TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Helmikuu 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

Haavoittuvuustiedotteita on julkaistu 8 helmikuun loppuun mennessä. Määrä on huomattava vuoteen 2023 verrattuna, jolloin vuoden ensimmäinen haavoittuvuustiedote julkaistiin vasta 14.2.[1]

Kiristyshaittaohjelmailmoitusten määrä on ollut laskussa loppuvuoden 2023 jälkeen. Helmikuussa kiristyshaittaohjelmista tehtiin kaksi ilmoitusta.

9.11.2023 alkaen organisaatioiden on ollut mahdollista suojata oma tekstiviestin lähettäjätunnuksensa. Eri organisaatiot ovat suojanneet jo yli 80 lähettäjätunnusta.

Kybersää helmikuu 2024

Tietomurrot ja -vuodot

- Verkkolaitteisiin kohdistuvat kirjautumisyritykset sekä M365-tilimurrot jatkuivat. Useissa M365-tapauksissa murtoon hyödynnettiin AiTM-kalastelua.
- Sosiaalisen median tilimurroissa tilien omistajilta vaadittiin lunnaita tilin palauttamiseksi.

Huijaukset ja kalastelut

- Yli 80 SMS-lähettäjätunnusta on suojattu huijauksia vastaan. Jokainen suojattu lähettäjätunnus vähentää rikollisten keinoja huijata viranomaisten ja yritysten nimissä.
- Liikennerikkeillä tai maksamattomilla autoveroilla pelottelevia SMS-huijausviestejä lähetetään silti paljon myös ilman uskottavaa lähettäjätunnusta.

Haittaohjelmat ja haavoittuvuudet

- Ivantin haavoittuvuudet osoittavat verkon reunalaitteiden tietoturvan kriittisyyden.
- Yhdysvaltojen kyberturvallisuusviranomainen CISA kertoi Ivanti-tietomurrostaan.
- Maaliskuun alussa julkaistiin haavoittuvuustiedote JetBrains TeamCity -ohjelmiston kriittisestä haavoittuvuudesta.

Automaatio ja IoT

- Älylahja voi yllättää ikävästikin – tutustu tuotteen tietoturva-ominaisuuksiin ennen ostopäätöstä. [2]
- Maatiloilla käytetyn automaation toimimattomuudella voi olla vakavia seurauksia. Kiristyshaittaohjelma maatilan ruokintaa ohjaavassa tietokoneessa uhkasi tuotantoeläinten hyvinvointia.[3, 4]

Verkkojen toimivuus

- Helmikuussa yleisissä viestintäpalveluissa oli 2 toimivuushäiriötä.
- Helmikuun alussa haktivistit kohdistivat palvelunestohyökkäyksiä ennätyksellisen suureen määrään kotimaisia organisaatioita.

Vakoilu

- Yhdysvaltalaisviranomaiset häiritsivät murretuista Ubiquiti EdgeRouter -laitteista muodostettua hyökkäysverkkoa.[5]
- Viranomaisten mukaan laitteita käytettiin mm. APT28-toimijan kampanjoissa varastettujen kirjautumistietojen välittämiseen ja keräämiseen sekä hyökkäysliikenteen reitittämiseen.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Yhdessä tekstiviestihuijauksia vastaan – jo yli 80 lähettäjätunnusta on suojattu.

Internetin verkkoalustoille ja muille digipalveluille tuli uusia velvollisuuksia, kun EU:n digipalveluasetuksen (DSA) soveltaminen alkoi 17.2.2024. Uuden sääntelyn tarkoitus on vähentää laitonta sisältöä ja lisätä palveluiden avoimuutta.[1]

Helmikuun kyberturvallisuuden yleiskuva

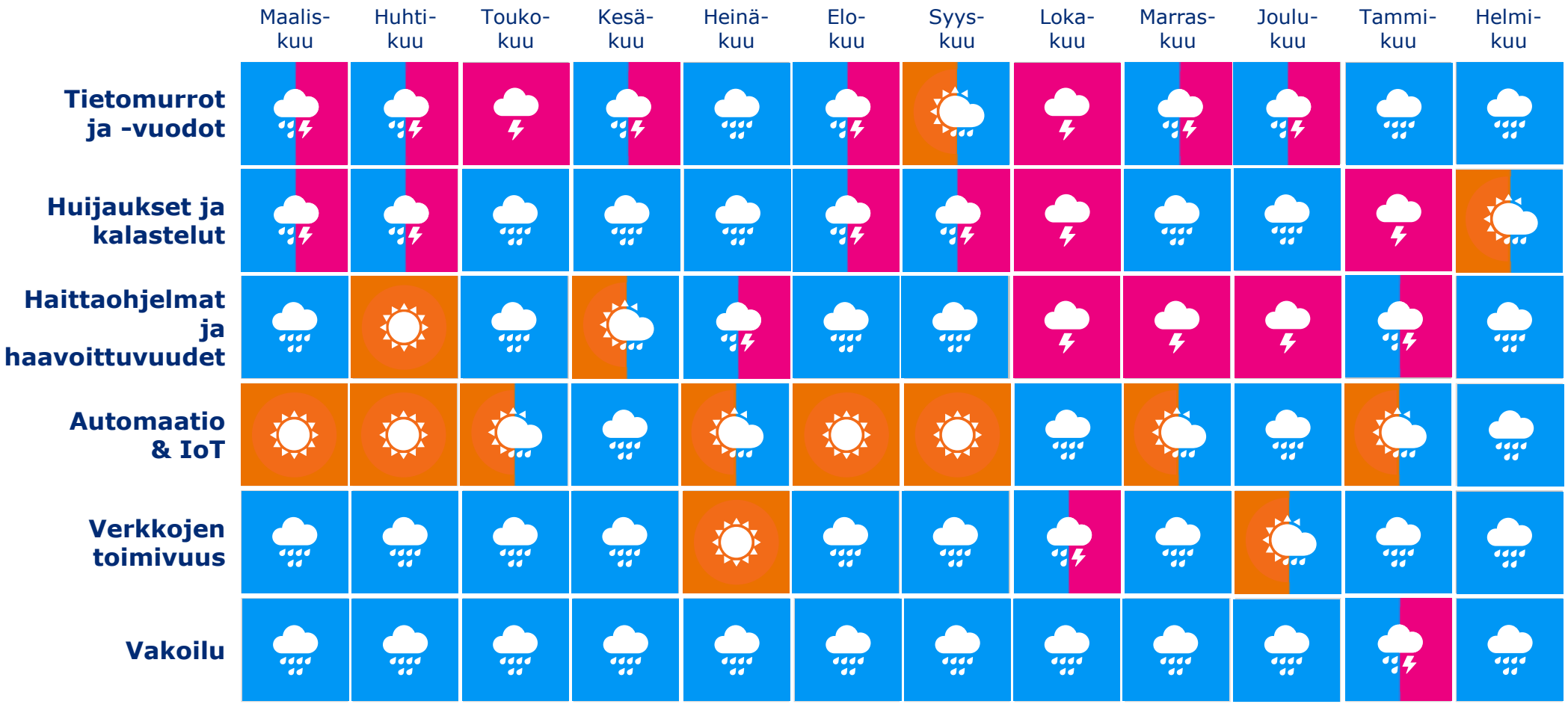
- Microsoft 365 –tietojenkalastelu nosti päätään jälleen helmikuussa. Turvapostiksi naamioidut huijausviestit johtivat tietojenkalastelusivulle, jossa kalasteltiin käyttäjätunnuksia ja salasanoja.
  - Kyberturvallisuuskeskus kehottaa kaikkia Microsoft 365 -asiakkaita viestimään sisäisesti kalasteluviestien uhista.
  - Kalastelusivuilla on käytetty kehittynyttä adversary-in-the-middle-automatiikkaa (AitM), joka joissakin tapauksissa kykenee myös monivaiheisen tunnistautumisen ohittamiseen.[6]
    - Monivaiheisen tunnistautumisen pakotettu käyttöönotto toimii tehokkaana suojautumiskeinona sekä perustana muille suojautumiskeinoille tietojenkalastelukampanjoita vastaan.
- Toimitusjohtajahuijauksia ja muita laskutuspetoksia on myös ollut liikkeellä helmikuussa.
  - Organisaatioissa tulisi tarjota työntekijöille, kesätyöntekijöitä ja harjoittelijoita unohtamatta, selkeät ohjeet organisaation laskutuskäytäntöihin sekä turvallisiin varmistuskäytäntöihin, ja niistä tulisi aina pitää kiinni.
  - Epäilyttävien viestien todenperäisyyden voi varmistaa soittamalla lähettäjälle puhelimitse.

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 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:
Haavoittuvuuksien nopeutuva hyväksikäyttö

Kyberrikolliset hyväksikäyttävät haavoittuvuuksia yhä nopeammin. Näin ollen myös päivittämisen pitäisi tapahtua yhä nopeammin, ja tarvittavista päivityksistä olisi syytä pitää huolta jatkuvasti, myös yleisinä loma-aikoina.

- Kyberrikolliset etsivät verkosta aktiivisesti päivittämättömiä järjestelmiä. Haavoittuvuuksien hyväksikäyttöä yritetään viimeistään, kun tieto haavoittuvuudesta on tullut julki.
- Usein päivittäminen ei valitettavasti yksin riitä, vaan järjestelmien turvaamiseksi olisi syytä myös tarkistaa, ettei haavoittuvuutta ole ehditty jo hyväksikäyttää ennen sen korjaamista. Myös järjestelmän tarkastus mahdollisesti luotujen takaovien, eli piilotettujen sisäänpääsyreittien, varalta voi olla perusteltua.
- Organisaatioiden olisi hyvä myös ennakoivasti tarkastella julkisesti verkkoon näkyvissä olevia palveluitaan ja varmistaa, ettei julkiseen verkkoon ole näkyvissä sellaisia palveluita, joille se ei ole välttämätöntä.
- Esimerkiksi tammikuussa julkaistiin Ivantin tuotteissa olleita kriittisiä haavoittuvuuksia. Kyberturvallisuuskeskuksen tekemien kartoitusten mukaan haavoittuvia palvelimia oli Suomessa useita satoja.[7]

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

Traficom on antanut uudistetun teletoiminnan tietoturvamääräyksen.[8]

- Määräys tulee pääosin voimaan 1.9.2024, ja se korvaa 4.3.2015 annetun teletoiminnan tietoturvamääräyksen.
- Uudistus edellyttää kaikilta teleyrityksiltä toimenpiteitä tietoturvallisuuden ja riskien hallinnan vaatimusten toteuttamiseksi ja dokumentoimiseksi.
- Uudistetussa määräyksessä huomioidaan viestinverkkojen ja -palvelujen kehittyminen sekä vastataan uusiin, tietoturvaa uhkaaviin ilmiöihin. Uudistetun määräyksen keskiössä ovat viestintäverkkojen kehityksen osalta erityisesti 5G-teknologian uudet arkkitehtuuriratkaisut, matkaviestinverkkojen uudet käyttötapaukset ja niihin liittyvät tietoturvavaatimukset.
- Määräysuudistus valmisteltiin laajassa yhteistyössä toimialan kanssa vuoden 2023 aikana.

Oikeudelliset asiat

Hallituksen esitysluonnos Finanssivalvonnasta annetun lain muuttamisesta sekä eräiksi siihen liittyviksi laeiksi (DORA-asetuksen ja DORA-muutosdirektiivin kansallinen täytäntöönpano).[9]

- Valtiovarainministeriö pyytää lausuntoa luonnoksesta hallituksen esitykseksi eduskunnalle laiksi Finanssivalvonnasta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi. Lausuntoja pyydetään 29.3.2024 mennessä.
- DORA-asetuksella ja DORA-muutosdirektiivillä yhdenmukaistetaan rahoitusalan digitaalista häiriönsietokykyä koskeva sääntely unionissa.
- Ehdotuksilla saatetaan kansallinen lainsäädäntö vastaamaan DORA-asetuksen ja DORA-muutosdirektiivin mukaisia vaatimuksia.
- Esitys sisältää NIS2-direktiivin sekä CER-direktiivin kansallista täytäntöönpanoa täydentävät ehdotukset direktiivien soveltamisalaan kuuluvien pankkitoiminnan ja finanssimarkkinoiden infrastruktuurin osalta.

Oikeudelliset asiat

Euroopan komissio antoi suosituksen merenalaisten datakaapeleiden suojelemisesta ja häiriönsietokyvystä.[10]

- Suosituksessa esitetään sekä kansallisia että EU-tasoisia toimenpiteitä merenalaisten datakaapeleiden suojelemiseksi.
- Suositellut toimenpiteet liittyvät esimerkiksi riskiarvioiden toteuttamiseen, datakaapeleihin liittyvän infrastruktuurin stressitestaamiseen, korjauskalustoon panostamiseen ja sen ylläpitämiseen sekä EU:n laajuiseen yhteistyöhön datakaapeleiden suojelemiseksi.
- Samaan aikaan komissio julkaisi myös toisen asiakirjan *(White Paper: How to master Europe's digital infrastructure needs?)*, jossa esitettiin laajemminkin tulevaisuuden toimenpiteitä digitaalisen infrastruktuurin kehittämiseksi ja sen turvallisuuden lisäämiseksi.

Oikeudelliset asiat

Liikenne- ja viestintäministeriön arviomuistioluonnos sähköisen viestinnän välitystietojen säilytysvelvollisuuteen liittyvän lainsäädännön muutostarpeista lausunnoilla 28.3.2024 asti.[11]

- Sähköisen viestinnän palveluista annetun lain 157 §:ssä on säädetty nimetyille teleyrityksille velvollisuus säilyttää sähköisen viestinnän välitystietoja.
- Viestinnän välitystiedot ovat teleoperaattorille tallentuvia tietoja viestinnän välittämisestä, eli esimerkiksi kännykkäpuheluiden osalta puhelinnumero, liittymän tilaajan nimi sekä viestinnän aika ja paikka.
- Euroopan unionin tuomioistuimen ratkaisukäytännön perusteella sähköisen viestinnän tietoja koskeva yleinen säilytysvelvollisuus muodostaa merkittävän rajoituksen yksityiselämän ja henkilötietojen suojaan. Viestinnän välitystiedot ovat kuitenkin välttämättömiä poliisi- ja turvallisuusviranomaisille rikosten selvittämiseksi ja syyteharkintaan saattamiseksi.
- Arviomuistiossa pohditaan vaihtoehtoja lainsäädännön muutostarpeille.

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) Kyberturvallisuuskeskuksen viikkokatsaus - 07/2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-072024
2) Lahjan antaja voi tehdä vahingossa karhunpalveluksen – viranomaiselta tärkeä muistutus https://www.is.fi/digitoday/tietoturva/art-2000010108170.html
3) Kyberhyökkäys voi pahimmillaan lamauttaa maatilan – tietoturva on arkipäivän riskienhallintaa https://www.maaseuduntulevaisuus.fi/paakirjoitus/a592f7cc-396c-4886-a306-0ac897e7d25b
4) Hakkerit iskivät vehmaalaiselle sikatilalle – emakoiden terveys vaarantui, kun ruokintaohjelmiston tilalla oli kiristysviesti https://www.maaseuduntulevaisuus.fi/maatalous/98511abf-992d-4a20-8c56-8a28c1f0ddd7
5) Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian
6) Detecting and mitigating a multi-stage AiTM phishing and BEC campaign https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/
7) Ivantin tuotteissa kriittisiä hyväksikäytettyjä haavoittuvuuksia https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_2/2024

Lähdeluettelo

8) Finlex: Määräys teletoiminnan tietoturvasta https://www.finlex.fi/fi/viranomaiset/normi/480001/50299
9) Lausuntopyyntö hallituksen esitysluonnoksesta laiksi Finanssivalvonnasta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=bde28301-9ceb-4793-a5cc-f6d31cc6cd93
10) Commission presents new initiatives for digital infrastructures of tomorrow https://ec.europa.eu/commission/presscorner/detail/en/ip_24_941
11) Työryhmän arviomuistioluonnos: data retention -lainsäädännön täsmentämisen vaihtoehdoista https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=b0083b22-7530-47da-be88-d0cf76fc23e0