



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Syyskuu 2024

#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



Traficomin Kyberturvallisuuskeskuksen kansallinen Hyökkäyspintakartoituspalvelu (Hyöky) täytti syyskuussa vuoden! Palvelu on suunnattu kunnille ja julkisen hallinnon organisaatioille, mutta sen tilausmahdollisuutta ollaan laajentamassa huoltovarmuuskriittisiin organisaatioihin. [\[1, 14\]](#)



Suomi sai kansainvälisen televiestintäliitto ITU:n koostamassa globaalissa kyberturvallisuusindeksissä täydet pisteet, sijoittuen vertailussa tasolle 1. [\[2\]](#)



Liikenne- ja viestintävirasto Traficom on myöntänyt ensimmäisen salaustuotehyväksynnän Naton turvallisuusluokitellun tiedon suojaamiseksi Insta SafeLink -salaustuoteratkaisulle. [\[3\]](#)

Kybersää syyskuu 2024

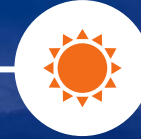
Tietomurrot ja -vuodot

- ▶ Tietomurtojen ilmoitettu määrä on jatkanut rauhallisella tasolla.
- ▶ Dropbox-teemainen M365-kalastelu ja siitä johtuneet tietomurrot ovat suurin yksittäinen kategoria.
- ▶ Viime vuoteen nähden kiristyshaittaohjelmahyökkäysten määrä on jäänyt matalammaksi.



Huijaukset ja kalastelut

- ▶ Traficomissa tehdyt tekstiviestihuijaukset alkoivat vähentyä, kun SMS sender ID:n rekisteröinti astui voimaan syyskuun lopulla.
- ▶ PRH:n nimiin väärennetyt huijaukset johtivat suomi.fi-tunnistautumisen näköiselle kalastelusivulle.



Haittaohjelmat ja haavoittuvuudet

- ▶ Lumma Stealer -haittaohjelmaa on levitetty uudella tavalla elokuusta lähtien.
- ▶ Red Hat OpenShiftistä on löydetty kaksi kriittistä haavoittuvuutta.
- ▶ CUPS-tulostusjärjestelmän haavoittuvuudet mahdollistavat mielivaltaisen koodin suorittamisen.



Automaatio ja IoT

- ▶ Rikolliset käyttävät paljon hyväkseen etäkäyttöohjelmistoja [\[4\]](#), joita teollisuusautomaation käyttäjät ovat asentaneet järjestelmiinsä.
- ▶ Tietoturvyhtiö Claroty mukaan 55 %:ssa internetiin kytketyistä teollisuusautomaatioympäristöistä on vähintään neljä eri etäkäyttöohjelmistoa [\[5\]](#).



Verkojen toimivuus

- ▶ Syyskuussa yleisissä viestintäverkoissa havaittiin kaksi toimivuushäiriötä.
- ▶ Kotimaiset organisaatiot ilmoittivat palvelunestohyökkäyksistä aiempaa vuotta aktiivisemmin.
- ▶ Finanssialalla ilmeni häiriöitä, jotka saivat näkyvyyttä myös mediassa. Nordea kertoi häiriöiden johtuneen osittain palvelunestohyökkäyksistä [\[6\]](#).



Vakoilu

- ▶ Yhdysvaltojen viranomaiset suorittivat alasajo-operaation laajalle Kiinaan yhdistetylle bottiverkolle. [\[7\]](#)
- ▶ APT-toimijat hyödyntävät bottiverkkoja mm. pahantahtoisen verkkoliikenteen alkuperän hämärtämiseen tai havaitsemisen hankaloittamiseen.



Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen



NIS2-direktiivin myötä organisaatioille tulee velvoite ilmoittaa merkittävistä tietoturvapoikkeamista valvovalle viranomaiselle. Julkaisimme artikkelin, jossa kerromme vinkkejä poikkeamanhallinnan prosessien kehittämiseksi organisaatioissa. [\[8\]](#)



Organisaatioiden tulee edelleen varautua eri tavoin palvelunestohyökkäyksiin. Haktivistien sovellustason palvelunestohyökkäykset ja nyt uutena aaltona ilmennyt *carpet bombing* -tekniikka ovat hyviä esimerkkejä hyökkääjien pyrkimyksistä kehittää menetelmiään jatkuvasti.



Toimintaympäristön jatkuva muutos asettaa odotuksia ja vaatimuksia niin organisaatioiden kuin laajemmin yhteiskunnan varautumiselle. Säännöllisen harjoitustoiminnan avulla voidaan parantaa yhteiskunnan kyberresilienssiä ja toimintavarmuutta. Kyberturvallisuuskeskus osallistuu vuosittain lukuisiin harjoituksiin ja tukee huoltovarmuuskriittisten organisaatioiden kyberharjoittelua viranomaispalveluna. [\[9\]](#)

Syyskuun kyberturvallisuuden yleiskuva

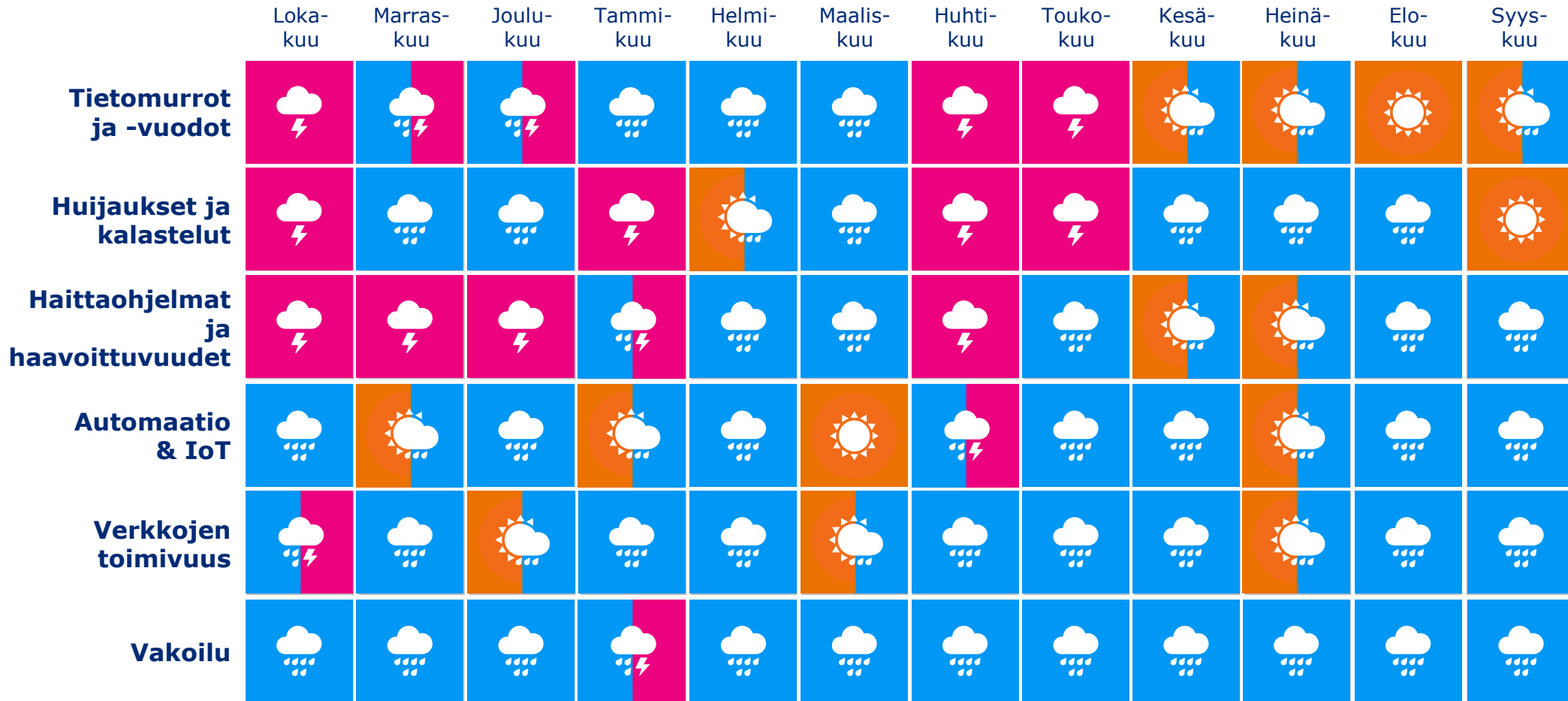
- ▶ Syyskuussa kyberturvallisuuden tapausrintamalla nähtiin lievää määrällistä kasvua rauhallisten kesäkuukausien jälkeen.
- ▶ Muutoin melko kirrkaassa syysässä on esiintynyt usvaa suomalaisiin organisaatioihin viime aikoina kohdistuneiden palvelunestohyökkäysten sekä erilaisten tietojenkalastelu- ja huijauskampanjoiden vuoksi.
 - ▶ Alkusyksystä Kyberturvallisuuskeskukselle on ilmoitettu aiempaakin aktiivisemmin palvelunestohyökkäyksistä. Muun muassa Nordea on kertonut lähiaikoina esiintyneiden häiriöiden johtuneen osittain palvelunestohyökkäyksistä. Toistaiseksi vaikutukset ovat muissa tapauksissa jääneet vähäisiksi. [\[10, 11\]](#)
 - ▶ Etenkin Dropbox-teemainen M365-tunnusten kalastelu on ollut alkusyksystä aktiivista. Kyberturvallisuuskeskukselle on raportoitu lukuisista M365-tilien tietomurroista Dropbox-kalastelujen seurauksena. [\[12\]](#)
 - ▶ Traficom in nimissä tehdyt tekstiviestihuijaukset näkyvät poliisin valtakunnallisessa petosrikosten tilannekuvassa. Poliisin mukaan pelkästään syyskuussa huijaustapausten yhteenlaskettu rikoshyöty oli yli 560 000 euroa. Sama ilmiö on näkynyt tilannekuvassa jo aiemmin kesällä, mutta syksyllä ilmiössä on nähty poliisin mukaan kasvua. [\[13\]](#)
- ▶ Lisäksi havaitsimme tavanomaista enemmän kahden eri bottiverkon toimintaa Suomessa.
 - ▶ Uudehko Quad7-bottiverkko ottaa haltuunsa varsinkin Asus ja TP-Link merkkisiä kotikäyttöön tarkoitettuja reitittämiä. Havaintoja on tehty myös jo useita vuosia toimineesta Mirai-bottiverkosta. [\[14\]](#)

Ilmiöiden ja toimialojen trendit

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



Kyberturvallisuuden trendit kulunut 12 kk

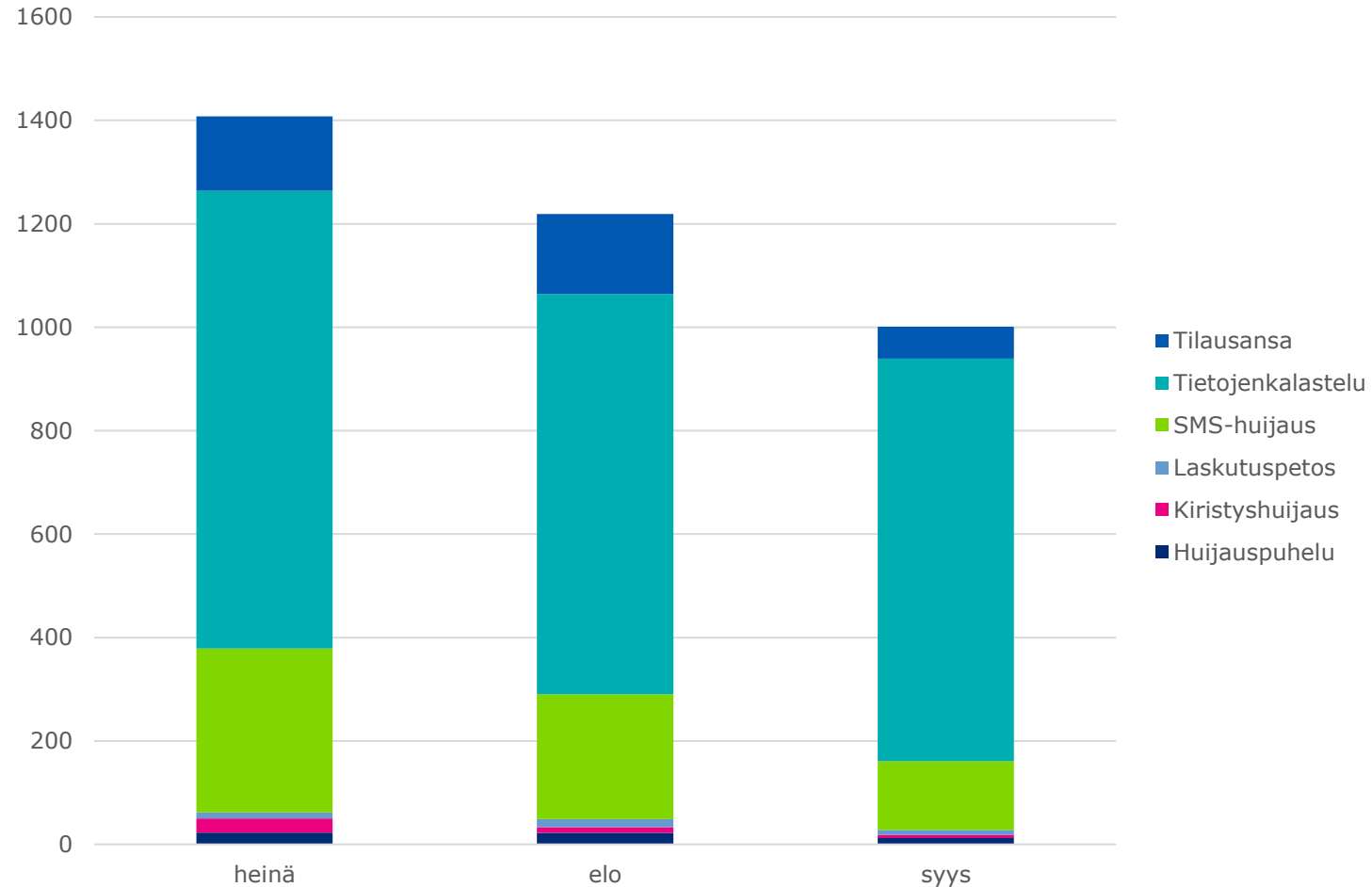




Käsiteltyjä huijaustapauksia Q3/2024

Vuoden 2024 kolmannen neljänneksen ilmiöitä ovat:

- ▶ Huijausten ja tietojenkalastelujen määrä korostui erityisesti kesälomakuukausina.
- ▶ Kaikenlaisia huijauksia ja kalasteluita lähetettiin suuria määriä niin tekstiviesteillä kuin sähköposteillakin.
- ▶ Traficomissa tehtiin runsaasti tekstiviestihuijauksia, kunnes TRAFICOM SMS sender-ID:n rekisteröinti astui voimaan syyskuun lopulla.
- ▶ Myös Omavero, Omakanta, suomi.fi ja PRH olivat suosittuja huijausteemoja.

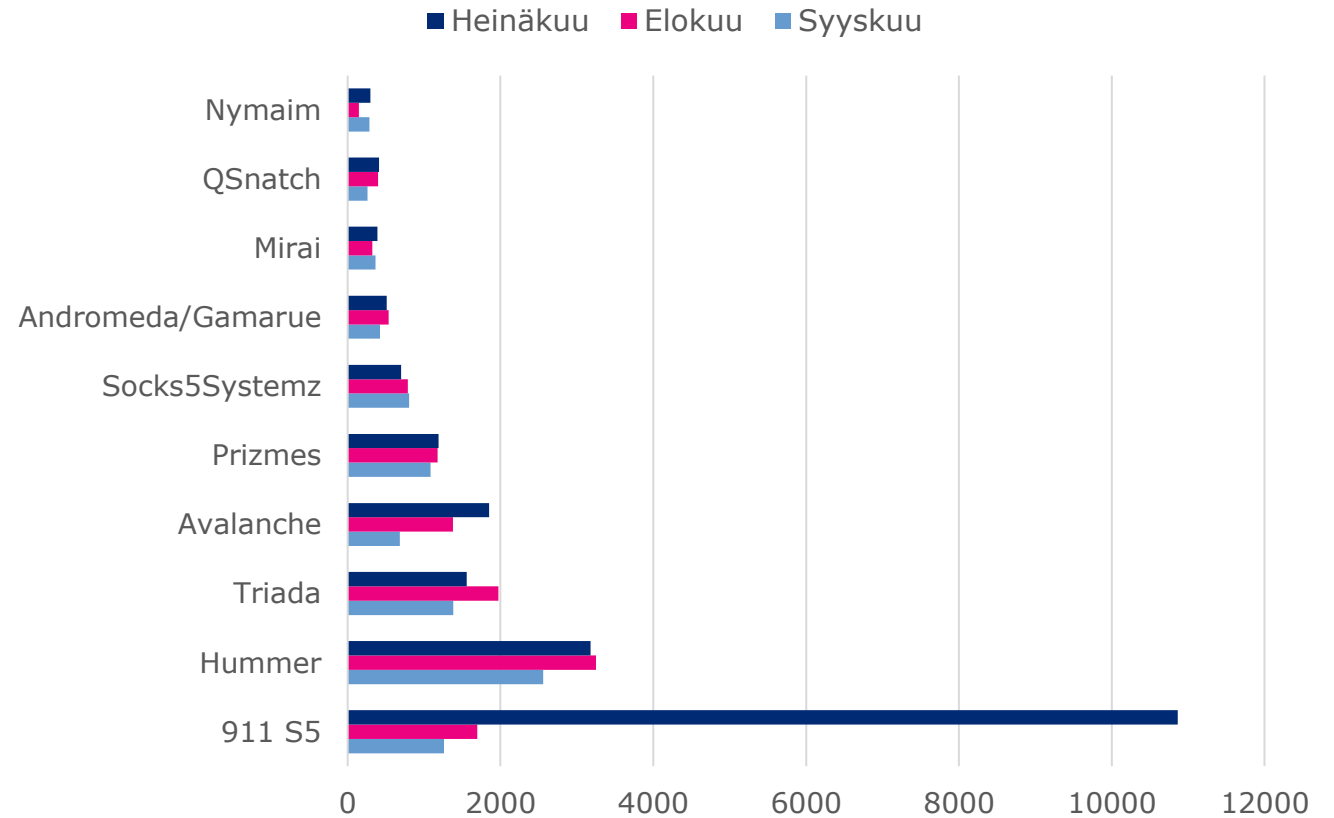




Autoreporterin haittaohjelmahavainnot

Torjumme haittaohjelmia yhteistyössä teleyritysten kanssa **Autoreporter-järjestelmän** avulla. Järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta. Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen.

Tilastossa kerromme **10 yleisintä ja nimettyä** haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyber-turvallisuuskeskuksen verkkosivuilla





Toimialakohtaiset havainnot

	Trendi 3kk	Edeltävä 3kk	
Elintarvike			Loppukesä oli elintarvikealalla poikkeuksellisen rauhallinen, vaikka käyttäjätunnusten kalastelua esiintyi runsaasti niin kuin muillakin toimialoilla. NIS2-direktiivin toimeenpanoon valmistautuminen on aiheuttanut kiirettä ja epätietoisuutta velvollisuuksista.
Energia			Toimialalla ei ole raportoitu erityisen vakavia tietoturvapoikkeamista tarkastelujakson aikana. Ilmoitukset koskivat pääasiassa VPN-palveluiden murtoyrityksiä, varelaskuja, kalasteluviestejä ja onnistuneita sähköpostitilimurtoja sekä julkiverkkoon turhan avoimesti näkyviä laitteita ja palveluita.
Finanssi			Finanssitoimiolla on raportoitu tavallista enemmän palvelunestohyökkäyksiä viimeisen kvartaalin aikana. Vaikka häiriöt ovat olleet pankkikohtaisesti toistuvia, ovat vaikutukset jääneet pääosin vähäisiksi. Finanssialan toimijat ovat jakaneet aktiivisesti tietoa Kyberturvallisuuskeskukselle.
Kemian- teollisuus			Tarkastelujaksolla on havaittu kasvavissa määrin kalastelu- ja huijauksen kampanjoita.
Logistiikka ja liikenne			Kvartaali oli aiempaan verrattuna rauhallisempi. Toimialalla on havaittu tietojenkalastelua mm. Dropbox-, pankki- ja postipakettiteemalla, joiden lisäksi ilmoituksia myös toimitusjohtajahuijauksista sekä vaikutuksiltaan pääosin vähäisiksi jääneistä palvelunestohyökkäyksistä. Kesällä virheellinen CrowdStrike-päivitys aiheutti toimialalla välillisiä ongelmia toimitusketjujen kautta.
Valtionhallinto			Etenkin tarkastelujakson loppua kohden palvelunestohyökkäysten määrä on jälleen kasvanut, mutta vaikutukset ovat jääneet vähäisiksi. Valtionhallintoon kohdistuu jatkuvasti kalasteluyrityksiä ja tietomurtojen yrityksiä, mutta Kyberturvallisuuskeskuksen tietoon ei ole tullut vakavia tietoturvapoikkeamia.
Media			Toimialalla ei ole raportoitu merkittävistä tietoturvapoikkeamista tarkastelujaksolla.
SOTE			Tietojenkalastelua esiintyy paljon ja käyttäjiä erehtyy jatkuvasti antamaan tunnuksiaan kalastelusivuille. Kesän aikana ilmoitettiin yhdestä vakavasta poikkeamasta, jossa rikollinen murtautui apteekin tietoverkkoon ja sai haltuunsa pääkäyttäjän valtuudet. Hyvinvointialueiden säästötavoitteet vaikeuttavat merkittävästi kyberturvallisuuden tarvitsemia investointeja ja henkilöstön osaamisesta huolehtimista.
Vesihuolto			Tarkastelujaksolla on havaittu kasvavissa määrin kalastelu- ja huijauksen kampanjoita.
Kunnat			Kuntaorganisaatioihin on kohdistunut etenkin Dropbox-teemaista kalastelua, joka on johtanut myös tilimurtoihin. Pahimmat vaikutukset saatu estettyä lievennystoimien avulla.
Kiinteistö ja rakennus			Tarkastelujaksolla useita M365-tilimurtoja, joista valtaosa saatu Dropbox-teemaisten kalasteluviestien seurauksena. Uhrien M365-tunnuksia on käytetty myös tunnusten jatkokalasteluun. Havaittu myös julkiverkkoon näkyviä mutta sinne kuulumattomia laitteita ja palveluita.

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

Tarve
kyberturvalli-
suuden
osaajille

Tekoälyn
riskienhallinta

Toimitus-
ketjujen
tietoturva

Säätelyn
tulevaisuus

Pilvi-
palvelujen
tietoturva

Teollisuus-
automaation
suojaaminen

IoT

6G

**Kuluttajien
tietoturva**

Haavoittu-
vuuksien
nopeutuva
hyväksikäyttö

Kvantti-
turvallinen
krypto

Osallistumi-
nen
digitaalisessa
ympäristössä



Pitkän aikavälin kybersää: Kyberturvallisuus kansalaistaitona

Tietoverkot ovat kiinteä osa yksilöiden ja yhteiskunnan arkea, jossa tietoturvasta huolehtiminen on niin aikuisia kuin lapsiakin koskettava tärkeä kansalaistaito. Lasten tietoturvataitojen ja kyberturvallisuusosaamisen kehittyminen on vanhempien ja lapsia kasvattavien aikuisten vastuulla.

- ▶ Kansalaisten kyberturvallisuusosaamisella tarkoitetaan kykyä toimia digitaalisessa ympäristössä vastuullisesti ja turvallisesti. Kyberturvallisuusosaamista voi verrata lukutaitoon, ja sitä edistäviä tavoitteita sisältyy yhtäläillä opetussuunnitelmien, koulutusten ja tutkintojen perusteisiin varhaiskasvatuksesta toisen asteen opetukseen. [\[15\]](#)
- ▶ Lapset ovat verkossa kuitenkin erityisen haauraassa asemassa, sillä heillä ei välttämättä ole vielä kykyä tunnistaa verkossa toimimisen vaaranpaikkoja, missä tarvitaan aikuisten tukea ja ohjausta. Tietoturvasta huolehtimisen lisäksi on tärkeää opastaa lasta vastuulliseen verkkokäyttäytymiseen sekä tunnistamaan laillisen ja laittoman toiminnan rajat verkossa itseä ja muita koskevien vahinkojen välttämiseksi.
- ▶ Lasten ja nuorten keskuudessa esimerkiksi pelaamisesta ja peleistä on tullut suosittu harrastus ja yhteydenpitoalusta, johon liittyy kuitenkin monia riskejä, joista on hyvä olla tietoinen. Lasten turvalliseen pelaamiseen kuuluu esimerkiksi omista tiedoista huolehtiminen, pelitilien suojaaminen sekä hyvän pelikäyttäytymisen edistäminen, kuten missä tahansa muussakin verkossa tapahtuvassa toiminnassa. Kirjoitimme aiheesta viikkokatsauksessamme syyskuussa. [\[14\]](#)
- ▶ Kyberturvallisuuskeskus haluaa osaltaan tukea lasten tietoturvataitojen kehittymistä. Olemme koonneet lapsille, vanhemmille ja kasvattajille kattavan paketin tietoturvaan liittyviä materiaaleja verkkosivuillemme. [\[16\]](#)
 - ▶ Lisäksi monet muut kansalliset ja kansainväliset tahot pyrkivät tukemaan ja kehittämään lasten ja nuorten turvallista toimintaa verkossa. Muun muassa EU-rahoitteinen Cyber Citizen -hanke [\[17\]](#), joka tähtää kansalaisten kyberturvallisuustaitojen kehittämiseen, sisältää kohdennettuja osuuksia erityisesti lapsille ja nuorille. Myös poliisi pyrkii edistämään vastuullista ja turvallista toimintaa verkossa sekä puuttumaan nuorten vakaviin tietoverkkorikoskierteisiin osana nuorten kyberrikollisuuden ehkäisyn Cybercrime Exit -toimenpideohjelmalla [\[18\]](#), joka käynnistettiin KRP:n kyberrikostorjuntakeskuksessa vuonna 2020.

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

- ▶ Traficom on antanut uudistetun teletoiminnan tietoturvamääräyksen [\[19\]](#)
 - ▶ Määräys on tullut pääosin voimaan 1.9.2024 ja se korvaa 4.3.2015 annetun Viestintäviraston määräyksen teletoiminnan tietoturvasta.
 - ▶ Määräystä sovelletaan yleiseen teletoimintaan ja sitä on valmisteltu yhteistyössä toimialan kanssa.
 - ▶ Uudistetussa määräyksessä määrätään tietoturvatoimenpiteistä kaikissa yleisissä viestintäverkoissa ja yleisesti saatavilla olevissa viestintäpalveluissa sekä rajapintojen, internetyhteyspalvelujen, tekstiviesti- ja multimediamviestipalvelujen ja sähköpostipalvelujen erityisistä vaatimuksista.
 - ▶ Määräys edellyttää kaikilta teleyrityksiltä toimenpiteitä tietoturvallisuuden ja riskien hallinnan vaatimusten toteuttamiseksi ja dokumentoimiseksi.



Oikeudelliset asiat

- ▶ Suomi on mukana New Yorkin julkilausumassa merikaapeliturvallisuudesta [\[20\]](#)
 - ▶ Yhdysvaltain aloitteesta laadittu yhteisjulistus [\[21\]](#) on julkaistu New Yorkissa YK:n yleiskokouksen yhteydessä Yhdysvaltojen järjestämässä sivutapahtumassa 25.9.2024.
 - ▶ Julkilausuman tavoitteena on kannustaa valtioita edistämään digitaaliseen talouteen tärkeään merikaapeli-infrastruktuuriin eheyttä, turvallisuutta ja saavutettavuutta.
 - ▶ Julkilausumassa painotetaan julkisen ja yksityisen sektorin tiivistä yhteistyötä, turvalliseksi todettujen laitetoimittajien suosimista, vahinkojen ennaltaehkäisyä sekä vahvempaa resilienssiä vaihtoehtoisten reititysten avulla.
 - ▶ Suomen allekirjoittamaan julkilausumaan osallistuu myös EU sekä useat muut samanmieliset kumppanimaat.
 - ▶ Julkilausuma ei ole oikeudellisesti sitova.



Oikeudelliset asiat

- ▶ LVM käynnistää säädöshankkeen EU:n gigabitti-infrasäädöksen toimeenpanosta [\[22\]](#)
- ▶ Euroopan unioni antoi huhtikuussa 2024 asetuksen toimenpiteistä gigabittitason sähköisten viestintäverkkojen käyttöönoton kustannusten vähentämiseksi. [\[23\]](#) Asetus korvaa yhteisrakentamisdirektiivin (2014/61/EU).
- ▶ Säädöshankkeessa muutetaan verkkoinfrastruktuurin yhteisrakentamisesta ja -käytöstä annettua lakia sekä mahdollisesti muita lakeja EU-asetuksen velvoitteiden toimeenpanemiseksi.
- ▶ EU:n tavoitteena on vauhdittaa erittäin suuren kapasiteetin verkkojen (very high capacity networks eli VHCN-verkkojen) rakentamista, jotta kaikilla EU:n alueilla olisi gigabitin yhteydet vuoteen 2030 mennessä.
- ▶ Hallituksen esitys on tarkoitus antaa eduskunnalle keväällä 2025. Asetusta tullaan soveltamaan pääosin lokakuusta 2025 alkaen.



Oikeudelliset asiat

- ▶ EU:n kyberturvallisuuden sertifiointijärjestelmä: state of the art -dokumenttien luettelon muuttaminen [\[24\]](#)
 - ▶ Komissio on julkaissut 18.10. saakka kommentoitavaksi täytäntöönpanoasetuksen luonnoksen, joka koskee EU:n kyberturvallisuuden sertifiointijärjestelmää (EUCC).
 - ▶ State of the art -dokumenteissa täsmennetään arviointimenetelmät, -tekniikat ja -välineet, joita sovelletaan tieto- ja viestintätekniikan tuotteiden sertifiointiin tai turvallisuusvaatimuksiin.
 - ▶ Nyt kommentoitavana on täytäntöönpanoasetuksen luonnos, jossa tarkoituksena on ottaa käyttöön uusi sertifiointielinten akkreditointiin liittyvä asiakirja, muuttaa kyberturvallisuuden testauslaitosten akkreditointia koskevaa asiakirjaa sekä tehdä useita muutoksia EUCC-asetuksen päätteksi.

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) Kansallinen hyökkäyspintakartoitus-palvelu (Hyöky) <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/hyoky>
- 2) Global Cybersecurity Index 2024 <https://www.itu.int/en/mediacentre/Pages/PR-2024-09-10-Global-Cybersecurity-Index.aspx>
- 3) Traficomin ensimmäinen NATO-tuotehyväksyntä salausratkaisulle <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficomin-ensimmainen-nato-tuotehyvaksynta-salausratkaisulle>
- 4) Challenging Assumptions: Enhancing the Understanding of Securing Internet-Exposed Industrial Control Systems <https://www.greynoise.io/blog/challenging-assumptions-enhancing-the-understanding-of-securing-internet-exposed-industrial-control-systems>
- 5) The Problem with Remote Access Tool Sprawl https://web-assets.claroty.com/resource-downloads/claroty-team82-report_secure-access-tool-sprawl.pdf
- 6) Nordean häiriötiedotteet <https://www.nordea.fi/henkiloasiakkaat/tuki/hairiotiedotteet.html>
- 7) Court-Authorized Operation Disrupts Worldwide Botnet Used by People’s Republic of China State-Sponsored Hackers <https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state>
- 8) Poikkeamien hallinnointi turvallisuuden parantajana <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/poikkeamien-hallinnointi-turvallisuuden-parantajana>
- 9) Harjoitustoiminta <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/harjoitustoiminta>
- 10) Kyberturvallisuuskeskuksen viikkokatsaus – 39/2024 <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-392024>
- 11) Kyberturvallisuuskeskuksen viikkokatsaus – 38/2024 <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-382024>
- 12) Kyberturvallisuuskeskuksen viikkokatsaus – 37/2024 <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-372024>

Lähdeluettelo

- 13) Poliisi - Traficom in nimissä tehtyjen petosten määrä kasvaa <https://poliisi.fi/-/traficomin-nimissa-tehtyjen-petosten-maara-kasvaa>
- 14) Kyberturvallisuuskeskuksen viikkokatsaus – 36/2024 <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-362024>
- 15) Opetushallitus - Kyberturvallisuus <https://www.oph.fi/fi/kyberturvallisuus>
- 16) Lasten tietoturvataidot <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/lasten-tietoturvataidot>
- 17) Cyber Citizen – Euroopan unionin laajuinen kyberkansalaistaitohanke <https://cyber-citizen.eu/>
- 18) Poliisi - Nuorten kyberrikollisuuden ehkäisy (Cybercrime Exit) <https://poliisi.fi/cybercrime-exit>
- 19) Määräys teletoiminnan tietoturvasta (TRAFICOM/248815/03.04.05.00/2022) <https://www.finlex.fi/fi/viranomaiset/normi/480001/50299>
- 20) LVM - Suomi mukaan New Yorkin julkilausumaan merikaapeliturvallisuudesta <https://lvm.fi/-/suomi-mukaan-new-yorkin-julkilausumaan-merikaapeliturvallisuudesta>
- 21) Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World <https://www.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/>
- 22) LVM - Säädöshanke EU:n gigabitti-infrasäädöksen toimeenpanosta käynnistyy <https://lvm.fi/-/saadoshanke-eu-n-gigabitti-infrasaadoksen-toimeenpanosta-kaynnistyy-tavoitteena-vauhdittaa-nopeiden-yhteyksien-kayttoonottoa>
- 23) EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2024/1309 https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=OJ:L_202401309
- 24) EU:n kyberturvallisuuden sertifiointijärjestelmä https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14334-EUn-kyberturvallisuuden-sertifiointijarjestelma-viimeisinta-kehitysta-edustavien-asiakirjojen-luettelon-muuttaminen_fi