TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Kesäkuu 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

Kesän aikana kyberturvallisuuden alalle on avautunut useita EU-rahoitusmahdollisuuksia. Rahoitusta on tarjolla niin yksityisen, julkisen kuin tutkimussektorinkin toimijoille.[1]

NIS2-direktiivin voimaantuloon on aikaa kolme kuukautta.

Loppukesällä tulossa on kolme tapahtumaa: 14.8. on Kybermittaripäivä, 27.8. pidetään Digitaalinen Eurooppa –hakemuskoulutus sekä 10.-11.9. järjestetään kansainvälinen brokerage-tapahtuma. Tulevat tapahtumamme on listattu verkkosivuillemme.[2]

Kybersää kesäkuu 2024

Tietomurrot ja -vuodot

- Kesäkuu oli melko rauhallinen tietomurtojen ja -vuotojen osalta.
- Facebook-käyttäjätilejä murrettiin vahvistuskoodeja kalastelevilla IKEA-teemaisilla huijauksilla.
- M365-tilimurtoja raportoitiin etenkin loppukuusta. Tilejä murrettiin esim. kalasteluviesteillä, joissa "jaettiin tiedosto".

Huijaukset ja kalastelut

- Traficomin nimissä lähetetyt sakkohuijaukset ilmestyivät uuteen hieman aiempaa eri tavalla kirjoitettuun osoitteeseen ”trafcom.info”.
- Kesäkuussa verottajan nimissä alkoi jälleen näkyä veronpalautus-aiheisia huijausviestejä.

Haittaohjelmat ja haavoittuvuudet

- Kesäkuu oli kokonaisuutena ilmiön osalta rauhallinen.
- Saimme muutamia ilmoituksia tekstiviestillä saapuneista Vultur-haittaohjelman levitysyrityksistä.

Automaatio ja IoT

- Operaattoreiden laitteet otsikoissa: Yhdysvalloissa 600 000 reitititintä hajosi hyökkäyksen seurauksena.[3] Suomessa eräiden modeemien sertifikaattien vanhenemisen johdosta turvattomia laitteita ei päästetä verkkoon.[4]
- Pienten mm. automaatiolaitteiden FreeRTOS-käyttöjärjestelmässä erittäin vakava puute voi aiheuttaa pitkään ongelmia.[5]

Verkkojen toimivuus

- Kesäkuussa yleisissä viestintäpalveluissa oli 10 toimivuushäiriötä.
- Palvelunestohyökkäyksiä raportoitiin kesäkuussa maltillisesti, eikä ilmoitetuilla poikkeamilla ollut merkittäviä palveluvaikutuksia.

Vakoilu

- Etähallintaratkaisustaan tunnettu TeamViewer kertoi yritysverkkoonsa kohdistuneesta tietomurrosta, josta syytetään Midnight Blizzardia (Nobelium, APT29). Murto ei tiettävästi ulottunut asiakasyhteyksiin tai tuotantoympäristöön.[6]
- Microsoft on lähettänyt ilmoituksia asiakkailleen, joihin Midnight Blizzardiin liitetty tietomurto talvella on voinut vaikuttaa.[7]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Julkaisimme uuden ohjeen kvanttiturvallisista algoritmeista ja niihin siirtymisestä.[8]

Muistutimme varautumisesta kesän aikana lisääntyviin laskutus- ja toimitusjohtajahuijauksiin. Tehokkain tapa suojautua laskutushuijauksilta on varmistaa asia epäselvissä tapauksissa puhelimitse ja alkuperäisiä laskuttajan yhteystietoja käyttämällä. Kesätyöntekijöille ja myös pidempään talossa olleillekin työntekijöille olisi tärkeää muistuttaa, mikä on omassa organisaatiossa oikea tapa käsitellä saapuvat laskut.[9]

Valtioneuvosto on 27.6.2024 asettanut verkkoturvallisuuden neuvottelukunnan uudelle toimikaudelle. Verkkoturvallisuuden neuvottelukunnan tehtävänä on seurata viestintäverkkojen ja teknologian kehittymistä ja verkkoturvallisuutta koskevan lainsäädännön soveltamiskäytäntöä sekä toimia viranomaisten päätöksenteon tukena. Neuvottelukunnan toimikausi on 1.7.2024–31.12.2027.[10]

Kesäkuussa 2024 Traficom hyväksyi luotetuiksi ilmoittajiksi kaksi yhteisöä, jotka torjuvat erityisesti lapsiin ja nuoriin kohdistuvaa laitonta sisältöä internetissä. Asema myönnettiin Pelastakaa Lapset ry:lle sekä Somis Enterprises Oy:lle, joka tarjoaa Someturva-palvelua.[11]

Kesäkuun kyberturvallisuuden yleiskuva

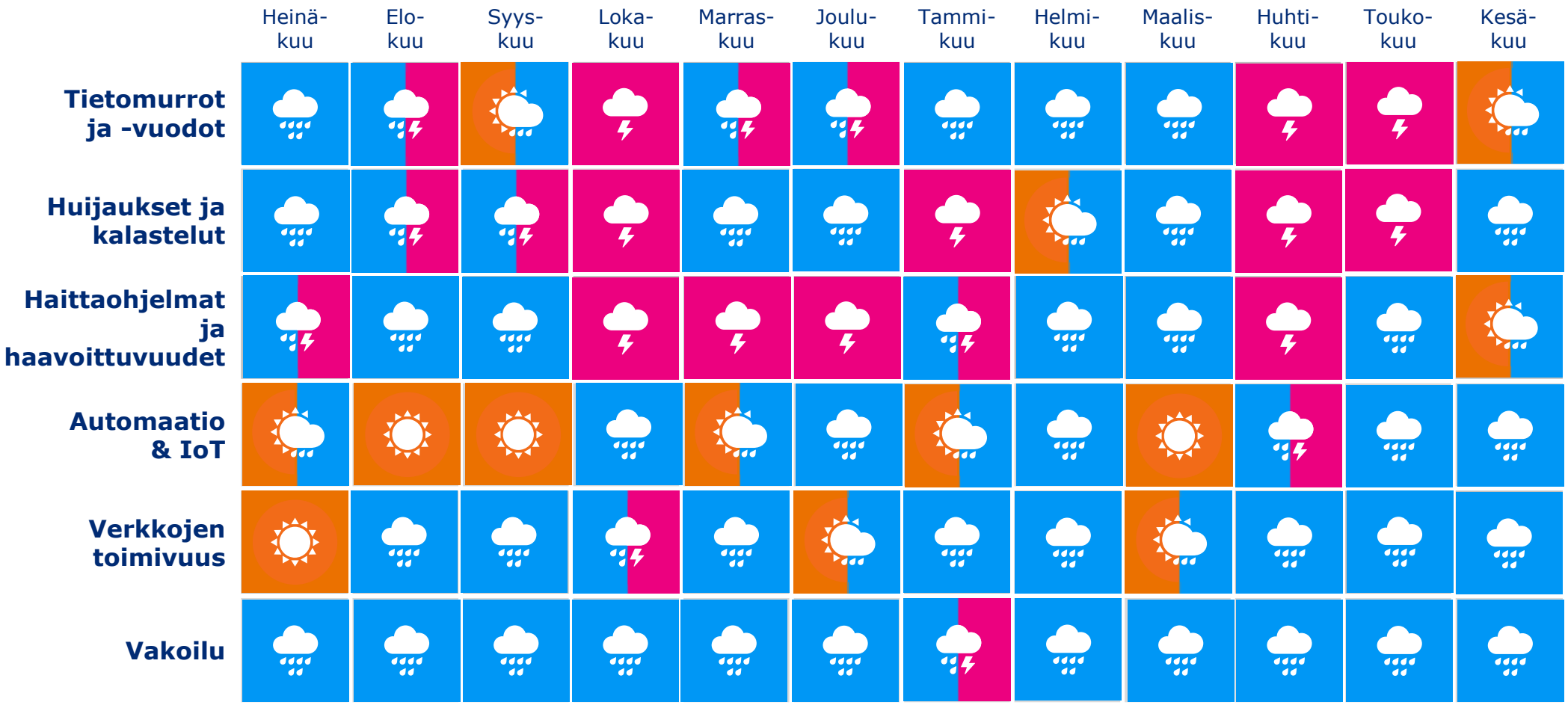
- Konsulttiyhtiön järjestelmien kautta tehtiin keväällä kymmeniä tuhansia perusteettomia hakuja esimerkiksi viranomaisten rekistereihin. Hyökkääjän epäillään tehneen haut autokorjaamon ja hinauspalvelun murrettujen käyttäjätunnusten avulla.
  - Kyseessä on niin kutsuttu toimitusketjuhyökkäys.
  - Toimitusketjuhyökkäyksen havainnointi ja hallinta ovat tärkeitä paitsi oman toiminnan jatkuvuuden kannalta, myös koska niillä on suuri merkitys organisaation maineelle ja luottamukselle verkostossa. Toimitusketjuhyökkäyksen uhrina ovat sekä toimittaja että asiakas. Tilanteen hallinta vaatii usein avoimuutta ja yhteistyötä osapuolilta.
  - Kalastelua voidaan hyödyntää toimitusketjuhyökkäysten tekemiseen.
- Kyberturvallisuuskeskukselle on viime aikoina tehty useita ilmoituksia erilaisista organisaatioihin kohdistuvista Microsoft 365 -käyttäjätilien kalasteluista. Osa kalasteluista on johtanut sähköpostitilin tietomurtoon.
  - Kalastelua tehdään erilaisilla, usein ajankohtaisilla teemoilla. Joskus kalastelussa voidaan hyödyntää jopa aiheita, joihin liittyen kohde odottaa yhteydenottoa, jolloin kalastelun tunnistaminen vaatii erityistä valppautta.
  - Tutustu ohjeeseemme Toimi näin Microsoft 365 –tilimurron sattuessa.[12]

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

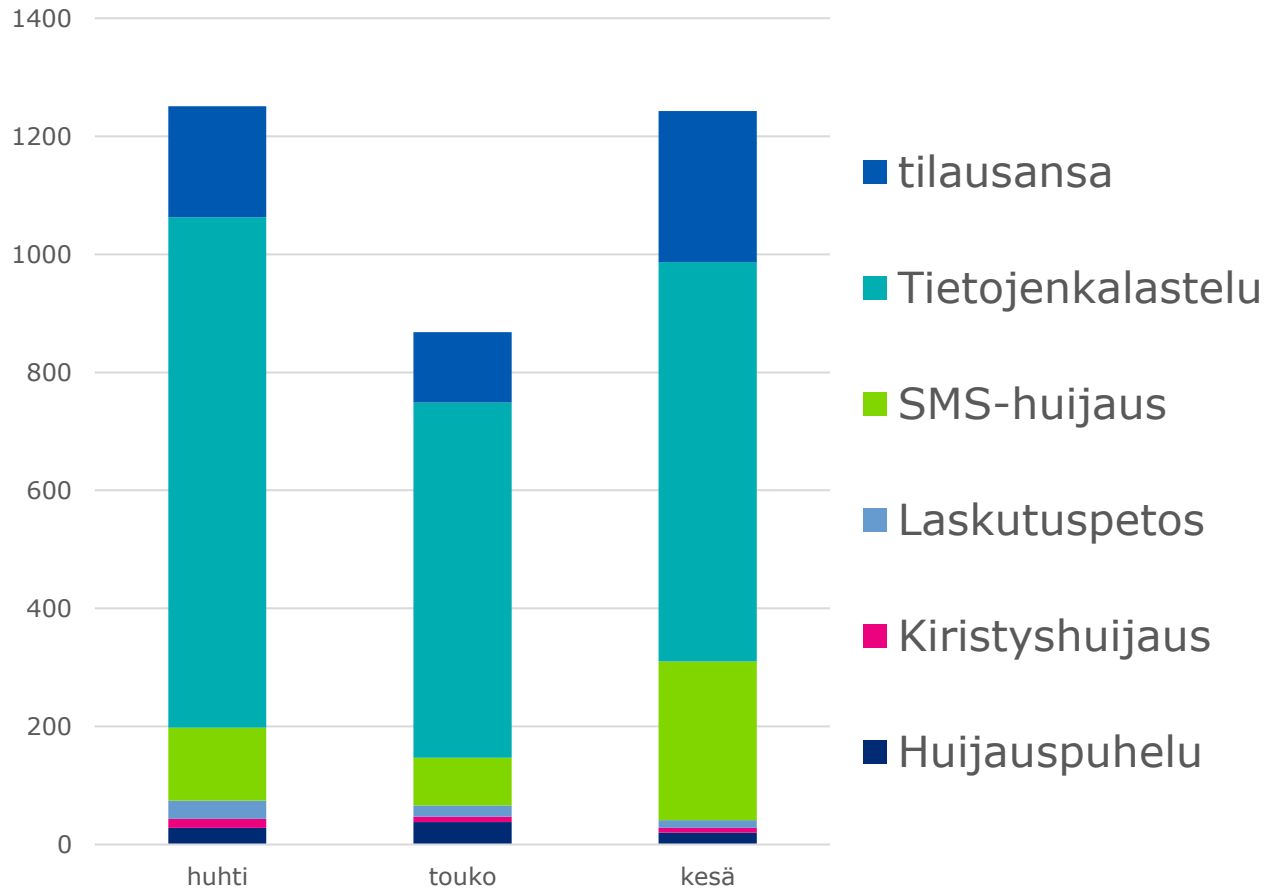


Käsiteltyjä huijaustapauksia
Q2/2024

3 kk

Vuoden 2024 toisen neljänneksen ilmiöitä ovat:

- Toukokuun tilastomerkintöjen notkahdukseen voi vaikuttaa uuden tilastointijärjestelmän käyttöönotto. Kesäkuussa tapahtumia kuitenkin on rekisteröity entiseen tapaan.
- Huijausviestejä tehtaillaan tutuista teemoista entistä enemmän tekstiviesteinä: veronpalautukset, kuriirihuijaukset, sakkohuijaukset ja pankkitunnuskalastelut näkyvät määrissä eniten.

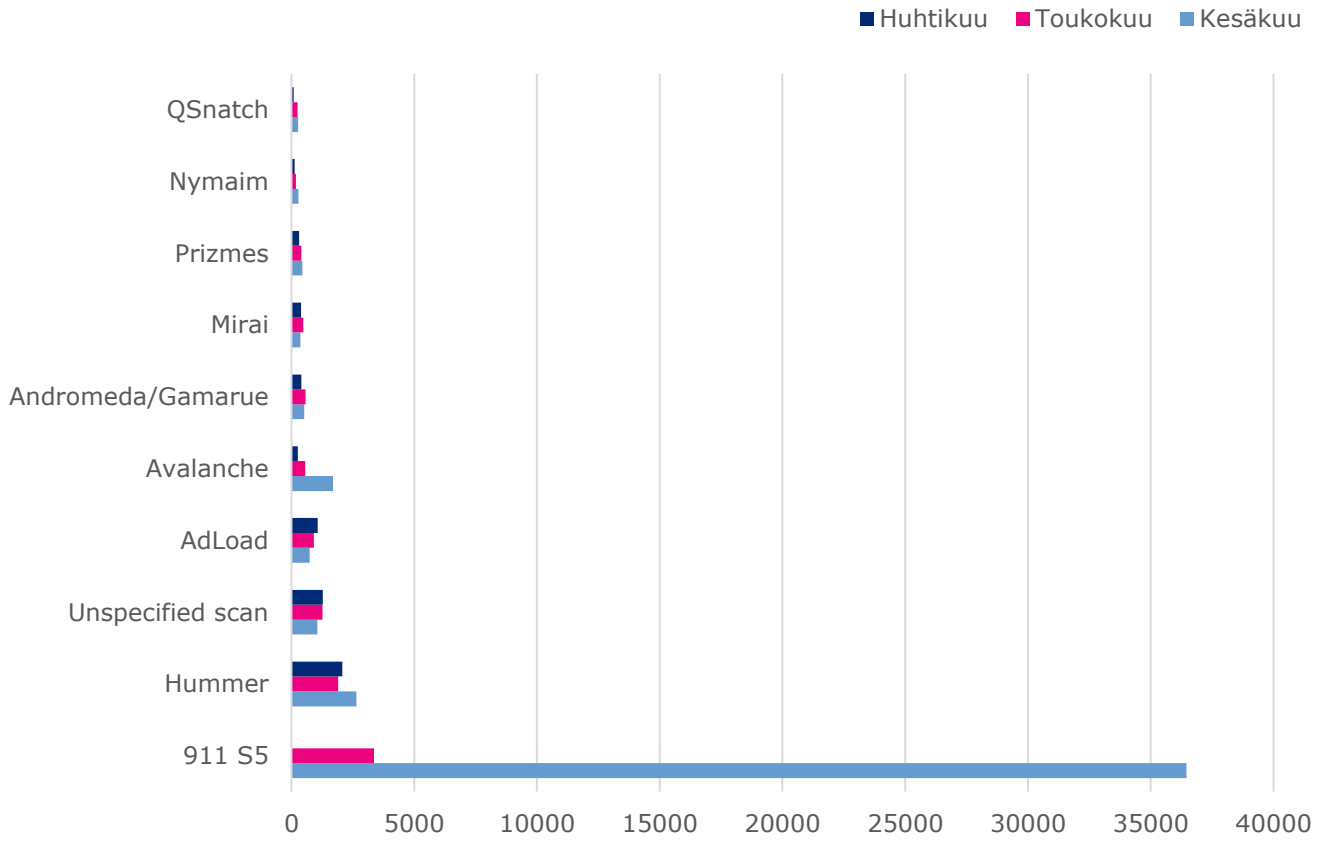


Autoreporterin haittaohjelmahavainnot

3 kk

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.

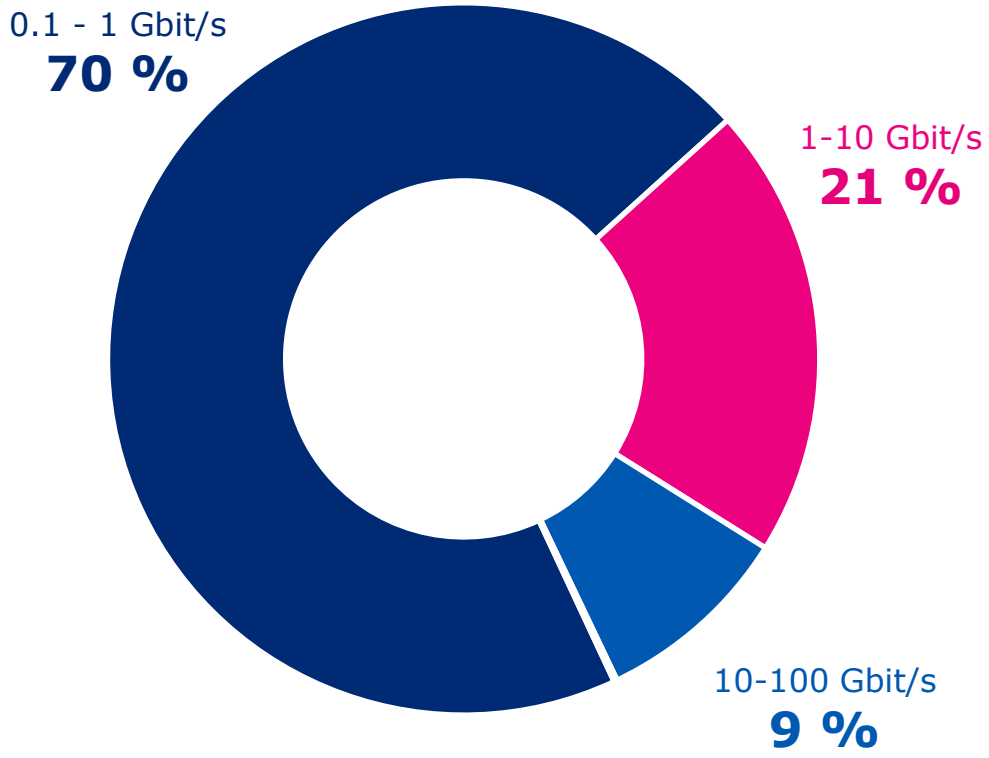
Tilastossa kerromme **10 yleisintä ja nimettyä** haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyber-turvallisuuskeskuksen verkkosivuilla



Palvelunestohyökkäysten tunnuslukuja
Q2/2024

3 kk

- **100 Gbit/s** oli suurin Suomessa nähty palvelunestohyökkäys Q2/2024.
- Noin 79% 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 organisaatioihin kohdistui tietomurtoja ja niiden yrityksiä. Myös erilaisista M365-teemaisista tietojenkalasteluista saatiin ilmoituksia.
Energia			Palvelunestohyökkäyksiä ja VPN-ratkaisuihin kohdistuneita tietomurtojen yrityksiä tapahtui edelleen. Sähköalan kyberturvallisuutta koskeva EU:n verkkosääntö (NCCS) tuli voimaan kesäkuussa, ja sitä sovelletaan asteittain.[13]
Finanssi			Pankkitunnusten kalastelu- ja huijauskampanjat jatkuivat eri pankkien nimissä. Loma-aikana korostuvat taloushallintoon kohdistuvat laskutushuijaukset. Erityisesti M365-kalastelussa kasvua.
Kemian-teollisuus			Onnistuneita M365 tietomurtoja, joita on pyritty hyödyntämään esimerkiksi laskutushuijausten yrityksissä. Kyberturvallisuuskeskuksen tiedossa ei ole onnistuneita laskutushuijauksia menneen kuluneen kvartaalin aikana. Osa M365-kalastelusta vaikuttaa kohdennetulta, esimerkiksi kohdeorganisaation tiettyyn kehitysprojektiin liittyen.
Logistiikka ja liikenne			Kvartaalin aikana havaittu runsaasti tietojenkalastelua mm. paketti- ja saapuva lähetys -teemalla. Toimialaan on kohdistunut palvelunestohyökkäyksiä Suomessa ja maailmalla mm. eri toimijoiden julkisia verkkosivuja kohtaan. Kiristyshaittaohjelmat ovat vaivanneet toimialaa maailmalla, ja erityinen piikki tässä hyökkäystyypissä on ollut havaittavissa toukokuun aikana.
Valtionhallinto			Alkuvuoteen verrattuna valtionhallintoon kohdistuvat palvelunestohyökkäykset vähenivät. Organisaatioiden nimissä on tehty kalastelua, ja ne ovat itse olleet kalastelun kohteena. Vakavia, useisiin tietomurtoihin johtaneita kampanjoita ei kuitenkaan ole tarkastelujaksolla nähty.
Media			Tarkastelujakson jälkimmäisellä puoliskolla muutama media-alan organisaatio joutui palvelunestohyökkäysten kohteeksi.
SOTE			Maailmalla terveydenhuoltosektorille on kohdistunut merkittäviä kyberturvallisuuspoikkeamia, joilla voi olla vaikutuksia monikansallisten yritysten globaaleille arvoketjuille. Viime aikoina on myös uutisoitu Suomessa terveysasemille tehdyistä tunkeutumisyrityksistä, joten fyysinen turvallisuus ja kulunvalvontakäytännöt on syytä huomioida kyberturvallisuuden lisäksi.
Vesihuolto			Mediassa uutisoitiin fyysisistä murtautumisista ja niiden yrityksistä vesihuoltolaitoksien erilaisiin tiloihin. Kyberpoikkeamailmoitukset pysyivät kuitenkin normaalilla tasolla. Lukituksen parantaminen ja valvonnan tehostaminen auttavat fyysisen murron riskin ja sen vaikutusten pienentämisessä.[8]
Kunnat			Kuntiin on kohdistunut jonkin verran kalastelua, jonka seurauksena tilejä on saatu murrettua ja murretuilta tileiltä lähetettyä kalasteluviestejä eteenpäin. Kuntaorganisaatioiden käyttäjätunnuksia ja salasanoja saatu kaapattua botnet-operaatioiden yhteydessä.

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:
Sääntely ulottuu uusiin teknologioihin ja uusille toimialoille 2020-luvulla

Lainsäädännön merkitys kyberturvallisuudelle on oleellinen. 2020-luvulla lainsäädäntöä ja sääntelyä kehitetään pitkäjänteisesti, jotta se vastaisi kybertoimintaympäristön muutoksiin paremmin. Kyberturvallisuus on poikkileikkaava teema, ja siksi lainsäädännön kehitys ei ole aina yksikertaista.

- Lainsäädäntöhankkeiden tarkoituksena on muun muassa selkeyttää digitaalisten palveluiden pelisääntöjä, luoda tekoälystä, älylaitteista ja datan hallinnasta turvallisempaa, sekä tarkentaa eri toimijoiden tietoturvavelvollisuuksia.
- Yritysten ja muiden organisaatioiden on hyvä varautua sääntelyn tiukkenemiseen ja muutoksiin. Tämä on tarpeen, sillä kyberhyökkäykset ovat yhä yleisempiä ja monimutkaisempia.
- Lainsäädäntö auttaa suojaamaan yksityisiä ja liike-elämän tietoja sekä parantamaan yleistä tietoturvaa ja toimivuutta.
- Sääntelyllä luodaan ja suunnitellaan aktiivisesti uusia digitaalisen turvallisuuden toimijoita EU:n pelikentälle. Hyvästä tietoturvasta on mahdollista tehdä kilpailuetu.

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

- Uudistettu kyberturvallisuusstrategia lausuntokierrokselle.
  - Liikenne- ja viestintäministeriö pyytää lausuntoja Suomen uudistetusta kyberturvallisuusstrategiasta vuosille 2024–2035.[14]
  - Lausunnot pyydetään antamaan lausuntopalvelussa 9.8.2024 mennessä.[15]
  - Edellinen kyberturvallisuusstrategia julkaistiin vuonna 2019, jonka jälkeen Suomen ja Euroopan turvallisuusympäristö on muuttunut merkittävästi muun muassa koronapandemian, Venäjän hyökkäyssodan ja Suomen Nato-jäsenyyden myötä.
  - Strategian neljä osa-aluetta ovat: 1) osaava, innovatiivinen ja kokeileva kyberekosysteemi; 2) vahva yhteiskunnan kyberresilienssi ja toimintavarmuus; 3) vankka kansallinen ja kansainvälinen yhteistoimintamalli sekä 4) oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti.
  - Jokaiselle osa-alueelle on muodostettu omat strategiset tavoitteet, joiden pohjalta laaditaan yhteiset konkreettiset kehittämistoimet.

Oikeudelliset asiat

- Euroopan komission täytäntöönpanosäädös NIS2-direktiivin velvoitteiden täsmentämiseksi tiettyjen toimijoiden osalta lausuntokierrokselle.
  - Euroopan komissio pyytää 25.7. mennessä lausuntoja luonnoksesta täytäntöönpanosäädökseksi, jolla täsmennetään NIS2-direktiivin 21 ja 23 artiklan velvoitteita tiettyjen digitaalisen infrastruktuurin toimijoiden osalta.[16]
  - Säännös koskee seuraavia toimijoita: DNS-palveluntarjoajat, aluetunnusrekisterit, pilvipalvelujen tarjoajat, datakeskuspalvelujen tarjoajat, sisällönjakeluverkkojen tarjoajat, hallintapalvelun tarjoajat, tietoturvapalvelun tarjoajat, verkossa toimivien markkinapaikkojen tarjoajat, verkossa toimivien hakukoneiden tarjoajat, verkkoyhteisöalustojen tarjoajat sekä luottamuspalvelujen tarjoajat.
  - Säännöksellä täsmennetään direktiivin 21 artiklan mukaisia riskienhallintavelvoitteita sekä sitä, milloin 23 artiklan mukainen poikkeama on katsottava merkittäväksi.

Oikeudelliset asiat

- Uudistettu kansallinen avaruusstrategia lausuntokierrokselle.
  - Työ- ja elinkeinoministeriö pyytää lausuntoja uudistetusta kansallisesta avaruusstrategiasta vuosille 2024–2030.[17]
  - Lausunnot pyydetään antamaan lausuntopalvelussa 31.8.2024 mennessä.[18]
  - Edellinen kansallinen avaruusstrategia julkaistiin vuonna 2018. Uudistetussa avaruusstrategiassa määritetään Visio 2030 "Suomi 2030: Maailman edistynein avaruustoimintaympäristö, josta hyötyy koko yhteiskunta".
  - Tavoitteet ja toimenpiteet vision saavuttamiseksi on määritetty neljän päämäärän kautta: 1) Hyödyntäminen, 2) Toimintaympäristö, 3) Toimintakyky, 4) Kansainvälinen yhteistyö. Kunkin päämäärän tavoitteissa ja toimenpiteissä huomioidaan eri sektoreiden toimijat.
  - Avaruusstrategiassa painotetaan avaruuspalveluiden hyödyntämistä yhteiskunnan eri sektoreilla. Avaruuspalveluiden avulla pystytään sujuvoittamaan monia arkisia toimintoja ja nostamaan tuottavuutta. Niitä hyödyntämällä voidaan myös parantaa yhteiskunnan puolustuskykyä ja turvallisuutta. Avaruuspalveluiden rooli osana kriittistä infrastruktuuria on huomioitava myös huoltovarmuussuunnittelussa.

Oikeudelliset asiat

- Euroopan komissio on julkaissut sähköalan kyberturvallisuutta koskevan EU:n verkkosäännön (NCCS).[13] [19]
  - Verkkosääntö tuli voimaan 13.6.2024, ja sitä sovelletaan asteittain eri menetelmien ja suunnitelmien laatimisen myötä.
  - Uusi kyberturvallisuusverkkosääntö täydentää EU:n sähkökauppa-asetusta asettamalla toimialakohtaiset kyberturvallisuuden huomioivat säännöt rajat ylittävälle sähkönsiirrolle. Verkkosääntö sisältää säännöt kyberturvallisuuden riskienhallinnasta, yhteisistä kyberturvallisuuden vähimmäisvaatimuksista, suunnittelusta, seurannasta, raportoinnista ja kriisinhallinnasta.
  - Verkkosäännön soveltamisalaan kuuluvat muun muassa sähköalan yritykset ja kriittiset tieto- ja viestintätekniikan palveluntarjoajat. Lopullinen toimijakohtainen soveltamisala määräytyy myöhemmin määriteltävien kriteerien kautta. Energiavirasto ilmoittaa kaikille toimijoille suoraan viimeistään 13.3.2025, että heidät on tunnistettu soveltamisalaan kuuluvaksi ehdokkaaksi.
  - Verkkosäännön on tarkoitus täydentää NIS2-direktiivissä säädettyjä verkko- ja tietojärjestelmien turvallisuutta koskevia yleisiä sääntöjä.

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) Ajankohtaiset EU-rahoitusmahdollisuudet kyberturvallisuusalalle https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ajankohtaiset-eu-rahoitusmahdollisuudet-kyberturvallisuusalalle
2) Kyberturvallisuuskeskuksen tapahtumat https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tapahtumat
3) Mystery miscreant remotely bricked 600,000 SOHO routers with malicious firmware update https://www.theregister.com/2024/05/31/pumoking_eclipse_remote_router_attack/
4) Vanhentuvat kaapelimodeemit https://elisa.fi/asiakaspalvelu/laitteet/vanha-kaapelimodeemi/
5) CVE-2024-38373 https://nvd.nist.gov/vuln/detail/CVE-2024-38373
6) TeamViewer links corporate cyberattack to Russian state hackers https://www.bleepingcomputer.com/news/security/teamviewer-links-corporate-cyberattack-to-russian-state-hackers/
7) Microsoft informs customers that Russian hackers spied on emails https://www.reuters.com/technology/cybersecurity/microsoft-tells-clients-russian-hackers-viewed-emails-bloomberg-news-reports-2024-06-27

Lähdeluettelo

8) Kyberturvallisuuskeskuksen viikkokatsaus - 25/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-252024#72391-1
9) Kyberturvallisuuskeskuksen viikkokatsaus - 24/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-242024
10) Verkkoturvallisuuden neuvottelukunta kolmannelle toimikaudelle https://lvm.fi/-/verkkoturvallisuuden-neuvottelukunta-kolmannelle-toimikaudelle
11) Uusia luotettuja ilmoittajia suojelemaan lapsia ja nuoria laittomalta sisällöltä internetissä https://traficom.fi/fi/ajankohtaista/uusia-luotettuja-ilmoittajia-suojelemaan-lapsia-ja-nuoria-laittomalta-sisallolta
12) Toimi näin Microsoft 365 -tilin tietomurron sattuessa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/toimi-nain-microsoft-365-tilin-tietomurron-sattuessa
13) Uusi verkkosääntö parantaa rajat ylittävän sähkönsiirron kyberturvallisuutta https://energiavirasto.fi/-/uusi-verkkosaanto-parantaa-rajat-ylittavan-sahkonsiirron-kyberturvallisuutta

Lähdeluettelo

14) Uudistettu kyberturvallisuusstrategia lausuntokierrokselle https://lvm.fi/-/uudistettu-kyberturvallisuusstrategia-lausuntokierrokselle
15) Lausuntopyyntö Suomen kyberturvallisuusstrategiasta https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=6a5bade7-849d-4586-bdc2-c146c40352dc
16) Cybersecurity risk management & reporting obligations for digital infrastructure, providers and ICT service managers https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en
17) Luonnos kansallisesta avaruusstrategiasta lausuntokierrokselle https://tem.fi/-/luonnos-kansallisesta-avaruusstrategiasta-lausuntokierrokselle
18) Kansallinen avaruusstrategia 2024-2030 https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=f988a1e7-7aa9-411e-a3bb-783231e6fe73
19) Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows http://data.europa.eu/eli/reg_del/2024/1366/oj