TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Tammikuu 2026

Kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

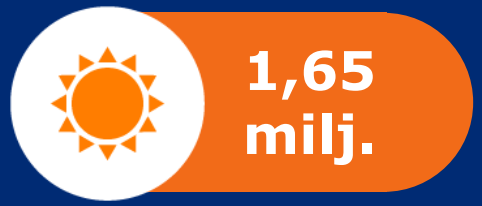
Tämä tuote on suunnattu ensisijaisesti eri tasoilla organisaatioiden tietoturvallisuuden parissa työskenteleville. Kybersää tarjoaa nopean kokonaiskuvan, mitä kyberturvallisuuskentällä on tapahtunut ja mitä on tulossa.

Kybersää voi olla:  rauhallinen  huolestuttava  vakava

Kuukauden tunnuslukuja

Vuonna 2025 Kyberturvallisuuskeskus vastaanotti 20 890 kyberpoikkeamailmoitusta. Luku on linjassa edellisvuoden kanssa. [1]

Suomalaisilta yritettiin huijata 148 miljoonaa euroa vuonna 2025, mikä tarkoittaa noin 38 % kasvua edellisvuoteen. Pankit saivat estettyä tai palautettua näistä yli puolet. [2]



Traficom on myöntänyt rahoitustukea yhteensä 1,65 milj. euroa kyberturvallisuuslain toimeenpanemisen tukemiseksi lain soveltamisalaan kuuluville pk-yrityksille. Tukea myönnettiin yhteensä 35 hakijalle. [3, 4]

Kybersään yleistilanne

Tammikuu oli sateinen

Kuukauden kybersäässä näkyivät jälleen eri laitevalmistajien verkonreunalaiteista löydetyt haavoittuvuudet, joiden hyväksikäyttöä on havaittu maailmanlaajuisesti.

Lisäksi M365-tilien kaappaukseen tähtääviä tietojenkalasteluviestejä liikkui edelleen runsaasti. M365-tietomurtojen tunnistaminen on vaikeaa ilman järjestelmän aktiivista valvontaa ja kirjautumislokien seurantaa.

Tarkastelujaksolla paljastui poikkeuksellinen tietomurto, jossa hyökkääjällä kerrotaan olleen luvaton pääsy energia-alan yrityksen verkkopalveluun lähes vuoden ajan. Tapaus paljastui, kun yrityksen verkkosivustolla havaittiin sinne kuulumatonta sisältöä.

- Julkisuudessa esitettyjen arvioiden mukaan hyökkääjä on päässyt käsiksi noin 31 000 sähkösopimustietoihin Suomessa. [5]

Tammikuussa puhuttivat myös tekoälyavustajien yleistyminen organisaatioissa, sekä niihin liittyvät tietoturva- ja kyberturvallisuushaasteet, jotka on huomioitava avustajien käyttöönottoa suunnitellessa ja niitä käyttäessä. Julkaisimme aiheesta artikkelin, joka kokoaa keskeiset näkökulmat ja suositukset AI-avustajien turvalliseen ja vastuulliseen käyttöön. [6]

Julkaisimme katsauksen vuoteen 2025

Kyberturvallisuuskeskuksen asiantuntijoiden koostama Kyberturvallisuuden vuosi 2025 -julkaisu tarjoaa kokonaiskuvan vuoden keskeisistä kyberuhista Suomessa. Lisäksi katsaus antaa suuntaviivoja organisaatioille,mitä vuosi 2026 mahdollisesti tuo mukanaan ja millaisia toimenpiteitä muuttuva uhkakenttä edellyttää. [7, 8]

Kyberturvallisuuskeskuksen **toimenpiteet ja vinkit varautumiseen**

Autonomisiin tekoälyagentteihin kohdistuu juuri nyt suuria odotuksia. Kielimalleilla toteutettavaan älykkäämpään automaatioon liittyy samalla uusia kyberturvallisuusriskejä. Traficomin ja Huoltovarmuuskeskuksen uusi ohjeistus auttaa organisaatioita suunnittelemaan, rakentamaan ja ylläpitämään agenttisia tekoälyjärjestelmiä turvallisesti. [9]

Traficomin trendiraportti nostaa esiin kolme liikenteen, viestinnän ja kyberturvallisuuden trendiä, joihin on lähivuosina kiinnitettävä huomiota. Yhteiskunnan digitalisoitumisen myötä kyberturvallisuus on yhä tärkeämpi osa kokonaisturvallisuutta. [10]

EU-rahoitteinen projekti SECURE myöntää rahoitustukea pk-yrityksille kyberkestävyyssäädöksen (CRA) toimeenpanemisen tukemiseksi. Tukea voivat hakea eurooppalaiset pk-yritykset, joita CRA:n velvoitteet koskevat. Haku on auki 29.3.2026 asti. [11, 12]

Valtiovarainministeriön ja Traficomin yhteistyössä valmistelema arviointikriteeristö julkisen hallinnon pilvipalveluille (Kansallinen kriteeristöpankki, KriPa): tavoitteena on tukea viranomaisten riskienhallintaa pilvipalveluiden käytössä sekä edistää turvallisuusluokitellun, salassa pidettävän ja julkisen tiedon asianmukaista suojaamista. Kriteeristön on määrä valmistua syksyn 2026 aikana. [13]

Kuukauden raekuuro
Puolan energiainfrastruktuuriin kohdistui laajamittaisia kyberhyökkäyksiä

Puolan energiainfrastruktuurin useisiin kohteisiin tehtiin joulukuun lopulla (29.12.) laajamittainen koordinoitu järjestelmiä ja tietoa tuhoava kyberhyökkäys, jossa jalansijoja oli saatu todennäköisesti jo kuukausia ennen tehtyjä vahingollisia toimia. Puolan kyberturvallisuusviranomainen julkaisi tapauksesta raportin tammikuussa. [14]

Hyökkäykset kohdistuivat etenkin uusiutuvan energian tuotantolaitoksien ja sähkön jakeluverkkoyhtiöiden (DSO) välissä sijaitseviin liittymispisteisiin, joissa sijaitsee verkon reunalaitteita sekä sähköverkon ohjaukseen käytettyjä teollisuusautomaatiolaitteita. Jakeluverkkoyhtiöiltä katosi näkyvyys ja hallinta liittymispisteisiin. Lämmön ja sähkön tuotantolaitoksen työasemilta ja palvelimilta tuhottiin tietoja ja osasta laitteista saatiin tehtyä käyttökelvottomia.

Vaikka tapaus oli vakava, se ei vaikuttanut sähkön- tai lämmöntuotantoon eikä Puolan sähköjärjestelmän tilaan.

Tapaus on herättänyt laajaa huomiota

- Puolan julkaiseman raportin mukaan hyökkäyksissä on tunnistettu viitteitä valtiollisten uhkatoimijoiden käyttämästä hyökkäysinfrastruktuurista.
- Kyseessä on ensimmäinen EU-jäsenmaan energiainfrastruktuuriin kohdistunut laajamittainen järjestelmien tuhoamistarkoituksessa tehty hyökkäys. Vastaavia kyberhyökkäyksiä on nähty aiemmin Ukrainassa.
- Tapaukset ovat herättäneet keskustelua kriittisen infrastruktuurin suojaamisen, riskienhallinnan sekä hyvien käytäntöjen jalkauttamisen tärkeydestä myös Suomessa.

Kybersään ilmiöt

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä.

Kybersään ilmiöt tammikuu 2026

1 kk

Tietomurrot ja -vuodot

Tammikuu oli pääosin rauhallinen. M365-tilien murtoilmoitukset lisääntyivät loppukuussa. Energia-alan verkkosivuille murtauduttiin ja henkilötietoja vaarantui.

Haittaohjelmat

Tammikuun aikana Kyberturvallisuuskeskukselle on ilmoitettu erilaisten kalastelukampanjoiden yhteydessä välitetyistä haittaohjelmista. Ilmoitusten määrät ovat kuitenkin olleet maltilliset.

Haavoittuvuudet

Tammikuussa oli useampia nollapäivähaavoittuvuuksia, joita käytettiin hyväksi tietomurroissa.

Huijaukset ja kalastelut

Yrittäjille oli suunnattu vakuuttavia PRH-huijauksia. Huijausviesteissä pyydettiin päivittämään yrityksen tiedot.

Uusi tekstiviestihuijaus pelottelee epäilyttävällä pankkitapahtumalla soittamaan annettuun puhelinnumeroon.

Automaatio ja IoT

Australian ja kuuden muun maan kyberturvallisuusviranomaiset ovat yhteistyössä luoneet ohjeistuksen teollisuusautomaation verkkoyhteyksien muodostamiseen kyberturvallisesti. Ohje on osa tuotantoympäristöjen kyberturvaamiseen keskittyvää yhteisjulkaisusarjaa.

Verkkojen toimivuus

Suurimmat palvelunestohyökkäyksiin käytettävät bottiverkot ja niiden kyvyt hyökkäyksiin kasvavat jatkuvasti. Isona tekijänä ovat huonosti suojatut kuluttajalaitteet.

Kybersään ilmiöt tammikuu 2026 1/2

1 kk

Tietomurrot ja -vuodot

- Tietomurtoilmoitusten suhteen tammikuu oli rauhallinen.
- M365-tilien tietomurtoilmoitukset kasvoivat loppukuussa.
- Energia-alan organisaation verkkosivuille murtauduttiin, sivuille julkaistiin luvattomia artikkeleita ja osa henkilötiedoista vaarantui.
- Kyberturvallisuuskeskus sai ilmoituksia WhatsApp- ja Telegram-tilien kaappauksista sekä kaappausyrityksistä. Ilmoitusten määrä väheni kuun loppua kohti.
- Lisäksi ilmeni useiden tuotteiden nollapäivähaavoittuvuuksien avulla tehtyjä tietomurtoja.

Haittaohjelmat

- Tammikuu on ollut haittaohjelmahavaintojen puolesta rauhallinen. Kyberturvallisuuskeskukselle on ilmoitettu kuitenkin erilaisten kalasteluviestien liitteenä olleen infostealer-haittaohjelmia. Näitä on jaettu esimerkiksi Discord-palvelun viestien välityksellä.
- Eri bottiverkkoihin liittyvää haittaohjelmaliikennettä havaitaan edelleen Suomessa. Laitteiden turvallisuus paranee, kun ne pidetään ajan tasalla ja hankitaan luotettavilta valmistajilta. Käyttäjän on tärkeää välttää tarpeettomia etäyhteyksiä ja asentaa ohjelmistoja vain luotettavista lähteistä.

Haavoittuvuudet

- Haavoittuvuus MongoDB-tietokantaohjelmistossa mahdollistaa luottamuksellisen tiedon paljastumisen. (CVE-2025-14847)
- Kriittinen haavoittuvuus FortiOS, FortiManager, FortiProxy ja FortiAnalyzer tuotteissa. Hyväksikäyttöä havaittu myös Suomessa. (CVE-2026-24858)
- Kriittisiä haavoittuvuuksia Ivanti Endpoint Manager Mobile (EPMM) tuotteessa. Haavoittuvuuden hyväksikäyttöä on havaittu maailmanlaajuisesti. (CVE-2026-1281 ja CVE-2026-1340)

Kybersään ilmiöt tammikuu 2026 2/2

1 kk

Huijaukset ja kalastelut

- Yrittäjille oli suunnattu vakuuttavan näköisiä PRH-huijauksia. Huijausviesteissä pyydettiin päivittämään yrityksen tiedot ajan tasalle, mutta linkki viekin PRH:n sijasta rikollisen verkkopalveluun.
- Tekstiviestihuijauksiin on tullut uudenlainen teema, jossa uhria pelotellaan epäilyttävällä pankkitapahtumalla soittamaan annettuun puhelinnumeroon. Numerossa ei vastaa pankki, vaan rikollinen huijari.

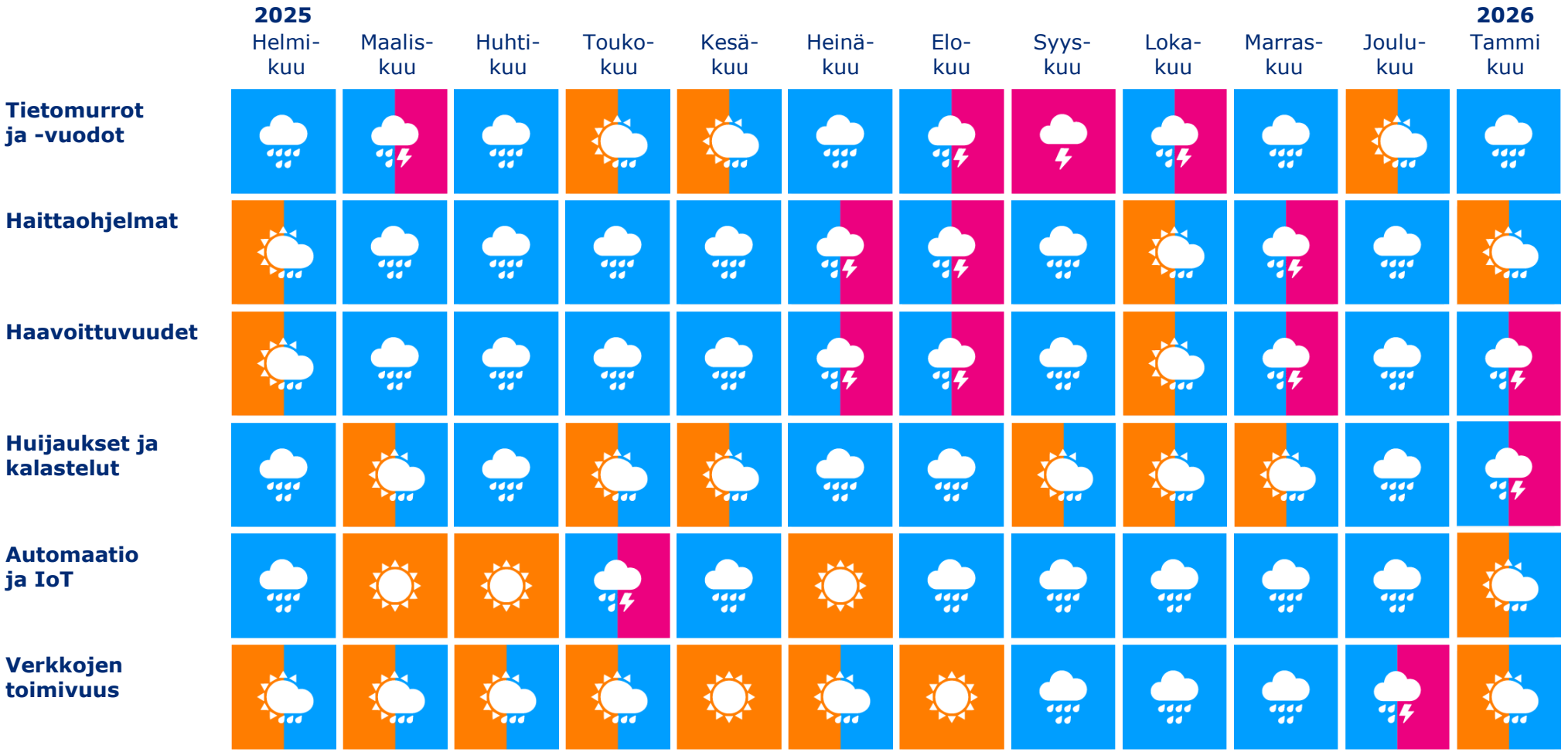
Automaatio ja IoT

- Kansainvälisenä yhteistyönä tuotettu ohje [15] esittelee kahdeksan tavoiteltavaa kyberturvallisuus-periaatetta teollisuusautomaation verkkoyhteyksien suunnitteluun ja luomiseen. Ne käsittelevät muun muassa riskienhallintaa, verkkoyhteyksien yhteyskäytäntöjä ja hallintaa sekä hyökkäyksen vaikutusten rajoittamista.
- Tuotantoympäristöjen verkkoyhteyksien puutteelliset tai virheelliset suojaukset ovat aiheuttaneet tietoturvapoikkeamia myös Suomessa.

Verkkojen toimivuus

- Tammikuussa yleisissä viestintäverkoissa ei havaittu vakavia toimivuushäiriöitä.
- Viime vuosina hypervolumetrisiin, eli yli 1Tb/s DDoS-hyökkäyksiin kykeneviä infrastruktuureja on tullut esille kasvavissa määrin. Suomessa ei ole vielä nähty esimerkkitapauksia.
- Monet bottiverkot hyödyntävät heikosti suojattuja kuluttajalaitteita, kuten halpaverkkokaupoista hankittuja medialaitteita tai tabletteja. [16]
- Bottiverkkoihin kaapataan myös pilvipalveluissa ylläpidettyjä virtuaalikoneita. Niistä koostuvat bottiverkot voivat olla vielä moninkertaisesti voimakkaampia.

Kybersään ilmiöt
kulunut 12 kk

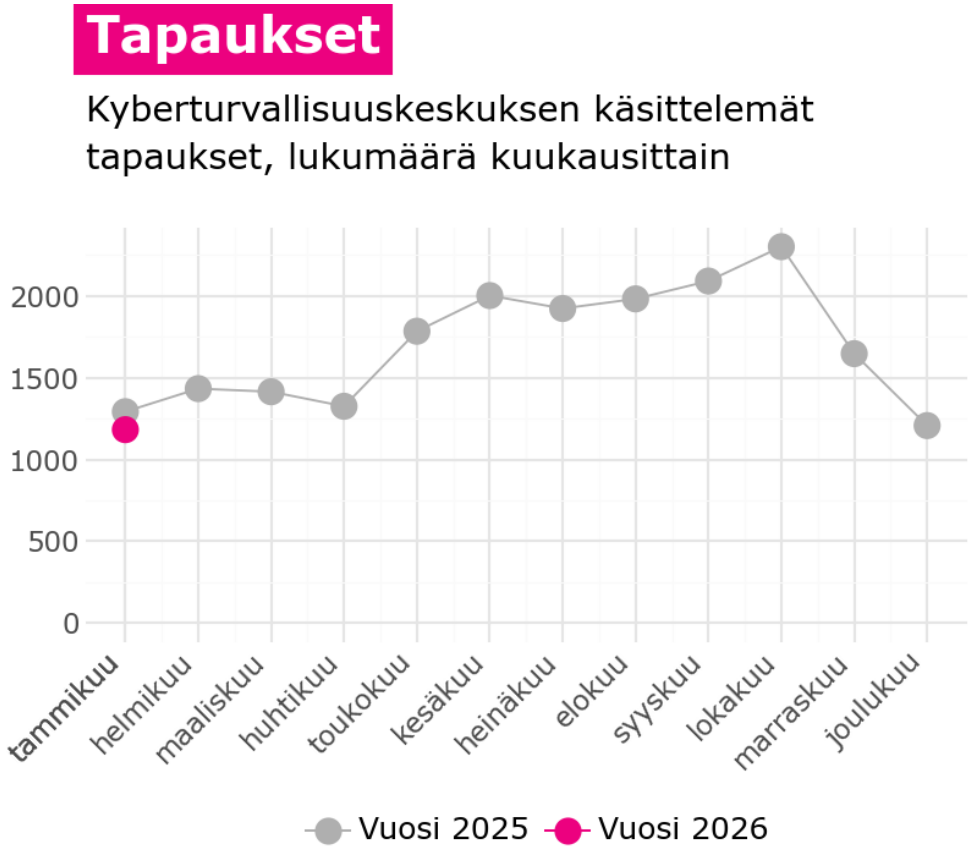


Kybersää lukuina

Osiossa kerromme Kyberturvallisuuskeskuksen
käsittelemien tapausten lukumääriä
ja havaintoja kuluneelta kuukaudelta.

Tapaukset

- Kyberturvallisuuskeskus käsitteli tammikuussa 1 183 tapausta.
- Ilmoitusten määrä on alkuvuodelle tyypillisesti koko vuoden keskiarvoa alhaisempi.
- Monet organisaatioiden kohtaamista poikkeamista ovat kuitenkin olleet merkittäviä. Esimerkiksi organisaatioihin kohdistuneita M365-tilimurtoja ilmoitettiin tammikuussa kolminkertainen määrä joulukuuhun verrattuna. Murrettuja tilejä käytetään usein esimerkiksi laskutuspetoksiin ja jatkokalasteluun.
- Joulukuussa havaittujen pitkittyneiden tapausten selvitykset jatkuivat myös tammikuussa. Esimerkiksi vuodenvaihteessa Itämerellä tapahtuneet kaapelivauriot työllistivät viranomaisia ja operaattoreita.



Kybersääennuste

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

Kybersääennuste

Kyberuhat pysyvät tavanomaisella tasolla

On odotettavissa, että organisaatioita piinanneet käyttäjätilien tunnusten kalastelu ja tilimurrot tuottavat lähikuukausina kerrannaisvaikutuksia. Rikolliset käyttävät kaapattuja tilejä laskutuspetoksiin, kuten toimitusjohtajahuijauksiin. Lisäksi tileiltä lähetetään jatkokalasteluviestejä.

Lomasesongit näkyvät toistuvasti tilimurtotilastoissamme: henkilökunnan palaaminen lomilta täyden sähköpostilaatikon ääreen lisää kalasteluun lankeamisen riskiä. Helmi–maaliskuun talvilomasesonki saattaa myös lisätä majoitus- ja matkateemaisten kalasteluviestien määrää.

Verkonreunalaitteiden haavoittuvuudet lisäävät hyökkäyspintaa pahantahtoisille toimijoille. Näissä löydetyt haavoittuvuudet voivat johtaa tietomurtoihin tai niiden yrityksiin.

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

Osiossa kerromme alaa koskevasta keskeisestä lainsäädännöstä, asetusten päivityksistä ja muista uudistuksista.

Oikeudelliset asiat
Euroopan komissio vahvistaa kyberkestävyyttä ja kyberturvallisuusvalmiuksia EU:ssa

- Euroopan komissio antoi 20.1.2026 ehdotuksen uudesta kyberturvallisuussääntelystä [17, 18], johon sisältyvät ehdotukset kyberturvallisuusasetuksen uudistamisesta (CSA2) ja kyberturvallisuusdirektiivin (NIS2) muuttamisesta.
- Päivitetyn kyberturvallisuusasetuksen tavoitteena on muun muassa selkeyttää ja yksinkertaistaa sertifiointimenettelyjä sekä vahvistaa koko EU:n kyberturvallisuusosaamista ENISA:n (Euroopan unionin verkko- ja tietoturvavirasto) toimintojen avulla. ENISA:n roolia on myös tarkoitus laajentaa operatiiviseen kyberuhkien havainnointiin ja torjuntaan.
- Tavoitteena on lisäksi vahvistaa EU:n tieto- ja viestintäteknologian toimitusketjujen turvallisuutta. Asetuksella luotaisiin toimitusketjujen turvallisuuskehys. EU:n jäsenvaltiot voisivat laatia riskiarvion tieto- ja viestintäteknologian toimitusketjuista ja tunnistaa siten keskeiset suojattavat osat, riskit ja haavoittuvuudet sekä toimenpiteet niiden suojaamiseksi. Korkean riskin toimijoille asetettaisiin monia toimintarajoitteita. Niiden valmistamia laitteita ei muun muassa saisi käyttää mobiiliviestintäverkoissa tietyn siirtymäajan jälkeen.
- Komissio ehdottaa myös kohdennettuja muutoksia EU:n kyberturvallisuusdirektiiviin (NIS 2). Direktiivin soveltamisalaa ehdotetaan laajennettavaksi merenalaisen tiedonsiirtoinfrastruktuurin tarjoajiin sekä eurooppalaisten digitaalisten identiteetti- ja yrityslompakoiden tarjoajiin. Tarkennuksia NIS 2 -direktiiviin ehdotetaan lisäksi energia- ja kemianteollisuuden toimijoiden osalta. Tulevaisuudessa eurooppalaisia kyberturvallisuussertifiointeja voisi hyödyntää direktiivin vaatimustenmukaisuuden osoittamisessa. Lisäksi ENISA:lle ehdotetaan uusia tehtäviä liittyen valvovien viranomaisten rajat ylittävään yhteistyöhön ja jäsenvaltioiden rajat ylittäviin kyberturvallisuusriskeihin.
- EU:ssa jäsenmaat ja Euroopan parlamentti muodostavat seuraavaksi omat näkemyksensä komission ehdotuksista.

Oikeudelliset asiat
EU tukee digitaalisia yhteyksiä yksinkertaisemmilla ja yhdenmukaistetuilla säännöillä digiverkkosäädöksessä

- Euroopan komissio antoi 21.1.2026 ehdotuksen uudesta digitaalisia verkkoja koskevasta asetuksesta (Digital Networks Act, DNA). [17, 19] Komission ehdotuksella pyritään nykyaikaistamaan, yksinkertaistamaan ja yhdenmukaistamaan EU:n viestintäverkkoja koskevaa sääntelyä. Komissio pyrkii luomaan tehokkaat sisämarkkinat helpottamalla rajat ylittävää liiketoimintaa. Lisäksi asetuksella pyritään keventämään yritysten hallinnollista taakkaa.
- Komission ehdotus sisältää niin sanotun yhden passin menettelyn, jonka mukaan teleyritykset voisivat jatkossa rekisteröityä toimimaan yhden menettelyn kautta useissa EU:n jäsenvaltioissa. Satelliittiviestintäpalveluille annettaisiin jatkossa EU:n laajuinen valtuutus, jolla kannustetaan luomaan EU:n laajuisia satelliittipalveluita EU:n strategisen autonomian vahvistamiseksi.
- Ehdotuksen mukaan verkkotoimiluvat olisivat kestoltaan nykyistä pidempiä, ja niiden uusiminen olisi lähtökohtaisesti mahdollista ilman uutta lupaprosessia. Taajuuksien käyttöä pyritään myös tehostamaan muun muassa lisäämällä taajuuksien yhteiskäyttöä.
- Komission ehdotus sisältää myös useita hallinnollisia uudistuksia. Viranomaiset saisivat uusia tehtäviä, muun muassa tehtävän laatia EU:n varautumissuunnitelma digitaaliselle infrastruktuurille.
- Asetuksen tavoitteena on myös kannustaa valokuituverkkoihin siirtymiseen sääntelemällä kupariverkon alasajoa ja kehittämällä markkinasääntelyä. Lisäksi komission ehdotus sisältää uusia viestintäverkkoihin liittyviä resilienssitoimenpiteitä eurooppalaisella tasolla sekä säännöksiä koskien muun muassa yleispalvelua, verkkoneutraliteettia ja käyttäjän oikeuksia.
- EU:ssa jäsenmaat ja Euroopan parlamentti muodostavat seuraavaksi omat näkemyksensä komission ehdotuksesta.

Oikeudelliset asiat
Valtioneuvosto kannattaa komission tavoitetta digisääntelyn yksinkertaistamisesta

- Euroopan komissio haluaa keventää digitaalialan sääntelyä ja se antoi 19.11.2025 ns. digiomnibus- ja tekoälyomnibus-ehdotukset. [20]
- Komissio julkaisi samalla dataunionistrategian ja ehdotuksen eurooppalaisia yrityslompakoita koskevaksi asetukseksi. Lisäksi komissio käynnisti julkisen kuulemisen digitaalialan toimivuustarkastuksesta (Digital Fitness Check), jossa tarkastellaan yritysten toimintaa sääntelevän EU:n digitaalialan sääntelyn johdonmukaisuutta ja yhteisvaikutuksia yrityksiin. Julkinen kuuleminen on auki 11.3.2026 saakka.
- Sääntelyä kevennettäisiin datan, tietosuojan, kyberturvallisuuden ja tekoälyn osalta. Tavoitteena on vähentää EU-sääntelyn aiheuttamaa hallinnollista taakkaa erityisesti yrityksiltä.
- Valtioneuvosto antoi 29.1.2026 kirjelmän eduskunnalle asiaa koskien.
- Valtioneuvosto kannattaa sääntelyn yksinkertaistamista. Valtioneuvosto pitää tärkeänä, että EU:n digi- ja kybersääntely muodostavat selkeän kokonaisuuden. Osana digitaalialan sääntelyn laajempaa tarkastelua (Digital Fitness Check) tulisi toteuttaa merkittäviä toimia, joilla entisestään vähennetään sääntelyn yrityksille aiheuttamaa hallinnollista taakkaa ja konkreettisesti edistetään sujuvampaa arkea, kilpailukykyä ja oikeusvarmuutta.
- Seuraavaksi EU:ssa jäsenmaat ja Euroopan parlamentti muodostavat omat näkemyksensä komission ehdotuksista.

Oikeudelliset asiat
Pilvipalvelujen turvallisuuskriteerit uudistuvat – uusi kansallinen kriteeristöpankki tulossa käyttöön

- Valtiovarainministeriö ja Traficom ovat yhteistyössä valmistelleet yhtenäistä arviointikriteeristöä julkisen hallinnon pilvipalveluille (Kansallinen kriteeristöpankki, KriPa). [13]
- Kriteeristön tavoitteena on tukea viranomaisten riskienhallintaa pilvipalveluiden käytössä sekä edistää turvallisuusluokitellun, salassa pidettävän ja julkisen tiedon asianmukaista suojaamista.
- Valmistelussa on hyödynnetty kansainvälisiä viitekehyksiä, viranomaisten hyviä käytäntöjä sekä kansallista uhkatietoa. Työn tavoitteena on tuottaa viranomaisille käytännöllinen ja riskiperustainen arviointiväline.
- KriPa korvaa valmistuessaan sekä Traficomin julkaiseman Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) sekä Tiedonhallintalautakunnan julkaiseman Julkisen hallinnon tietoturvallisuuden arviointikriteeristön (Julkri) pilvipalveluiden osalta.
- Ohjeluonnokseen pyydetään nyt lausuntoja. Lausuntoaikaa on 13.4.2026 asti. Lausunnot pyydetään lähettämään ensisijaisesti Lausuntopalvelun kautta.
- Pilvikriteeristön on tarkoitus valmistua syksyn 2026 aikana.

Oikeudelliset asiat
Valtioneuvosto hyväksyi kriittistä infrastruktuuria koskevan riskiarvion

- Valtioneuvosto hyväksyi 15. tammikuuta 2026 kriittistä infrastruktuuria ja kriittisten toimijoiden häiriönsietokykyä koskevan kansallisen riskiarvioinnin. [21]
- Yhteiskunnan kriittisen infrastruktuurin suojaamista ja häiriönsietokyvyn parantamista koskeva laki (ns. CER-laki) tuli voimaan 1.7.2025. Lain mukaan kriittistä infrastruktuuria ja kriittisiä toimijoita koskeva kansallinen riskiarvio laaditaan vähintään neljän vuoden välein.
- Riskiarviossa käsitellään keskeisiin palveluihin kohdistuvia merkityksellisiä riskejä, rajat ylittäviä riippuvuuksia ja toimialojen keskinäisriippuvuuksia.
- Suomen lainsäädännön taustalla on EU:n CER-direktiivi, joka velvoittaa jäsenmaita tunnistamaan yhteiskunnan kannalta kriittiset toimijat ja vahvistamaan niiden kykyä kestää häiriöitä ja kriisejä. Riskiarviota hyödynnetään kriittisten toimijoiden määrittämisessä.
- Kriittistä infrastruktuuria ja yhteiskunnan häiriönsietokykyä koskeva riskiarvio ei ole julkinen. Laajempi kansallinen riskiarvio julkaistaan syksyllä 2026.

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.

Lähdeluettelo
1/2

1. Kyberturvallisuuden vuosi 2025 -julkaisu
https://vuosiraportit.traficom.fi/fi/kyberturvallisuus/kyberturvallisuuden-vuosi-2025/kybertilannekuva-2025
2. Suomalaisilta yritettiin huijata 148 milj. euroa vuonna 2025
https://www.finanssiala.fi/uutiset/suomalaisilta-yritettiin-huijata-148-miljoonaa-euroa-vuonna-2025/
3. Kansallinen koordinointikeskus - kansallisesti myöntämämme rahoitukset
https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/kansallinen-koordinointikeskus/kansallisesti-myontamamme-rahoitustuet
4. Traficom myönsi rahoitustukea yhteensä 165 milj. euroa
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-myonsi-rahoitustukea-yhteensa-165-milj-euroa
5. Vakava haavoittuvuus suositussa sähköyhtiössä – asiakkaiden tiedot vaarassa
https://www.is.fi/digitoday/art-2000011785693.html
6. Älykkäät avustajat, uudet riskit - Tietoturvanäkökulmia AI-avustajien käyttöön
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/alykkaat-avustajat-uudet-riskit-tietoturvanakokulmia-ai-avustajien-kayttoon
7. Kyberturvallisuuden vuosi 2025 (Tietoturva Nyt -artikkeli)
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-vuosi-2025-uhkataso-pysyi-kohonneena-vakavien-tapausten-maarat
8. Kyberturvallisuuden vuosi 2025
https://vuosiraportit.traficom.fi/fi/kyberturvallisuus/kyberturvallisuuden-vuosi-2025
9. Tekoälyagenttien kyberturvallisuus
https://traficom.fi/fi/julkaisut/tekoalyagenttien-kyberturvallisuus
10. Traficomin trendiraportti 2026
https://traficom.fi/fi/julkaisut/traficomin-trendiraportti-2026
11. Kyberturvallisuuskeskuksen viikkokatsaus 3/2026
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-32026

Lähdeluettelo
2/2

12. SECURE: Strengthening EU SMEs Cyber Resilience
https://www.secure4sme.eu
13. Valtiovarainministeriön lausuntopyyntö julkisen hallinnon pilvipalvelukriteereistä
https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=e0c2d465-717b-480c-979a-c60b96848db7&proposalLanguage=da4408c3-39e4-4f5a-84db-84481bafc744
14. Energy Sector Incident Report - 29 December 2025
https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/
15. Secure connectivity principles for Operational Technology (OT)
https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/secure-connectivity-principles-for-operational-technology
16. Kimwolf Botnet Lurking in Corporate, Govt. Networks
https://krebsonsecurity.com/2026/01/kimwolf-botnet-lurking-in-corporate-govt-networks/
17. Komissio antoi ehdotukset uudesta kyberturvallisuussääntelystä ja digiverkkoasetuksesta
https://lvm.fi/-/komissio-antoi-ehdotukset-uudesta-kyberturvallisuussaantelysta-ja-digiverkkoasetuksesta
18. Komissio vahvistaa kyberkestävyyttä ja kyberturvallisuusvalmiuksia EU:ssa
https://ec.europa.eu/commission/presscorner/detail/fi/ip_26_105
19. EU tukee digitaalisia yhteyksiä yksinkertaisemmilla ja yhdenmukaistetuilla säännöillä digiverkkosäädöksessä
https://ec.europa.eu/commission/presscorner/detail/fi/ip_26_107
20. Valtioneuvosto kannattaa komission tavoitetta digisääntelyn yksinkertaistamisesta
https://lvm.fi/-/valtioneuvosto-kannattaa-komission-tavoitetta-digisaantelyn-yksinkertaistamisesta
21. Valtioneuvosto hyväksyi kriittistä infrastruktuuria koskevan riskiarvion
https://valtioneuvosto.fi/-/1410869/valtioneuvosto-hyvaksyi-kriittista-infrastruktuuria-koskevan-riskiarvion