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus taikka muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti.
- Lausunto pyydetään toimittamaan Liikenne- ja viestintävirastolle lausuntopalvelun kautta viimeistään 5.6.2026.

Oikeudelliset asiat
Liikenne- ja viestintäministeriön kysely kyberturvallisuuslain vaikutuksista

- Liikenne- ja viestintäministeriössä on käynnistetty hanke kyberturvallisuuslain (124/2025) seurannasta ja arvioinnista.
- Tarkoituksena on tarkastella lain vaikuttavuutta, tehokkuutta ja tarkoituksenmukaisuutta sekä kehittämistoimenpiteitä.
- Osana hanketta ministeriö on julkaissut Lausuntopalvelu.fi –palvelussa kyselyn, jossa kerätään tietoja kyberturvallisuuslain vaikutuksista sen soveltamisalaan kuuluville yrityksille ja organisaatioille.[17]
- Kysely on tarkoitettu ensisijaisesti sellaisille yrityksille ja organisaatioille, joihin sovelletaan kyberturvallisuuslain velvoitteita, sekä edunvalvojille, jotka edustavat kyberturvallisuuslain soveltamisalaan kuuluvia organisaatioita.
- Kyselyssä kartoitetaan muun muassa kyberturvallisuuslain ymmärrettävyyttä ja toimeenpantavuutta, ajantasaisuutta, viranomaisyhteistyön ja raportointivelvoitteiden toimivuutta sekä tarpeita lainsäädäntömuutoksille.
- Kysely on avoinna 15.6.2026 asti.

Oikeudelliset asiat
Lausuntoyhteenveto sijaintiselvityspalvelua koskevasta lakiesityksestä julkaistu

- Liikenne- ja viestintäministeriö pyysi 29.1.-12.3.2026 välisenä aikana lausuntoja hallituksen esitysluonnoksesta, joka koskee lakia maanalaisen verkkoinfrastruktuurin sijaintitiedoista. Lausuntoja saatiin 58 ja ministeriö julkaisi lausuntoyhteenvedon 21.4.2026.[18]
- Lausuttavana olleella lakiesityksellä mahdollistettaisiin maanalaisen verkkoinfrastruktuurin sijaintitietojen parempi selvittäminen.
- Lakiesitys mahdollistaisi verkkotietojen selvittämisen yhden sähköisen tietopisteen kautta. Esitys sisältäisi useita uusia turvallisuuteen liittyviä vaatimuksia.
- Lausunnonantajat pitivät kaivuuvahinkojen ehkäisyä, tietoturvan parantamista ja toimintatapojen yhdenmukaistamista kannatettavina tavoitteina, mutta kriittisiä näkemyksiä esitettiin erityisesti sijaintiselvityspalvelun keskitetystä järjestelmästä.

Oikeudelliset asiat
Hallitus vauhdittaa tekoälyn hyödyntämistä julkisessa hallinnossa

- Suomi vahvistaa tekoälyn hyödyntämistä osana julkisten palvelujen ja hallinnon uudistamista. Vuonna 2026 toteutettavassa selvityksessä tavoitteena on tunnistaa konkreettiset ja nopeasti toteutettavat toimet, joilla tekoälyä voidaan hyödyntää tehokkaammin erityisesti julkisessa hallinnossa jo olemassa olevia ratkaisuja hyödyntäen.[19]
- Selvitys täydentää hallituksen digitaalisuuden ja datatalouden kasvuhankkeita sekä Suomen kansallista Digikompassia. Työssä huomioidaan EU-lainsäädäntö sekä käyttäjien perusoikeudet, turvallisuus ja esteettömyys.

Oikeudelliset asiat
EU vahvistaa digitaalista suvereniteettia

- Euroopan komissio otti käyttöön noin 180 milj. euron pilvipalveluhankinnan, jonka tavoitteena on tarjota EU-instituutioille turvallisia ja EU-lainsäädännön mukaisia pilvipalveluja sekä vähentää riippuvuutta ulkomaisista toimijoista.[20]
- Neljä eurooppalaista palveluntarjoajaa valittiin rinnakkain, jotta vältetään riippuvuus yhdestä toimijasta ja parannetaan järjestelmän luotettavuutta sekä joustavuutta.[21]
- Hankinta toimii mallina tuleville pilvipalveluratkaisuille: se osoittaa, että korkeat suvereniteetti- ja turvallisuusvaatimukset voidaan saavuttaa käytännössä ja ohjaa markkinaa kohti EU-arvojen mukaisia ratkaisuja.[20]
- Cloud Sovereignty Framework tuo selkeät ja standardoidut kriteerit suvereniteetin arviointiin (esim. juridinen kontrolli, turvallisuus ja toimitusketju), jolloin vaatimukset voidaan sisällyttää konkreettisesti hankintoihin.[22]
- Digitaalisen suvereniteetin vahvistamista on käsitelty myös kansallisella tasolla. Yhteiskunnan uudistamisen ministerityöryhmä linjasi 27.4. järjestetyssä kokouksessaan toimista, joilla digitaalista suvereniteettia vahvistetaan nykyisen hallituskauden loppuun mennessä.[23]

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
1/3

1. https://traficom.fi/fi/uutiset/matkaviestin-ja-satelliittinavigointipalveluiden-hairiot-jatkuvat-suomessa-edelleen
2. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-182026
3. https://www.project-agile.eu/
4. https://defence-industry-space.ec.europa.eu/eu115-million-programme-agile-and-rapid-defence-innovation-agile-2026-03-26_en
5. https://www.traficom.fi/fi/uutiset/tekoaly-ja-keskinaisriippuvuudet-muovaavat-teknologisen-toimintaympariston-uusiksi-kyberturvallisuuden-skenaariot-2035-varoittavat-riskeista
6. https://www.traficom.fi/fi/julkaisut/kyberturvallisuuden-skenaariot-2035
7. https://traficom.fi/fi/uutiset/traficomin-verkkosivujen-julkaisualusta-uudistettu
8. https://www.gartner.com/en/newsroom/press-releases/2026-03-17-gartner-predicts-ai-applications-will-drive-50-percent-of-cybersecurity-incident-response-efforts-by-2028
9. https://www.kyberturvallisuuskeskus.fi/fi/tapahtumat/eun-kyberkestavyyssaados-cra-tulee-voimaan-infotilaisuus-362026
10. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/liity-finmisp-palveluun

Lähdeluettelo
2/3

11. CERT-EU: Threat Landscape Report 2025:/https://www.cert.europa.eu/publications/threat-intelligence/tlr2025
12. https://www.kyberturvallisuuskeskus.fi/fi/ohjeet-ja-oppaat/ohjeet-ja-oppaat-tietoturva-ammattilaisille/aitm-adversary-middle-hyokkaykset-ja-niiden-torjunta
13. https://www.ic3.gov/CSA/2026/260429
14. https://www.darkreading.com/cyber-risk/wartime-usage-of-compromised-ip-cameras-highlight-their-danger. 27.3.2026
15. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-113a. 23.4.2026
16. https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=33270cab-43de-4da3-9d4e-4314dd312303
17. https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1bfc0c5a-7bff-4c82-9bf9-17d30f0827c6
18. https://valtioneuvosto.fi/hanke?tunnus=LVM013:00/2025
19. https://lvm.fi/-/194055633/hallitus-vauhdittaa-tekoalyn-hyodyntamista-julkisessa-hallinnossa
20. https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17

Lähdeluettelo
3/3

21. https://interoperable-europe.ec.europa.eu/collection/sovereignty/news/first-commission-tender-sovereign-cloud ja https://europeansting.com/2026/04/20/commission-awards-e180-million-tender-for-sovereign-cloud-to-four-european-providers/

22. https://www.global-political-spotlight.com/articles/government-briefs/eu-awards-180m-sovereign-cloud-procurement-2026-04-17

23. https://lvm.fi/-/10623/ministerityoryhma-linjasi-digitaalisen-suvereniteetin-vahvistamisesta-tiekartta-ohjaa-toimia-hallituskauden-loppuun