TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Marraskuu 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

Alankomaiden poliisi onnistui takavaroikomaan 250 palvelinta, joita käytettiin bulletproof hostingin (BPH) yhteydessä. BPH on usein kyberrikollisuuden yhteydessä käytetty järjestely, jossa internet-palveluntarjoaja jättää tietoisesti puutumatta palvelunsa välityksellä tapahtuvaan laittomaan toimintaan. [1]

Ruotsalaiseen Miljödataan kohdistuneessa tietomurrossa uutisoidaan altistuneen jopa 1,5 miljoonan asiakkaan arkaluontoisia tietoja. Yrityksen asiakaskuntaan kuuluu muun muassa suuri osa Ruotsin kunnista. [2, 3]

Reutersin ja Ylen uutisoinnin mukaan jopa 10 % somejätti Metan mainostuloista saattaa muodostua huijausmainoksista. Meta pyrkii rajoittamaan mainostilan myymistä huijareille, mutta automaattinen mainosmyynti estetään vain silloin, jos ostajaa epäillään huijariksi 95% todennäköisyydellä. [4, 5]

Kybersää marraskuu 2025

Tietomurrot ja -vuodot

- Microsoft 365 -tilimurtoja koskeva varoitus poistettiin 27.11.2025. Tilimurtojen uhka on tästä huolimatta säilynyt korkeana. Monivaiheinen tunnistautuminen ei yksin riitä uhkan torjumiseen.
- Haavoittuvuuksia hyväksikäyttämällä tehtiin tietomurtoja:
  - Microsoft WSUS Remote Code Execution CVE-2025-59287
  - Adobe Commerce and Magento Open Source CVE-2025-54236
  - ASUS AiCloud - CVE-2025-2492

Huijaukset ja kalastelut

- Valeverkkokaupat kalastelevat kuluttajien rahoja loppuvuoden tarjouksien vanavedessä. Joulusesongin tarjouskampanjat ovat huijarien suosiossa.
- Traficomin ja suomalaisten teleoperaattorien yhteistyössä kehittämä huijauspuheluiden estoratkaisu voitti Euroopan rikoksentorjuntakilpailun. Estoratkaisu oli aiemmin syksyllä valittu myös Suomen rikoksentorjuntakilpailun voittajaksi.

Haittaohjelmat ja haavoittuvuudet

- Kriittinen ja hyväksikäytetty haavoittuvuus Fortinet FortiWeb -tuotteessa (CVE-2025-64446)
- Shai-Hulud-haittaohjelman toinen aalto tartuttanut laajasti npm-paketteja ja kerännyt niitä käyttävistä järjestelmistä tunnuksia sekä arkaluontoisia tietoja. Organisaatioiden tulee tarkastaa kehitysinfrastruktuurinsa epäilyttävien merkkien varalta.
- Murrettuihin verkkokauppoihin piilotettu Magecart-haittaohjelma varastaa asiakkaiden maksukorttitietoja.

Automaatio ja IoT

- CRA:n täytäntöönpanoasetus (EU) 2025/2392 tärkeiden ja kriittisten tuotteiden teknisistä kuvauksista on julkaistu EUR-lexissä.
- Aisurun kaltaiset, monikäyttöiset bottiverkot antavat hyökkääjälle monipuolisia kyvykkyyksiä. Vaikka bottiverkkoja pystyttäisiin tekemään toimintakyvyttömäksi, laitteet säilyvät edelleen haavoittuvina ja niistä voidaan muodostaa uusia bottiverkkoja

Verkkojen toimivuus

- Suurimmat palvelunestohyökkäyksiin käytettävät bottiverkot kasvavat jatkuvasti ja niistä raportoidaan entistä suurempia hyökkäyksiä. Turvattomien IoT-laitteiden määrän kasvu ruokkii tätä ilmiötä ja sama kehitys jatkunee myös tulevaisuudessa.
- Microsoft raportoi torjuneensa onnistuneesti Aisuru-bottiverkon ennätyksellisen yli 15 Tbps palvelunestohyökkäyksen, jossa hyökkäysliikennettä lähetettiin yli 500 000 lähdeosoitteesta. Aisuru koostuu kaapatuista kotireitittimistä ja IoT-laitteista, kuten valvontakameroista.

Vakoilu

- Kyberuhkatoimijat hyödyntävät edelleen sekä jo tunnettuja että uusia haavoittuvuuksia verkkolaitteisiin kohdistuvissa tietomurroissa. Marraskuussa kohteina olivat mm. Cisco-laitteet.
- Iranilaiseen kybertoimijaan liittyvä tietovuoto paljasti yksityiskohtia ryhmän toiminnasta.
- Iraniin liitetyssä raportoinnissa nousi esiin myös mm. puolustusteollisuuteen ja ilmailualaan kohdistuva kiinnostus.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Verkkosovellusten turvallisuusuhkia kartoittava OWASP on päivittämässä Top 10 -listaustaan. Uudessa listauksessa otsikointi ja uhkien sijoitukset ovat muuttumassa jonkin verran. Toimitusketjuihin liittyvät uhkat ovat myös nousemassa uutena kategoriana mukaan. [6, 7]

Digitaalisen skimmauksen riski kasvaa suurten alennusmyyntien ja pyhien alla. Digitaalisessa skimmauksessa rikolliset asentavat verkkokauppaan haitallista koodia ja varastavat sitä kautta maksuprosessissa annettavat tiedot. Vaikka Black Friday on jo takana päin, kannattaa riski huomioida myös joululahjaostoksilla. Lue lisää tietoturva Nyt!-artikkelista *”Näkymätön varas verkkokaupassasi - Digitaalisella skimmauksella voi olla merkittäviä taloudellisia vaikutuksia”.* [8]

Julkaisimme pilvipalveluiden pääkäyttäjätunnuksia käsittelevän Tietoturva Nyt!-artikkelin joulukuun alussa. Lue vinkkejä pääkäyttäjätunnusten turvaamiseen artikkelissa *“Pilvipalveluiden pääkäyttäjätunnusten hallinta – parhaat käytännöt”.* [9]

Marraskuun kyberturvallisuuden yleiskuva

Marraskuun kybersäätila oli yleiskuvaltaan sateinen, mutta samalla melko rauhallinen. Kuukauden aikana havaittiin muutamia huomionarvoisia ilmiöitä Suomessa ja maailmalla.

Kyberturvallisuuskeskukselle tehdyissä ilmoituksissa uudempina havaintoina näkyivät ClickFix-tekniikalla tehdyt hyökkäykset ja Shai-Hulud 2.0 haittaohjelma. Kesäkaudella tutuksi tullutta BadBox 2.0 haittaohjelmaa havaitaan edelleen.

- ClickFix-hyökkäyksissä internetin käyttäjä erehdytetään suorittamaan haittaohjelma laitteellaan. Hyökkäysmenetelmässä jäljitellään "Vahvista, että olet ihminen"- ja CAPTCHA-tarkistusten kaltaisia pieniä tehtäviä, joiden ratkaisemiseen käyttäjät ovat tottuneet arkisen verkkoselauksen yhteydessä. [10]
- Shai-Hulud 2.0 on kehitysympäristöissä leviävä tietokonemato. Madon leviäminen on ollut erittäin nopeaa ja se on tartuttanut useita suosittuja npm-paketteja. Näiden joukossa on ollut lukuisia Zapier-, ENS Domains-, PostHog- ja Postman-julkaisijoiden paketteja. Uusia haittakoodin sisältäviä paketteja tunnistetaan jatkuvasti. [11] Suomessa haittaohjelmasta on tehty muutamia ilmoituksia.

Microsoft 365 tileihin kohdistuvien tietomurtojen kasvu taittui marraskuussa ja poistimme syyskuusta asti voimassa olleen vakavan varoituksen marraskuun lopussa. M365 tietomurtoilmoitusten määrä on toistaiseksi palannut elokuun tasolle, mutta ilmiöön liittyvä uhka ei ole poistunut.

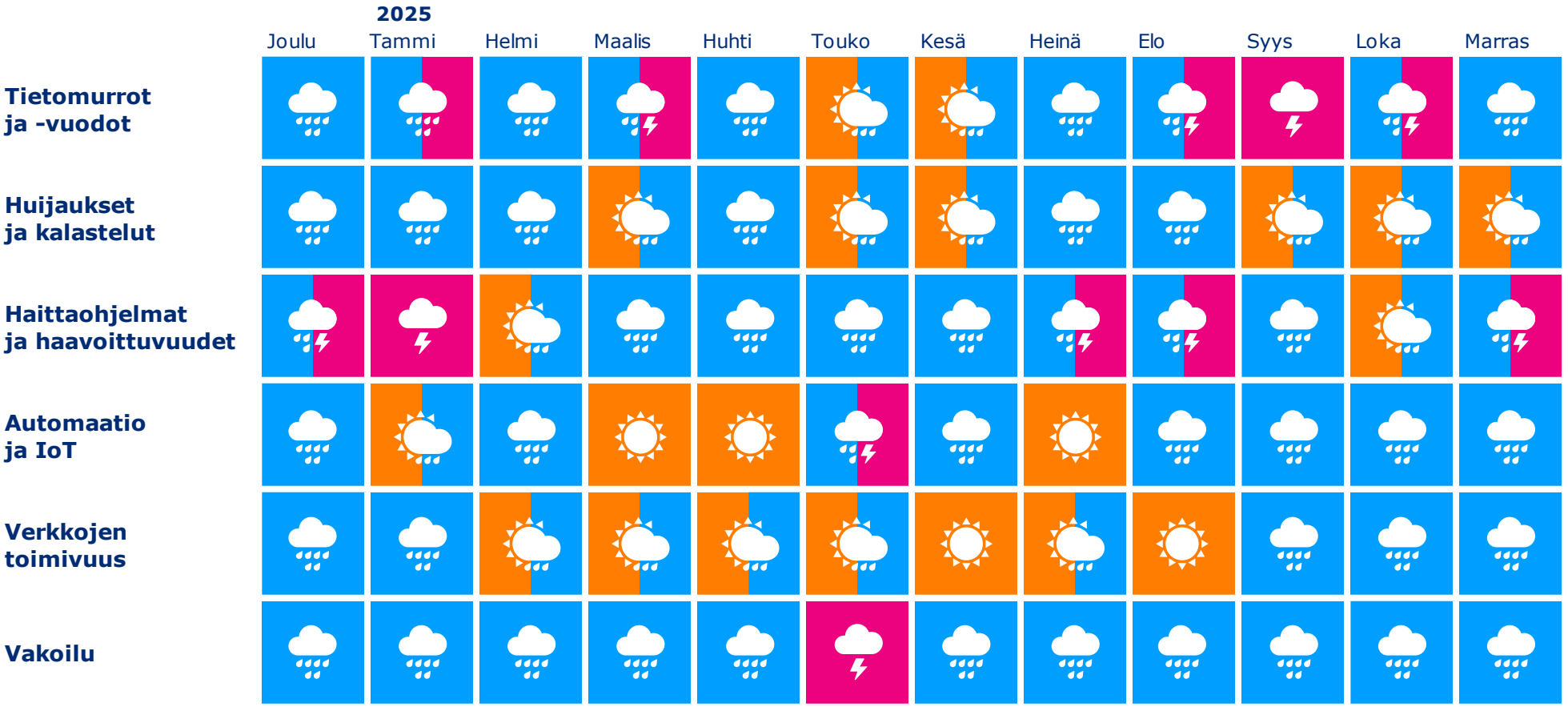
CloudFlaren palveluissa oli kansainvälinen häiriö 18.11., joka vaikutti useiden suosittujen palveluiden saatavuuteen. [12] Häiriö näkyi kohtalaisen laajasti internetin peruskäyttäjille, sillä se esti hetkellisesti esimerkiksi X:n ja ChatGPT:n käytön. [13]

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

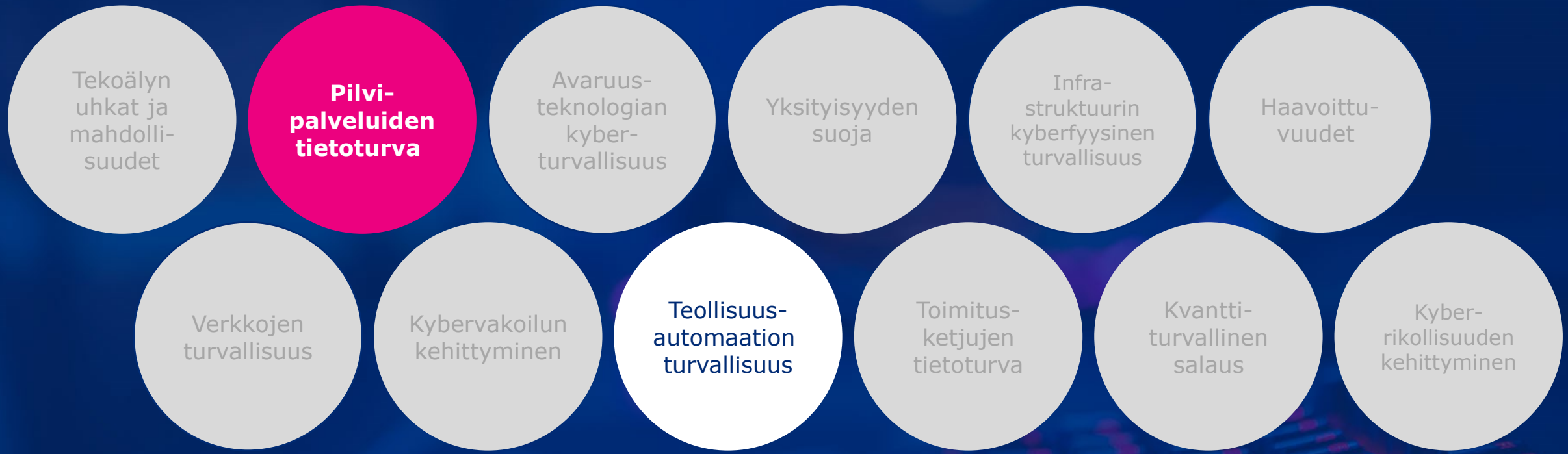
1 kk



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: Pilvipalveluiden tietoturva

Pilvipalvelut tarjoavat laajan valikoiman joustavia ja kustannustehokkaita ratkaisuja. Niitä tarjoaa tällä hetkellä kourallinen suuria yrityksiä, joiden laaja asiakaskunta ja resurssit edistävät tietoturvatoimien ja alustojen, sekä turvallisuuden ja tehokkuuden kehittymistä.

- Pilvipalvelujen hyötyjä ovat joustavuus, tietoturvan hyvä perustaso ja kustannussäästöt. Niiden käyttö edellyttää kuitenkin teknistä osaamista ja riittävää resursointia.

Pilvipalveluilla on myös omat turvallisuuteen liittyvät erityispiirteensä. Palveluihin kohdistuvat häiriöt tai kyberhyökkäykset saattavat estää palvelun käytön hyvinkin laajalla alueella, mikä luo uusia haasteita perinteisempiin paikallisesti toimiviin palveluihin nähden.

- Pilvipalveluiden käyttöönottoon on syytä varautua asianmukaisesti ja toimintaa kannattaa harjoitella etukäteen. Myös poikkeustilanteet ja toimintaympäristön muutokset tulee huomioida.

Datan sijaintiin liittyvät seikat muodostuvat myös huomioitavaksi asiaksi. Tallennetun tiedon fyysinen sijainti vaikuttaa olennaisesti siihen, minkä maan lainsäädäntöä tähän sovelletaan.

- Pilvipalveluita käytettäessä on syytä huomioida se, että datan tallennuspaikka ei välttämättä ole Suomessa. Ulkomailla sijaitseva data saattaa olla paikallisten viranomaisten toimivallan piirissä, joten palvelua valittaessa kannattaa suosia oikeusvaltioita, joissa yksityisyys ja tietosuoja on turvattu lainsäädännöllä.

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.

Euroopan komission Digital Omnibus -ehdotus

Euroopan komission Digital Omnibus - asetusehdotus ja sitä täydentävä AI Digital Omnibus - asetusehdotus (yhdessä ”Digital Omnibus”) julkaistiin 19.11.2025.

- Ehdotus sisältää useita keskeisiä muutosehdotuksia EU:n digitaalisen sääntelyn päivittämiseksi.
- Tavoitteena on yksinkertaistaa ja johdonmukaistaa EU:n digitaalista sääntelyä, pienentää sääntelystä aiheutuvia kustannuksia ja parantaa EU:n kilpailukykyä.
- Muutokset koskevat useaa eri sääntelyä, mm. tekoälyasetusta, data-asetusta, yleistä tietosuoja-asetusta sekä vaikuttaisi esim. poikkeamailmoitusvelvoitteisiin.
- Poikkeamailmoitukset keskitettäisiin EU:n kyberturvallisuusviraston (ENISA) ylläpitämään ilmoituskanavaan, jonka kautta ilmoitettaisiin jatkossa tietosuoja-asetuksen, NIS2-direktiivin, eIDAS-asetuksen, DORA-asetuksen, CER-direktiiviin ja sähköalan verkkosääntöön (NCCS) perustuvat ilmoitukset tietoturvaloukkauksista ja poikkeamista.
- Ehdotukset etenevät seuraavaksi Euroopan parlamentin ja Euroopan neuvoston eli jäsenmaiden käsittelyyn. Ehdotukset edellyttävät kummankin instituution hyväksyntää.

Hallituksen esitys kyberkestävyysasetuksen (CRA) toimeenpanoa koskevaksi lainsäädännöksi (HE 179/2025 vp)

Hallitus antoi eduskunnalle Euroopan unionin uuden kyberkestävyysasetuksen (Cyber Resilience Act, CRA) kansallista toimeenpanoa koskevan lakiesityksen 27.11.2025. [14]

- Esityksellä ehdotetaan säädettäväksi uusi laki eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista. Säännöksillä täydennetään asetuksen soveltamista.
- Asetuksen velvoitteet koskevat internetiin tai toisiin laitteisiin yhdistettävien laitteiden ja ohjelmistojen (esim. älykellot, pelit, televisiot, etähallintajärjestelmät) valmistajien velvollisuutta suunnitella ja varmistaa tuotteet kyberturvallisuusvaatimusten mukaisesti.
- Tuotteiden vaatimuksenmukaisuutta arvioivat laitokset voisivat hakea Traficomilta ilmoittamista kyberkestävyysasetuksen mukaisiin arviointitehtäviin.
- Myös markkinavalvontaa koskevat viranomaistehtävät keskitettäisiin Traficomiin.
- Ehdotetut lait on tarkoitettu tulemaan voimaan pääosin 1.6.2026.
- Kyberkestävyysasetuksen soveltaminen alkaa siirtymäajan jälkeen 11.12.2027. Aktiivisesti hyödynnettyjen haavoittuvuuksien ilmoittamista sovelletaan kuitenkin jo 11.9.2026 alkaen ja ilmoitettuja laitoksia koskevaa sääntelyä 11.6.2026 alkaen.

Julkaistuja täytäntöönpanoasetuksia

CRA täytäntöönpanoasetus (EU) 2025/2392

- EU:n kyberkestävyyssäädöksen eli CRA:n täytäntöönpanoasetus (EU) 2025/2392 tärkeiden ja kriittisten tuotteiden teknisistä kuvauksista on julkaistu. [15]
- Digitaalisia elementtejä sisältävien tuotteiden valmistajien on ilmoitettava viranomaisille kaikista aktiivisesti hyödynnetyistä haavoittuvuuksista tai tietoturvallisuuteen vaikuttavista poikkeamista.

eIDAS-asetus (EU) 910/2014 Luottamuspalveluja koskevat täytäntöönpanoasetukset

- 2025/2160 Soveltamissäännöt ei-hyväksyttyjen luottamuspalvelujen tarjoamiseen kohdistuvien riskien hallintaa koskevien viitestandardien, eritelmien ja menettelyjen osalta [16]
- 2025/2162 Arviointilaitoksia ja arviointiraporttia koskevia tarkennuksia [17]
- 2025/2164 Trusted listin tekniset määräykset koskien käyttöä ja toteutusta [18]

Päivitetty määräys valmiussuunnittelun järjestämisestä liikennejärjestelmässä

Liikenne- ja viestintävirasto on päivittänyt valmiussuunnittelun järjestämistä liikennejärjestelmässä koskevan määräyksen. [19]

- Määräys on keskeinen osa virastossa tehtävää työtä liittyen liikennejärjestelmän turvallisuuteen ja toimintavarmuuteen.
- Määräykseen on lisätty liikennemuotokohtaiset erityismääräykset ilmailua koskien. Raideliikennettä koskevia erityismääräyksiä on päivitetty ja useita määräyskohtia on osoitettu aiempaa laajemmalle joukolle raideliikenteen toimijoita. Lisäksi määräyksen yleisiä osia on päivitetty.
- Uusi määräys kumoaa vanhan määräyksen ja tuli voimaan keskiviikkona 26.11.2025. Toimijoilla on neljän kuukauden siirtymäaika nykyisen valmiussuunnitelmansa päivittämiselle.

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) Dutch police seizes 250 servers used by “bulletproof hosting” service https://www.bleepingcomputer.com/news/security/dutch-police-seizes-250-servers-used-by-bulletproof-hosting-service/
2) Data breach at major Swedish software supplier impacts 1.5 million https://www.bleepingcomputer.com/news/security/data-breach-at-major-swedish-software-supplier-impacts-15-million/
3) Integritetsskyddsmyndigheten inleder granskning efter Miljödata-läckan https://www.svt.se/nyheter/inrikes/integritetsmyndigheten-inleder-granskning-efter-miljodata-lackan
4) Meta is earning a fortune on a deluge of fraudulent ads, documents show https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/
5) Somejätti laskee tienaavansa miljardeja huijausmainoksilla, Reutersin näkemät asiakirjat paljastavat https://yle.fi/a/74-20193060?origin=rss
6) OWASP Highlights Supply Chain Risks in New Top 10 List https://www.darkreading.com/application-security/owasp-highlights-supply-chain-risks-new-top-10
7) The Ten Most Critical Web Application Security Risks https://owasp.org/Top10/2025/0x00_2025-Introduction/
8) Näkymätön varas verkkokaupassasi - Digitaalisella skimmauksella voi olla merkittäviä taloudellisia vaikutuksia https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/nakymaton-varas-verkkokaupassasi-digitaalisella-skimmauksella-voi-olla-merkittavia
9) Pilvipalveluiden pääkäyttäjätunnusten hallinta – parhaat käytännöt https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/pilvipalveluiden-paakayttajatunnusten-hallinta-parhaat-kaytannot
10) Haittaohjelma voidaan aktivoida huomaamatta ClickFix-tekniikan avulla - Tutustu ilmiöön ja suojaudu https://kyberturvallisuuskeskus.fi/fi/ajankohtaista/haittaohjelma-voidaan-aktivoida-huomaamatta-clickfix-tekniikan-avulla-tutustu-ilmioon
11) Shai-Hulud-hyökkäyksen toinen aalto - toimenpidesuositukset organisaatioille https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/shai-hulud-hyokkayksen-toinen-aalto-toimenpidesuositukset-organisaatioille
12) Cloudflare outage on November 18, 2025 https://blog.cloudflare.com/18-november-2025-outage/
13) Cloudflare apologises for outage which took down X and ChatGPT https://www.bbc.com/news/articles/c629pny4gl7o
14) HE 179/2025 Hallituksen esitys eduskunnalle kyberkestävyysasetuksen toimeenpanoa koskevaksi lainsäädännöksi https://www.finlex.fi/fi/hallituksen-esitykset/2025/179
15) Document 32025R2392 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R2392&qid=1764577062755
16) Komission täytäntöönpanoasetus (EU) 2025/2160 https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L_202502160
17) Komission täytäntöönpanoasetus (EU) 2025/2162 https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L_202502162
18) Komission täytäntöönpanoasetus (EU) 2025/2164 https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L_202502164
19) Valmiussuunnittelun järjestäminen liikennejärjestelmässä https://www.finlex.fi/fi/viranomaiset/maarayskokoelmat/traficom-rautatieliikenne/2025/51222