TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Maaliskuu 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

Vuonna 2023 Kyberturvallisuuskeskukselle ilmoitettujen tietoturvapoikkeamien määrä oli yhteensä 18 625, kun vuonna 2022 luku oli 12 947.[1] Alkuvuoden 2024 aikana meille on ilmoitettu 6 241 tietoturvapoikkeamaa. Kyberturvallisuuskeskukselle kannattaa aina ilmoittaa tietoturvapoikkeamahavainnoista.

Tietoturva 2024 –seminaariin osallistui paikan päällä ja etäyhteyksin yhteensä yli 3 000 osallistujaa.[2]

Koulutus on edelleen merkittävässä osassa organisaatioiden tietoturvaa. Saamiemme ilmoitusten mukaan kalastelukampanjoissa on vaarantunut jopa yli 100 saman organisaation työntekijän käyttäjätunnusta.

Kybersää maaliskuu 2024

Tietomurrot ja -vuodot

- Kuukauden tietomurtojen ilmiönä oli organisaatioihin kohdistuneet erilaiset sähköpostikalastelut ja tietomurrot.
- Olemme edelleen saaneet tasaisesti ilmoituksia erilaisiin verkon sisääntulolaitteisiin kohdistuneista skannauksista ja haavoittuvuuksien hyväksikäyttö- sekä murtoyrityksistä.

Huijaukset ja kalastelut

- Ajoneuvoveroteemaiset tekstiviestihuijaukset kalastelivat pankkitunnuksia Traficomin nimissä.
- Kaikkien pankkien lisäksi Posti, OmaKanta ja OmaVero ovat olleet pankkitunnuskalasteluviestien aiheina.

Haittaohjelmat ja haavoittuvuudet

- Linux-jakeluiden XZ Utils -tiedostonpakkausohjelman 5.6.0 ja 5.6.1 versiot sisältävät haitallista koodia, joka sallii luvattoman pääsyn luoden takaportin järjestelmään.

Automaatio ja IoT

- Matter-protokollasta vastaava Connectivity Standards Alliance (CSA) on julkaissut kyberturva-merkin IoT-tuotteille ja sopinut merkkien vastavuoroisesta tunnustamisesta Singaporen kyberviranomaisen (CSA) kanssa.
- Myös Yhdysvaltojen viestintäkomissio on julkaissut vapaaehtoisen kyberturvamerkin IoT-tuotteille.

Verkkojen toimivuus

- Maaliskuussa yleisissä viestintäpalveluissa oli 3 toimivuushäiriötä.
- Haktivistit kohdistivat jälleen palvelunestohyökkäyksiä Suomeen maaliskuun lopulla.
- Havainnoista huolimatta palvelunestohyökkäyksillä ei ollut merkittäviä vaikutuksia.

Vakoilu

- Useat maat kertoivat lisätietoja APT31:n kybervakoilusta.[3]
- Kiinaan yhdistetyn APT31:n kerrottiin hyödyntäneen murrettuja ruotsalaisia reitittimiä eri maihin kohdistuneissa hyökkäyksissä ja pyrkineen hankkimaan tietoa brittipoliitikkojen sähköposteista.[4, 5]
- KRP kertoi, että APT31:n yhteys eduskunnan tietomurtoon vuosina 2020–2021 on vahvistunut.[6]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Traficomin ja Huoltovarmuuskeskuksen tekoälypohjaisia kyberturvallisuusratkaisuja käsittelevä selvitys on julkaistu.[7]

Traficom jatkaa 5G-kyberturvallisuuden hakkerointitapahtumasarjaa uudella Hack the Networks -tapahtumalla toukokuussa 2024. Ilmoittaudu mukaan hackathoniin 14.4.2024 mennessä![8]

Tietoturvan vuosi 2023 -katsaus arvioi uhkatason pysyvän kohonneena myös vuonna 2024.[1]

Maaliskuun kyberturvallisuuden yleiskuva

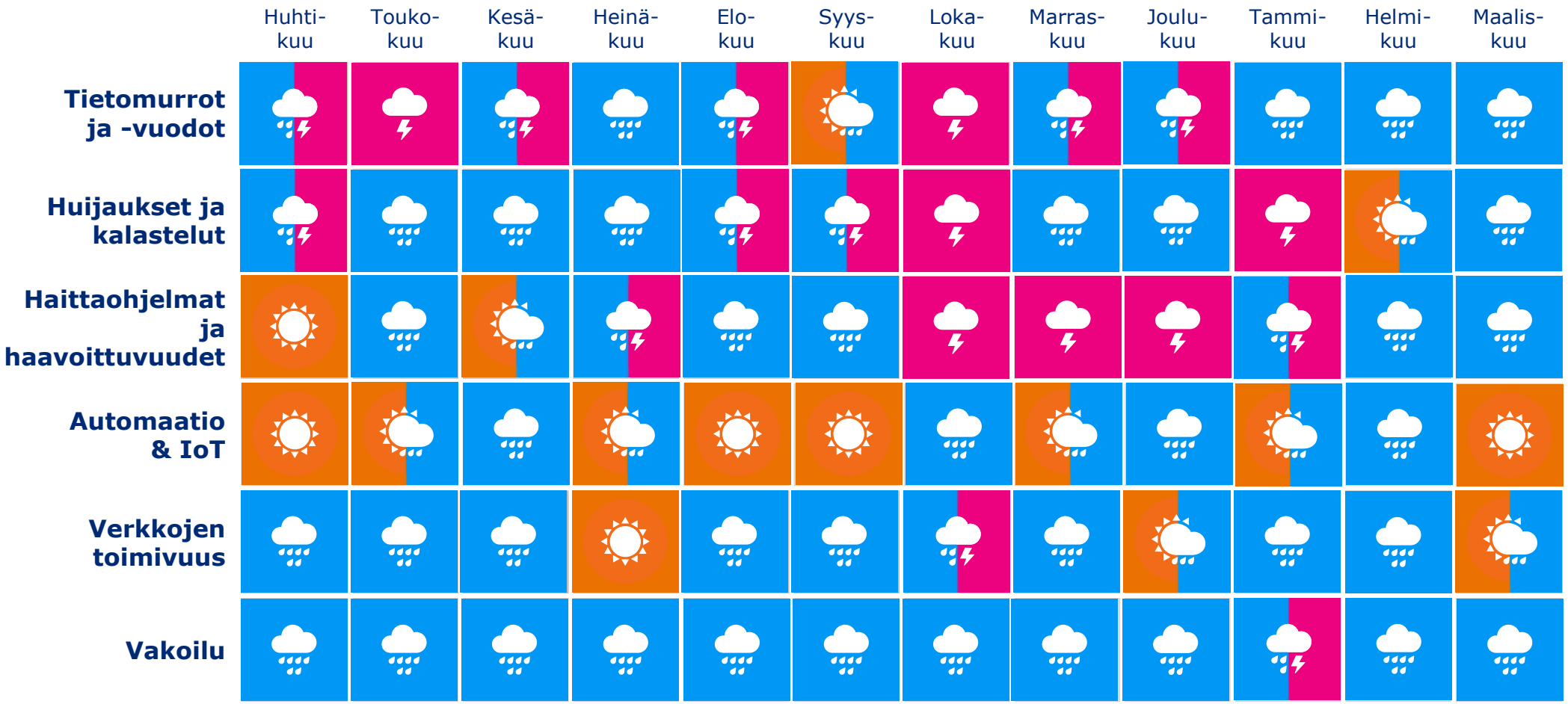
- Maaliskuun aikana organisaatioita ovat kiusanneet yhä niin palvelunestohyökkäykset kuin tietomurtojen yrityksetkin. Rikollisten kohteena ovat olleet esimerkiksi erilaiset verkon sisääntulolaitteet.
- Maaliskuun ja huhtikuun vaihteessa julkisuuteen tulleen XZ Utils -ohjelmistopaketin haavoittuvuuden paljastuttua käyttäjiä kehotettiin ensiapuna poistamaan saastunut päivitys. Mahdollisia hyväksikäyttöjä etsitään, haavaa korjaavia päivityksiä julkaistaan ja tapausta tutkitaan laajasti paraikaa.
  - Toistaiseksi vakavia haavoittuvuuden hyväksikäyttöjä ei ole tiedossa.
  - Rikolliset käyttivät XZ Utils -ohjelmistopaketin kriittisen haavoittuvuuden työstöön useita vuosia ja hyökkäystä on kuvailtu yhdeksi edistyneimmistä tähän mennessä paljastuneista toimitusketjuhyökkäyksistä.
  - Lue lisää XZ Utils –ohjelmistopaketin tapauksesta Viikkokatsauksestamme 14/2024.[9]
- Maaliskuun lopussa aloimme julkaista Kyberturvallisuuskeskuksen Viikkokatsauksen osana Ajankohtaiset huijaukset –osiota, johon kerätään viikon aikana saapuneiden ilmoitusten perusteella esimerkkejä liikkeellä olevista huijauksista.

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

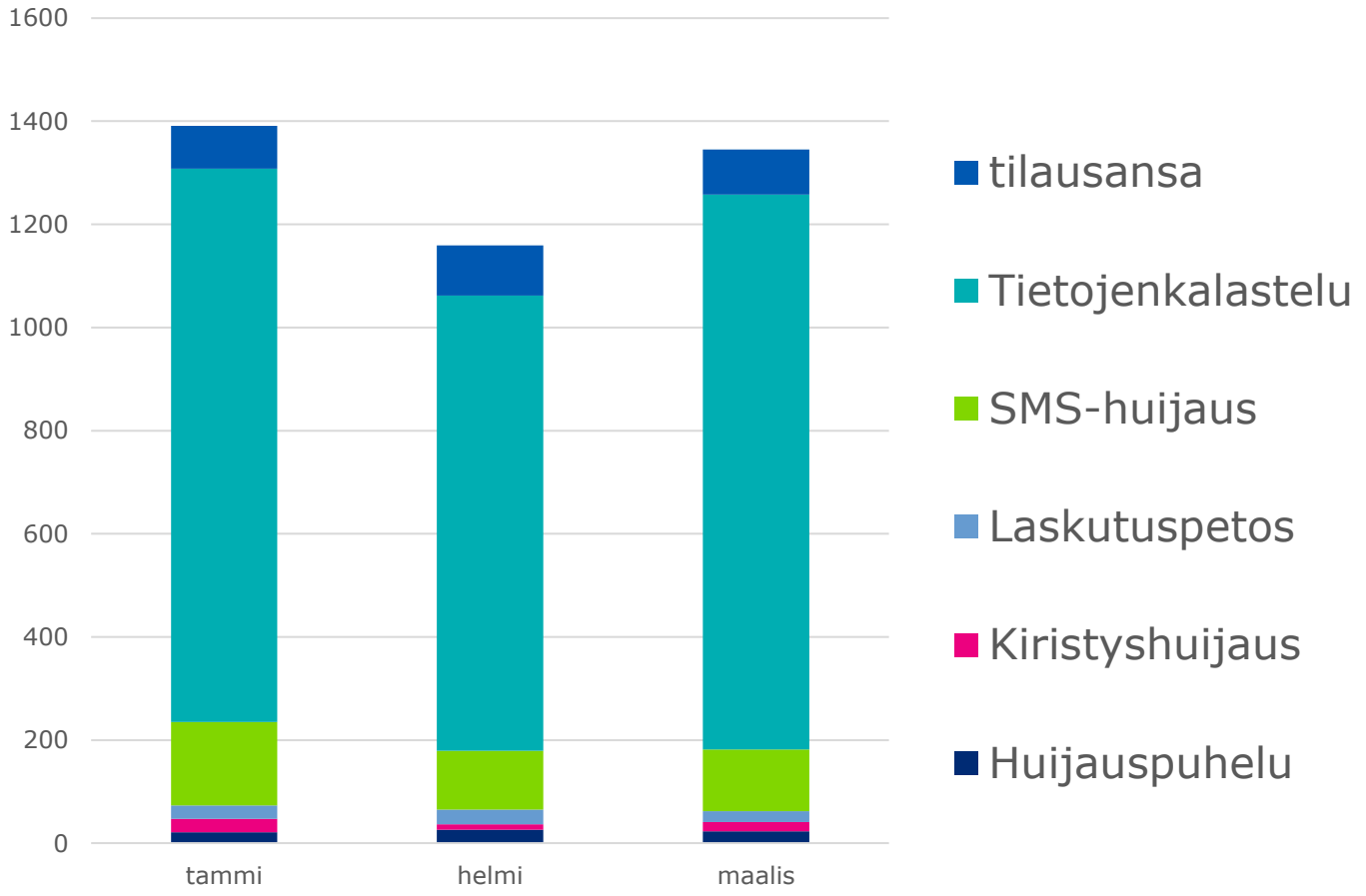
1 kk



Käsiteltyjä huijaustapauksia
Q1/2024

Vuoden 2024 ensimmäisen neljänneksen ilmiöitä ovat:

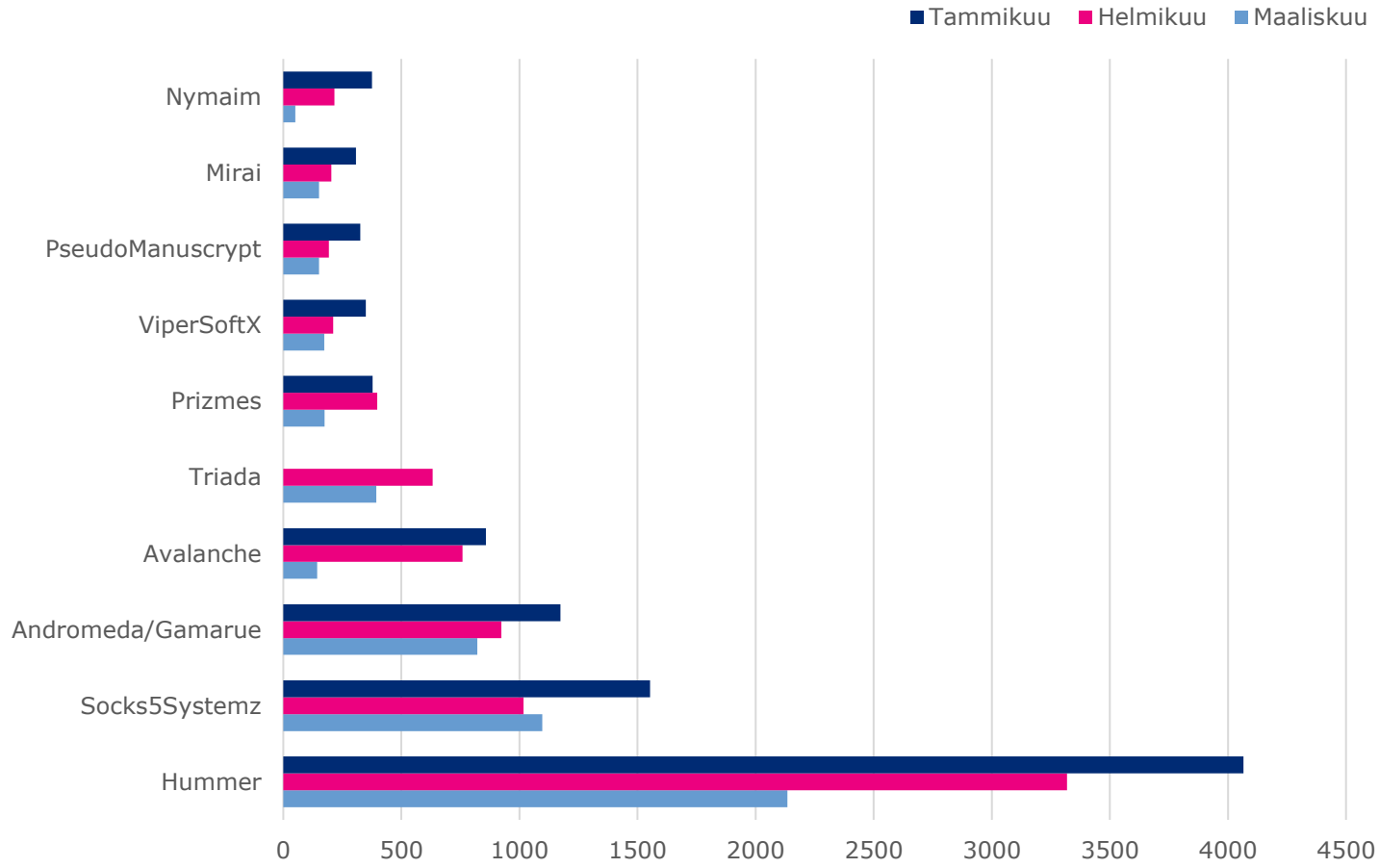
- Pankkitunnusten kalastelu ja tilausansat ovat jatkuneet aktiivisina.
- Rekrytointihuijaukset alkavat useimmiten ulkomailta tulevalla whatsapp-viestillä. Huijari pyytää saada etäkäyttöyhteyden uhrin tietokoneelle muka perehdytyskoulutusta varten.
- Huijauksiin käytetään kaikkia viestivälineitä sähköposteista ja tekstiviesteistä pikaviestimiin ja puheluihin.



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.

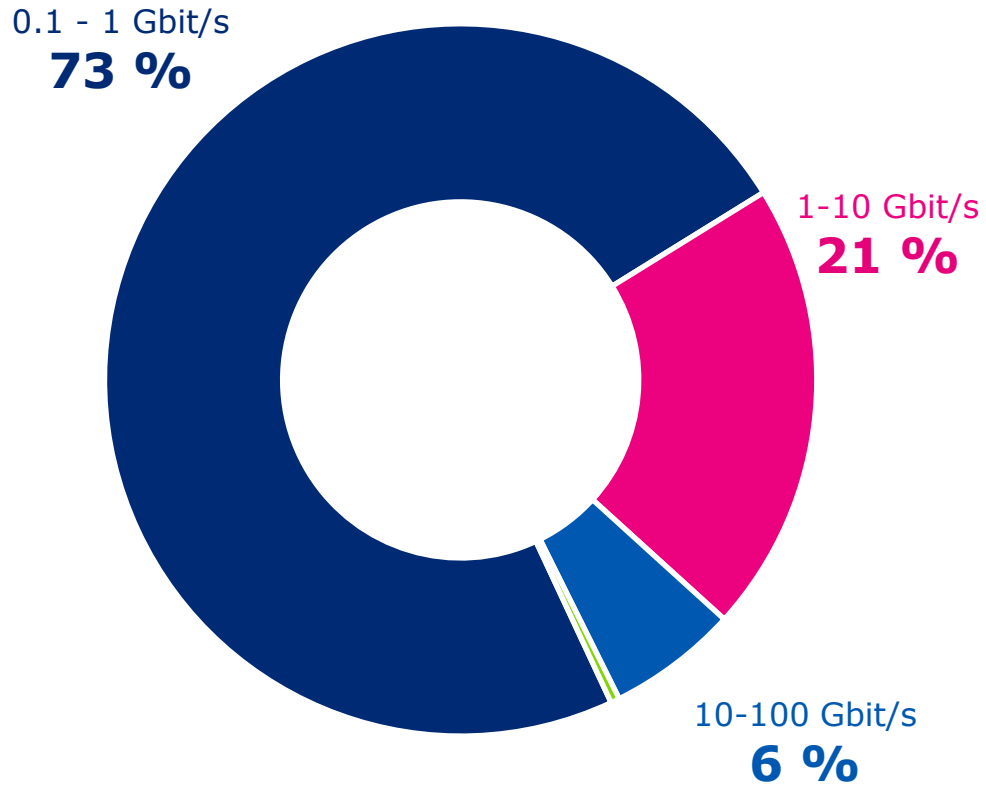
Tilastossa kerromme **10 yleisintä ja nimettyä** haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyber-turvallisuuskeskuksen verkkosivuilla



Palvelunestohyökkäysten tunnuslukuja
Q1/2024

3 kk

- **197 Gbit/s** oli suurin Suomessa nähty palvelunestohyökkäys Q1/2024.
- Noin 73% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



3 kk

Toimialakohtaiset havainnot

	Trendi **3kk**	Edeltävä **3kk**	
Elintarvike			Elintarvikealan yritykset ilmoittivat ensimmäisellä vuosineljänneksellä enemmän poikkeamailmoituksia kuin edellisellä neljänneksellä. Eräs yritys sai hyvän valvonnan ansiosta pysäytettyä todennäköisen kiristyshaittaohjelmahyökkäyksen valmistelun. Uutisiin asti päätyi sikatilan tietojärjestelmiin tehty kiristyshaittaohjelmahyökkäys.
Energia			Ilmoitettujen poikkeamien määrä ei juurikaan muuttunut. Tietomurtojen yritysten määrät kasvoivat, kohteina olivat etenkin Internetiin näkyvät VPN-ratkaisut. Sektorin toimijoita joutui palvelunestohyökkäysten kohteeksi. Euroopan komissio julkaisi rajat ylittävien sähkönsiirtojen kyberturvallisuusnäkökohtia koskevan verkkosäännön.[10]
Finanssi			Pankkitunnusten kalastelu- ja huijauskampanjat jatkuivat eri pankkien nimissä. Yksittäiset taloudelliset menetykset ovat olleet merkittäviä. Tekstiviestihuijausten määrää vähenee lähettäjätunnusrekisteröintien voimaanastumisen myötä.
Kemian-teollisuus			Ilmoitetuissa poikkeamissa lievää nousua.
Logistiikka ja liikenne			Toimialalla on alkuvuoden aikana ilmoitettu tasaisesti mm. palvelunestohyökkäyksistä, pankkikalasteluista, sekä rekrytointihuijauksista.
Valtionhallinto			Valtionhallinnon organisaatiot ovat olleet useasti erilaisten palvelunestohyökkäysten kohteena alkuvuodesta. Osa organisaatioista on myös havainnut itseään koskevaa tiedonkeruuta ja kartoitustoimintaa. Kyberturvallisuuskeskukselle on ilmoitettu myös sosiaalisen median valetileistä, joissa on jaettu valheellista tietoa organisaation tai sen henkilöstön nimissä.
Media			Ilmoitetuissa poikkeamissa ei merkittäviä muutoksia.
SOTE			Kyberturvallisuuskeskus on saanut sote-alalta vähemmän poikkeamailmoituksia kuin vuoden 2023 viimeisellä neljänneksellä. Maailmalla terveydenhuollon arvoketjut ovat pysyneet korostuneesti kiristyshaittaohjelmahyökkäysten kohteina. Yhdysvalloissa Change Healthcarea vastaan tehtyä hyökkäystä on luonnehdittu maan historian vakavimmaksi.
Vesihuolto			Ilmoitetuissa poikkeamissa lievää nousua.
Kunnat			Kuntiin on kohdistunut paljon kalastelua, joissa tilejä on murrettu eri tiedostonjakopalveluiden kautta jaettavan PDF-tiedoston avulla. Myös monivaiheinen tunnistautuminen on osassa tapauksista ohitettu AiTM-tekniikan avulla. Lisäksi kuntien palveluihin on toteutettu useita palvelunestohyökkäyksiä

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 kyber-turvallisuuden osaajille

Tekoälyn riskienhallinta

Toimitus-ketjujen tietoturva

Sääntelyn tulevaisuus

Pilvi-palvelujen tietoturva

Teollisuus-automaation suojaaminen

IoT

6G

Kuluttajien tietoturva

Haavoittu-vuuksien nopeutuva hyväksikäyttö

Kvantti-turvallinen krypto

Osallistu-minen digitaalisessa ympäristössä

Pitkän aikavälin kybersää:
Kvanttiturvallinen krypto

Kvanttilaskennalle haavoittuvien julkisen avaimen salausmenetelmien korvaamiseksi on käynnissä useita kvanttiturvallisten algoritmien standardointiin tähtääviä hankkeita, ja ensimmäisten standardien odotetaan valmistuvan tänä vuonna. Kvanttiturvallisia toteutuksia (esim. Signal) on jo tehty standardiluonnosten perusteella.[11, 12]

Uudet toteutukset tulevat vaatimaan laajoja järjestelmäpäivityksiä monessa organisaatiossa, ja maailmanlaajuisesti päivitykset voivat jatkua monta vuotta. Mitä pidempään päivittäminen kestää, sitä suuremman riskin kvanttilaskenta muodostaa. Monet tahot ovatkin tehneet omia ohjeistuksiaan siirtymälle ja esim. USA edellyttää valtionhallinnossa käytettyjen CNSA-tuotteiden päivityksiä viimeistään 2030 alussa.[11, 13]

Kiinnostus kvanttilaskennan kaupallisille sovelluksille kiihdyttää kvanttikoneiden kehitystä. Toistaiseksi edes tehokkaimmatkaan kvanttikoneet eivät pysty murtamaan salausmenetelmiä, eikä ole varmaa, onko sellaisten toteuttaminen ylipäätään mahdollista. On kuitenkin arvioitu, että kryptografisesti merkittävien koneiden tulo olisi todennäköistä 30 vuoden sisällä, mutta hyvin epätodennäköistä 5 vuoden sisällä.[11, 14]

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

- Euroopan parlamentti hyväksyi maailman ensimmäiset tekoälysäännöt.[15]
  - Euroopan parlamentti hyväksyi 13.3.2024 tekoälysäädöksen (AI Act), jolla edistetään innovointia ja taataan, että tekoäly on turvallista ja perusoikeuksien mukaista. Säännöissä vahvistetaan tekoälyä koskevat velvoitteet, jotka perustuvat sen mahdollisiin riskeihin ja vaikutustasoon.
  - Säännöissä muun muassa kielletään tietyt kansalaisten oikeuksia uhkaavat tekoälysovellukset, määritellään lainvalvontaa koskevat poikkeukset, asetetaan suuririskisille tekoälyjärjestelmille velvoitteita ja asetetaan yleiskäyttöisille tekoälyjärjestelmille avoimuusvaatimuksia.
  - Kansallisella tasolla on perustettava sääntelyn testiympäristöjä ja suoritettava testausta todellisissa olosuhteissa, ja ne on saatettava pk-yritysten ja startup-yritysten saataville.
  - Säädös hyväksytään virallisesti ennen vaalikauden loppua ja myös neuvoston on vielä annettava virallinen hyväksyntänsä. Säädös tulee voimaan 20 päivän kuluttua siitä, kun se on julkaistu virallisessa lehdessä. Säädöstä sovelletaan kahden vuoden kuluttua sen voimaantulosta, lukuun ottamatta joitakin erityissäännöksiä koskevia poikkeuksia.

Oikeudelliset asiat

- Euroopan neuvosto hyväksyi oikeudellisen kehyksen digitaaliselle lompakolle. [16, 17]
  - Euroopan neuvosto hyväksyi 26.3.2024 uuden kehyksen eurooppalaiselle digitaaliselle identiteetille (e-ID) varmistaakseen luotettavan ja turvallisen digitaalisen identiteetin kaikille eurooppalaisille.
  - Asetuksen mukaan jokaisen jäsenvaltion on luotava kansalaistensa käyttöön digitaalisen identiteetin lompakko. Lompakon käyttöönottaminen on vapaaehtoista.
  - Digilompakko mahdollistaa tunnistautumisen palveluihin sekä dokumenttien tallentamisen, jakamisen ja sähköisen allekirjoittamisen kaikkialla EU:ssa.
  - Asetus tulee voimaan 20 päivän kuluttua sen julkaisemisesta virallisessa lehdessä. Asetus pannaan kokonaisuudessaan täytäntöön vuoteen 2026 mennessä.

Oikeudelliset asiat

- Euroopan komissio hyväksyi EU:n sähköalan kyberturvallisuutta koskevan uuden verkkosäännön.[10][18]
  - Euroopan komissio hyväksyi 11.3.2024 säädöksen, jolla puututaan rajat ylittävien sähkövirtojen kyberturvallisuusnäkökohtiin. Säädöksellä pyritään parantamaan EU:n sähköjärjestelmien häiriönsietokykyä ja varmuutta.
  - Säädös koskee kyberturvallisuusriskien arviointia, yhteisiä kyberturvallisuutta koskevia vähimmäisvaatimuksia, suunnittelua, raportointia ja seurantaa sekä kriisinhallintaa.
  - Säädös siirtyy seuraavaksi Euroopan parlamentin ja neuvoston käsiteltäväksi.

Oikeudelliset asiat

- Liikenne- ja viestintävirasto arvioi radioviestinnän luottamuksellisuutta AIS, ADS-B ja RID-järjestelmissä.[19, 20]
  - Yleisesti vastaanotettavaksi tarkoitettua radioviestintää sekä sen välitystietoja saa käsitellä viestinnän luottamuksellisuuden estämättä. Lain mukaan yleisesti vastaanotettavaksi tarkoitettuna radioviestintänä pidetään aina: 1) televisio- ja radio-ohjelmistojen lähetyksiä; 2) hätäkutsuja; 3) yleisellä kutsukanavalla harjoitettavaa radioviestintää; 4) radioamatööriviestintää; ja 5) lyhytaaltoradioviestintää 27 megahertsin taajuusalueella. Muissa tapauksissa arvioidaan tapauskohtaisesti, onko radioviestintä tarkoitettu yleisesti vastaanotettavaksi.
  - Liikenne- ja viestintäviraston arvion mukaan eräiden ilmailun ja merenkulun automaattisten tunnistusjärjestelmien (AIS, ADS-B sekä RID) yleislähetteitä voidaan pitää yleisesti vastaanotettavaksi tarkoitettuna radioviestintänä.

Oikeudelliset asiat

- Tiedonhallintalautakunnalta suositus tietoturvallisuuden vähimmäisvaatimuksista.[21]
  - Suositus opastaa tiedonhallintalain (906/2019) asettamien tietoturvallisuuden vähimmäisvaatimusten täyttämisessä. Vähimmäisvaatimusten osana organisaatioiden tulee tunnistaa ja arvioida tietojenkäsittelyyn liittyvät riskit sekä toteuttaa toimenpiteet riskien pienentämiseksi hyväksyttävälle tasolle.
  - Suositus on tarkoitettu ensisijaisesti tiedonhallintalaissa määritetyille tiedonhallintayksiköille ja viranomaisille, mutta näiden lisäksi suositusta voivat hyödyntää kaikki muutkin toimijat, jotka käsittelevät viranomaisten asiakirjoja.
- Valtiovarainministeriöltä opas julkishallinnon organisaatioille pilvipalveluihin siirtymisestä.[22]
  - Opas on tietolähde organisaatioille pilvipalveluiden tietoturvallisuudesta, mahdollisuuksista, riskeistä ja parhaista käytännöistä. Siinä kuvataan myös keskeiset tekniset ratkaisut ja prosessit sekä eri alustojen tietoturva-arkkitehtuurit. Opas on suunnattu ensisijaisesti pilvipalveluiden käyttöönottoa suunnitteleville tai jo käyttäville organisaatioille ja asioiden parissa työskenteleville.

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)

Yhteiskunnan kannalta kriittisten organisaatioiden ilmoituslomake: https://eservices.traficom.fi/dataservices/forms/NISlomake.aspx

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) Tietoturvan vuosi 2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-vuosi-2023-katsaus-arvioi-uhkatason-pysyvan-kohonneena-myos-vuonna-2024
2) Tietoturva 2024 -seminaarissa puhutti tekoäly ja kvanttiteknologia https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2024-seminaarissa-puhutti-tekoaly-ja-kvanttiteknologia
3) Chinese Hackers Hijack Swedish Routers to Launch Cyber Attacks https://cybersecuritynews.com/chinese-hackers-hijack-swedish-routers
4) UK calls out China state-affiliated actors for malicious cyber targeting of UK democratic institutions and parliamentarians https://www.ncsc.gov.uk/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians
5) UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity
6) Poliisi jatkanut eduskunnan tietojärjestelmiin kohdistuneen tietomurron tutkintaa https://poliisi.fi/-/poliisi-jatkanut-eduskunnan-tietojarjestelmiin-kohdistuneen-tietomurron-tutkintaa

Lähdeluettelo

7) Tekoäly on yhä keskeisempi tekijä tulevaisuuden tietoturvaratkaisuissa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekoaly-yha-keskeisempi-tekija-tulevaisuuden-tietoturvaratkaisuissa
8) Hack the Networks 2024 https://hackthenetworks.fi/fi
9) Kyberturvallisuuskeskuksen viikkokatsaus - 14/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-142024
10) EU:n sähköntoimitukset – kyberturvallisuutta koskevat alakohtaiset säännöt (verkkosääntö) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13101-EUn-sahkontoimitukset-kyberturvallisuutta-koskevat-alakohtaiset-saannot-verkkosaanto-_fi
11) The PQC Migration Handbook https://ir.cwi.nl/pub/32988/PQC_migration_handbook_EN_2.0.pdf
12) Quantum Resistance and the Signal Protocol https://signal.org/blog/pqxdh/
13) Announcing the Commercial National Security Algorithm Suite 2.0 https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
14) Cryptographically Relevant Quantum Computers (CRQCs) & The Quantum Threat https://www.splunk.com/en_us/blog/learn/crqcs-cryptographically-relevant-quantum-computers.html

Lähdeluettelo

15) Parlamentti hyväksyi maailman ensimmäiset tekoälysäännöt https://www.europarl.europa.eu/news/fi/press-room/20240308IPR19015/parlamentti-hyvaksyi-maailman-ensimmaiset-tekoalysaannot
16) MEPs back plans for an EU-wide digital wallet https://www.europarl.europa.eu/news/en/press-room/20240223IPR18095/meps-back-plans-for-an-eu-wide-digital-wallet
17) Eurooppalainen digitaalinen identiteetti (e-ID): neuvosto hyväksyi oikeudellisen kehyksen turvalliselle ja luotettavalle digitaaliselle lompakolle https://www.consilium.europa.eu/fi/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/
18) New network code on cybersecurity for EU electricity sector https://energy.ec.europa.eu/news/new-network-code-cybersecurity-eu-electricity-sector-2024-03-11_en?prefLang=fi
19) Luottamuksellinen viestintä https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/luottamuksellinen-viestinta

Lähdeluettelo

20) Radioviestinnän luottamuksellisuutta koskevien säännösten soveltaminen alusten ja ilma-alusten tunnistamiseen ja seurantaan tarkoitettuihin AIS-, ADS-B- ja RID-radiolähetteisiin https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Arviomuistio%20radioviestinn%C3%A4n%20luottamuksellisuus%20AIS%2C%20ADS-B%20ja%20RID.pdf
21) Suositus tietoturvallisuuden vähimmäisvaatimuksista https://julkaisut.valtioneuvosto.fi/handle/10024/165487
22) Uusi opas auttaa julkishallinnon organisaatioita pilvipalveluihin siirtymisessä https://vm.fi/-/uusi-julkaisu-auttaa-julkishallinnon-organisaatioita-pilvipalveluihin-siirtymisessa