TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Toukokuu 2025

#kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä.

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

Kybersää voi olla:  rauhallinen  huolestuttava  vakava

Kuukauden tunnuslukuja

KrebsOnSecurity -verkkosivuihin kohdistui toukokuussa palvelunestohyökkäys, jonka yhteydessä sivustoa kuormitettiin yli 6,3 Tbit/s volyymillä.[1] Tämä ja muut viime aikoina havaitut hypervolymetriset hyökkäykset saattavat enteillä laajojen ja aiempaa suorituskykyisempien IoT-bottiverkkojen paluuta globaaliin uhkakenttään.[2 & 3]

Jyväskylässä kahdesti vuodessa järjestettävään valtakunnalliseen kyberharjoitukseen osallistui 120 valtionhallinnon henkilöä. Eri skenaarioiden yhteydessä päästiin kehittämään teknisiä taitoja sekä eri toimijoiden välistä yhteistoimintaa.[4]

Irlanti määräsi toukokuussa TikTok–palvelulle 530 miljoonan euron sakon EU:n yleisen tietosuoja-asetuksen (GDPR) rikkomisesta. Palvelu oli siirtänyt käyttäjätietoja Euroopasta Kiinaan asetuksen vastaisesti. Ilmiö on yksityisyyden suojan kannalta huolestuttava, mutta tapaus osoittaa myös EU:n jäsenvaltioiden kyvyn puuttua asetuksen vastaiseen toimintaan.[5]

Kybersää toukokuu 2025

Tietomurrot ja -vuodot

- Toukokuu oli huhtikuun tapaan tietomurtoilmoitusten osalta rauhallinen.
- Sähköpostitilimurroissa hyödynnettiin kolmannen osapuolen tarjoamia sähköpostisovelluksia kaapattujen M365-tilien viestien lukemiseen ja varastamiseen käyttäjän huomaamatta.

Automaatio ja IoT

- FBI on antanut varoituksen verkkorikollisista, jotka hyödyntävät kotiverkkoihin kytkettyjä esineiden internetin laitteita rikolliseen toimintaan BADBOX 2.0 -bottiverkon avulla.[6]

Huijaukset ja kalastelut

- Kesän lomakausi tuo mukanaan huijaukset johtajien nimissä. Ohjeista kesäsijaiset huijausten varalta, sillä huijarit tekevät kotiläksynsä huolella ja keksivät aina uusia konnankoukkuja.
- Nyt valppaana! -kampanja tarjoaa tietoturvaohjeita nyt myös viittomakielellä.

Verkkojen toimivuus

- Toukokuussa yleisissä viestintäverkoissa havaittiin yhteensä 7 toimivuushäiriötä.
- Perinteiset massiivisiin liikennemääriin perustuvat palvelunestohyökkäykset ovat edelleen yleisiä ja entistä voimakkaampia.[1]
- Mattopommitukset, sovellustason hyökkäykset ja hyökkäysliikenteen mukauttaminen käyttöönotettujen suojausten ohittamiseen ovat entistä yleisempiä.

Haittaohjelmat ja haavoittuvuudet

- Eri teemaisissa huijauksissa ja kalasteluissa on käytetty infostealer-haittaohjelmia tiedon anastamisessa. Onnistuneiden huijausten ja kalasteluiden seurauksena näitä haittaohjelmia on asennettu kohdelaitteelle.

Vakoilu

- Useat länsimaat varoittavat Venäjään liitettävän APT28-toimijan pyrkivän vakoilemaan logistiikka- ja teknologia-alaa.
- Lisäksi Alankomaat ja Microsoft kertoivat mm. viranomaisia vakoilevasta, todennäköisesti Venäjään liitetystä toimijasta Laundry Bear/Void Blizzard.
- Tsekki yhdisti ulkoministeriöönsä kohdistuneen vakoiluoperaation APT31-ryhmään ja Kiinaan.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Euroopan unionin haavoittuvuustietokanta EUVD (European Union Vulnerability Database) otettiin käyttöön 13.5.2025.[7] EUVD tarjoaa kauan kaivatun vaihtoehdon yhdysvaltalaisen CVE-tietokannan rinnalle, jonka rahoituksen jatkuvuudesta on ollut lähiaikoina epäselvyyttä.

CISA julkaisi 21.5. raportin Ukrainaa tukevien maiden teknologia- ja logistiikkayrityksiin kohdistuvasta kybertiedustelusta ja -vaikuttamisesta. Teksti valottaa vuonna 2022 alkanutta Venäjän vaikuttamista sekä sotilastiedustelupalvelu GRU:n alaisten yksiköiden tekniikoita, taktiikoita, prosesseja ja näiden kohdentumista Ukrainaa tukevissa maissa toimiviin yrityksiin.[8]

M365-tilimurroissa hyödynnetyt sähköpostisovellukset pyytävät laajoja käyttöoikeuksia murrettuun sähköpostilaatikkoon. Sovelluksille myönnettävät käyttöoikeudet tulisi rajoittaa vain pääkäyttäjien hyväksyttäviksi.[9]

Kyberturvallisuuskeskuksen yhteydessä toimiva kyberturvallisuuden tutkimuksen, kehityksen ja innovaatioiden kansallinen koordinointikeskus on saanut EU:n Digitaalinen Eurooppa -ohjelmasta osarahoituksen nelivuotiselle jatkokaudelleen. Euroopan komissio rahoittaa hanketta neljällä miljoonalla eurolla, ja lähes koko summa tullaan jakamaan rahoitustukena suomalaisille toimijoille. Kyberturvallisuuskeskus järjestää kesäkuussa kaikille avoimen webinaariin, jossa esitellään ajankohtaisia näkymiä kansallisesti haettavista rahoitustuista ja EU-rahoitusmahdollisuuksista kyberturvallisuuden kehittämiseen.[10]

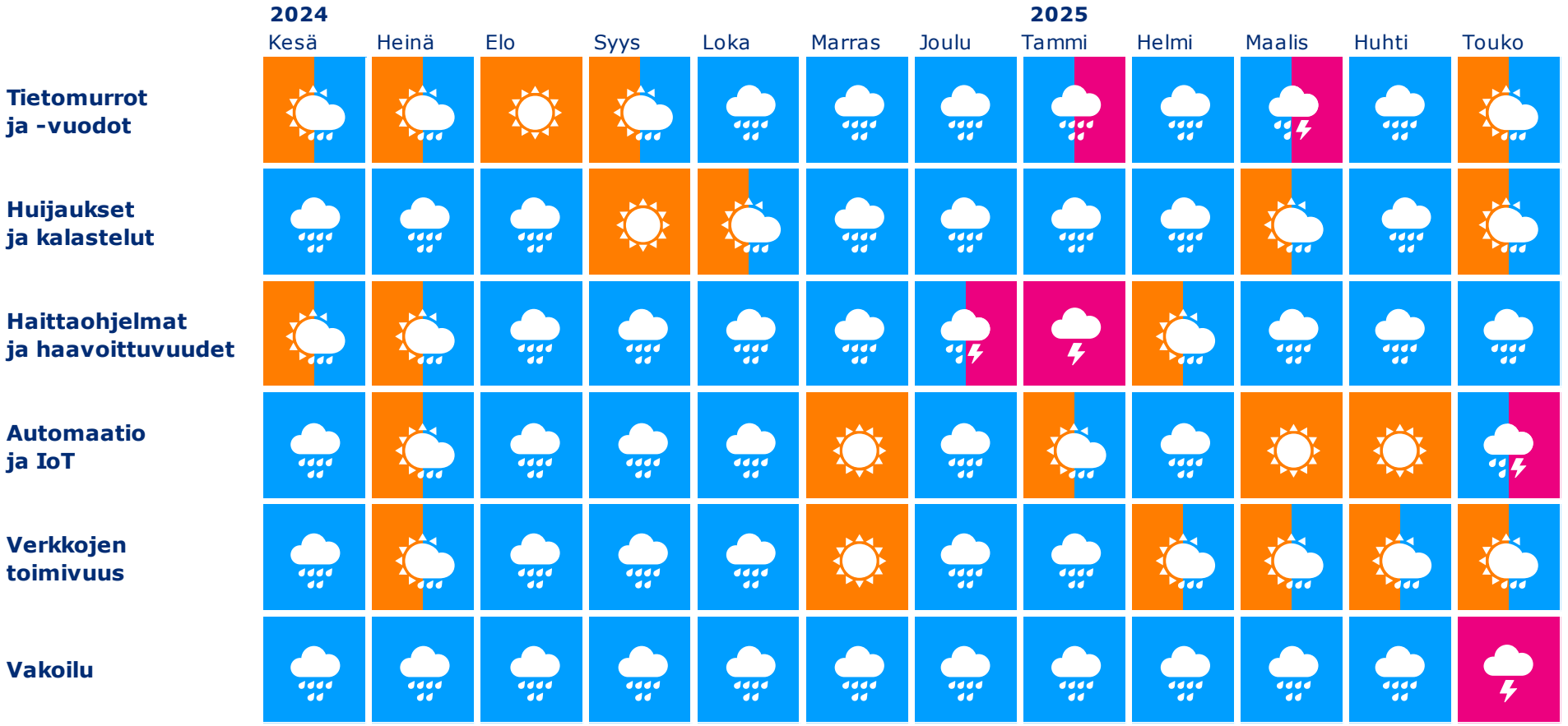
Toukokuun kyberturvallisuuden yleiskuva

- Alkanut kesäkausi aktivoi jälleen pahantekijöitä, mikä näkyi etenkin petoksiin sekä tietojenkalasteluun liittyvissä havainnoissa. Toisaalta kulunut kuukausi nostatti osittain myrskypilviä, kun useat länsimaat kertoivat joutuneensa valtiollisiin kyberuhkatoimijoihin yhdistettyjen hyökkäysten kohteeksi.
  - Kaksivaiheisen tunnistautumisen ohittavissa adversary-in-the-middle (AiTM) -tyyppisissä kalasteluyrityksissä nähtiin nousevaa trendiä kuun lopussa. Havainnoissa painottuivat pankki-, posti-, vero- ja ajoneuvoteemaiset viestit sekä huijaukset.
- Erilaisten tietoteknisten laitteiden haavoittuvuudet ovat edelleen keskeinen huolenaihe kyberturvallisuuden alalla. Ostovaiheessa kannattaa laitteen ominaisuuksien ja elinkaaren ohella kiinnittää huomiota myös valmistajaan.
  - Älytelevision hankinta koskettaa nyt monia kotitalouksia televisiolähetysten siirtyessä teräväpiirtoaikaan myös kaupallisilla kanavilla 1.7. alkaen. Osa markkinoilla olevista laitteista saattaa kuitenkin vaarantaa kotitalouksien tietoturvan. Tietoturvapuutteita on havaittu etenkin tuntemattomien valmistajien, halvoissa, verkon kautta myydyissä Android-TV-laitteissa. Hankintapäätöksessä kannattaa suosia tunnettuja ja luotettavia merkkejä pelkän hinnan sijaan.[11]
  - Haavoittuvien verkon reunalaitteiden muodostama uhka säilyi merkittävänä. Reunalaitteiden, kuten palomuurien ja VPN-laitteiden haavoittuvuuksien hyväksikäyttöä on havaittu Euroopassa ja maailmalla, uhkan koskettaessa myös suomalaisia organisaatioita. Verkon valvonta, ohjelmistojen nopea päivittäminen ja elinkaarensa päähän tulleiden laitteiden korvaaminen ylläpidetyillä tuotteilla ovat kriittisen tärkeitä toimia uhkilta välttymiseksi.
- Tekoälysovellukset yleistyvät organisaatioiden ja yksityishenkilöiden käytössä. Kyberrikolliset ovat pyrkineet hyväksikäyttämään suosion kasvua tietomurtoihin ja haittaohjelmien levittämiseen.
  - Hyökkääjät hyödyntävät väärennettyjä tekoälysovelluksia ja verkkosivuja, joiden yhteyteen on piilotettu haittaohjelmia tai haitallista koodia. Haittaohjelman lataamiseen tähtääviä verkkosivuja on mainostettu esimerkiksi sosiaalisen median ja hakukoneiden manipuloinnin kautta.[12 & 13] Sovelluksia ladattaessa kannattaa aina punnita niiden tarpeellisuutta ja luotettavuutta. Ilmaissovellusten kohdalla kannattaa mahdollisuuksien mukaan pyrkiä myös selvittämään julkaisijan luotettavuus.

Ilmiöiden ja toimialojen trendit

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä eri aikaväleillä. Toimialakohtaisissa nostoissa on esitelty eri toimialojen tilannetta yleistasolla.

Kyberturvallisuuden trendit
kulunut 12 kk



Pitkä aikaväli ja lähitulevaisuus

Osiossa on esitelty pitkän aikavälin ja lähitulevaisuuden kyberturvallisuuden ilmiöitä. Seuraamiemme pitkän aikavälin ilmiöiden joukosta analysoidaan kuukausittain yksi ilmiö. Top 5 –kyberuhkat kertovat puolestaan lähitulevaisuuden uhkista.

Pitkän aikavälin (5v+) kybersää: ilmiöt joita seuraamme

Pitkän aikavälin kybersää: Yksityisyyden suoja

Tietosuoja ulottuu läpi yhteiskunnan, ja sen merkitys kasvaa digitalisoitumisen edetessä. Tietosuoja on perusoikeus, joka turvaa ihmisten oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Oikeus yksityisyyden suojaan on yksi keskeinen osa tietosuojaa. Seuraavat huomiot laadittiin yhteistoiminnassa valvovana viranomaisena toimivan Tietosuojavaltuutetun toimiston kanssa.

- Tietosuoja on ehdoton edellytys vahvan ja toimivan demokratian sekä oikeusvaltion toteutumiselle. Esimerkiksi henkilörekisterin tietojen luotettavuuden tai käytettävyyden menettäminen on todellinen ja laajavaikutteinen riski niin viranomaisille kuin muille toimijoille.

- Organisaatioiden kannalta tietosuojakysymysten huomioiminen jo tuotteiden, palveluiden ja toiminnan suunnitteluvaiheesta lähtien mahdollistaa tietosuojan toteuttamisen kustannustehokkaasti ja tarkoituksenmukaisesti. Samalla se tukee myös liiketoimintatavoitteita ja toimivia EU:n sisämarkkinoita.

Digitaalisen maailmaan, sekä globaalin turvallisuus- ja toimintaympäristön muutokset luovat haasteita tietosuojalle. Tulevaisuudessa on entistäkin tärkeämpää huomioida, että henkilötietoja voidaan hyödyntää tavoilla, jotka voivat vakavasti vaarantaa henkilöiden ja yhteiskunnan turvallisuuden.

- Tekoälyjärjestelmien käyttö ja algoritminen päätöksenteko lisääntyvät. Samalla myös tietosuojakysymysten merkitys kasvaa, koska tekoälymallit saattavat usein joutua käsittelemään henkilötietoja. Tekoälyn käyttö voi myös aiheuttaa syrjintää tai vaarantaa tietosuojaa, vaikka tämä ei olisi tarkoitus. Keskeistä on turvata yksityisyyden suoja ja muut ihmisoikeudet, kun tekoälyjärjestelmiä kehitetään ja käytetään. Tekoälyn toimintaa on myös valvottava ja testattava säännöllisesti.

- Henkilötietoja hyödyntävän informaatiovaikuttamisen ennakoidaan lisääntyvän. Kansalaistaidoissa korostuu ymmärrys yksityisyyden suojan merkityksestä sekä informaatiovaikuttamisesta ja sen havaitsemiskeinoista. Tulevaisuudessa kuluttajan tulisi ymmärtää, miten käyttäjien henkilötietoja tyypillisesti käsitellään verkkopohjaisissa tekoälypalveluissa sekä mitä oikeuksia käyttäjällä on rekisteröitynä.

- EU:n tekoälylainsäädännön ja muun eurooppalaisen digisääntelyn toimeenpano tuo uusia tehtäviä tietosuojaviranomaisille. Viranomaisten keskeisenä tehtävänä on pyrkiä harmonisoimaan tietosuojalainsäädännön tulkintoja ja tukea myös organisaatioita tietosuojatyössä. Euroopan tietosuojaneuvosto onkin jo käynnistänyt toimenpiteitä näihin teemoihin liittyen. Kansallisten digisäädöksiä valvovien viranomaisten sujuvan yhteistyön merkitys korostuu jatkossa entisestään.

- Vaikka maailma muuttuu ja uusia tietosuojariskejä syntyy, tietosuojatyön perusperiaatteet säilyvät: organisaation on edelleen muun muassa tiedettävä, mitä varten, millä perusteella ja tarkemmin mitä tietoja kerätään. Lisäksi on huolehdittava siitä, että tiedot on asianmukaisesti suojattu ja ihmisille on kerrottu avoimesti heihin liittyvien tietojen käsittelyperiaatteista.

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

- Hallitus antoi 8.5.2025 eduskunnalle esityksen EU:n tekoälyasetusta täydentäväksi lainsäädännöksi[14]
  - Esityksessä ehdotetaan säädettäväksi laki tekoälyjärjestelmien valvonnasta sekä muutettavaksi muun muassa tuotteiden markkinavalvontaa ja sakon täytäntöönpanoa koskevia lakeja.
  - Lailla pantaisiin täytäntöön EU:n tekoälyasetuksen täydentävät kansalliset säännökset koskien toimivaltaisia viranomaisia. Lisäksi Liikenne- ja viestintävirasto nimettäisiin toimimaan keskitettynä yhteyspisteenä. Laissa säädettäisiin viranomaisten toimivallasta määrätä seuraamuksia tiettyjen laissa yksilöityjen asetuksen säännösten rikkomisesta. Laissa säädettäisiin myös seuraamusmaksulautakunnasta ja sen toimivallasta määrätä seuraamusmaksu vakavimmista asetuksen säännösten rikkomisesta.
  - EU:n tekoälyasetuksen tavoitteena on varmistaa, että markkinoille tulevat tai käyttöön otettavat tekoälyjärjestelmät eivät vaaranna ihmisten turvallisuutta, terveyttä tai perusoikeuksia. Asetus luo yhtenäiset säännöt tekoälyjärjestelmien tarjoamiselle, käyttöönotolle ja käytölle EU:n alueella. Sääntely keskittyy erityisesti haitallisiin tekoälyn käyttötapauksiin, esimerkiksi vaarallisimmat tekoälyn käyttötapaukset kiellettäisiin ja ns. suuririskisille tekoälyjärjestelmille asetettaisiin tiukennettuja vaatimuksia.
  - Ehdotetut lait on tarkoitettu tulemaan voimaan 2.8.2025 alkaen.

Oikeudelliset asiat

- Tietosuojavaltuutetun toimistolta ohjeistusta tietosuojan huomioimisesta tekoälyjärjestelmien kehittämisessä ja käytössä[15]
  - Tietosuojavaltuutetun toimisto on koonnut verkkosivuilleen ohjeistusta siitä, miten organisaation on otettava tietosuojalainsäädännön vaatimukset huomioon, kun se kehittää tai ottaa käyttöön tekoälyjärjestelmää.
  - Tekoälyjärjestelmää kehittävän tai käyttävän organisaation on varmistettava, että järjestelmä ja toimintatavat ovat sellaisia, että kaikki tekoälyjärjestelmässä tapahtuvaan henkilötietojen käsittelyyn liittyvät tietosuojaoikeudet pystytään toteuttamaan tehokkaasti. Tekoälyjärjestelmien käyttöä sääntelee myös EU:n tekoälyasetus, jossa määritellään esimerkiksi kielletyt tekoälyn käyttötapaukset ja asetetaan vaatimuksia suuririskisille tekoälyjärjestelmille.
  - Ohjeistus ei ole tyhjentävä, vaan organisaation on arvioitava lainsäädännöstä tulevat vaatimukset aina tapauskohtaisesti. Organisaatio on vastuussa siitä, että se noudattaa tietosuojasääntelystä tulevia vaatimuksia ja pystyy osoittamaan sen. Osoitusvelvollisuus edellyttää esimerkiksi tiettyjen toimenpiteiden tekemistä ja dokumentointia.

Oikeudelliset asiat

- Suomi vaikuttaa EU:n kyberturvallisuusasetuksen tarkistukseen[16]
  - Euroopan komission on tarkoitus antaa vuoden 2025 lopulla säädösehdotus vuonna 2019 voimaan tulleen kyberturvallisuusasetuksen tarkistamisesta. Liikenne- ja viestintäministeriö antoi eduskunnalle asiasta selvityksen 26.5.2025.
  - EU:n kyberturvallisuusasetuksella säädetään Euroopan kyberturvallisuusvirasto ENISA:n tehtävistä sekä luodaan puitteet eurooppalaisille kyberturvallisuussertifiointijärjestelmille.
  - Suomi pitää tärkeänä muun muassa sitä, että muuttunut toimintaympäristö huomioidaan kattavasti kyberturvallisuusasetusta tarkasteltaessa, ja että yksityisen sektorin toimijat otetaan entistä laajemmin mukaan EU-tason kybervarautumisen vahvistamiseen.
  - Suomi suhtautuu myönteisesti tavoitteeseen sujuvoittaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien valmistelua, hyväksymistä ja tarkistamista. Kyberturvallisuuden sertifiointijärjestelmien kehittäminen on tärkeä osa EU:n kyberturvallisuuden ja teknologioiden turvallisuuden edistämistä. Suomi katsoo, että sertifioinnilla tulisi voida täyttää lainsäädännön kyberturvallisuuden minimivaatimukset.
  - Suomi katsoo, että tieto- ja viestintätekniikan toimitusketjujen turvallisuuden ja kriisinkestävyyden vahvistaminen on keskeinen osa EU:n teknologista omavaraisuutta. Suomi suhtautuu alustavasti myönteisesti uusiin ja mahdollisesti nykyistä velvoittavampiin EU-tason toimenpiteisiin, joilla parannettaisiin tieto- ja viestintäteknologioiden toimitusketjujen turvallisuutta.

Oikeudelliset asiat

- Suositus palvelun pilviperiaatteista – IaaS-palvelun tietosuoja[17]
  - Valtiovarainministeriö on julkaissut 5.5.2025 ensimmäisen suosituksen julkaisusarjassa, joka käsittelee pilvipalveluiden toimittamisen periaatteita. Tarkoituksena on ollut koostaa eri näkökulmista koostuva, tiivis työmateriaali pilvipalveluiden hankintojen tueksi.
  - Suositus on laadittu sellaiseen muotoon, että sitä voi soveltaa sekä hankinnan, että sopimuksen muotoilussa. Suositus on pyritty laatimaan teknologiasta ja liiketoimintamallista riippumattomaksi.
  - Suositus keskittyy IaaS -palveluiden (Infrastructure as a Service) tietosuojan varmistamiseen. Periaatteet eivät välttämättä sovi lainkaan sovellettavaksi muihin pilvipalvelutyyppeihin.
  - Suositus ei ole kattava listaus pilvipalveluiden periaatteista, vaan näiden lisäksi organisaation tulee arvioida ja sovittaa riittävät järjestelyt pilvipalveluiden laadun ja turvallisuuden varmistamiseksi.

Epäiletkö tietoturvaloukkausta?

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

- Sähköinen lomake: https://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 täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot

Lähdeluettelo

1) KrebsOnSecurity Hit With Near-Record 6.3 Tbps DDoS - https://krebsonsecurity.com/2025/05/krebsonsecurity-hit-with-near-record-6-3-tbps-ddos/
2) Hyper-volumetric attacks continue spill into Q2 - https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/#hyper-volumetric-attacks-continue-spill-into-q2
3) A Brand-New Botnet Is Delivering Record-Size DDoS Attacks - https://www.wired.com/story/eleven11bot-botnet-record-size-ddos-attacks/
4) Kyberhyökkäys voi edellyttää päätöksentekoa valtioneuvostotasolla asti – yhteistä osaamista kehitetään KYHA-harjoituksilla - https://www.jamk.fi/fi/uutiset/2025/kyberhyokkays-voi-edellyttaa-paatoksentekoa-valtioneuvostotasolla-asti-yhteista-osaamista-kehitetaan
5) Irish Data Protection Commission fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China - https://www.dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following
6) FBI: BADBOX 2.0 Android malware infects millions of consumer devices - https://www.bleepingcomputer.com/news/security/fbi-badbox-20-android-malware-infects-millions-of-consumer-devices/
7) Consult the European Vulnerability Database to enhance your digital security! - https://www.enisa.europa.eu/news/consult-the-european-vulnerability-database-to-enhance-your-digital-security
8) Russian GRU Targeting Western Logistics Entities and Technology Companies - https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a
9) Overview of user and admin consent - https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/user-admin-consent-overview
10) Kansalliset ja EU-rahoitusmahdollisuudet kyberturvallisuuden kehittämiseen -webinaari 18.6.2025 - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kansalliset-ja-eu-rahoitusmahdollisuudet-kyberturvallisuuden-kehittamiseen-webinaari
11) TV on älylaite, jonka turvallisuudesta tulee huolehtia - Ole tarkkana Android TV -medialaitteiden kanssa- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tv-alylaite-jonka-turvallisuudesta-tulee-huolehtia-ole-tarkkana-android-tv
12) Text-to-Malware: How Cybercriminals Weaponize Fake AI-Themed Websites - https://cloud.google.com/blog/topics/threat-intelligence/cybercriminals-weaponize-fake-ai-websites/
13) Cybercriminals camouflaging threats as AI tool installers - https://blog.talosintelligence.com/fake-ai-tool-installers/
14) Hallituksen esitys TEM/2025/57 - https://valtioneuvosto.fi/paatokset/paatos?decisionId=3723
15) Tietosuoja tekoälyjärjestelmien kehittämisessä ja käytössä - https://tietosuoja.fi/tekoalyjarjestelmat-ja-tietosuoja
16) Suomi vaikuttaa EU:n kyberturvallisuusasetuksen tarkistukseen - https://lvm.fi/-/suomi-vaikuttaa-eu-n-kyberturvallisuusasetuksen-tarkistukseen
17) Suositus palvelun pilviperiaatteista : Sarja A: IaaS -palvelun tietosuoja, 5.5.2025 - https://julkaisut.valtioneuvosto.fi/handle/10024/166271