TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Joulukuu 2023

#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

Joulukuussa yleisissä viestintäpalveluissa ei ollut yhtään toimivuushäiriötä.

Joulukuussa meille ilmoitettiin kuusi Akira-kiristyshaittaohjelmahavaintoa.

Tammikuussa Kyberturvallisuuskeskus on mukana järjestämässä kahta webinaaria: Kyberala murroksessa -seminaaria 23.1.2024, sekä alkuvuodesta 2024 auki olevien kyberturvallisuusrahoitushakujen esittelyn webinaaria 18.1.2024. Vielä ehtii ilmoittautua mukaan![1, 2]

Kybersää joulukuu 2023

Tietomurrot ja -vuodot

- Tietomurtojen ilmoitusmäärä laski vuoden 2023 mediaanitasolle, mutta seurauksiltaan vakavien tietomurtojen määrä kasvoi joulukuussa.
- Järjestelmiin ja luottamukselliseen tietoon oli useissa tapauksissa päästy murrettujen pääkäyttäjätunnusten avulla.

Huijaukset ja kalastelut

- Heti joulukuun aluksi nähtiin tuhansittain OmaVeron nimissä tehtyjä huijausviestejä, joissa luvattiin veronpalautuksia.
- Whatsapp-viestipalvelussa liikkui paljon työtarjoushuijauksia.
- Allekirjoituspalveluita käytettiin verukkeena tietojenkalasteluun.

Haittaohjelmat ja haavoittuvuudet

- Poikkeuksellisen paljon ilmoituksia Akira-kiristyshaittaohjelmasta (6kpl joulukuussa).
- Atlassianin tuotteista korjattu läjä mielivaltaisen koodin etänä suorittamisen mahdollistavia haavoittuvuuksia.
- Ivantin VPN-tuotteessa kaksi hyväksikäytettyä nollapäivähaavoittuvuutta.[5]

Automaatio ja IoT

- Ukrainan turvallisuuspalvelu SBU kertoi löytäneensä Ukrainasta murrettuja IoT-videokameroita, joita on käytetty sotilaallisiin tiedustelutarkoituksiin.[3, 4]

Verkkojen toimivuus

- Joulukuussa yleisissä viestintäpalveluissa ei ollut yhtään toimivuushäiriötä.
- Palvelunestohyökkäyksiä raportoitiin eri sektoreilta. Suurimmalla osalla ei vaikutuksia palveluiden toimintaan.
- HSL kertoi julkisesti uudenvuoden aattona tapahtuneista palvelunestohyökkäyksistä, jotka vaikuttivat palveluihin.

Vakoilu

- Julkisuudessa Venäjään yhdistetty Callisto-ryhmä on pyrkinyt vakoilemaan kohteita länsimaissa lähettämällä kohdistettuja kalasteluviestejä henkilöiden yksityiskäytössä oleviin sähköposteihin. Tällä kierretään organisaatioiden käyttämiä tietoturvakontrolleja.
- Callisto tunnetaan myös mm. nimillä Star Blizzard ja Coldriver.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Monivaiheinen tunnistautuminen suojaa käyttäjätunnuksia myös verkkoinfrastruktuurissa ja voi ehkäistä esimerkiksi brute force -hyökkäyksen onnistumisen. Tutustu monivaiheisen tunnistautumisen ohjeeseemme.[6]

Kyberturvallisuuskeskus on avannut haettavaksi rahoitustukea modernien tietoturvaratkaisujen ja -innovaatioiden käyttöönottoon. Rahoitustukea voivat hakea mikroyritykset sekä pienet ja keskisuuret yritykset. Haku on auki 1.3.2024 klo 16:15 asti.[7]

Traficom laatii suositusta NIS2-direktiivin kyberturvallisuuden riskienhallinnan toimenpiteistä.[8]

Joulukuun kyberturvallisuuden yleiskuva

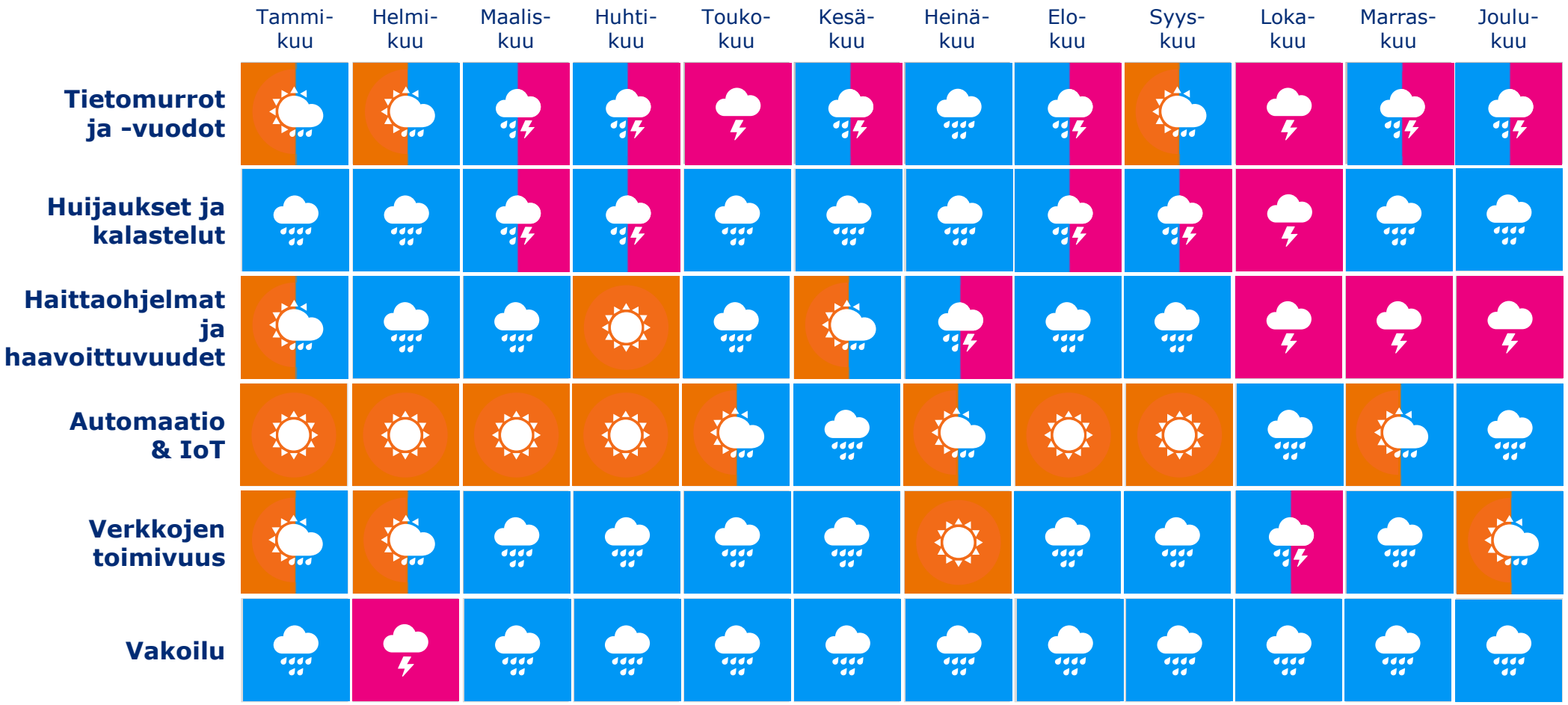
- Tunnettujen haavoittuvuuksien hyödyntäminen tietomurroissa jatkui, mikä näkyi meille ilmoitettujen kiristyshaittaohjelmatapausten määrässä
  - Valtaosa ilmoituksista koski Akira-kiristyshaittaohjelmaa. Akiran on havaittu hyödyntävän edelleen syksyistä Ciscon verkkolaitehaavoittuvuutta (CVE-2023- 20269), joka mahdollistaa *brute force* -hyökkäyksen. Hyökkäyksen onnistumisen voi estää ottamalla käyttöön monivaiheisen tunnistautumisen Ciscon VPN-palvelussa.
- Tammikuun alussa Ivanti julkaisi kaksi kriittistä haavoittuvuutta, jotka vaikuttavat sen kahteen eri tuotteeseen. Haavoittuvuuksia on jo hyväksikäytetty. Lukuisten kotimaisten organisaatioiden on syytä reagoida haavoittuvuuksiin välittömästi.[5]
  - Kyberturvallisuuskeskuksen tekemien kartoituksien perusteella haavoittuvia palvelimia on Suomessa useita satoja. Haavoittuvuuksia korjaavia ohjelmistopäivityksiä ei toistaiseksi ole saatavilla, mutta haavoittuvuuksien hyväksikäyttöä estävät pikakorjaukset on julkaistu.[5]
  - Vaikka haavoittuvuuksien vaikutuksia rajoittavat toimenpiteet ottaisi käyttöön, on silti syytä analysoida järjestelmä mahdollisesti jo tapahtuneen tietomurron varalta.[5]
  - Tietoturvayhtiö Volexityn mukaan haavoittuvuuksien hyväksikäyttöä on havaittu joulukuun 2023 alkupuolelta lähtien.[5]

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

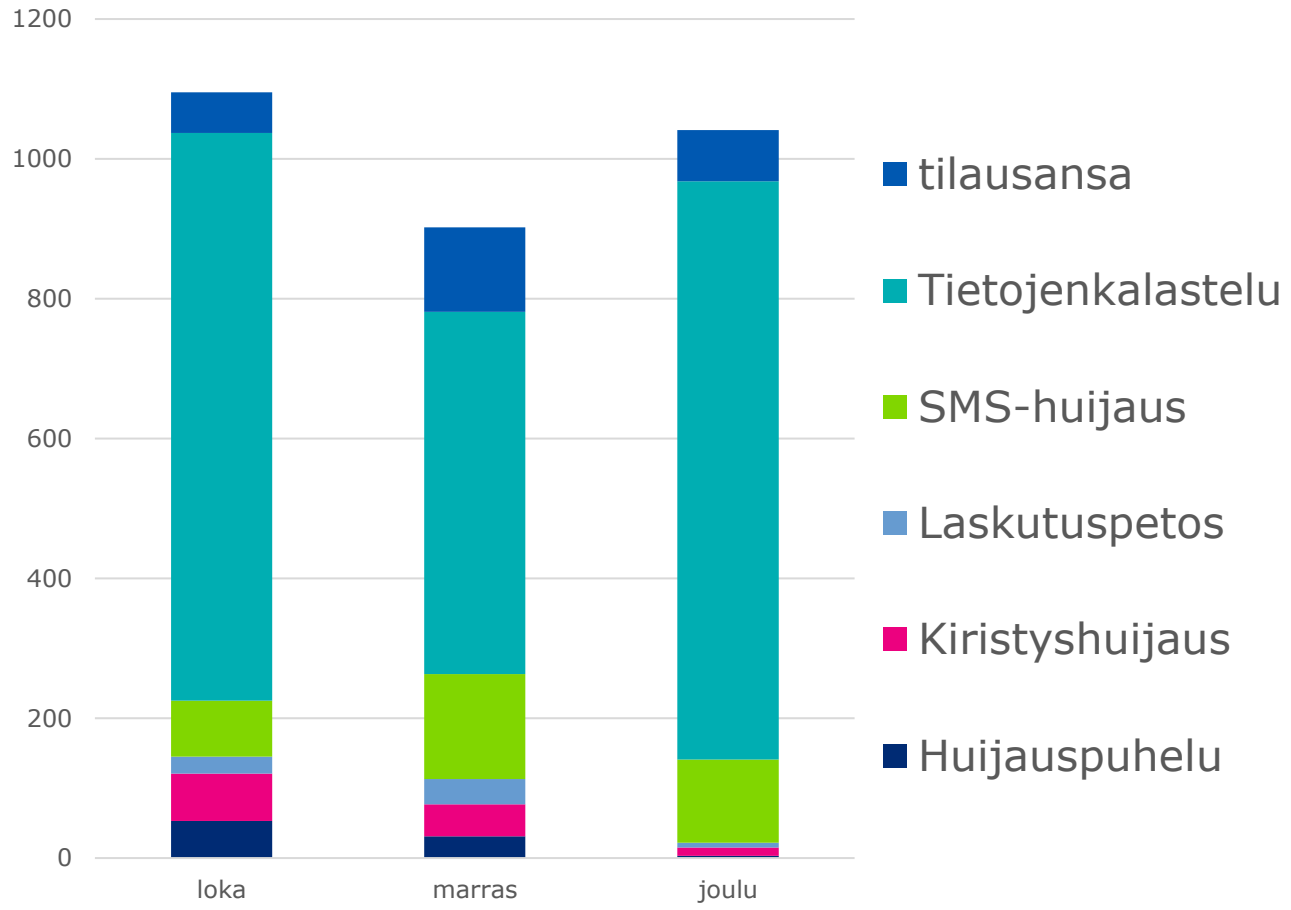


Käsiteltyjä huijaustapauksia
Q4/2023

3 kk

Vuoden 2023 viimeisen neljänneksen ilmiöitä ovat:

- Suomalaisista puhelinnumeroista soitettujen huijauspuheluiden määrä on romahtanut.
- Tekstiviestien käyttö huijauksiin on tullut jäädäkseen.
- Tietojenkalastelu ja erilaiset verkkokauppahuijaukset lisääntyivät vuodenvaihteen sesonkien lähestyessä.

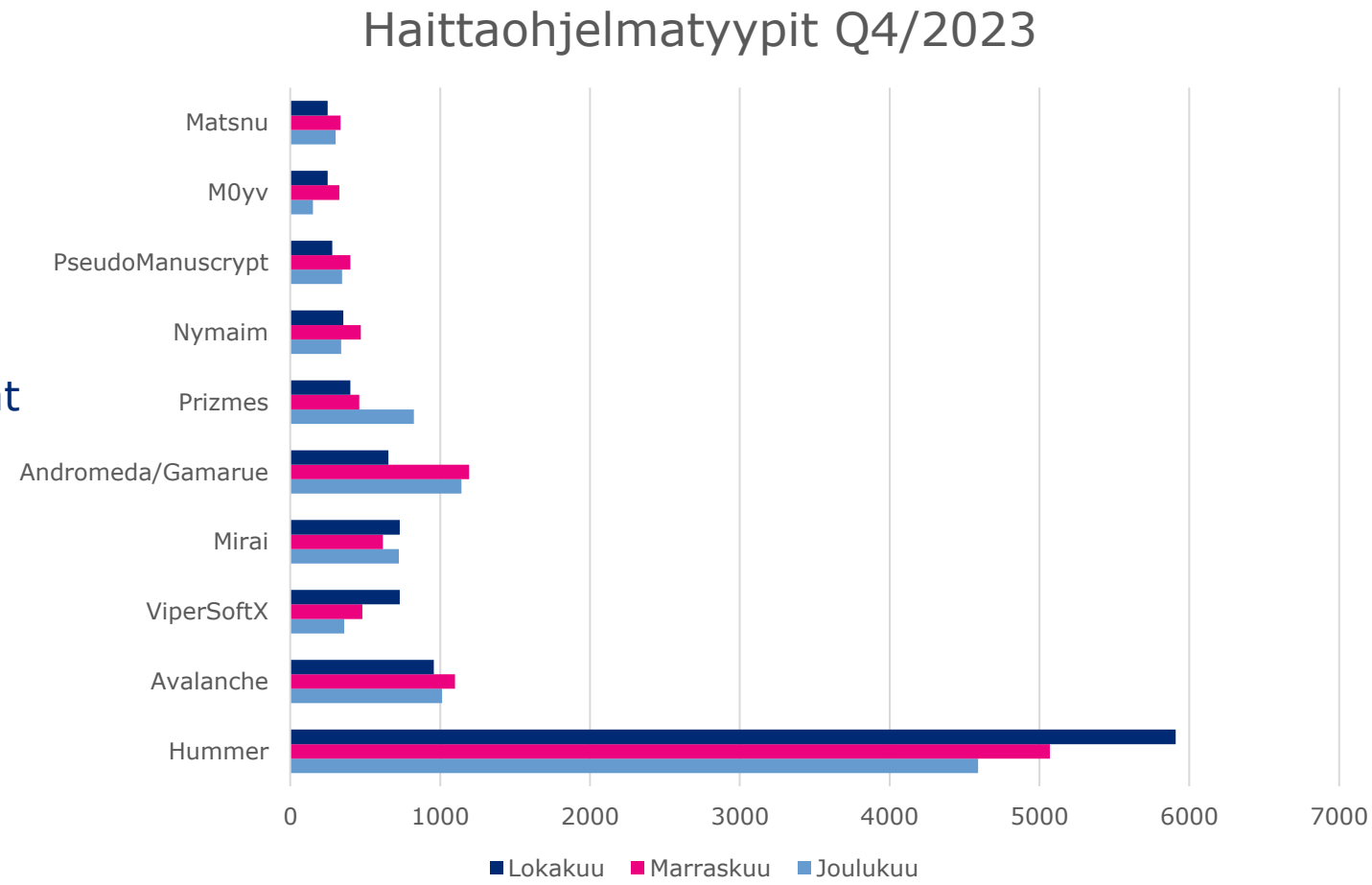


Autoreporterin haittaohjelmahavainnot

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.

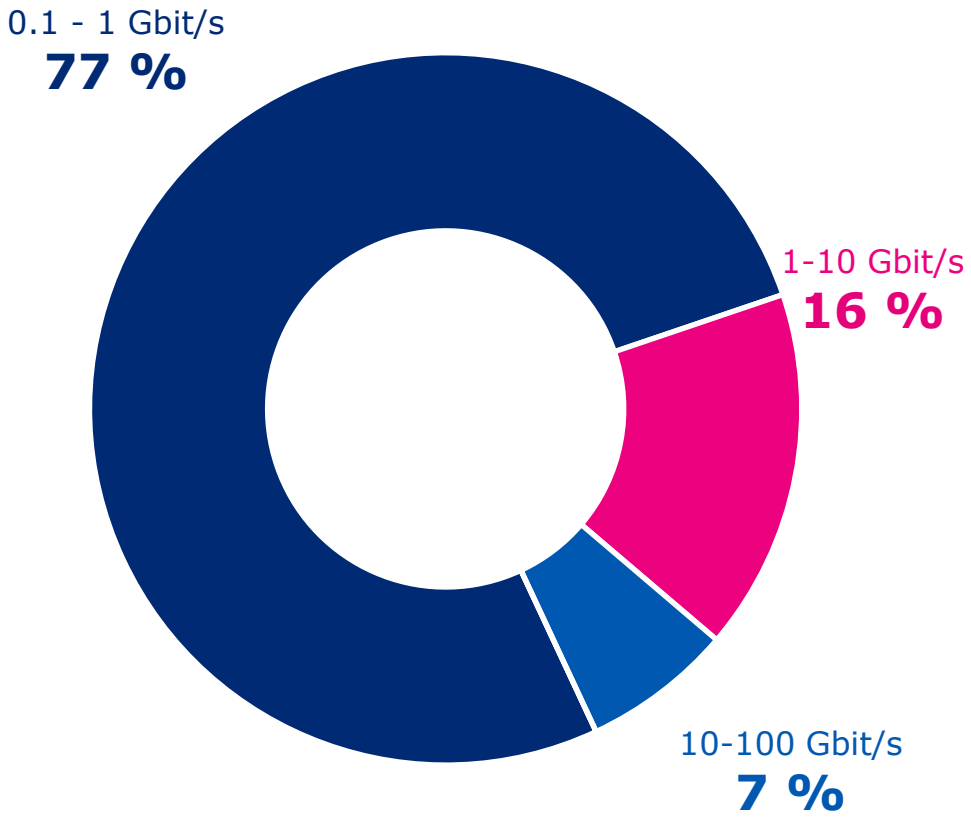
Tilastossa kerromme **10 yleisintä ja nimettyä** haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyber-turvallisuuskeskuksen verkkosivuilla



3 kk

Palvelunestohyökkäysten tunnuslukuja
Q4/2023

- **78.9 Gbit/s** oli suurin Suomessa nähty palvelunestohyökkäys Q4/2023.
- Noin 75% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Toimialakohtaiset havainnot

3 kk

	Trendi 3kk	Edeltävä 3kk	
Elintarvike			Poikkeamailmoitusten määrä kasvoi hieman hiljaisen kesän jälkeen, mutta oli edelleen suhteellisen pieni. Kahdeksasta vuosineljänneksen aikana tulleesta ilmoituksesta peräti kaksi koski kohdennettuja kiristyshaittaohjelmahyökkäyksiä.
Energia			Ilmoitettujen poikkeamien määrässä ei suuria muutoksia. Joitakin tietomurtoja, joissa syinä mm. liian hitaasti päivitetyt Internetiin näkyvillä olevat järjestelmät.
Finanssi			Pankkitunnusten kalastelu jatkuu eri muodoissaan.
Teollisuus			Ilmoitettujen poikkeamien määrässä ei muutoksia, mutta etenkin tietomurrot lisääntyivät. Mukana oli myös joitakin kiristyshaittaohjelmatapauksia.
Logistiikka ja liikenne			Palvelunestohyökkäykset toimialaa kohtaan jatkuvat. QR-koodimuotoista tietojenkalastelua on ollut liikkeellä. Lisäksi laskutushuijaukset ja kiristyshaittaohjelmat ovat vaivanneet toimialaa.
Valtionhallinto			Tietomurtoihin tähtäävä tietojenkalastelu on ollut aktiivista ja etenkin lokakuussa nähty Microsoft 365 –tileihin kohdistettu kampanja edellytti reagointia myös valtionhallinnossa. Valtionhallinnon organisaatioita on edelleen ollut venäjämielisten haktivistien palvelunestohyökkäyksien kohteena.
Media			Ilmoitetuissa poikkeamissa ei merkittäviä muutoksia.
SOTE			Lokakuussa levinnyt tietomurtoaalto kosketti laajasti sote-sektoria ja johti lukuisiin käyttäjätilien murtoihin ja kalastelun leviämiseen. Hyvinvointialueiden tietotekniset järjestelmät ovat monenkirjavia ja niiden turvallisuuden hallinta tuottaa päivittäistä päänvaivaa ICT-henkilöstölle.
Vesihuolto			Ilmoitettujen poikkeamien määrä on kasvanut. Mukana oli esimerkiksi websivujen lomakkeiden väärinkäyttötapauksia. Internetiin näkyvien automaatioprosessien ohjauksessa käytettyihin laitteisiin kohdistuneista tietomurroista uutisoitiin laajasti maailmalla.
Kunnat			Lokakuussa levinnyt tietomurtoaalto kosketti laajasti kuntasektoria ja johti lukuisiin tilimurtoihin ja kalastelun leviämiseen. Lokakuussa myös erästä kuntaa vastaan tehtiin vakava kyberhyökkäys.

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

Pula puolijohteista

Tekoälyn käyttö kyberrikolli-suudessa

Suurvalta-kilpailun vaikutukset sääntelyyn

Älylaitteiden elinkaari ja kierrätys

Kyber-vakoilun ja rikollisuuden rajojen hämärtymi-nen

IoT

6G

Kiristyshaitta-ohjelmien käyttö murroksessa

Teknologia osana suurvalta-kilpailua

Sääntelyn ulottuminen uusille toimialoille

Osallistu-minen digitaalisessa ympäristössä

Pitkän aikavälin kybersää:
Sääntelyn ulottuminen uusille toimialoille

Tietoturvaan liittyvää sääntelyä on tulossa runsaasti tulevaisuudessa. Organisaatioiden on hyvä ottaa muuttuva sääntely huomioon ja varautua siihen mahdollisimman hyvissä ajoin etukäteen.

- Lähiaikoina voimaan on astumassa esimerkiksi NIS2-direktiivi, jonka odotetaan astuvan voimaan Suomessa syksyllä 2024. Direktiivin tavoitteena on kyberturvallisuuden yhteisen tason varmistaminen kaikkialla Euroopan unionissa.[9] Direktiivissä soveltamisalaa on laajennettu kattamaan uusia toimialoja, kuten elintarvikealaa sekä jätehuoltoa.[10]
- Muita lähitulevaisuuden EU-säädöksiä ovat esimerkiksi CER-direktiivi, kyberkestävyyssäädös, kybersolidaarisuussäädös sekä kyberturvallisuusasetus:
  - CER-direktiivillä vahvistetaan kriittisen infrastruktuurin kriisin- ja häiriönsietokykyä.
  - EU:n kyberkestävyyssäädös (CRA) pyrkii turvaamaan älylaitteiden riittävän tietoturvan tason. Lisäksi säädöksellä halutaan parantaa kuluttajien mahdollisuutta arvioida älylaitteiden tietoturvaa. Säädöksen tavoitteena on yhdenmukaistaa älylaitteiden markkinoille tuomisen säännöt.[11]
  - Kybersolidaarisuussäädös pyrkii vahvistamaan EU:n valmiuksia havaita merkittäviä tietoturvauhkia sekä uhkiin valmistautumista ja reagoimista.[12]
  - Kyberturvallisuusasetuksella luodaan EU:n laajuinen sertifiointikehys ICT-tuotteille, -palveluille ja -prosesseille.[13]
- Pidemmällä aikavälillä EU pyrkii säätelemään myös esimerkiksi tekoälyä. EU on jo ehdottanut tekoälyn oikeudellista kehystä, jolla on tarkoitus puuttua tekoälyn tuomiin riskeihin.[14]
- Lisäksi EU:ssa on valmistelussa monia eri digi- ja datasäädöksiä, joiden tarkoituksena on tehdä digitaalisesta toimintaympäristöstä mahdollisimman toimiva, turvallinen ja oikeudenmukainen.[15]

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

Digitaalisesta henkilöllisyystodistuksesta eurooppalaiseen lompakkosovellukseen.[16]

- Suomessa on valmisteltu digitaalista henkilöllisyystodistusta, jonka tarkoituksena on ollut rakentaa kännykkäsovelluksessa toimiva, passin tai henkilökortin kaltainen henkilöllisyyttä osoittava asiakirja.
- Suomen digitaalisen henkilöllisyystodistuksen valmistelun tarkoituksena oli, että sen olisi voinut laajentaa sopimaan eurooppalaisen lompakkosovelluksen vaatimuksiin. Kun sopu EU:n lompakkosovellusta koskevasta lainsäädännöstä on nyt saatu, päällekkäisen valmistelun sijaan painopiste siirrettiin suoraan eurooppalaisen lompakkosovelluksen toteuttamiseen.
- Digitaalista henkilöllisyystodistusta viedään nyt erillisen sovelluksen sijaan eteenpäin osana eurooppalaisen, eIDAS-asetuksen vaatimukset täyttävän lompakkosovelluksen kehittämistä.
- Mahdollisuus henkilöllisyyden sähköiseen osoittamiseen EU-maissa on edelleen tärkeä, mutta ei enää yksinään riittävä tavoite. Yhä useammin on tarve osoittaa sähköisesti myös muita henkilöön liittyviä tietoja, kuten tieto suoritetusta tutkinnosta, hankitusta ammattipätevyydestä tai voimassaolevasta ajo-oikeudesta.

Oikeudelliset asiat

EU digitaalisen identiteetin lompakko:[17]

- Kaikilla EU:n kansalaisilla, EU:ssa asuvilla henkilöillä ja EU:ssa toimivilla yrityksillä on oikeus saada käyttöönsä EU:n digitaalisen identiteetin lompakko, joka olisi hyväksyttävä kaikissa EU-maissa.
- Julkiset palvelut ja tietyt yksityiset palvelut (suuret alustat ja palvelut, joiden on lain mukaan käytettävä käyttäjien vahvaa todentamista, kuten Meta, Amazon, Apple ja Facebook) ovat velvollisia tunnustamaan EU:n digitaalisen identiteetin lompakot.
- Käyttäjät voivat käyttää sitä henkilöllisyytensä digitaaliseen todentamiseen kirjautuessaan sekä julkisiin että yksityisiin verkkopalveluihin kaikkialla EU:ssa.
- Mahdollisia käyttötilanteita ovat käyttöasioinnin lisäksi esim. verkkopankkiin kirjautuminen, maksutapahtuman käynnistäminen, lainan hakeminen, veroilmoituksen tekeminen ja yliopistoon ilmoittautuminen.
- Olennaista itsehallittava identiteetti, eli käyttäjä voi itse hallita mitä tietoja itsestään jakaa.
- Jäsenmaiden on saatettava EU:n digitaalisen identiteetin lompakko kansalaistensa käyttöön 24 kk sen jälkeen, kun on hyväksytty täytäntöönpanosäädökset, joissa vahvistetaan lompakkoa koskevat tekniset eritelmät. Täytäntöönpanosäädökset hyväksytään 6 ja 12 kuukautta asetuksen hyväksymisen jälkeen.

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) Osallistu alkuvuodesta 2024 auki olevien kyberturvallisuusrahoitushakujen esittelyn webinaariin 18.1.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/osallistu-alkuvuodesta-2024-auki-olevien-kyberturvallisuusrahoitushakujen-esittelyn
2) Kyberala murroksessa -seminaari 23.1.2024 https://tietoturvamerkki.fi/fi/kyberala-murroksessa-seminaari-2312024
3) SBU blocks surveillance cameras hacked by Russia to identify targets in Kyiv https://kyivindependent.com/sbu-blocks-surveillance-cameras-hacked-by-russians-to-spy-on-targets-in-kyiv/
4) Kremlin’s eye: Russian surveillance cameras spied on Ukraine for years https://euromaidanpress.com/2023/12/13/kremlins-eye-russian-surveillance-cameras-spied-on-ukraine-for-years/
5) Ivantin tuotteissa kriittisiä hyväksikäytettyjä haavoittuvuuksia https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_2/2024
6) Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Lähdeluettelo

7) Kansallisesti myöntämämme rahoitustuet https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/kansallinen-koordinointikeskus/kansallisesti-myontamamme-rahoitustuet
8) Traficom laatii suositusta NIS2-direktiivin kyberturvallisuuden riskienhallinnan toimenpiteistä https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-laatii-suositusta-nis2-direktiivin-kyberturvallisuuden-riskienhallinnan
9) Traficom laatii suositusta NIS2-direktiivin kyberturvallisuuden riskienhallinnan toimenpiteistä https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/traficom-laatii-suositusta-nis2-direktiivin-kyberturvallisuuden-riskienhallinnan
10) Kyberturvallisuusdirektiivi vahvistaa koko EU:n kyberturvallisuustasoa – kansallinen toimeenpanohanke käynnistyi https://lvm.fi/-/kyberturvallisuusdirektiivi-vahvistaa-koko-eu-n-kyberturvallisuustasoa-kansallinen-toimeenpanohanke-kaynnistyi-1903681
11) EU:n kyberresilienssisäädös https://digital-strategy.ec.europa.eu/fi/policies/cyber-resilience-act
12) Kyberturvallisuuteen liittyvää yhteisvastuuta koskeva EU:n säädös https://digital-strategy.ec.europa.eu/fi/policies/cyber-solidarity
13) EU:n kyberturvallisuusasetus https://digital-strategy.ec.europa.eu/fi/policies/cybersecurity-act

Lähdeluettelo

14) Tekoälyä koskeva sääntelykehysehdotus https://digital-strategy.ec.europa.eu/fi/policies/regulatory-framework-ai
15) EU:n digisäädöksillä luodaan pelisääntöjä digitaalisen ajan toimintaympäristöön https://vm.fi/eu-n-digisaadokset
16) EU:n neuvosto ja parlamentti ovat päässeet sopuun eurooppalaista lompakkosovellusta koskevasta lainsäädännöstä https://vm.fi/-/eu-n-neuvosto-ja-parlamentti-ovat-paasseet-sopuun-eurooppalaista-lompakkosovellusta-koskevasta-lainsaadannosta
17) Komissio tyytyväinen yhteisymmärrykseen EU:n digitaalisen identiteetin lompakosta https://ec.europa.eu/commission/presscorner/detail/fi/ip_23_5651