TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Helmikuu 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

Vuonna 2022 pankkitunnuskalastelulla suomalaisilta huijattiin 10 miljoonaa euroa.

ENISA & CERT-EU julkaisivat yhdessä raportin varoittaakseen tiettyjen uhkatoimijoiden jatkuvasta toiminnasta.

Helmikuun päivitystiistaina tarjottiin korjaukset esimerkiksi kolmeen jo hyväksikäytettyyn nollapäivähaavoittuvuuteen.

Kybersää helmikuu 2023

Tietomurrot ja -vuodot

- PowerApps-pohjaiset kalastelut aiheuttivat edelleen merkittäviä määriä tietomurtoja. MFA:lla on helppo suojautua ilmiöltä.(1)
- Rikolliset seuraavat julkaistuja haavoittuvuusilmoituksia aktiivisesti, ja pyrkivät hyödyntämään haavoittuvuuksia tehdäkseen tietomurtoja.

Huijaukset ja kalastelut

- Vuokranmaksuhuijauksilla yritettiin saada maksamaan vuokra huijarin tilille.(2)
- Finanssiala kertoo, että vuonna 2022 pankkitunnuskalastelulla suomalaisilta huijattiin 10 miljoonaa euroa.

Haittaohjelmat ja haavoittuvuudet

- Helmikuun alussa maailmalla levisi aggressiivisesti VMWare ESXi -ohjelmiston haavoittuvuutta hyödyntävä kiristyshaittaohjelmakampanja.(3)
- Päivitystiistai toi korjauksia lukuisiin haavoittuvuuksiin, joukossa oli myös nollapäivähaavoittuvuuksia.(1)

Automaatio ja IoT

- Julkaisimme ohjeen teollisuusautomaation tärkeimmistä kyberturvallisuuskontrolleista.(4)

Verkkojen toimivuus

- Helmikuussa yleisissä viestintäpalveluissa oli yksi merkittävä toimivuushäiriö.
- Ilmoitettujen palvelunestohyökkäysten määrä on laskenut selvästi loppuvuodesta.
- Osa hyökkäyksistä aiheutti lieviä vaikutuksia palveluiden saatavuuteen. (2)

Vakoilu

- Euroopan unionin kyberturvallisuusvirasto (ENISA) ja CERT-EU julkaisivat yhdessä raportin varoittaakseen tiettyjen uhkatoimijoiden jatkuvasta toiminnasta.(1)
- ENISA ja CERT-EU kannustavat voimakkaasti kaikkia julkisen ja yksityisen sektorin organisaatioita EU:ssa soveltamaan julkaisussa lueteltuja suosituksia.(1)

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Julkaisimme uuden ohjeen paikallisiin matkaviestinverkkoihin liittyvistä kyberuhkista ja riskienhallinasta. Ohje tarjoaa tietoa paikallisia matkaviestinverkkoja harkitseville organisaatioille.(5)

EU:n kyberturvallisuuden osaamiskeskuksen Suomen kansallinen koordinointikeskus aloitti toimintansa vuoden 2023 alussa Liikenne- ja viestintävirasto Traficomissa.(6)

Sote-alan toiminnan jatkuvuus riippuu entistä enemmän kyberturvallisuudesta. Suomessa alan kyberturvallisuuden parantamiseksi tehdään yhteistyötä monella rintamalla, kuten Kyberturvallisuuskeskuksen fasilitoimissa tiedonvaihtoverkostoissa.(7)

Helmikuun kyberturvallisuuden yleiskuva

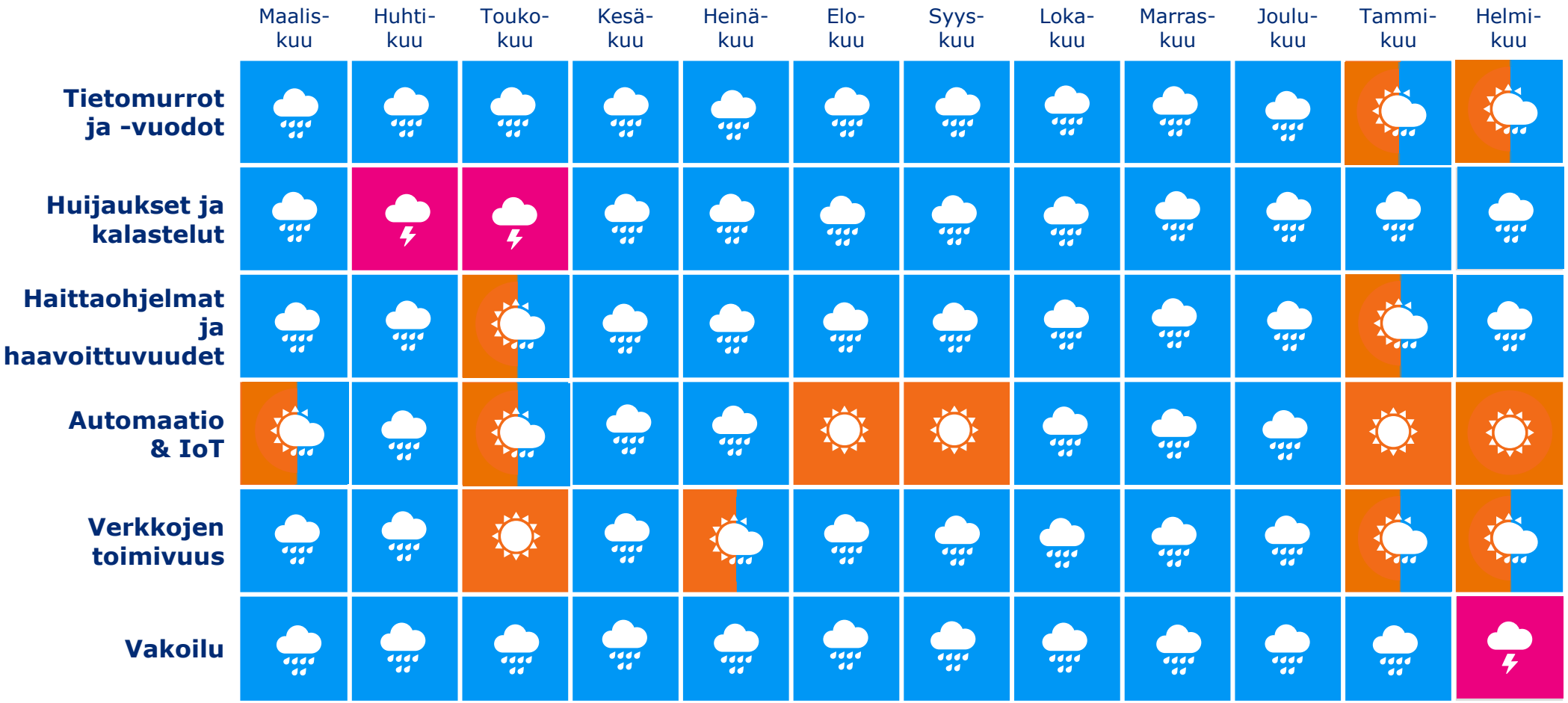
- Rauhallisemman vuodenvaihteen ja tammikuun jälkeen ilmoitusmäärät ovat palanneet normaalille tasolle, ilmoituksia tulee edelleen monipuolisesti.
- Helmikuun lopussa saatiin runsaasti ilmoituksia uudesta huijausmuodosta, jossa tekstiviestin vastaanottajaa houkutellaan siirtämään vuokrarahoja rikollisille.
- Länsi-Uudenmaan käräjäoikeus määräsi Vastaamo-tietomurrosta epäillyn vangittavaksi.
- Ilmoitettujen palvelunestohyökkäysten määrä on jatkanut laskua.
- VMWare ESXi -ohjelmistohaavoittuvuus on aktiivisesti hyväksikäytetty ja hyväksikäyttö on aiheuttanut maailmalla merkittäviä vaikutuksia.
  - Suomessa Kyberturvallisuuskeskukselle on toistaiseksi ilmoitettu vain yksittäisiä haavoittuvuuden hyväksikäyttötapauksia.

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



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 kyberturvallisuuden osaajille
- Pula puolijohteista
- Tekoälyn käyttö kyberrikollisuudessa
- Suurvaltakilpailun vaikutukset sääntelyyn
- Älylaitteiden elinkaari ja kierrätys
- Kybervakoilun ja rikollisuuden rajojen hämärtyminen
- **IoT**
- **6G**
- Kiristyshaitta ohjelmien käyttö murroksessa
- Teknologia osana suurvaltakilpailua
- Sääntelyn ulottuminen uusille toimialoille
- Osallistuminen digitaalisessa ympäristössä

Pitkän aikavälin kybersää:
Tarve kyberturvallisuuden osaajille

Kyberturvallisuuden osaaminen on elintärkeä osa myös muiden kuin tietoturva-alan palveluita ja ratkaisuja tuottavien yritysten toimintaa. Siksi kyberturvallisuuden osaajia tarvitaan kaikilla aloilla, ja osaajien tarve toimialoilla on vain kasvanut viime vuosina.

- Kyberturvallisuuden osaajia tarvitaan pitkällä aikavälillä hyvin laajalla profiililla. Kyberturvallisuus läpileikkaa yhteiskuntaa aina teknisestä ja hallinnollisesta tasosta poliittiselle tasolle asti. Koulutussektorilla on tärkeä rooli kyberturvallisuuden osaajapulan umpeen kuromisessa, mutta osaajien lisääminen vie aikaa. Myös organisaatiot voivat itse vaikuttaa asiaan.
- EU:n Kyberturvallisuusvirasto ENISA korostaa raportissaan osaajapulan koostuvan kahdesta ilmiöstä; nykyisten osaajien ammattitaiton ylläpitäminen ja kehittäminen tehtävien vaatimalla tavalla, ja toiseksi uusien vaativien kyberturvallisuuden tehtävänkuvien täyttäminen osaajapulasta kärsivillä toimialoilla.(8)
- Esimerkiksi Maailman talousfoorumi WEF on korostanut Global Cybersecurity Outlook 2023 –julkaisussaan ratkaisuna esimerkiksi rohkeampaa rekrytointia perinteisten teknisten alojen ulkopuolelta, sekä organisaatioiden järjestämää aktiivista lisäkouluttamista.(9)
- Organisaatioiden kannattaa tunnistaa ja reagoida osaajatarpeisiinsa ajoissa, koska osaamisen saaminen riittävälle tasolle kestää vielä pitkään.

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 komissio on julkaissut ilmailun tietoturvanhallinnan vaatimuksia vahvistavat EU-asetukset (Part-IS, information security)
  - Nyt julkaistut asetukset yhdenmukaistavat ja tarkentavat tietoturvanhallinnan velvoitteita suhteessa ilmailun turvallisuuteen kohdistuviin riskeihin ja kattavat ilmailun keskeisimmät toimijat.(10)(11)
  - Ilmailun kyberturvallisuudella tarkoitetaan sitä, että toimijat tunnistavat ja hallitsevat sellaisia tieto- ja viestintäteknisiin järjestelmiin ja siviili-ilmailussa käytettävään dataan kohdistuvia tietoturvariskejä, jotka vaikuttavat tai saattavat vaikuttaa lentoturvallisuuteen tai ilmailun turvaamiseen sekä vahvistavat ilmailujärjestelmän häiriönsietokykyä.
  - Part-IS:n tavoitteena on varmistaa, että siviili-ilmailun toimintaan osallistuvat organisaatiot ja viranomaiset kykenevät tunnistamaan, suojaamaan, havaitsemaan, reagoimaan ja palautumaan lentoturvallisuuteen vaikuttavista tietoturvatapahtumista.
  - Euroopan Unionin lentoturvallisuusvirasto EASA julkaisee kevään aikana hyväksyttävät asetusten vaatimusten täyttämisen menetelmät (AMC-materiaali) sekä ohjemateriaalin (GM).
  - Liikenne- ja viestintävirasto Traficom on ollut mukana tekemässä Part-IS-asetuksia ja AMC- ja GM-materiaalia. Traficom osallistuu myös EASAn vetämään jäsenvaltioiden työryhmään, jossa valmistellaan asetusten käyttöönottoa ja jaetaan parhaita käytäntöjä.

Oikeudelliset asiat

- Digitaalinen henkilöllisyys ja henkilötunnusjärjestelmän uudistaminen siirtyvät eteenpäin
  - Eduskunnan jäljellä oleva toimikausi ei riitä asioiden käsittelemiseen valiokunnassa, mikä tarkoittaa, että seuraava hallitus päättää lakiesitysten edistämisestä. Uusien lakien oli alun perin tarkoitus tulla voimaan syyskuussa 2023.(12)
  - Esityksen digitaalisesta henkilöllisyydestä oli tarkoitus luoda pohja digitaalisen henkilöllisyystodistuksen, ulkomaalaisen digitaalisen asiointivälineen ja luonnollisen henkilön tunnistusvälineen käyttöönotolle. Tavoitteena oli myös luoda edellytykset EU:n digitaaliselle lompakolle.
  - Esityksellä henkilötunnusjärjestelmän uudistamiseksi luotaisiin edellytykset uuden yksilöintitunnuksen käyttöönotolle, uudelle etärekisteröitymismenettelylle ja mahdollistettaisiin henkilötunnuksen antaminen ulkomaalaisille nykyistä aikaisemmin ja laajemmin sekä poistettaisiin sukupuolitieto henkilötunnuksesta.
  - EU-tasolla valmistelu jatkuu edelleen ja eIDAS-asetukseen liittyvät lompakkoratkaisujen rajat ylittävän käytön pilotoinnit käynnistyvät EU:ssa tänä vuonna.

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) Kyberturvallisuuskeskuksen viikkokatsaus - 7/2023
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-72023
2) Kyberturvallisuuskeskuksen viikkokatsaus - 9/2023
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-92023
3) HAAVOITTUVUUS 6/2021 - Haavoittuvuuksia VMwaren tuotteissa - päivitä heti
   https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuuksia-vmwaren-tuotteissa-paivita-heti
4) Teollisuusautomaation tärkeimmät kyberturvallisuuskontrollit
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/teollisuusautomaation-tarkeimmat-kyberturvallisuuskontrollit
5) Uudessa ohjeessa tietoa paikallisiin matkaviestinverkkoihin liittyvistä kyberuhkista ja riskienhallinasta
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uudessa-ohjeessa-tietoa-paikallisiin-matkaviestinverkkoihin-liittyvista-kyberuhkista

Lähdeluettelo

6) Kyberturvallisuuden tutkimus- ja kehitystoimintaan vahvistusta Suomessa ja Euroopassa - EU:n kyberturvallisuuden osaamiskeskuksen Suomen kansallinen koordinointikeskus aloitti toimintansa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-tutkimus-ja-kehitystoimintaan-vahvistusta-suomessa-ja-euroopassa
7) Sosiaali- ja terveydenhuoltoalalla kyberturvallisuutta parannetaan monessa verkostossa https://www.kyberturvallisuuskeskus.fi/fi/fi/ajankohtaista/ttn_17022023
8) Addressing Skills Shortage and Gap Through Higher Education https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education
9) Global Cybersecurity Outlook 2023 https://www.weforum.org/reports/global-cybersecurity-outlook-2023/

Lähdeluettelo

10) Kyberturvallisuuden uusi EU-sääntely vahvistaa ilmailun turvallisuutta ja häiriönsietokykyä https://www.traficom.fi/fi/ajankohtaista/kyberturvallisuuden-uusi-eu-saantely-vahvistaa-ilmailun-turvallisuutta-ja

11) Part-IS regulation published, completing regulatory framework for cyber-resilient aviation https://www.easa.europa.eu/en/newsroom-and-events/news/part-regulation-published-completing-regulatory-framework-cyber-resilient

12) Lakiesityksiä digitaalisesta henkilöllisyydestä ja henkilötunnuksen uudistamisesta ei ehditä käsitellä tällä istuntokaudella https://vm.fi/-/lakiesityksia-digitaalisesta-henkilollisyydesta-ja-henkilotunnuksen-uudistamisesta-ei-ehdita-kasitella-talla-istuntokaudella