TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Elokuu 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

Käräjäoikeus on antanut tuomion laajassa tietojenkalastelukampanjassa, jossa S-pankin asiakkaat menettivät yhteensä noin 2,4 miljoonaa euroa.[1]

Julkaisimme uuden työkalun kyberharjoituksen suunnittelun avuksi.

Kybersää elokuu 2023

Tietomurrot ja -vuodot

- Elokuussa tietomurroissa näkyi kesällä julkaistun Citrix Netscaler -ohjelmiston haavoittuvuuden hyväksikäyttö. Haavoittuvuuden hyödyntäminen vaikutti olleen erittäin nopeaa ja automatisoitua.
- Muutoin ilmoitusmäärät ovat laskeneet alkuvuoden ns. normaalitasolle.

Huijaukset ja kalastelut

- Elokuinen kalastelu on ollut erittäin aktiivista.
- Hotellipalvelu booking.com:n lähettämiä viestejä käytetään maksukorttitietojen kalasteluun.
- Pankkitunnuksia kalastellaan taas sekä ajankohtaisella veronpalautusteemalla että postin viestiksi väärennetyillä tekstareilla.

Haittaohjelmat ja haavoittuvuudet

- Heinäkuinen Citrix Netscaler -haavoittuvuus johti useisiin tietomurtoihin Suomessa.
- Päivitykset tulisi edelleen asentaa mahdollisimman pian, kun ne ovat tulleet tarjolle.
- Yhdysvaltain viranomaiset kertovat Qakbot-haittaohjelman toiminnan estämisestä kansainvälisen operaation avulla.[2]

Automaatio ja IoT

- EU:n radiolaitedirektiivin(RED) tietoturvasäädöksen harmonisoitujen standardien lausuntokierros on käynnistynyt.

Verkkojen toimivuus

- Elokuussa yleisissä viestintäpalveluissa oli yhdeksän merkittävää toimivuushäiriötä.
- Sähkökatkot aiheuttivat osan häiriöistä.
- Palvelunestohyökkäysten osalta elokuu oli rauhallinen eikä havaituilla poikkeamilla ollut merkittäviä vaikutuksia palveluihin.

Vakoilu

- Kohdistettu tietojenkalastelu voi tapahtua myös Teamsin kautta.
- Microsoftin raportin mukaan yksi kampanja hyödynsi Teamsin kautta lähetettyjä kalasteluviestejä, joiden tavoitteena oli kaapata kohteen käyttäjätili. Viesteissä esiinnyttiin IT-tukena tai tietoturvatiimin edustajana.[3]

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kyberturvallisuuskeskus on julkaissut uuden työkalun helpottamaan kyberharjoituksen suunnittelua.[4]

Julkaisimme ohjeen tietojen poistamiseksi Yango-taksipalvelusta.[5]

Tietoturva 2023 –seminaari järjestetään 12.10.2023. Tilaisuutta voi seurata maksutta verkossa. Ilmoittaudu mukaan nyt![6]

Ketjutontun avoin tuloskatsauswebinaari järjestetään 5.10.2023.[7]

Traficom on julkaissut merenkulun kyberturvallisuusasioita koskevat internetsivut.[8]

Elokuun kyberturvallisuuden yleiskuva

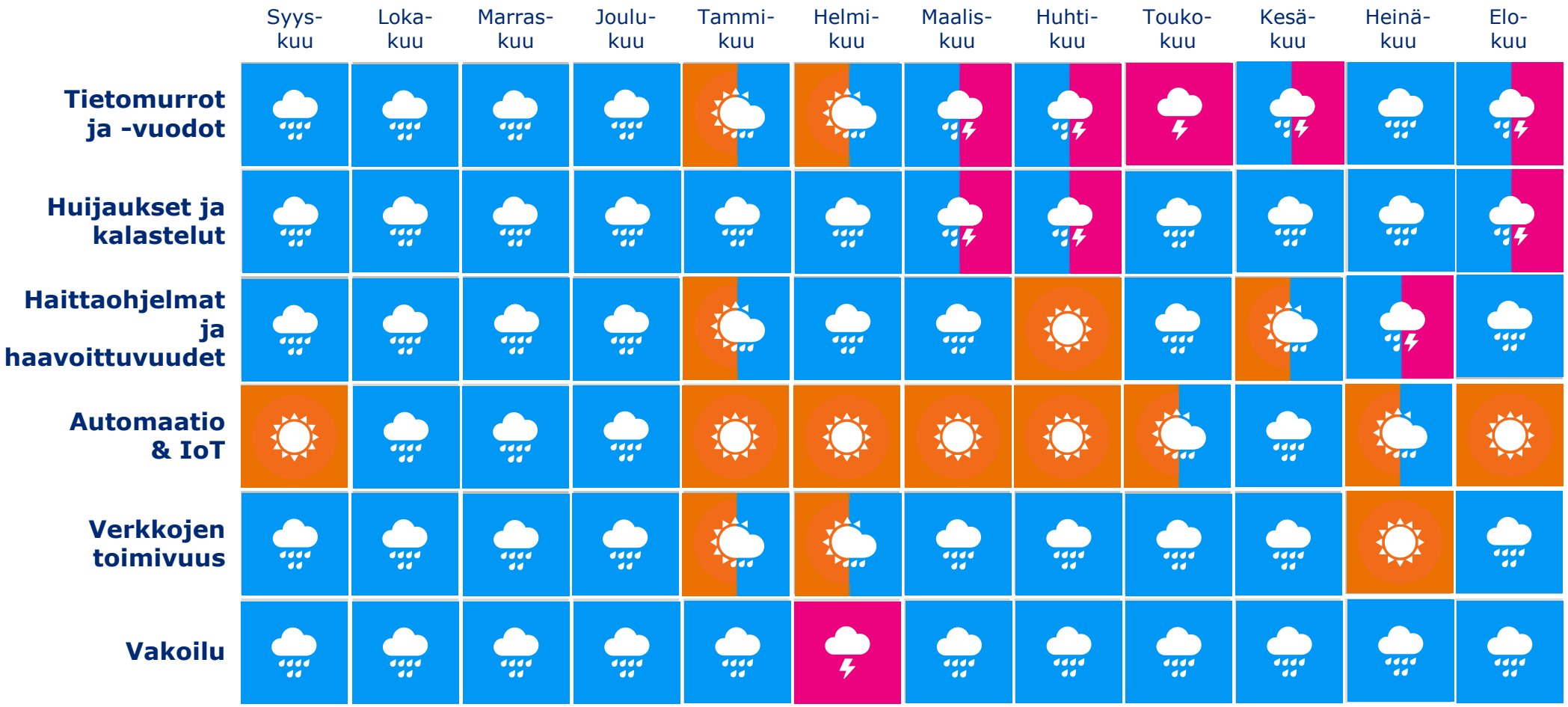
- Elokuun aikana nähtiin paljon turvapostiteemaisia huijausviestejä. Myös tunnettujen toimijoiden kuten Poliisin, Postin ja Veron nimissä yritettiin jälleen huijata tietoja sekä rahaa viestien vastaanottajilta.
- Elokuussa nähtiin verkon yli hyväksikäytettävän Citrix Netscaler -haavoittuvuuden erittäin nopea ja automatisoitu hyväksikäyttökampanja. Hyväksikäyttö mahdollisti järjestelmään takaportin (webshell) jättämisen, ja se säilyi järjestelmän päivityksenkin jälkeen.
- Syyskuun alkupuolella haktivistiryhmä ilmoitti hyökänneensä useita eurooppalaisia kyberturvallisuusviranomaistahoja kohtaan.
  - Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus oli yksi ilmoitetuista kohteista.
  - Palvelunestohyökkäysten vaikutus palveluiden toimintaan on yleensä tilapäinen. Niitä on usein rinnastettu verkossa toteutettuun ruuhkaan tai mielenilmaukseen, joiden tavoitteena onkin saada aikaan uutisointia.

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
- 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:
Kybervakoilun ja rikollisuuden rajojen hämärtyminen

- Suojelupoliisin mukaan kybervakoilu on edullinen ja tehokas tiedustelun keino, jonka avulla voidaan pyrkiä pääsemään käsiksi isoihin määriin salassa pidettäviä tietoja.[9]
- Kybervakoilua voidaan tehdä esimerkiksi hyödyntämällä haavoittuvuuksia, joiden kautta voidaan päästä käsiksi järjestelmiin.
- Yhdysvallat ja Iso-Britannia ovat asettaneet pakotteita Trickbot-haittaohjelmaan ja Conti-kiristyshaittaohjelmaan linkitetyn venäläisen kyberrikollisryhmän jäseniä vastaan. Ryhmällä on kytköksiä venäläisiin tiedustelupalveluihin.[10]
  - Ryhmän toimet ja kohteet ovat olleet samansuuntaisia kuin Venäjän tiedustelupalveluilla, ja ryhmän toimet ovat linjassa myös Venäjän valtiollisten tavoitteiden kanssa.[11]
- Onkin tärkeää, että järjestelmät päivitetään ja pidetään aina ajan tasalla.

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

EU:n radiolaitedirektiivin (RED) delegoidun tietoturvasäädöksen ((EU) 2022/30) harmonisoitujen standardien lausuntokierros on käynnistynyt 30.8.2023.

- Artiklan 3 kohtaa 3 d, e ja f tarkentavat standardit kuvaavat vaatimukset, joilla suojataan viestintäverkkoja ja parannetaan käyttäjien yksityisyyden suojaa. Lisäksi ne estävät taloudelliseen hyötyyn tähtääviä petoksia, joissa hyödynnetään verkkoon liitettyjä laitteita.
  - Tietoturvavaatimukset koskevat radiolaitedirektiivin soveltamisalaan kuuluvia internetiin liitettäviä leluja ja laitteita, kuten lastenhoitoon liittyviä ja päälle puettavia laitteita. Tuotteet, jotka eivät täytä vaatimuksia, voidaan poistaa markkinoilta.
- Komissio päätti 20.7.2023 siirtää vaatimusten soveltamisen aloittamista vuodella. Soveltaminen aloitetaan 1.8.2025.
- Standardit ovat lausunnolla 4.11.2023 saakka, ja niihin voi tutustua SFS:n lausuntoportaalissa.[12]

Oikeudelliset asiat

Rautateiden kansainvälinen kyberturvallisuusstandardin luonnos "IEC CD 63452 Railway applications - Cybersecurity" etenee kohti kansallista lausuntokierrosvaihetta.

- Kehitettävä standardi on ensimmäinen laatuaan, ja sillä on keskeinen merkitys rautateiden kyberturvallisuuden kehityksessä. Suomessa Sesko ry:n jäsenet Väylävirasto ja Traficom ovat tiiviisti osallistuneet standardointiryhmän työskentelyyn
  - Standardiluonnos on kehitetty CENELEC-standardointiorganisaation teknisen eritelmän (TS) 50701 pohjalta.
- Kehitettävän standardin käytännön soveltaminen on tärkeässä roolissa Digirata -hankkeessa, jossa uudistetaan junien kulunvalvonta Suomessa. Digirata-hankkeessa sovelletaan jo mainittua rautateiden kyberturvallisuuden teknistä eritelmää (TS 50701 Railway applications - cybersecurity).

Oikeudelliset asiat

Hyväksyttävät menetelmät ja ohjeet ilmailun kyberturvallisuuden EU-vaatimusten täyttämiseen julkaistu.[13]

- Euroopan unionin lentoturvallisuusvirasto EASA julkaisi 13.7.2023 hyväksyttävät menetelmät vaatimusten täyttämiseksi (AMC-materiaali) sekä ohjemateriaalin (GM) ilmailun tietoturvanhallintaa koskeviin EU-asetuksiin (Part-IS, information security)
- Aiemmin julkaistut asetukset ja nyt julkaistu AMC- ja GM-materiaali yhdenmukaistavat ja tarkentavat tietoturvanhallinnan velvoitteita suhteessa ilmailun turvallisuuteen kohdistuviin riskeihin sekä kattavat ilmailun keskeisimmät toimijat

Oikeudelliset asiat

Tietosuojavaltuutettu (TSV) kieltää väliaikaisesti Yango-taksipalvelun henkilötietojen siirrot Suomesta Venäjälle.[14, 15]

- TSV on 8.8.2023 antanut Yandex LLC:lle ja Ridetech International B.V.:lle määräyksen keskeyttää Yango-taksipalvelussa kerättyjen asiakkaiden henkilötietojen siirtämisen Venäjälle ja lopettamaan kerättyjen henkilötietojen käsittelyn. Kyse on väliaikaisesta määräyksestä, joka on voimassa kolme kuukautta 27.9. alkaen.
  - Taustalla Venäjällä syyskuun alussa voimaan astuva lainsäädäntöuudistus, jonka nojalla Venäjän turvallisuuspalvelulla olisi jatkossa oikeus saada taksitoiminnassa käsiteltäviä tietoja. Yangon taksisovelluksessa kerättyjä tietoja voivat olla esimerkiksi asiakkaan sijaintitiedot sekä taksikyydin osoitetiedot.
  - TSV katsoo, että Yangon ei välttämättä ole mahdollista suojata henkilötietoja EU:n lainsäädännön edellyttämällä tavalla etenkään Venäjän lainsäädäntöuudistuksen jälkeen.
- Asian tarkempaa selvittämistä jatketaan Alankomaiden ja Norjan tietosuojaviranomaisten kanssa.

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) S-Pankin asiakkailta tietoja huijanneelle viisi vuotta vankeutta https://www.talouselama.fi/uutiset/s-pankin-asiakkailta-tietoja-huijanneelle-viisi-vuotta-vankeutta/e4c26ba8-c972-41c8-b1e4-68f078354d3f
2) Qakbot Malware Disrupted in International Cyber Takedown https://www.justice.gov/opa/pr/qakbot-malware-disrupted-international-cyber-takedown
3) Midnight Blizzard conducts targeted social engineering over Microsoft Teams https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/
4) Uusi työkalu helpottaa kyberharjoituksen suunnittelua https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uusi-tyokalu-helpottaa-kyberharjoituksen-suunnittelua
5) Tietoturva 2023 -seminaari https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2023-seminaari
6) Miten pyydän tietojeni poistamista Yango-taksipalvelulta? https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/miten-pyydan-tietojeni-poistamista-yango-taksipalvelulta
7) Tonttu-projektit https://www.kyberturvallisuuskeskus.fi/fi/tonttu
8) Merenkulun kyberturvallisuus https://www.traficom.fi/fi/liikenne/merenkulku/merenkulun-kyberturvallisuus

Lähdeluettelo

9) Suojelupoliisi torjuu vakoilua myös verkossa https://supo.fi/kybervakoilu
10) UK sanctions members of Russian cybercrime gang https://www.gov.uk/government/news/uk-sanctions-members-of-russian-cybercrime-gang
11) United States and United Kingdom Sanction Additional Members of the Russia-Based Trickbot Cybercrime Gang https://home.treasury.gov/news/press-releases/jy1714
12) Lausuntopyyntöpalvelu https://lausunto.sfs.fi/
13) Hyväksyttävät menetelmät ja ohjeet ilmailun kyberturvallisuuden EU-vaatimusten täyttämiseen julkaistu https://traficom.fi/fi/ajankohtaista/hyvaksyttavat-menetelmat-ja-ohjeet-ilmailun-kyberturvallisuuden-eu-vaatimusten
14) Tietosuojavaltuutettu kieltää Yango-taksipalvelun henkilötietojen siirrot Suomesta Venäjälle väliaikaisesti https://tietosuoja.fi/-/tietosuojavaltuutettu-kieltaa-yango-taksipalvelun-henkilotietojen-siirrot-suomesta-venajalle-valiaikaisesti
15) Tietosuojaviranomaiset jatkavat Yango-taksipalvelun tietojen siirron tutkintaa https://tietosuoja.fi/-/tietosuojaviranomaiset-jatkavat-yango-taksipalvelun-tietojen-siirron-tutkintaa