TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Maaliskuu 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

89 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys vuoden 2023 ensimmäisellä kvartaalilla.

Tietomurtojen, murron yritysten ja kiristyshaittaohjelmien määrä on noussut alkuvuoden keskiarvosta 35 %.

Tietoturvan kehittämisen tukea on myönnetty maaliskuun loppuun mennessä jo 102 yritykselle.

Kybersää maaliskuu 2023

Tietomurrot ja -vuodot

- Maaliskuussa ilmoitukset erilaisista tietomurroista nousivat noin 35 % vuoden alun keskiarvosta.
- Edelleen suuria määriä sosiaalisen median tilejä murretaan erilaisten ”kilpailujen” varjolla.

Huijaukset ja kalastelut

- Maaliskuu alkoi ikävästi vuokran-maksuhuijauksilla. Vuokrarästi-aiheiset tekstiviestit kilahtivat tuhansiin suomalaispuhelimiin.[1]
- ”Hei äiti” -huijaustekstarit saivat jatkoa ”Hei isä” -viesteistä. Huijari väittää olevansa lapsi, jonka puhelin meni rikki, ja pyytää rahaa.

Haittaohjelmat ja haavoittuvuudet

- Toimitusketjuhyökkäys 3CXDesktopApp-videoneuvotteluohjelmistoon.[2]
- Kriittinen haavoittuvuus Microsoft Outlookissa.[3]
- Apple julkaisi korjaavia päivityksiä useiden tuotteiden kriittisiin haavoittuvuuksiin.[4]

Automaatio ja IoT

- Internetiin liittyvien tuotteiden kyberturvallisuusvaatimuksia ja sääntelyn kehittämistä käsittelevät tilaisuudet jatkuvat 18.4. Tampereella ja 25.4. Jyväskylässä. Traficom järjestää tilaisuudet yhteistyössä paikallisten toimijoiden kanssa.[5]

Verkkojen toimivuus

- Maaliskuussa yleisissä viestintäpalveluissa oli seitsemän merkittävää toimivuushäiriötä.
- Häiriöiden syinä olivat esimerkiksi päivitys- ja muutostyöt.
- Palvelunestohyökkäyksien määrä oli maaliskuussa tavallinen. Muutamalla hyökkäyksellä oli vaikutuksia verkkosivujen tai palveluiden saatavuuteen.

Vakoilu

- Toimitusketjuhyökkäykset ja haavoittuvuuksien hyödyntäminen olivat yhä suosittuja menetelmiä myös valtiollisten toimijoiden työkalupakissa.
- 3CXDesktopApp-ohjelmiston toimitusketjuhyökkäys ja Outlookin kriittistä haavoittuvuutta hyödyntäviä tapauksia liitettiin julkisuudessa valtiollisiin toimijoihin.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Tietoturvan kehittämisen tukea on myönnetty kuun loppuun mennessä yhteensä jo noin 2,5 miljoonaa euroa 102 yritykselle. Tukea myönnetään niin kauan kuin tuen myöntämiseksi varattu 6 miljoonan euron määräraha riittää.[2]

Kyberturvallisuuskeskus on mukana viranomaisten ja yritysten Varo, varmista, varoita -yhteiskampanjassa. Kampanjan tarkoituksena on muistuttaa, että huijauksia on mahdollista välttää.[2]

Kyberturvallisuuskeskuksen uusin toteutettavuustestauksen Tonttu-projekti Ketjutonttu auttaa suomalaisia yrityksiä ja niiden toimittajia hallitsemaan toimitusketjuihin liittyviä kyberriskejä.[7]

Maaliskuun kyberturvallisuuden yleiskuva

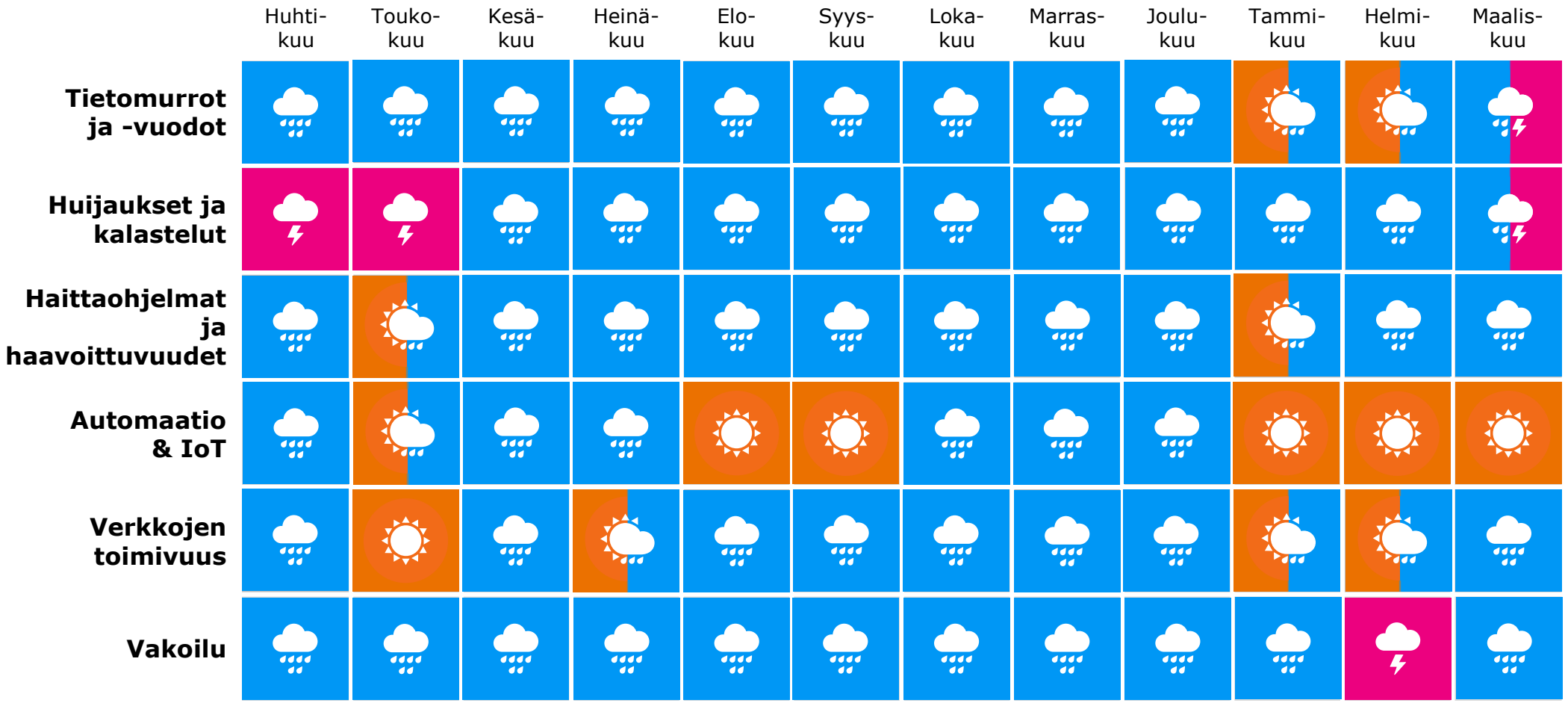
- Maaliskuun aikana saimme useita ilmoituksia tietomurroista ja tietomurtojen yrityksistä. Saimme ilmiöstä huomattavasti enemmän ilmoituksia kuin helmikuun aikana.
- Kuun alussa saimme useita ilmoituksia toimitusjohtajahuijauksista tai niiden yrityksistä. Rahallisia vahinkoja ei saamiemme ilmoitusten mukaan ollut tapahtunut.
- Maaliskuussa palvelunestohyökkäyksiä ilmoitettiin useilta eri sektoreilta, hyökkäykset olivat kuitenkin lyhytkestoisia ja vaikutukset jäivät vähäisiksi.
- Saimme myös pitkästä aikaa ilmoituksia Emotet-haittaohjelmasta, jonka levittämistä oltiin yritetty sähköpostilla lähetettävien OneNote-liitteiden avulla.

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

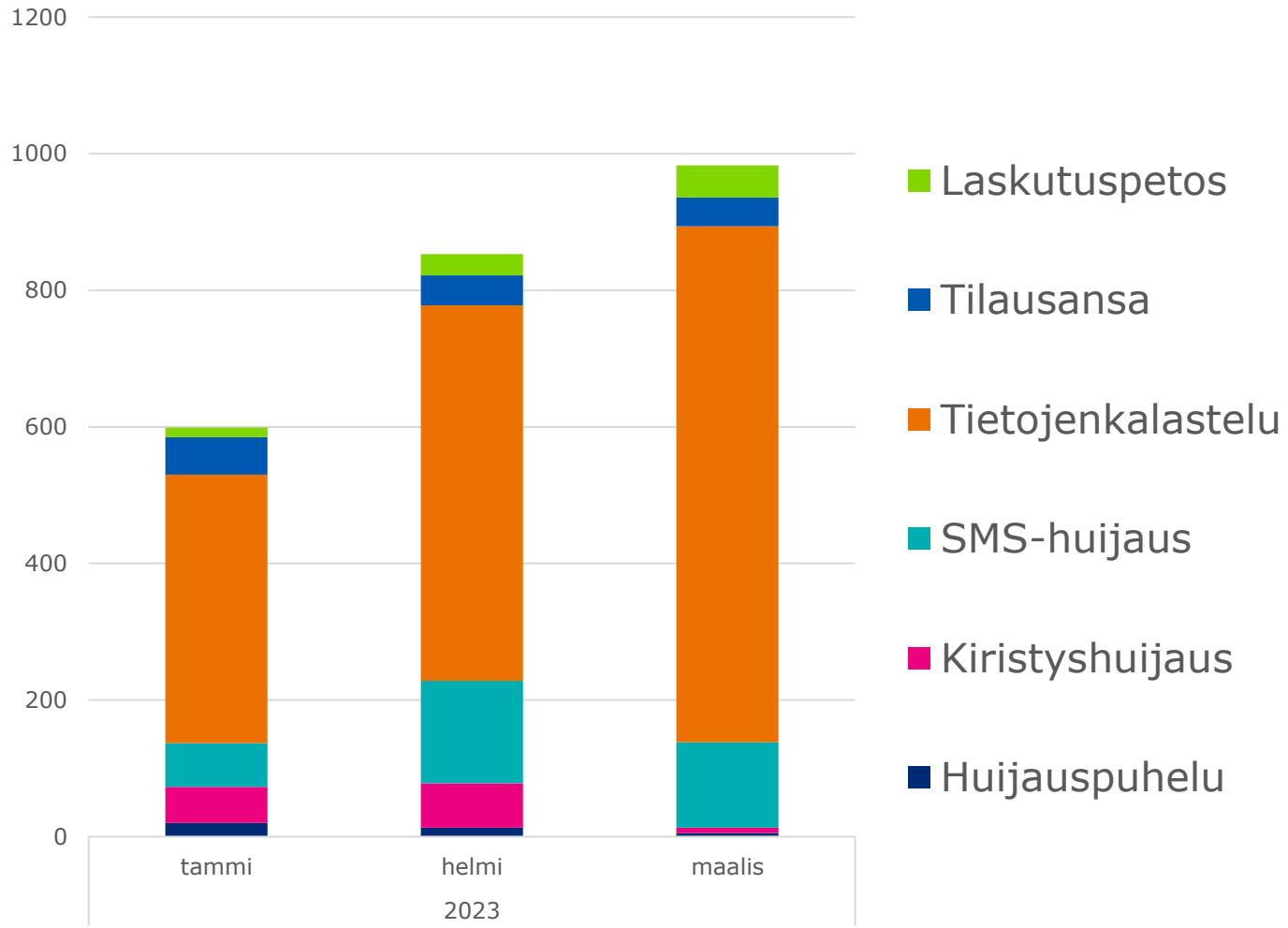


Käsiteltyjä huijaustapauksia
Q1/2023

3 kk

Vuoden 2023 ensimmäisen neljänneksen ilmiöitä ovat:

- Pankkitunnuskalastelu lisääntyy ja monipuolistuu jatkuvasti.
- Tekstiviestihuijauksia lisäsi suuri määrä vuokranmaksuhuijausviestejä.
- Poliisiviranomaisten nimissä lähetettyjä kiristyshuijauksia lähetettiin paljon alkuvuodesta.
- Toimitusjohtajahuijaukset ja muut laskutuspetokset ovat selvästi lisääntyneet kaiken muun huijaamisen ohella.

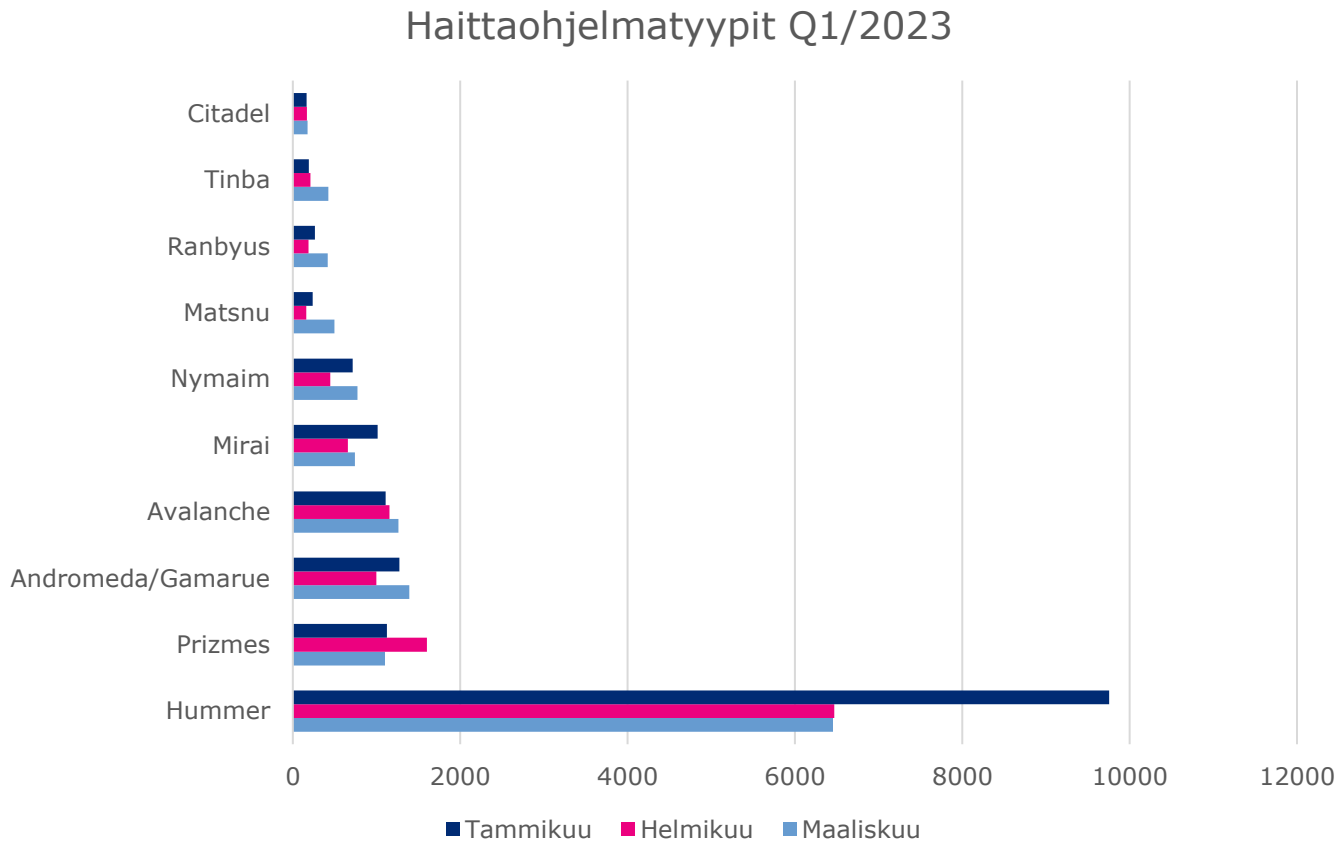


Autoreporterin haittaohjelmahavainnot

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.

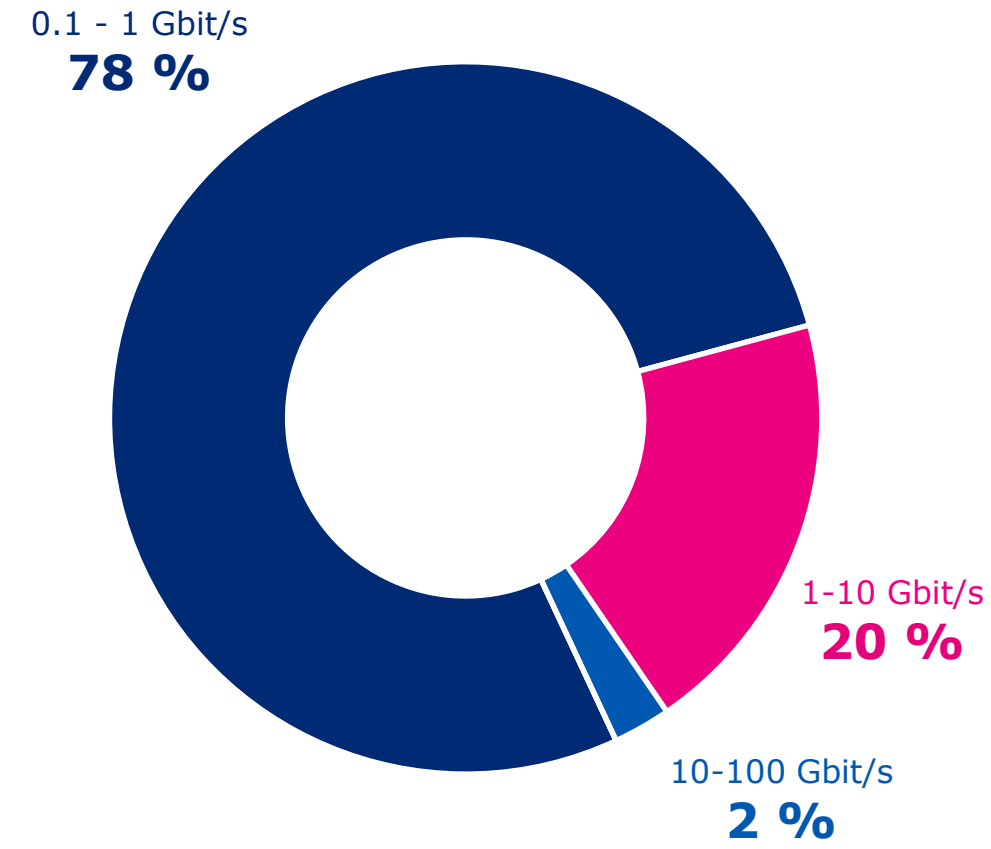
Tilastossa kerromme **10 yleisintä ja nimettyä** haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Autoreporterin tietoihin voi perehtyä tarkemmin Kyberturvallisuuskeskuksen verkkosivuilla.



3 kk

Palvelunestohyökkäysten tunnuslukuja
Q1/2023

- **89 Gbit/s** oli suurin Suomessa nähty palvelunestohyökkäys Q1/2023.
- Noin 77 % hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Toimialakohtaisia nostoja

3 kk

	Trendi **3kk**	
Elintarvike		Havaittu tietojenkalastelukampanjoita.
Energia		Havaittu tietojenkalastelukampanjoita.
Finanssi		Liikkeellä pankkihuijauksia.
Teollisuus		Havaittu tietojenkalastelukampanjoita.
Logistiikka ja liikenne		Havaittu palvelunestohyökkäyksiä.
Julkishallinto		Havaittu huijaus- ja tietojenkalasteluyrityksiä.
Media		Havaittu tietojenkalastelukampanjoita.
SOTE		Alkuvuodesta havaittiin haktivistien tekemiä palvelunestohyökkäyksiä. Hyvinvointialueiden toiminnan käynnistyminen on sujunut kyberturvallisuuden kannalta valtaosin hyvin.
Vesihuolto		Havaittu tietojenkalastelukampanjoita.

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:
Teknologia osana suurvaltakilpailua

Suurvaltakilpailulla tarkoitetaan kilpailua poliittisesta, taloudellisesta, sotilaallisesta ja teknologisesta johtoasemasta maailmassa. Suomalaisissakin yrityksissä on hyvä kiinnittää huomiota Yhdysvaltojen ja Kiinan kiihtyvään kamppailuun taloudellisesta ja teknologisesta johtajuudesta.[8]

- Teknologian saralla suurvaltakilpailun vaikuttamisvälineenä on käytetty esimerkiksi vientivalvontaa. Pahimmissa tapauksissa suurvalta voisi jopa estää sellaisten tuotteiden pääsyn markkinoilleen, joissa on hyödynnetty kilpailevaan suurvaltaan liitettyä teknologiaa.[8]
- Suurvaltakilpailulla voi olla vaikutuksia myös suomalaisyritysten toimintamahdollisuuksiin erityisesti tilanteissa, joissa halutaan tehdä yhteistyötä kilpailevien suurvaltojen kanssa.[9]
- Suurvaltojen teknologinen kilpailu vaikuttaa Suomessa erityisesti teknologia-alaan, johon on keskittynyt osaamista ja vientiä.[9]
- Valtiot voivat pyrkiä edistämään tarkoitusperiään myös kybervakoilun keinoin. Kybervakoilua voidaan käyttää esimerkiksi teknologisen osaamisen saavuttamiseksi (teollisuusvakoilu) tai tiedon hankkimiseksi poliittisesta päätöksenteosta ja sen valmistelusta.

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

- Sisäministeriön vetämä kansallinen lainsäädäntöhanke CER-direktiivin täytäntöönpanemiseksi Suomessa etenee.[10][11]
  - CER-direktiivin tavoitteena on yhteiskunnan elintärkeiden palveluiden mahdollisimman häiriöttömän toiminnan sekä jatkuvuuden varmistaminen.
    - Keskiössä on proaktiivinen suojautuminen häiriöiltä: häiriöiden ehkäiseminen, niiden vaikutusten minimointi ja rajaaminen sekä nopea palautuminen normaalitoimintaan.
  - Direktiivin täytäntöönpanosta vastaa sisäministeriö ja täytäntöönpanoa varten on asetettu lainsäädäntöhanke sekä perustettu poikkihallinnollinen työryhmä
    - Sääntelyä sovellettava kansallisesti 18.10.2024 alkaen.
  - Uusi sääntely tuo vaatimuksia jäsenvaltioille, valvoville viranomaisille ja soveltamisalan piiriin kuuluville kriittisille organisaatioille:
    - Kansallinen ja viranomaistaso: kansallisen häiriönhallintastrategian laatiminen, kansallisen tason riskien arviointi ja riskienhallinta, soveltamisalaan kuuluvien kriittisten toimijoiden määrittäminen ja niiden riskiperusteinen viranomaisvalvonta.
    - Soveltamisalaan kuuluvat kriittiseksi tunnistetut toimijat seuraavilta toimialoilta: liikenne, energia, pankkiala, rahoitusmarkkinoiden infrastruktuuri, terveys, vesi- ja jätevesihuolto, digitaalinen infrastruktuuri, julkishallinto, avaruus ja elintarvikkeiden tuotanto, jalostus ja jakelu
    - Kriittisillä toimijoilla on velvoite toteuttaa toimenpiteitä häiriönsietokykynsä varmistamiseksi, dokumentoida ne ja ilmoittaa poikkeamista
    - CER-direktiivillä on linkki EU:n kyberturvallisuusdirektiiviin (NIS2), sillä se tulee koskemaan osittain samoja toimijoita Suomessa

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 osoitteeseen kyberturvallisuuskeskus@traficom.fi

Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä: https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot

Lähdeluettelo 1/2

1) Kyberturvallisuuskeskuksen viikkokatsaus - 9/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-92023
2) Kyberturvallisuuskeskuksen viikkokatsaus - 13/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-132023
3) HAAVOITTUVUUS 3/2023 https://www.kyberturvallisuuskeskus.fi/fi/kriittinen-haavoittuvuus-microsoft-outlookissa
4) HAAVOITTUVUUS 5/2023 https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_5/2023
5) Kohti kyberturvallisia älytuotteita - Traficomin Kyberturvallisuuskeskuksen tapahtumat valmistajille https://tietoturvamerkki.fi/fi/tapahtumat
6) Kyberturvallisuuskeskuksen viikkokatsaus – 11/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-112023
7) Kyberturvallisuuskeskuksen viikkokatsaus - 12/2023 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-122023
8) Kiina ja Yhdysvallat – haaste yrityksille : Suurvaltakilpailun vaikutukset suomalaisyrityksille https://julkaisut.valtioneuvosto.fi/handle/10024/163272

Lähdeluettelo 2/2

9) Raportti: Yhdysvaltain ja Kiinan suurvaltakamppailu vaatii valppautta suomalaisyrityksiltä https://ek.fi/ajankohtaista/tiedotteet/raportti-yhdysvaltain-ja-kiinan-suurvaltakamppailu-vaatii-valppautta-suomalaisyrityksilta/
10) CER-lainsäädäntöhankkeen sivu: https://valtioneuvosto.fi/hanke?tunnus=SM047:00/2022
11) CER-direktiivin teksti EurLex-palvelussa: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022L2557&from=EN