TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Heinäkuu 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

Julkaisimme heinäkuussa neljä haavoittuvuustiedotetta.[1] Vakavien haavoittuvuuksien määrä on tänä vuonna ollut nousussa. Syy on erityisesti tekoälypohjainen haavoittuvuuksien metsästys.

Suomen tiedusteluviranomaiset julkaisivat heinäkuussa kansainvälisten kumppaneiden kanssa kaksi varoitusta Venäjän aktiivisesta kybertoiminnasta länsimaita, ml. Suomea kohtaan.[2, 3]

Kybersään yleistilanne heinäkuussa 2026

Heinäkuun kybersäässä raportoitiin kesäsateita

Keskikesällä Kyberturvallisuuskeskukselle ilmoitettiin vähemmän tietoturvapoikkeamia kuin tavallisena kuukautena, mutta ilmoitusten määrä on jälleen kääntynyt nousuun. Tämä on aiemmilta vuosilta tuttua kesien säätrendien mukaista, kun lomakausi vaikuttaa ilmoitusaktiivisuuteen.

Tummia pilviä heinäkuiselle kybertaivaalle toivat kuitenkin kiristyshaittaohjelmahyökkäykset, joita toteutettiin Suomessa kourallinen. Alkuvuonna kiristyshaittaohjelmien osalta oli kohtuullisen poutaista, mutta ilmojen lämmetessä kyberrikolliset aktivoituivat.

Tämän vuoden trendejä mukaillen julkaistiin heinäkuussa jälleen useita haavoittuvuuksia. Kyberturvallisuuskeskuksen haavoittuvuustiedotteisiin näistä nostettiin neljä. Keskeinen syy haavoittuvuuksien määrien huomattavalle lisääntymiselle on tekoälypohjainen haavoittuvuuksien etsiminen.

M365-tietomurrot ovat jo vuosia liikkuneet aalloissa. Kesällä tilanne on ollut rauhallisempi, mutta syksyä kohti on odotettavissa jälleen tilimurtokampanjoiden aktivoitumista.

Tekoälyjärjestelmien kehittyvät kyvykkyydet ja niihin ja niiden käyttöön liittyvä potentiaalinen uhka oli pinnalla myös heinäkuussa. Samalla on hyvä muistaa, että generatiivinen tekoäly tarjoaa merkittäviä mahdollisuuksia myös puolustajille.[4]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Muistutimme heikosti suojattujen verkkolaitteiden riskistä. Puutteellisesti suojattu tai valvottu verkkolaite voi mahdollistaa suoran väylän organisaation sisäverkkoon ja kriittisiin järjestelmiin. Verkkolaitteiden suojaamiseksi on tärkeää kohdistaa riittävästi resursseja, ja niihin liittyviä poikkeamatilanteita on syytä harjoitella.[5]

WhatsApp-pikaviestisovelluksessa otettiin käyttöön käyttäjätunnukset, mikä voi mahdollistaa ja lisätä uskottavia huijauksia. Organisaatioiden kannattaa harkita virallisten käyttäjätunnustensa varaamista mahdollisimman varhaisessa vaiheessa.[6]

ClickFix-menetelmällä levitettyjen haittaohjelmatapausten määrät ovat jälleen olleet kasvussa heinäkuussa. ClickFix-hyökkäystekniikan vaikutuksia voi estää ja rajata organisaatioiden teknisillä toimenpiteillä, joista olemme kertoneet viime vuonna.[7]

Kuukauden raekuuro
Viranomaiset varoittivat Venäjän kyberuhkasta

Heinäkuussa Suomen tiedustelupalvelut ja useat kansainväliset viranomaiset julkaisivat kaksi yhteistä varoitusta Venäjän valtiollisesta kybervakoilusta länsimaita kohtaan.

Heikosti suojatut verkkolaitteet jälleen kohteena

Suojelupoliisi ja sotilastiedustelu yhdessä kansainvälisten kumppaneiden kanssa varoittivat Venäjän turvallisuuspalvelu FSB:hen yhdistetyn kyberuhkatoimijan toiminnasta heikosti suojattuja reitittimiä ja muita verkkolaitteita kohtaan. FSB:n pitkäaikaisen kybertoiminnan kohteena on etenkin kriittinen infrastruktuuri.[8]

Varoituksessa nostettu uhka kohdistuu ensisijaisesti yritystason verkkolaitteisiin. Yhdysvaltojen NSA jakoi varoituksen teknisen ohjeistuksen.[9]

Sähköpostijärjestelmät uhkatoimijan tähtäimessä

Kansainväliset viranomaiset ja Suomen tiedustelupalvelut varoittivat myös venäläisestä valtiojohtoisesta kyberuhkatoimijasta. Laundry Bear -toimija on murtautunut pääsääntöisesti sähköpostijärjestelmiin. Toimija muodostaa uhkan etenkin kriittisen infrastruktuurin, puolustusteollisuuden ja julkishallinnon organisaatioille, myös Suomessa.

Laundry Bear -uhkatoimija on murtautunut ja kohdistanut toimintaa useisiin länsimaisiin toimijoihin valtionhallinnossa ja yksityisellä sektorilla.

Laundry Bear on hyödyntänyt muun muassa Zimbra Collaboration Suite -ohjelmiston nollapäivähaavoittuvuutta, johon julkaistiin korjaus marraskuussa 2025. Hyväksikäyttökampanja jatkuu kuitenkin edelleen.[10, 11]

Kybersään ilmiöt

Osiossa käymme läpi kyberturvallisuuden ilmiöiden kehitystä ja trendejä.

Kybersää
heinäkuu 2026

1 kk

Tietomurrot- ja vuodot

WordPress-tietomurtoja on ilmoitettu paljon Kyberturvallisuuskeskukselle. Kiristyshaittaohjelmailmoitusten määrä on kasvanut alkuvuoteen nähden.

M365-tietomurtojen määrä on lomakaudella vähentynyt merkittävästi.

Haittaohjelmat

Heinäkuun aikana on havaittu haittaohjelman levittämistä erityisesti ClickFix-tekniikkaa käyttäen tavanomaista enemmän. WordPress-tietomurrot ovat altistaneet verkkosivuja tällaiselle haittaohjelman levitykselle.

Haavoittuvuudet

Haavoittuvuuksia on löydetty edelleen kiihtyvällä tahdilla. Heinäkuussa ylitettiin 40 000 CVE-tunnisteen raja vuodelle 2026, kun koko vuonna 2025 CVE-tunnisteita annettiin hieman yli 45 000.

Huijaukset ja kalastelut

Johtajahuijauksilla on heinäkuussa yritetty petoksia lomakauden sijaisina toimineita työntekijöitä kohtaan.

Havainnot viittaavat kasvaneeseen AI-työkalujen käyttöön huijausten toteutuksessa.

Automaatio ja IoT

Useiden yhdysvaltalaisten vesilaitosten automaatiojärjestelmiä vastaan on hyökätty. Järjestelmät ovat olleet heikosti suojattuja tai suojaus on puuttunut kokonaan. Järjestelmien omistajien tulee parantaa suojausta yhdessä järjestelmien toimittajien kanssa.

Verkkojen toimivuus

Suomalaisiin organisaatioihin on kohdistunut muutamia palvelunesto-hyökkäyksiä, mutta näiden vaikutukset saatavuuteen olivat vähäisiä.

Kybersää
heinäkuu 2026 1/2

1 kk

Tietomurrot ja -vuodot

- Heinäkuussa havaittiin runsaasti WordPress-sivustoihin kohdistuneita tietomurtoja, joita on käytetty ClickFix-tekniikkaa hyödyntävien haittaohjelmien levittämiseen.
- Kiristyshaittaohjelmailmoitusten määrä on kasvanut alkuvuoteen verrattuna. Useissa tapauksissa organisaatioiden tietoja on vuotanut tai niiden julkaisemisella on uhattu.
- M365-tietomurtojen määrä on vähentynyt lomakauden aikana merkittävästi. Tapausmäärien odotetaan jälleen kasvavan merkittävästi lomakauden päättyessä.

Haittaohjelmat

- Ilmoitukset ClickFix-tekniikalla levitettävistä haittaohjelmista ovat olleet heinäkuun aikana kasvussa. ClickFix-tekniikalla levitetään haittaohjelmia erityisesti murrettujen verkkosivujen kautta.
- WordPress-verkkoalustaan tehtyjen tietomurtojen kasvanut määrä näkyy myös haittaohjelmien levityksessä, kun murrettuja verkkosivuja on hyödynnetty haitallisen koodin tai ohjelmien levittämisessä.
- Kuukauden aikana erilaisista haittaohjelmahavainnoista on ilmoitettu Kyberturvallisuus-keskukselle, mutta havainnot eivät ole viitanneet suurempiin haittaohjelmailmiöihin.

Haavoittuvuudet

- WordPress-tuotteessa paljastui haavoittuvuuksia (wp2shell), joiden ketjuttaminen mahdollistaa etäkoodin suorittamisen ilman tunnistautumista. Haavoittuvuuksien hyväksikäyttöä on havaittu myös Suomessa (CVE-2026-63030, CVE-2026-60137).[12]
- Linux Kernelin versioista 6.0-7.1. julkaistiin haavoittuvuus, joka mahdollistaa oikeuksien korotuksen paikalliselle käyttäjälle (CVE-2026-53362).[13]
- Kriittinen haavoittuvuus julkaistiin NGINX-tuotteissa. Haavoittuvuus mahdollistaa käyttöoikeudettoman hyökkääjän etäkoodin suorituksen (CVE-2026-42533).[14]

Kybersää
heinäkuu 2026 2/2

1 kk

Huijaukset ja kalastelut

- Rikolliset ovat huijanneet aktiivisesti esiintyen eri organisaatioiden johtajina. Johtajahuijauksilla on heinäkuussa yritetty petoksia lomakauden sijaisina toimineita työntekijöitä kohtaan.
- Havainnot viittaavat kasvaneeseen AI-työkalujen käyttöön huijausten toteutuksessa.
- Tekoälyvälineillä on rakennettu myös poliisin nimiin väärennettyjä huijausvideoita, joita on kohdistettu Suomessa asuviin ulkomaalaistaustaisiin henkilöihin. Huijausvideopuheluihin on käytetty pikaviestipalveluita, kuten WhatsApp ja Google Meet.

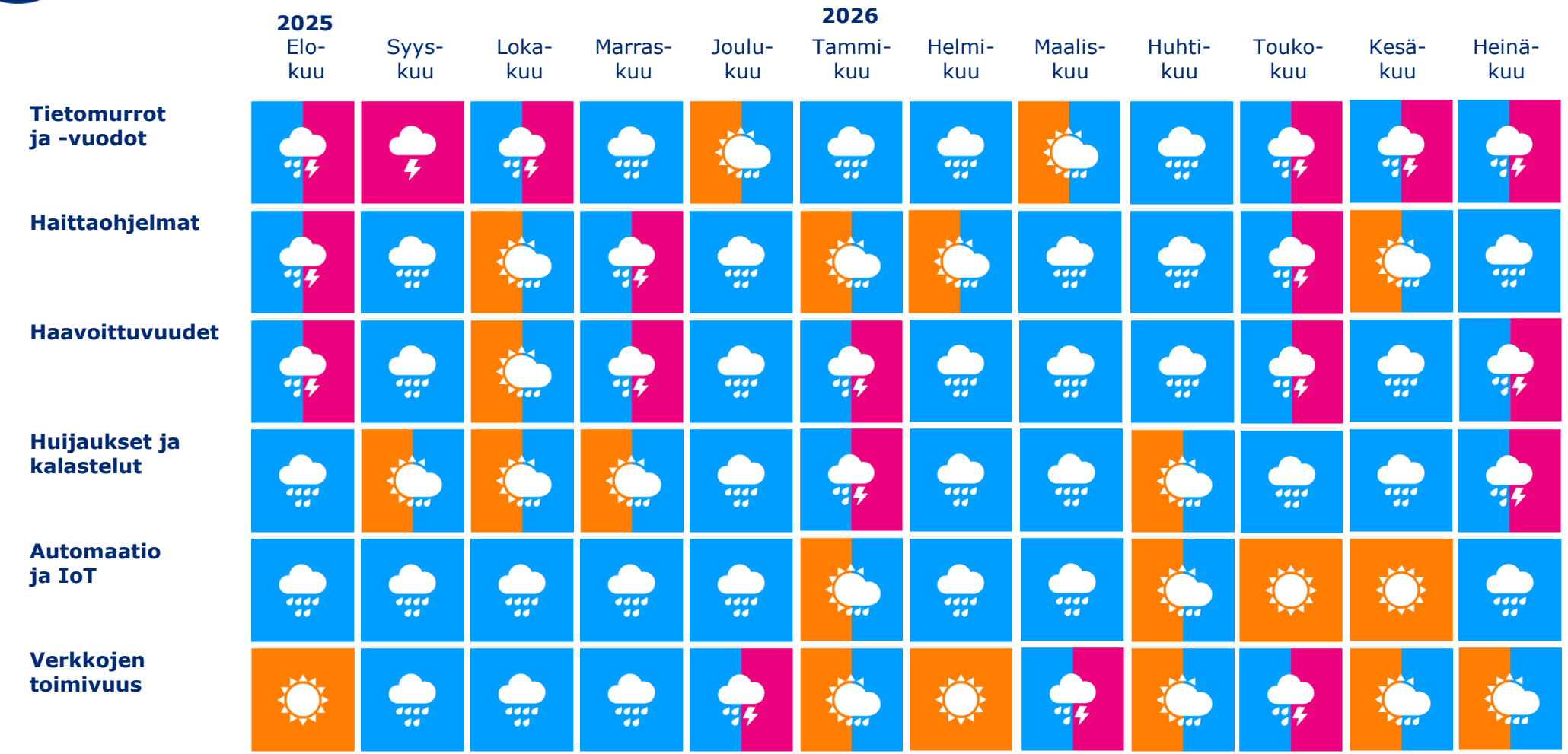
Automaatio ja IoT

- Useiden yhdysvaltalaisten vesilaitosten automaatiojärjestelmiä vastaan on hyökätty heinäkuun lopulta lähtien. Hyökkäykset ovat johtaneet maltillisen mittaisiin käyttökatkoihin. Tapauksissa järjestelmät ovat olleet heikosti suojattuja tai suojaus on puuttunut kokonaan.[15, 16]
- Hyökkääminen on teknisesti helppoa. Hyökkäyksen toteutuminen riippuu vain hyökkääjän motivaatiosta.
- Suomessakin monet automaatio-järjestelmät ovat suojattomia.
- Automaatiojärjestelmien omistajien tulee parantaa suojausta yhdessä järjestelmien toimittajien kanssa.

Verkkojen toimivuus

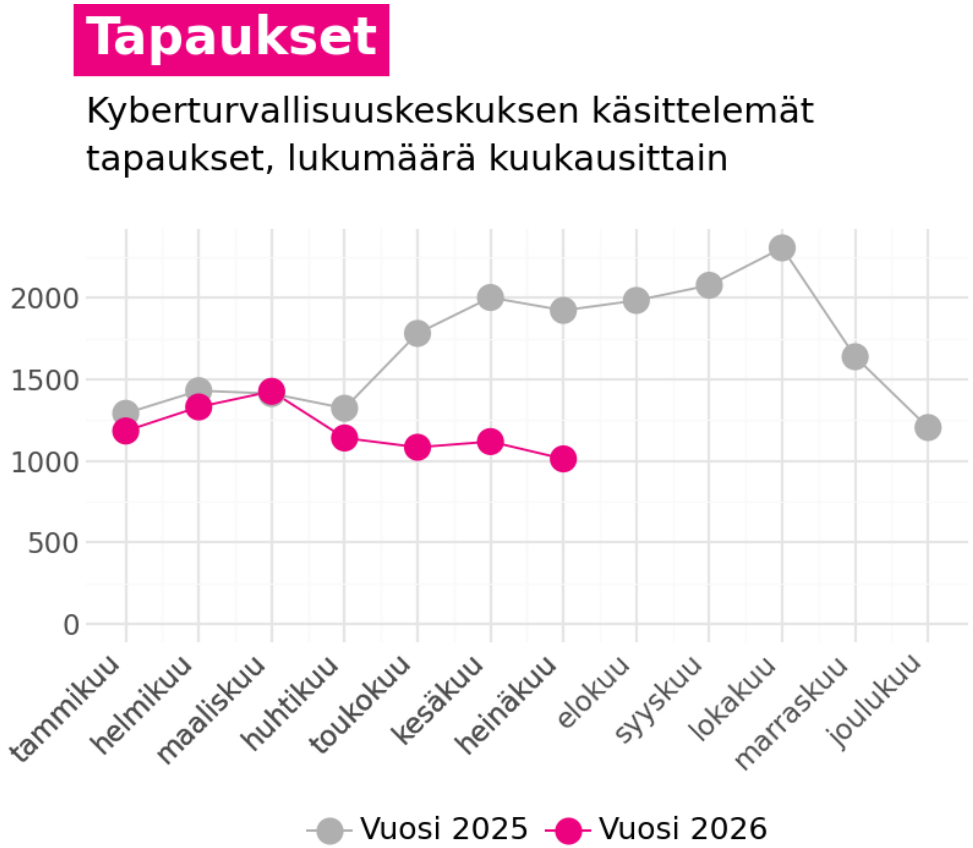
- Heinäkuussa julkaistussa raportissa tunnistettiin uusi palvelunesto-hyökkäystapa CDN-palveluita vastaan hyödyntämällä HTTP/3- ja HTTP/1.1-protokollien välistä muunnosta liikenteen moninkertaistamiseen.[17]
- Palvelunestohyökkäyksiä saatetaan käyttää hämäyksenä osana laajempia kyberoperaatioita.

Kybersään ilmiöt
kulunut 12 kk



Tapaukset

- Kyberturvallisuuskeskus käsitteli heinäkuussa 1012 tapausta.
- Ilmoitusten määrä on 12 kuukauden keskiarvoon nähden huomattavasti pienempi, sillä keskiarvo on noin 1458 tapausta kuukaudessa. Kyberturvallisuuskeskukselle ilmoitetaan kesäkaudella yleisesti vähemmän tapauksia.
- Vaikka ilmoitettujen tapausten määrä on ollut heinäkuun aikana tavanomaista vähäisempi, on osalla tapauksia ollut merkittäviä vaikutuksia. Kiristyshaittaohjelma-hyökkäyksiä on ilmoitettu Kyberturvallisuuskeskukselle alkuvuoteen verrattuna enemmän.
- Kuukauden aikana on noussut ilmi useita vakavia haavoittuvuuksia, kuten WordPress-verkkoalustaan kohdistuneet haavoittuvuudet, joita on aktiivisesti hyväksikäytetty useissa tietomurroissa.



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

M365-laitekoodikalastelun avulla tehtyjen M365-tilien tietomurtojen määrän odotetaan kasvavan voimakkaasti loppukesällä ja alkusyksystä. Organisaatioiden on syytä varautua tilanteeseen ja estää laitekoodikirjautuminen käyttäjiltä erillisellä Device Code Flow -pääsynhallintapolitiikalla (CA policy) sekä monitoroida käyttäjiä, jotka palvelua tarvitsevat.[18]

Kehittyviin tekoälyjärjestelmiin liittyvä keskustelu kyberturvallisuudesta tulee pysymään pinnalla myös syksyllä.

Organisaation varautuminen

- Haavoittuvuuksien määrän kasvun ja nollapäivähaavoittuvuuksien nopean hyväksikäytön vuoksi on haavoittuvuuksien tilannetta syytä seurata organisaatioissa aktiivisesti. Huomiota tulee kiinnittää etenkin päivitysprosesseihin.
- Verkon reunalaitteiden suojaaminen on keskeinen osa organisaation kybervarautumista. Riskien hallinta edellyttää ennakoivaa päivityshallintaa, turvallisia konfiguraatioita, monivaiheista tunnistautumista ja poikkeamien tehokasta valvontaa.[19]

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) vaatimukset selkiytyvät

- Euroopan komissio on 27.7. julkaissut käytännönläheisen ohjeistuksen CRA-säädöksen soveltamisen tueksi.[20, 21]
- Ohjeistus on suunnattu erityisesti valmistajille, ohjelmistokehittäjille sekä muille yrityksille, jotka saattavat markkinoille digitaalisia tuotteita.
- Ohjeistus selventää tuotteiden soveltamisalaa, toimitusketjujen vastuita ja kyberturvallisuus-vaatimuksia koko tuotteen elinkaaren ajalle.
- Yritykset voivat hyödyntää ohjetta vaatimustenmukaisuuden suunnittelussa sekä tunnistaa kehitystarpeita esimerkiksi riskienhallinnassa ja haavoittuvuuksien hallinnassa.
- Komission ohjeistus ei ole oikeudellisesti sitova, mutta se tarjoaa erityisesti pk-yrityksille tukea vaatimustenmukaisuuden suunnitteluun.
- **Kyberkestävyyssäädöksen ensimmäiset velvoitteet, jotka koskevat haavoittuvuuksien ja tietoturva-poikkeamien raportointia, tulevat voimaan 11. syyskuuta 2026.**[22]
- Säädöksen keskeiset kyberturvallisuus-vaatimukset alkavat koskea valmistajia 11. joulukuuta 2027.

Oikeudelliset asiat
EU:n kyberturvallisuutta ja tekoälyä koskeva toimintasuunnitelma

- Euroopan komissio on 7.7.2026 esitellyt toimintasuunnitelman kyberturvallisuuteen ja tekoälyn käyttöön liittyen.[23]
- Toimintasuunnitelmalla pyritään luomaan yhtenäinen lähestymistapa kehittyneimpien tekoälymallien turvalliseen käyttöönottoon, tekoälyn hyödyntämiseen kyberturvallisuudessa sekä vastaamaan tekoälyä koskeviin kyberturvallisuusriskeihin.
- Organisaatioita kannustetaan mm. käyttämään tekoälyä ja avoimen lähdekoodin tekoälymalleja haavoittuvuuksien tehokkaampaan hallintaan ja kyberhyökkäyksien torjumiseen.
- Toimintasuunnitelma täydentää EU:n olemassa olevaa sääntelykehikkoa tekoälyyn ja kyberturvallisuuteen liittyen.
  - Sääntelykehikkoon kuuluvat tekoälyasetus, kyberkestävyyssäädös (CRA), NIS2-direktiivi, DORA-asetus ja kybersolidaarisuussäädös.
- Toimintasuunnitelmalla pyritään myös EU:n omien tekoälykyvykkyyksien kehittämiseen.

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: 029 534 5000 (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/haavoittuvuudet
2. https://supo.fi/-/suojelupoliisi-ja-sotilastiedustelu-varoittavat-yrityksia-venajan-fsb-n-verkkovakoilusta
3. https://supo.fi/-/suojelupoliisi-ja-sotilastiedustelu-varoittavat-yrityksia-venalaisesta-laundry-bear-kyberuhkatoimijasta
4. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/mita-tekoalyn-tekemiksi-kutsutut-tietomurrot-oikeastaan-kertovat
5. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/heikosti-suojatut-verkkolaitteet-avaavat-vaylan-kyberhyokkayksille
6. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/whatsapp-ottaa-kayttoon-kayttajatunnukset-kayttajien-kannattaa-varautua-uusiin-huijausyrityksiin
7. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/haittaohjelma-voidaan-aktivoida-huomaamatta-clickfix-tekniikan-avulla-tutustu-ilmioon-ja-suojaudu
8. https://supo.fi/-/suojelupoliisi-ja-sotilastiedustelu-varoittavat-yrityksia-venajan-fsb-n-verkkovakoilusta
9. https://media.defense.gov/2026/Jul/09/2003959498/-1/-1/0/CSA_IMPROVE_ROUTER_HYGIENE.PDF
10. https://supo.fi/-/suojelupoliisi-ja-sotilastiedustelu-varoittavat-yrityksia-venalaisesta-laundry-bear-kyberuhkatoimijasta
11. https://media.defense.gov/2026/Jul/22/2003965244/-1/-1/0/CSA_RUSSIA_PHISHING_TARGET_ZIMBRA.PDF

Lähdeluettelo
2/2

12. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-18
13. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-17
14. https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet/haavoittuvuus-2026-19
15. https://www.cbsnews.com/minnesota/news/cyberattack-malware-braham-water-plant-outage/
16. https://therecord.media/iran-cyberattacks-water-treatment
17. https://arxiv.org/abs/2607.26589
18. https://kyberturvallisuuskeskus.fi/fi/uutiset/uusi-aalto-m365-tietojenkalastelussa-ai-avusteinen-laitekoodin-kalastelukampanja
19. https://www.kyberturvallisuuskeskus.fi/fi/uutiset/heikosti-suojatut-verkkolaitteet-avaavat-vaylan-kyberhyokkayksille
20. https://kyberturvallisuuskeskus.fi/fi/uutiset/kyberkestavyyssaadoksen-vaatimukset-selkiytyvat-eu-komissio-julkaisi-uuden-soveltamisohjeen
21. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation
22. https://kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/kyberkestavyyssaados-cyber-resilience-act-cra
23. https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence