TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Elokuu 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

ClickFix-tapausten määrässä oli huomattavaa kasvua elokuussa aiempiin kuukausiin verrattuna.

EU:n tekoälyasetuksen mukainen tekoälyn avoimuussääntely astui voimaan elokuun alussa ja sen tarkoituksena on varmistaa, että sivustojen käyttäjät tietävät asioivansa tekoälyn kanssa. Velvoitteet koskevat sekä tekoälyjärjestelmien tarjoajia että niiden käyttäjiä.

Kybersään yleistilanne elokuussa 2026

Kybersäässä jatkuu edelleen sateisena

Elokuun kyberturvallisuustilanne Suomessa painottui erityisesti tietojenkalasteluun, verkkopalvelujen murtoihin sekä EU-sääntelyn mukanaan tuomiin uusiin velvoitteisiin. Odotetusti myös M365-tietomurtojen määrä oli kasvussa kesälomien jäljiltä.

Kalastelut olivat monipuolisia: palkanmaksuhuijauksia, kyberturvallisuusasiantuntijaksi tekeytymistä ja Signal-pikaviestisovelluksen tukena esiintymistä.

Elokuussa jatkui heinäkuussa julkaistun Wordpressin ydinohjelmiston haavoittuvuuden hyväksikäyttö, jossa murrettuja sivustoja on käytetty haittaohjelmien levittämiseen sivuston kävijöille. Haavoittuvuuden avulla on tehty todella merkittävä määrä tietomurtoja suomalaisiin verkkosivuihin.

Ulkomailla on ukkostanut toden teolla

- Julkinen sektori on ollut useissa maissa kyberhyökkäysten kohteena.
- Latvian ajoneuvorekisterijärjestelmä joutui tietomurron ja -vuodon uhriksi elokuussa. Murrossa hyökkääjät saivat käsiinsä vuosien ajalta 1,2 miljoonan ihmisen henkilötietoja. [1]
- Saksassa Berliinin osavaltion kahteen ministeriöön tehtiin tietoja varastava kiristyshaittaohjelmahyökkäys, jonka seurauksena ministeriöt jouduttiin irrottamaan verkosta. [2]
- Ranskassa koko vuoden piinanneet merkittävät tietomurrot jatkuivat elokuussa julkitulleella verohallintoon kohdistuneella hyökkäyksellä, jossa n. 680 000 henkilön tai yrityksen tiedot vietiin. [3]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Pidä verkkosivustojen julkaisujärjestelmät (kuten Wordpress) ja niiden lisäosat koko ajan tasalla ja poista tarpeettomat lisäosat sekä käyttäjätilit. Päivitimme kesällä opastamme Wordpressin tietoturvaan. [4]

Viranomaiset ja järjestöt ovat yhdessä käynnistäneet kampanjan turvallisen netinkäytön puolesta uuden lukuvuoden alkajaisiksi. Traficomin ja poliisin Nyt valppaana verkossa –sivusto tarjoaa käytännöllisiä vinkkejä huoltajille ja lapsille arjen tietoturvaan. [5]

Julkaisimme ohjeet, jotka auttavat yrityksiä ymmärtämään, milloin tekoälyn käytöstä tai sen tuottamasta sisällöstä tulee kertoa käyttäjille. Käytännössä tämä koskee esimerkiksi sivustoille luotavia chatboteja, joiden osalta käyttäjille on aina kerrottava, että tämä keskustelee tekoälyrobotin kanssa. Suosittelemme yrityksiä hyödyntämään komission julkaisemaa ohjeistusta, käytännesääntöjä ja ikoneja velvoitteiden toteuttamisessa. [6]

Kuukauden raekuuro
ClickFix-hyökkäysten määrä kasvoi huomattavasti elokuussa

Elokuussa raportoitujen ClickFix-hyökkäysten määrä on poikkeuksellisen suuri aiempaan verrattuna, vaikka ilmiö itsessään ei olekaan uusi. Kesän tapausmäärien taustalla vaikuttavat kaksi ajallisesti lähekkäin ilmennyttä WordPress-haavoittuvuutta, joiden hyväksikäyttö on mahdollistanut haitallisen sisällön lisäämisen useille verkkosivuille.

Kyberrikolliset ovat lisänneet verkkosivuille haitallista sisältöä, joka voi näyttää aidolta CAPTCHA-tarkistukselta ("En ole robotti" -tarkistus). Sivustolla oleva huijausikkuna väittää, että käyttäjän pitää tehdä jokin tarkistus ennen sivun käyttöä. Huijausikkunassa oleva teksti pyytää käyttäjään avaamaan tietokoneella erillisen ohjelman ja seuraamaan annettuja ohjeita.

Menetelmän kasvava suosio liittyy mahdollisesti siihen, että verkkoselaimet sisältävät nykyään tehokkaita tietoturvamekanismeja, jotka vaikeuttavat perinteisten selainpohjaisten hyökkäysten onnistumista. Tämän seurauksena hyökkääjät pyrkivät siirtämään hyökkäyksen ratkaisevan vaiheen käyttäjän itse suoritettavaksi, jolloin teknisten suojausten ohittaminen on helpompaa.

On todennäköistä, että rikolliset jatkavat toimintatavan käyttöä, koska ovat havainneet sen tehokkaaksi.

ClickFix-hyökkäyksiltä suojautuminen on mahdollista ja verrattain helppoa. [7]

Kybersään ilmiöt

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä.

Kybersää
elokuu 2026

1 kk

Tietomurrot- ja vuodot

- Elokuussa ilmoitettiin runsaasti tietomurtoja.
- Suurimmassa osassa tietomurroissa hyökkääjät hyödynsivät haavoittuvuuksia hyökkäysvektorina.
- Microsoft 365 -tietomurroissa korostui laitekoodikalastelu.

Haittaohjelmat

- Elokuun aikana havaittiin monia verkkosivustoja, joissa jaettiin haittaohjelmia ClickFix-tekniikkaa hyödyntäen.
- Tarkastelujakson aikana Kyberturvallisuuskeskukselle ilmoitettiin kaksi kiristyshaittaohjelmatapausta.

Haavoittuvuudet

Haavoittuvuuksien määrän kasvutrendi jatkui nousevana myös elokuussa.

Haavoittuvuuksien kautta tapahtuneita tietovuotoja on havaittu elokuussa.

Huijaukset ja kalastelut

- Rikolliset huijasivat jälleen lomalta palaavia työntekijöitä.
- Älä usko puhelimessa huijaria, joka väittää soittavansa teknisestä tuesta tai kyberturvallisuuden vuoksi.

Automaatio ja IoT

- Slovakian hankkimat liikennekamerat osoittautuivat tietoturvattomiksi ja venäläisvalmisteisiksi ja muodostavat riskin hyväksikäytölle sotilastiedustelussa.
- Kiinalaisen ZBT:n valmistamista reitittimistä on löytynyt useita takaportteja.

Verkkojen toimivuus

- Palvelunestohyökkäykset eivät aiheuttaneet merkittäviä häiriöitä Suomessa.
- Verkot toimivat normaalisti.

Kybersää
elokuu 2026 1/2

1 kk

Tietomurrot ja -vuodot

- Haavoittuvien WordPress-sivustojen tietomurrot muodostivat merkittävän osan haavoittuvuuksia hyödyntämällä tehdyistä tietomurroista.
- Elokuussa ilmoitetuista Microsoft 365 -tietomurroista 51 % toteutettiin laitekoodikalastelulla ja 44 % AiTM-kalastelulla. Rikolliset hyödynsivät myös Microsoft Teams -keskusteluja lähestyessään talousjohtajia ja painostaessaan heitä tekemään rahansiirtoja tai maksamaan laskuja kiireellisesti.
- Heinäkuussa tapahtunut tietomurto osoittautui jatkotutkimuksissa vakavaksi: tapauksessa vuoti yli 10 000 henkilön henkilötietoja.

Haittaohjelmat

- Elokuussa havaittiin useita verkkosivustoja Suomen verkkoavaruudessa, joissa jaettiin haittaohjelmia ClickFix-tekniikkaa hyväksikäyttämällä. WordPress-verkkosivustojen tietomurtojen määrä on myös johtanut ClickFix-tapauksien merkittävään kasvuun.
- Elokuun aikana Kyberturvallisuuskeskukselle ilmoitettiin kahdesta kiristyshaittaohjelmatapauksesta. Molemmissa tapauksissa hyökkäyksen takana oli kansainvälisesti tunnettuja rikollisryhmiä, kuten Qilin- ja Krybit-ryhmittymät.

Haavoittuvuudet

- N-able N-Central-palvelimessa vakava ja aktiivisesti hyväksikäytetty haavoittuvuus (CVE-2026-18556, CVE-2026-18577)
- Metabase – ohjelmistossa haavoittuvuus, joka mahdollistaa tunnistautumattoman hyökkääjän SQL-injektiohyökkäyksen etänä (CVE-2026-72898)
- Citrix Netscaler ADC ja Gateway – tuotteissa kriittisiä haavoittuvuuksia (CVE-2026-19489, CVE-2026-19490)

Kybersää
elokuu 2026 2/2

1 kk

Huijaukset ja kalastelut

- Elokuussa kyberrikollisten huomio kohdistui lomaltapalaajiin. Odottavan sähköpostitulvan joukkoon oli lähetetty myös "kiireellisiä" kalasteluviestejä, joiden tarkoituksena oli saada lomalta palaavat työntekijät avaamaan huijauslinkkejä.
- Älä luota turvallisuusviranomaisena esiintyvään huijariin. Jos joku väittää puhelimessa soittavansa kyberturvallisuuden vuoksi tai tarjoavansa pakollista sovelluspäivitystä tai tukea, soittajaa ei pidä uskoa. Puhelimessa ei pidä koskaan kertoa salasanoja, palautusavaimia, tunnuslukuja, pin-koodeja tai muita vahvistuskoodeja.

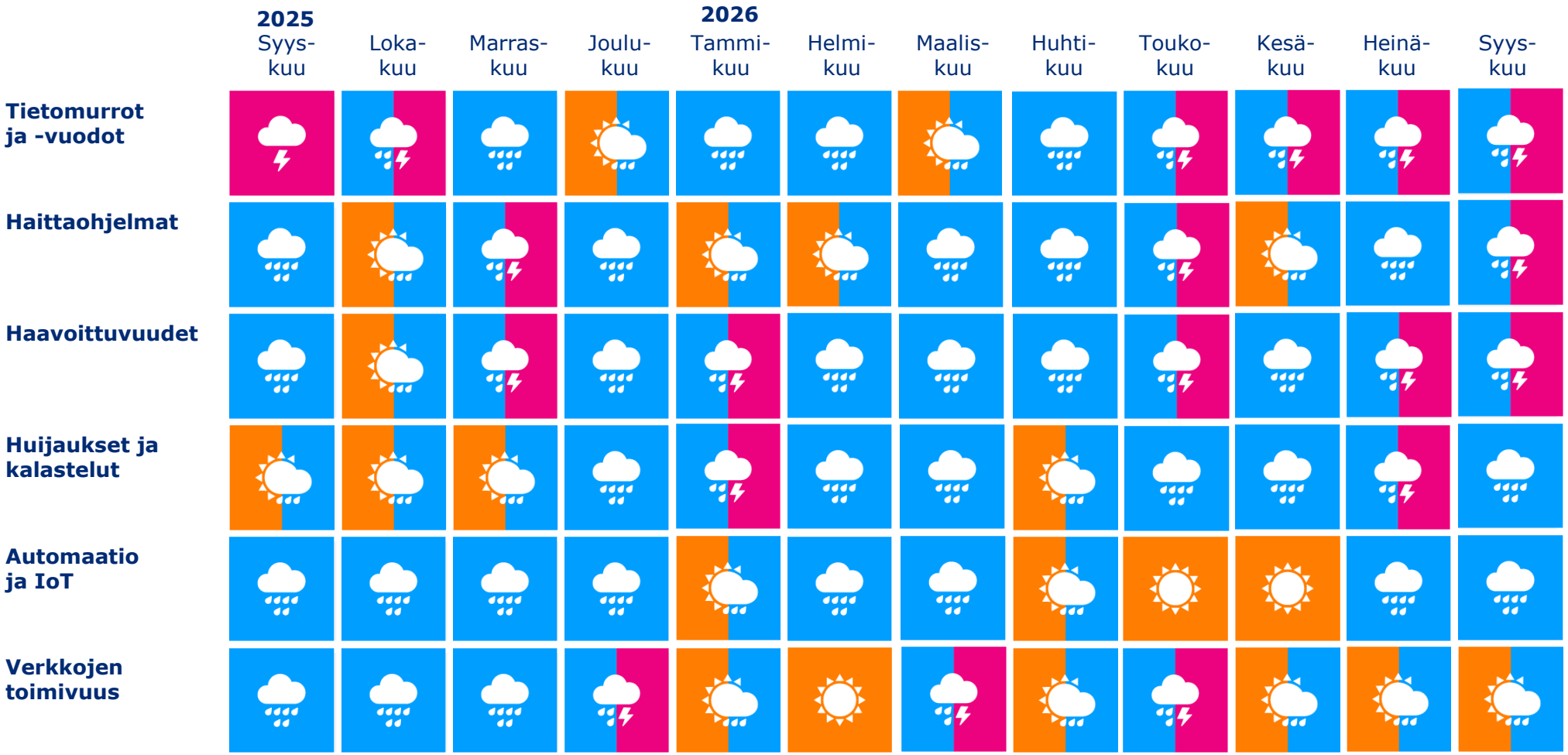
Automaatio ja IoT

- Sadoittain Slovakian valtion hankkimia liikennevalvontakameroita osoittautui venäläisvalmisteisiksi. Niistä paljastui dokumentoimattomia takaportteja, joiden kautta ne pystyi ottamaan täydellisesti hallintaan. Kamerat oli myynyt kyproslainen pöytälaatikkofirma. Tietoturvattomia liikennekameroita on hyväksikäytetty muualla maailmalla vakoilussa ja sotilastiedustelussa, ja tämä on huolena myös Slovakiassa. [8] [9]
- Kiinalaisen ZBT:n valmistamista reitittimistä on löytynyt useita takaportteja, joiden kautta ne pystyy ottamaan hallintaan. ZBT:n valmistamia laitteita myydään myös monien muiden brändien nimillä. [10]

Verkkojen toimivuus

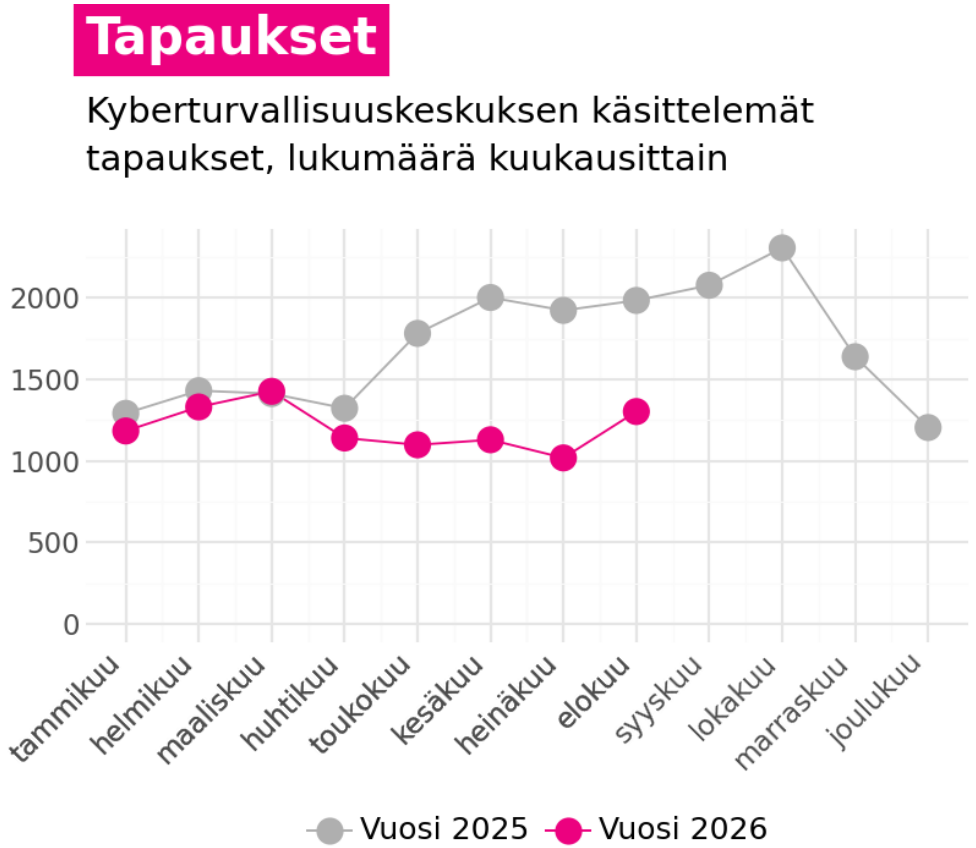
- Kaapatuista IoT-, palvelin- ja pilvi-infrastruktuureista koostuvien super-bottiverkkojen määrä on kasvamassa ja niiden potentiaalinen hyökkäysliikenteen määrä muodostaa merkittävän riskin digitaalisten palvelujen saatavuudelle. [11] [12]
- Venäjämielinen haktivisti-ryhmittymä Server Killers on ottanut vastuun useista Euroopassa tapahtuneista palvelunesto-hyökkäyksistä, joista merkittävimpänä voi pitää Norjan julkishallintoon kohdistunutta hyökkäystä. [13]

Kybersään ilmiöt
kulunut 12 kk



Tapaukset

- Kyberturvallisuuskeskus käsitteli elokuussa 1302 tapausta.
- Ilmoitusten määrä on 12 kuukauden keskiarvoon nähden 7% vähemmän.
- Kesä-heinäkuun jälkeen havaittiin kasvua Kyberturvallisuuskeskukselle tehdyissä ilmoituksissa, mikä on tyypillistä kesälomakauden päättyessä.
- Elokuu oli kiireinen niin Kyberturvallisuuskeskukselle kuin yrityksillekin. Kriittisiä ja vakavia haavoittuvuuksia ilmeni miltei päivittäisellä tasolla, mikä vaatii aktiivisia toimenpiteitä haavoittuvuuksien hyödyntämisten estämiselle.
- Lisäksi lukuisat WordPress-tietomurrot ja ClickFix-tekniikalla haittaohjelmien levittämiset näkyivät runsaasti tapaustilastossa.



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

Kybersäähän ei ole odotettavissa merkittäviä muutoksia. On todennäköistä, että kesällä nähtyjen haavoittuvuuksien hyväksikäyttö jatkuu.

On odotettavissa, että tapausmäärät kasvavat edellisvuoden tapaan syksyä kohti mentäessä.

Organisaation varautuminen

- Haavoittuvuuksien näkökulmasta on erittäin tärkeää, että organisaatiot kartoittaisivat omia laitteitaan ja järjestelmiään säännöllisesti, koska havaituissa tapauksissa on esimerkkejä sellaisista vanhentuneista laitteista ja ohjelmistoista, joiden käytössä olemisesta organisaatiot eivät olleet tietoisia.
- Päivityssyklin muuttuminen nopeaksi vaatii aktiivista seurantaa.
- Laitevalmistajat ilmoittavat usein ennakkoon tulevista päivityksistä, joten ilmoituksia kannattaa seurata ja suunnitella omaa toimintaansa niiden perusteella.

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 Kyberkestävyyssäädöksen (CRA) ilmoittamisvelvollisuus alkaa

- CRA:n haavoittuvuuksien ja tietoturvapoikkeamien raportointia koskevat velvoitteet tulevat voimaan 11. syyskuuta 2026.
- Valmistajien on ilmoitettava aktiivisesti hyödynnetyistä haavoittuvuuksista ja vakavista tietoturvapoikkeamista määräaikojen puitteissa ENISAn keskitetyllä raportointialustalla (Single Reporting Platform, SRP).
- Ennakkovaroitus on tehtävä 24 tunnin kuluessa siitä, kun valmistaja on saanut asiasta tiedon, ja ilmoitusta täydennetään 72 tunnin kuluessa.
- Haavoittuvuuden loppuraportti toimitetaan 14 vuorokauden kuluessa siitä, kun korjaus tai lieventävä toimenpide on saatavilla.
- Vakavaa tietoturvapoikkeamaa koskeva loppuraportti toimitetaan kuukauden kuluessa poikkeamailmoituksesta.
- ENISA on valmistellut ohjeen haavoittuvuuksien ja poikkeamien ilmoittamiseen SRP:ssä. [14]
- Traficomin Kyberturvallisuuskeskus on koonnut valmistajille listan tarkistettavista asioista ja linkit keskeisiin ohjeisiin. [15]

Oikeudelliset asiat
Korkein hallinto-oikeus vahvisti Traficomin tulkintoja evästeiden käytöstä

- Korkein hallinto-oikeus (KHO) antoi kaksi evästeitä koskevaa ennakkopäätöstä, joissa vahvistettiin Traficomin tulkinta suostumuksen edellytyksistä. [16]
- Molemmissa tapauksissa on kyse Liikenne- ja viestintävirasto Traficomin vuosina 2023 ja 2024 antamista päätöksistä, joissa velvoitettiin muuttamaan verkkosivustojen evästekäytäntöjä vastaamaan sähköisen viestinnän palveluista annetun lain edellytyksiä (917/2014).
- Ratkaisut vahvistavat, että suostumuksen pyytämistä koskevasta velvollisuudesta poikkeamisen kynnys on korkea.
- KHO katsoi ratkaisussaan KHO:2026:64, että personointievästeiden käyttö edellyttää käyttäjän suostumusta. Lisäksi KHO vahvisti, että verkkokutsut merkitsevät SVPL:ssä tarkoitettua päätelaitteelle tallennettujen tietojen käyttöä ja siten niihin soveltuu samat edellytykset kuin eväisteiden käytölle.
- KHO arvioi toisessa ratkaisussaan KHO:2026:65 käyttäjän suostumuksen vapaaehtoisuutta. Evästeistä kieltäytymisen tulee olla yhtä helppoa, kuin suostumuksen antamisen. Ratkaisu korostaa käyttäjän aidon valinnan merkitystä suostumusta pyydettäessä.

Oikeudelliset asiat
Kyberturvallisuuslain seurannan ja arvioinnin loppuraportti julkaistu

- Liikenne- ja viestintäministeriö on julkaissut loppuraportin kyberturvallisuuslain seurannasta ja arvioinnista 31.8.2026. [17]
- Lakia pidetään yleisesti onnistuneena ja sen toimeenpano on vahvistanut organisaatioiden kyberturvallisuutta.
- Haasteita lain toimeenpanolle on aiheuttanut viranomaisten resurssien puute.
- Kyberturvallisuuslain seurantahankkeessa arvioitiin lain tavoitteiden toteutumista ja soveltamista ensimmäisen voimassaolovuoden ajalta.
- Laki tuli voimaan huhtikuussa 2025 ja sillä toimeenpantiin EU:n kyberturvallisuusdirektiivi (NIS 2).
- Direktiivin tavoitteena on vahvistaa EU:n ja jäsenvaltioiden kyberturvallisuutta kriittisillä toimialoilla.
- Selvityksen perusteella keskitetyn kansallisen poikkeamaraportointijärjestelmän kehittämisestä olisi hyötyä kyberturvallisuuslain soveltamisalaan kuuluville toimijoille.

Oikeudelliset asiat eIDAS-uudistusta täydentävä lainsäädäntö vahvistettu

- Tasavallan presidentti vahvisti 4.9.2026 lait, joilla täydennetään rajat ylittävää sähköistä tunnistamista, luottamuspalveluita ja eurooppalaista digitaalista identiteettiä koskevaa EU:n asetusta (eIDAS-asetusta). [18]
- Uutena säädettiin laki eräistä rajat ylittävän sähköisen asioinnin mahdollistavista palveluista, joka mahdollistaa eurooppalaisen digitaalisen identiteetin lompakon (EU Digital Identity Wallet) tarjoamisen Suomessa.
- Lompakon avulla käyttäjä voi tunnistautua sähköisesti sekä hallinnoida virallisesti vahvistettuja tietojaan turvallisesti ja yhdenmukaisesti EU:ssa.
- Lain mukaan Digi- ja väestötietoviraston tehtävänä on tarjota Suomessa lompakkoa. Myös muut tahot voivat tarjota Suomessa lompakkoa.
- Liikenne- ja viestintävirasto Traficom toimii valvontaviranomaisena.
- Samalla säädetään uudesta digitaalisesta henkilöllisyystodistuksesta sekä päivitetään sähköistä tunnistamista ja luottamuspalveluja koskevaa kansallista sääntelyä.
- Lait tulevat voimaan 1.10.2026.

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

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

Lähteet

Lähdeluettelo
1/2

1. https://eng.lsm.lv/article/society/crime/18.08.2026-data-of-12-million-people-breached-in-recent-csdd-cyberattack.a659333/
2. https://www.bbc.com/news/articles/cm2q7gv3l5qo
3. https://www.lemonde.fr/en/politics/article/2026/08/18/french-government-embroiled-in-taxpayer-data-hack-decried-as-country-s-most-serious-ever_6756624_5.html?srsltid=AfmBOorLaiFdWFc5ntbEwVU6PlrveIyALS1Xfkv1LUFzYRUXX61AhWaq
4. https://kyberturvallisuuskeskus.fi/fi/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/vinkkeja-wordpress-julkaisujarjestelman-tietoturvaan
5. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/koulujen-alkaessa-hyva-muistuttaa-lasten-turvallisesta-netinkaytosta
6. https://www.traficom.fi/fi/uutiset/tekoalyn-kaytosta-nyt-kerrottava-aiempaa-avoimemmin-traficom-julkaisi-ohjeet-uusiin-velvoitteisiin
7. https://kyberturvallisuuskeskus.fi/fi/uutiset/varo-vaarennettyja-captcha-tarkistuksia-verkkosivuilla
8. https://www.is.fi/digitoday/tietoturva/art-2000012241463.html
9. https://www.documentcloud.org/documents/28565254-tlp-clear-en-nero-r-one-skcert-20260807-10177-v1/
10. https://www.vulncheck.com/blog/zbt-darklantern-speakingstone

Lähdeluettelo
2/2

11. https://www.pressebox.com/pressrelease/link11-gmbh/fewer-attacks-more-force-link11s-european-cyber-report-finds-new-ddos-records-for-the-first-half-of-2026/boxid/1310715?utm_source=chatgpt.com
12. https://www.bleepingcomputer.com/news/security/massive-ddos-attack-disrupts-norways-government-digital-services/
13. https://www.thebarentsobserver.com/news/prorussian-hackers-declare-cyberwar-on-norway/456591
14. https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp
15. https://kyberturvallisuuskeskus.fi/fi/uutiset/valmistaja-varaudu-ennalta-kyberkestavyyssaadoksen-mukaiseen-haavoittuvuuksien-ja-poikkeamien-ilmoittamiseen
16. https://kyberturvallisuuskeskus.fi/fi/uutiset/korkein-hallinto-oikeus-vahvisti-traficomin-tulkintoja-evasteiden-kaytosta
17. https://lvm.fi/-/kyberturvallisuuslaki-kokonaisuutena-onnistunut-haasteena-valvonnan-resurssien-puute
18. https://valtioneuvosto.fi/paatokset/paatos?decisionId=6923