TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Kesäkuu 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

Maailmanlaajuinen FortiBleed-hyökkäyskampanja on ulottunut jopa 194 maahan. Suomessa vaikutuksia on ollut kaiken kaikkiaan 20 kohteeseen.[1]

Uusi kyberkestävyyslaki astui voimaan 1.6. Suomessa. Kuuntele kesäkuussa järjestetyn infotilaisuuden tallenne.[2]

Traficomin VM-rahoitushakemus hallintopäätöksiä valmistelevalle agenttiratkaisulle lupa- ja valvontapalveluihin sai eduskunnan hyväksynnän ja hankkeelle myönnettiin 1,2 miljoonan euron rahoitus.[3]

Kybersään yleistilanne kesäkuussa 2026

Kesäkuun kybersäässä nähtiin tummia pilviä, mutta myrskyltä vältyttiin toistaiseksi

Maailmanlaajuisen FortiBleed-hyökkäyskampanjan vaikutukset näkyivät myös Suomessa noin 20 laitteen vaarantumisena. Vaikka kampanja nosti tummia pilviä horisonttiin, ei merkittäviä vaikutuksia ole toistaiseksi ilmennyt.

Kuukausi toi mukanaan kesälomakaudelle tyypilliset huijaukset, joiden suhteen erityisesti tuoreiden kesätyöntekijöiden tulee olla valppaana. Sen sijaan M365-tilimurtoilmoitukset lähtivät kesäkuun loppua kohden odotettuun laskuun.

Lisäksi Microsoftin Secure Boot -varmenteiden uusiminen nousi kesäkuussa ajankohtaiseksi, sillä varmenteiden vanheneminen edellytti organisaatioilta toimia laitteiden turvallisen käynnistyksen varmistamiseksi.[4]

Kyberturvallisuuskeskus arvioi vuoden 2026 ensimmäisen puolikkaan tilannetta

Kyberturvallisuuden tilanne Suomessa on vuoden 2026 ensimmäisellä puoliskolla pysynyt vakaana. Vaikka uhkakuvassa ei ole tapahtunut merkittäviä äkillisiä muutoksia, kyberuhkat ovat kehittyneet teknologian ja hyökkääjien toimintatapojen mukana. Erityisesti tekoälyn hyödyntäminen hyökkäyksissä, M365-tilimurtojen kasvu sekä toimitusketjuihin kohdistuvat riskit ovat nousseet keskeisiksi huolenaiheiksi.[5]

Kuukauden raekuuro
Kesälomakausi ja sijaisjärjestelyt luovat otollisen maaperän toimitusjohtajahuijauksille

Kesäkaudella organisaatioissa työskentelee tavallista enemmän sijaisia ja uusia työntekijöitä, jotka eivät välttämättä tunne vakiintuneita toimintatapoja tai varmistusprosesseja. Tämä tekee ajankohdasta erityisen houkuttelevan rikollisille.

Tyypillisesti huijauksissa esiinnytään yrityksen johdon edustajana ja pyydetään kiireellisiä toimenpiteitä, kuten tilisiirtoja, lahjakorttiostoja tai laskujen maksamista. Tekosyynä voidaan käyttää esimerkiksi kiireellistä yrityskauppaa tai muuta poikkeustilannetta.

Rikolliset hyödyntävät aktiivisesti puheluita, tekstiviestejä, sähköposteja, pikaviestejä ja sosiaalista mediaa. Siksi pelkkä väite yhteydenoton alkuperästä, kuten esimerkiksi pankista, viranomaiselta tai tunnetulta yritykseltä ei takaa viestin aitoutta.[6]

Riskien pienentämiseksi organisaatioita kehotetaan:

- varmistamaan, että maksujen hyväksymis- ja tarkistusprosessit tunnetaan kaikilla organisaatiotasoilla
- tarkistamaan poikkeukselliset pyynnöt aina toista viestintäkanavaa käyttäen
- välttämään kiireessä tehtäviä taloudellisia päätöksiä
- varmistamaan henkilöllisyys tarvittaessa kasvotusten

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on luonut muistilistan lomalaisille arjen kyberturvallisuuden varmistamiseksi lomakaudella.[7]

Suojaa verkon reunalaitteet: Poista verkon reunalaitteiden hallintapaneelit ja muut käyttöliittymät näkyvistä internetistä. Pidä laitteet aina päivitettyinä ja valvo niiden toimintaa. Ota käyttöön monivaiheinen tunnistautuminen myös VPN-kirjautumisessa aina kun mahdollista.[8]

Kesälomakausi on huijareiden sesonkia. Lue vinkit kuinka välttyä huijatuksi tulemiselta.[9,10]

Kybersään ilmiöt

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä.

Kybersää
Kesäkuu 2026

1 kk

Tietomurrot- ja vuodot

Verkon eri reunalaitteisiin kohdistui tietomurtoja, joissa hyödynnettiin haavoittuvuuksia sekä vuotaneita käyttäjätunnuksia. Murtojen runsaasta määrästä huolimatta vakavilta vaikutuksilta vältyttiin.

Haittaohjelmat

Kuukauden aikana haittaohjelmia on levitetty sähköpostiviestien liitetiedostoissa sekä haitallisten verkkosivujen kautta ClickFix-tekniikkaa hyödyntäen. Määrällisesti haittaohjelmahavainnot ovat olleet maltillisia.

Haavoittuvuudet

Kesäkuun aikana uusien haavoittuvuuksien löytymisen trendi on jatkanut kasvuaan. Tekoälyn hyödyntäminen haavoittuvuuksien löytämiseen on synnyttänyt paljon keskustelua maailmanlaajuisesti.

Huijaukset ja kalastelut

Lastensuojelun nimissä lähetetyissä huijausviesteissä kalasteltiin pankkitunnuksia. Yrityksiä koitettiin huijata verkkotunnuksen uusimiseen liittyvillä teemoilla. Klarnan nimissä tehdyissä huijauspuheluissa koitettiin saada uhri asentamaan UltraViewer-etäyhteysohjelma koneelleen.

Automaatio ja IoT

Kyberturvallisuuskeskus järjesti kyberkestävyyslakia koskevan infotilaisuuden 3.6., jossa esitettyihin kysymyksiin koostetut vastaukset ja tilaisuuden tallenne löytyvät tapahtumasivulta.[11]

Verkkojen toimivuus

Palvelunestohyökkäykset eivät aiheuttaneet merkittäviä häiriöitä Suomessa.

Kybersää
Kesäkuu 2026 1/2

1 kk

Tietomurrot ja -vuodot

- Tietomurtojen sisäänmenovektorina hyödynnetään yhä useammin haavoittuvuuksia. Kesäkuussa mm. useita Palo Alton GlobalProtect VPN-laitteita murrettiin haavoittuvuutta CVE-2026-0257 hyväksikäyttäen.
- FortiBleed-hyökkäyskampanjan yhteydessä vaarantui yli 70 000 Fortinetin FortiGate-palomuuri- ja SSL-VPN-laitteita laitetta ympäri maailman. Suomessakin havaittiin sen seurauksena tietomurtoja ja yhteensä n.20 laitteen tiedot vuodettiin.[1]
- M365-tietomurtoilmoitukset vähenivät loppukuuta kohden edellisvuosien tapaan. Trendin mukaisesti seuraavaa tietomurtoaaltoa voidaan odottaa lomakauden jälkeen, alkusyksystä.

Haittaohjelmat

- Kyberturvallisuuskeskukselle on ilmoitettu yksittäisistä kohdennetuista sähköpostiviesteistä, joiden liitetiedostoihin on ollut piilotettuna haittaohjelma. Näillä on pyritty kaappaamaan tietokoneen hallinta taikka tietokoneelle liitettyjä tilejä ja käyttäjätunnuksia, kuten M365-tilejä.
- ClickFix-tekniikalla tehtävät haittaohjelmien jakelut ovat yleistyneet kuukauden aikana. ClickFix-tekniikalla levitetään haittaohjelmia epäilyttävien taikka murrettujen verkkosivujen kautta. Haittaohjelmat ovat kuitenkin havaittu usein tarpeeksi ajoissa, ettei vahinkoja ole päässyt syntymään.

Haavoittuvuudet

- Haavoittuvuuksien trendi on jatkanut kasvuaan entisestään ja näillä näkymin uusien löydettyjen haavoittuvuuksien määrä tulee olemaan yli 50 tuhatta vuonna 2026.
- Kyberturvallisuuskeskus julkaisi kesäkuun alussa haavatiedotteen Check Point VPN – haavoittuvuudesta (CVE-2026-50751), joka oli aktiivisen hyväksikäytön kohteena.[12]
- Maailmalla on käyty paljon keskustelua mahdollisuudesta käyttää tekoälyä uusien haavoittuvuuksien löytämiseen.

Kybersää
Kesäkuu 2026 2/2

1 kk

Huijaukset ja kalastelut

- Lukuisia lastensuojelun nimissä tehtyjä huijauksia ilmoitettiin. Viestejä on lähetetty erilaisilla lastensuojeluun liittyvillä teemoilla sekä tekstiviestitse että sähköpostilla ja esimerkiksi turvapostia imitoiden. Kalastelusivuja on havaittu myös .fi-verkkotunnuksella. Huijauksessa havitellaan pankkitunnuksia.
- Yrityksille lähetettiin huijausviestejä ”DMS Finlandin” nimissä. Viesteissä pyydettiin uusimaan verkkotunnus.
- Klarnan nimissä soitettiin huijaus-puheluita, joiden yhteydessä hyökkääjä pyrki saamaan uhrin asentamaan koneelle UltraViewer-etäyhteysohjelman.

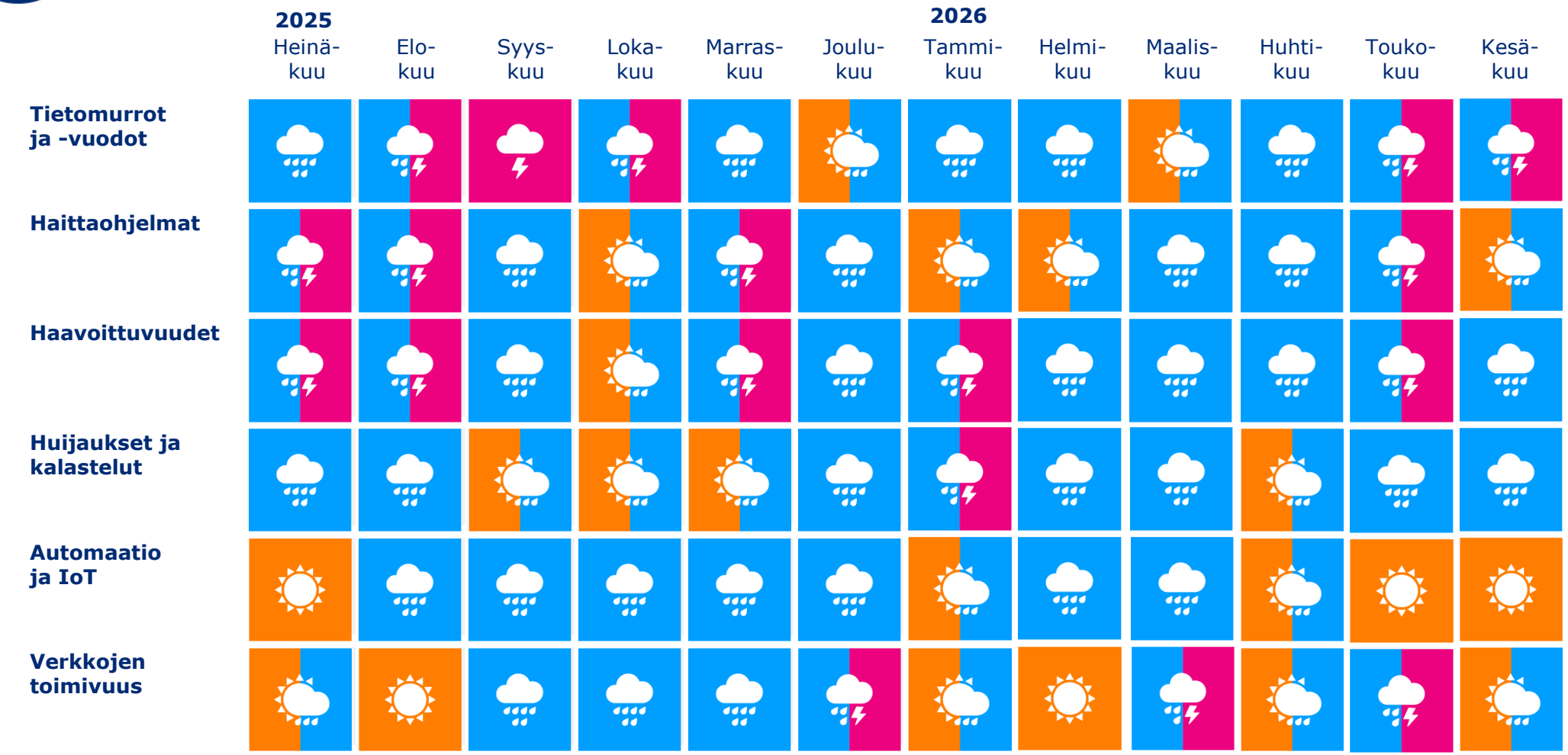
Automaatio ja IoT

- Kyberturvallisuuskeskus järjesti kyberkestävyyslakia koskevan infotilaisuuden 3.6., jossa esitettyihin kysymyksiin koostetut vastaukset ja tilaisuuden tallenne löytyvät tapahtumasivulta.

Verkkojen toimivuus

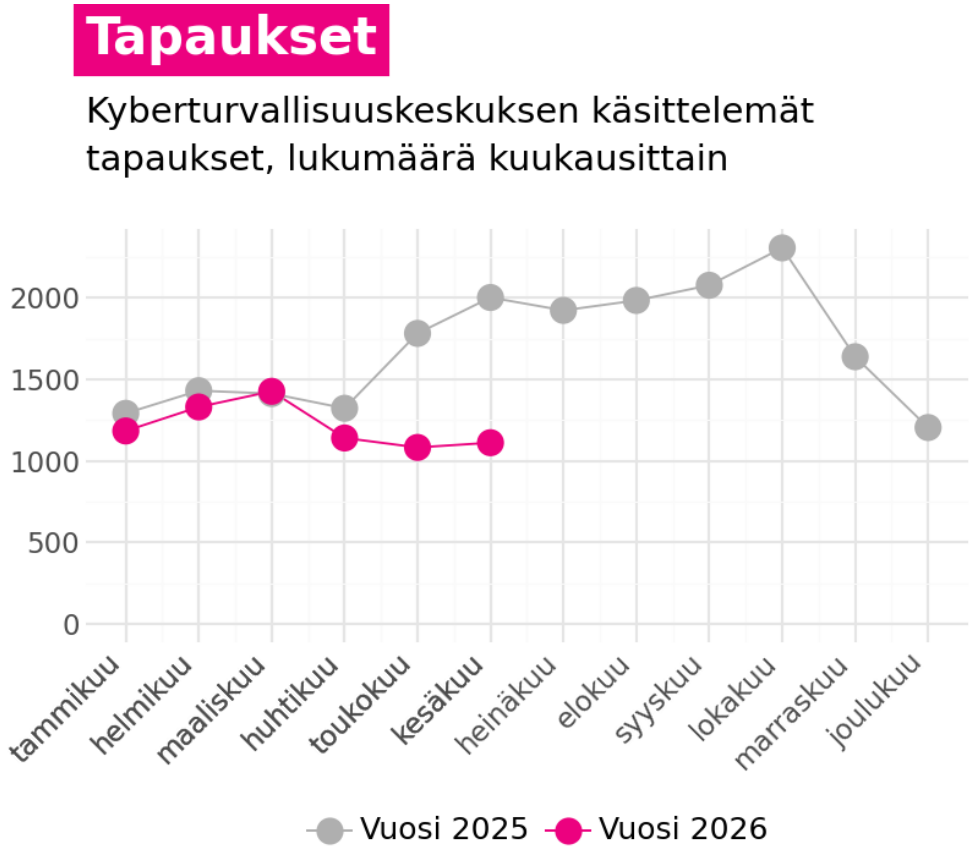
- Yleisissä viestintäverkoissa havaittiin kesäkuussa kolme lievempää ja yksi vakavampi toimivuushäiriö Suomessa, jonka vuoksi puheliikenne oli osittain estynyt itsenäistä 5G-verkkoa käyttävissä liittymissä.
- Suomessa havaittujen palvelunestohyökkäysten vaikutukset rajautuivat väliaikaisiin häiriöihin.
- Vaikka palvelunestohyökkäykset ovat viime vuosina arkipäiväistyneet, voi niillä kuitenkin edelleen olla haittaavia vaikutuksia ja niitä vastaan kannattaa suojautua.

Kybersään ilmiöt
kulunut 12 kk



Tapaukset

- Kyberturvallisuuskeskus käsitteli kesäkuussa 1111 tapausta.
- Ilmoitusten määrä on 12 kuukauden keskiarvoon nähden huomattavasti vähäisempi. Kyberturvallisuuskeskukselle tehtävien ilmoitusten määrä yleensä laskee kesäkuukausina tavanomaisesta tasosta.
- Tapausmäärien laskusta huolimatta kesäkuussa havaittiin muutamia merkittäviä poikkeamia.
- Esimerkiksi maailmanlaajuinen FortiBleed-kampanja näkyi myös Suomessa. Kampanjassa hyväksikäytettiin jo aikaisemmin vuotaneita tai anastettuja käyttäjätunnuksia tietomurtojen tekemisessä. Lisäksi haavoittuvuudet sekä toimitusketjujen turvallisuus ja näistä syntyneet poikkeamat ovat pitäneet kyberkenttää kiireisenä.
- Vaikka tapaukset eivät toistaiseksi ole johtaneet vakaviin seurauksiin, potentiaalisten vaikutusten ennaltaehkäiseminen on vaatinut niin organisaatioilta kuin Kyberturvallisuuskeskukselta aktiivisia toimia.



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

Kesäkuussa aktivoituneen FortiBleed-hyökkäyskampanjan vaikutusten odotetaan pysyvän Suomessa maltillisina. Kyberturvallisuuskeskus seuraa tilannetta aktiivisesti.

Kesälomakauden vaikutusten odotetaan jatkuvan heinä-elokuulle erilaisten huijausten muodossa.

Kyberturvallisuuskeskukselle tulevat ilmoitukset tyypillisesti vähenevät kesäkaudella, mutta määrät lähtevät jälleen nousuun organisaatioiden lomakauden päättyessä alkusyksystä.

Organisaation varautuminen

- Verkon reunalaitteiden suojaaminen on keskeinen osa organisaation kybervarautumista. Riskien hallinta edellyttää ennakoivaa päivityshallintaa, turvallisia konfiguraatioita, monivaiheista tunnistautumista ja poikkeamien tehokasta valvontaa.[13]
- Lomakauden päätyttyä on odotettavissa kasvava määrä M365-tilimurtoja. Organisaatioiden on syytä ottaa käyttöön suojaustoimia tilimurtoja vastaan.[8]

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 tuli voimaan 1.6.2026

- Kyberkestävyyssäädöstä (CRA) täydentävä kyberkestävyyslaki (439/2026) tuli voimaan 1.6.2026.
- Liikenne- ja viestintäministeriö ja Liikenne- ja viestintävirasto Traficom pitivät 3.6. yhteisen sidosryhmätilaisuuden lain voimaantulosta ja soveltamisesta.
- Tilaisuuden tallenne ja tilaisuudessa esitetyt kysymykset vastauksineen on julkaistu tapahtumasivuilla.[14]
- CRA:n mukaiseksi vaatimustenmukaisuuden arviointilaitokseksi voi nyt hakeutua, kun kyberkestävyyssäädöksen IV luvun mukaiset ilmoittavan viranomaisen velvollisuudet astuivat voimaan 11.6.2026 alkaen.

Oikeudelliset asiat
Euroopan komissio julkaisi EU:n teknologisen suvereniteetin paketin

- Euroopan komissio on julkaissut 3.6.2026 EU:n teknologisen suvereniteetin paketin.[15]
- Paketti sisältää:
  - kaksi lainsäädäntöehdotusta: sirusäädös 2.0 (Chip Act 2.0), sekä pilvipalveluja ja tekoälyä edistävä säädös (Cloud and AI Development Act, CADA)
  - sekä kaksi ei-lainsäädännöllistä aloitetta: avoimen lähdekoodin strategia (EU Open Source Strategy), sekä energia-alan digitalisaatiota ja tekoälyä koskeva strateginen etenemissuunnitelma (Strategic Roadmap for Digitalisation and AI in Energy).
- Tavoitteena on vahvistaa Euroopan valmiuksia puolijohteissa, tekoälyssä, pilvipalveluissa ja avoimessa lähdekoodissa.
- Paketin taustalla ovat yhä enenevät geopoliittiset ja kyberturvallisuushaasteet sekä EU:n kilpailukykyhaasteet suhteessa Yhdysvaltoihin ja Kiinaan.
- Paketin tarkoituksena on vähentää rakenteellisia riippuvuuksia ja varmistaa, että Euroopassa voidaan kehittää, hyödyntää ja turvata eurooppalaisten tarvitsemia teknologioita.

Oikeudelliset asiat
Turvallisuutta ja uutta talouskasvua tietoverkoista (TUUTTI) –hankkeen ensimmäisen vaiheen raportti julkaistu

- Liikenne- ja viestintäministeriö on julkaissut 17.6.2026 TUUTTI-hankkeeseen liittyvän raportin: *Kokonaistilannekuva viestintäverkoista, markkinoista ja palveluista sekä kehityssuunnat ja näkymä keskeisiin päätösajankohtiin kohti 2030-lukua*.[16]
- Tarkastelun lähtökohtana on, että turvalliset ja toimintavarmat viestintäverkot ovat yhteiskunnan toimivuuden, huoltovarmuuden, investointien ja datatalouden kasvun perusta.
- Raportti kokoaa viestintäverkkojen nykytilan ja keskeiset muutostekijät. Se tarkastelee kiinteitä verkkoja, matkaviestinverkkoja, satelliitti- ja avaruuspalveluja, maa- ja merikaapeleita sekä lähetysverkkoja osana verkkojen, datan, laskennan, energian, osaamisen ja turvallisuuden kokonaisuutta.
- Raportti tunnistaa riskejä ja mahdollisuuksia, jotka liittyvät kriittisiin riippuvuuksiin, kyberturvallisuuteen, geopoliittiseen toimintaympäristöön, investointien ennakoitavuuteen sekä digitaaliseen ja teknologiseen suvereniteettiin.
- Kokonaistilannekuvan pohjalta raportti esittää jatkovalmistelun painopisteitä ja lyhyen aikavälin valmistelukokonaisuuksia, kuten peruspalvelujen ja viimesijaisen turvaverkon tarkastelun, matkaviestinverkkojen toimilupakokonaisuuksien valmistelun, kiinteiden viestintäverkkojen rakentamisen tilannekuvan sekä EU- ja standardointivaikuttamisen vahvistamisen. Raportti tukee ministeriön valmistelua sekä kansallista ja EU-tason vaikuttamista.

Oikeudelliset asiat
Korkein hallinto-oikeus piti voimassa Verkkokauppa.comille määrätyn seuraamusmaksun tietosuojarikkomuksista

- Korkein hallinto-oikeus on saattanut voimaan tietosuojavaltuutetun ja tietosuojavaltuutetun toimiston seuraamuskollegion päätöksen Verkkokauppa.com Oyj:n toiminnasta. Yhtiö oli rikkonut tietosuojalainsäädäntöä, kun se oli jättänyt määrittelemättä säilytysajat asiakastilien tiedoille.[17]
- Tietosuojavaltuutetun toimiston seuraamuskollegio määräsi Verkkokauppa.comille 856 000 euron suuruisen hallinnollisen seuraamusmaksun maaliskuussa 2024, sillä yhtiö ei ollut määritellyt, kuinka kauan verkkokauppa-asiakkaiden asiakastilien tietoja säilytetään. Asiakastietoja säilytettiin yhtiön mukaan niin kauan, kunnes asiakas itse oli pyytänyt tietojen poistamista.
- Hallinto-oikeus alensi aiemmin seuraamusmaksun määrän 792 639 euroon yrityksen viimeisimmän liikevaihdon perusteella. Muilta osin Hallinto-oikeus hylkäsi Verkkokauppa.comin valituksen. Korkein hallinto-oikeus ei muuttanut hallinto-oikeuden ratkaisua.
- Korkein hallinto-oikeus katsoo, että yhtiöllä on ollut velvollisuus määrittää keräämilleen henkilötiedoille säilytysajat, eikä säilytysaikaa voida perustaa yksinomaan henkilön omien toimenpiteiden varaan. Yhtiö ei siis voinut jättää henkilötietojen säilytysaikaa määrittämättä sen perusteella, että asiakas voi itse pyytää tietojen poistamista tai tehdä toimenpiteitä niiden poistamiseksi.

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)

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti osoitteesta www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot.

Lähteet

Lähdeluettelo
1/2

1. https://kyberturvallisuuskeskus.fi/fi/uutiset/fortibleed-kyberhyokkayskampanjan-vaikutukset-nakyvat-myos-suomessa
2. https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuskeskuksen-tapahtumat/eun-kyberkestavyyssaados-cra-tulee-voimaan-infotilaisuus-362026
3. https://vm.fi/-/valtionhallinnon-tekoalyohjelman-ensimmaiset-rahoituspaatokset-tehty
4. https://kyberturvallisuuskeskus.fi/fi/uutiset/windowsin-secure-bootin-varmenteet-vanhenevat-kesakuusta-2026-alkaen-mita-se-tarkoittaa-organisaatioille-ja-kayttajille
5. https://www.traficom.fi/fi/uutiset/kyberturvallisuuden-ensimmainen-vuosipuolisko-2026-kyberuhkien-torjuminen-vaatii-vahvempaa-varautumista-ja-resursointia
6. https://www.traficom.fi/fi/uutiset/kesalomat-lisaavat-toimitusjohtajahuijausten-riskia-syvavaarennokset-tekevat-huijauksista-entista-uskottavampia
7. https://www.traficom.fi/fi/uutiset/kesan-kybermuistilista-auttaa-lomailemaan-turvallisemmin
8. https://kyberturvallisuuskeskus.fi/fi/uutiset/verkon-reunalaitteiden-riskit-ovat-merkittava-uhka-organisaatioille
9. https://www.traficom.fi/fi/uutiset/varaatko-kesalomamatkoja-huijausviesteja-liikkuu-matkavarauspalveluiden-nimissa
10. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/valepomon-viesti-voi-tulla-kalliiksi-tunnista-toimitusjohtajahuijaus-ajoissa

Lähdeluettelo
2/2

11. https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuskeskuksen-tapahtumat/eun-kyberkestavyyssaados-cra-tulee-voimaan-infotilaisuus-362026
12. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-16
13. https://kyberturvallisuuskeskus.fi/fi/uutiset/uusi-aalto-m365-tietojenkalastelussa-ai-avusteinen-laitekoodin-kalastelukampanja
14. https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuskeskuksen-tapahtumat/eun-kyberkestavyyssaados-cra-tulee-voimaan-infotilaisuus-362026
15. https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy
16. https://urn.fi/URN:ISBN:978-952-243-926-0
17. https://tietosuoja.fi/-/korkein-hallinto-oikeus-piti-voimassa-verkkokauppa.comille-maaratyn-seuraamusmaksun-tietosuojarikkomuksista