TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Toukokuu 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

36

Modernien tietoturvaratkaisujen ja -innovaatioiden käyttöönoton tukea myönnettiin 36 yritykselle.[1]

560 MILJ.

Julkisten tietojen mukaan 560 miljoonaa lipunvälityspalvelu Ticketmasterin käyttäjätietoa on vuotanut tietomurron seurauksena.[2]

~70

Traficomin ja Huoltovarmuuskeskuksen järjestämä Hack the Networks -tapahtuma keräsi Otaniemeen noin 70 hakkeria testaamaan paikallisten 5G-verkkojen tietoturvaa.[3]

Kybersää toukokuu 2024

Tietomurrot ja -vuodot

- Helsingin kaupungin kasvatuksen ja koulutuksen toimialaan kohdistui laaja tietomurto.
- Viranomaisrekistereihin tehtiin kymmeniä tuhansia luvattomia hakuja asiakasorganisaatioon kohdistuneen tietomurron seurauksena.
- Rikollisten haltuun on päätynyt arvion mukaan satojatuhansia henkilötietoja.

Huijaukset ja kalastelut

- M365-tilimurroissa on havaittu uusi Microsoft Planner -kalasteluteema.
- Toukokuun päätteeksi käynnistyi laaja tekstiviestihuijauskampanja, jossa uhkailtiin maksamattomalla sakolla Traficomin nimissä. Linkki johti pankkitunnuskalasteluun.

Haittaohjelmat ja haavoittuvuudet

- 911 S5 -bottiverkossa tuhansia suomalaisia IP-osoitteita mukana.
- Pankkitietoja varastetaan uudella Android-haittaohjelmalla.
- Check Point Quantum Gateway -palomuurituotteiden haavoittuvuutta hyväksikäytetty.

Automaatio ja IoT

- Poliittisesti motivoituneet hakkerit kohdistivat maailmalla hyökkäyksiä teollisuuden ohjausjärjestelmiin.
- Tietomurtoja tapahtui mm. heikosti suojattuihin ohjelmoitaviin logiikkaohjaimiin ja teollisuusreitittimiin.[4, 5]
- Automaatiojärjestelmien turvallisuuskontrollit on hyvä tarkastaa säännöllisesti.[6]

Verkkojen toimivuus

- Huhtikuussa yleisissä viestintäpalveluissa oli 10 toimivuushäiriötä.
- Palvelunestohyökkäyksiä raportoitiin kuukauden aikana vähän ja niiden vaikutukset jäivät lieviksi.

Vakoilu

- Puola kertoi valtionhallintoonsa kohdistuneesta kampanjasta, jossa kohteille oli lähetetty haitallisia sähköposteja. Tekijänä arvioitiin olevan Venäjän sotilastiedusteluun yhdistetty APT28-ryhmä.[7, 8, 9]
- Saksassa puolestaan kerrottiin APT28:n vakoilleen sosiaalidemokraattisen puolueen sähköposteja vuonna 2022 alkaneessa murrossa.

Kyberturvallisuuskeskuksen toimenpiteet ja vinkit varautumiseen

Kyberuhkien lieventäminen rajallisilla resursseilla - ohje kansalaisyhteiskunnalle on julkaistu.[10]

Traficom on laatinut suositusluonnoksen NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä. Suositusluonnoksessa esitetään myös perustason tietoturvakäytännöt. Kyberhygieniakäytännöt luovat perustan organisaation kyberturvallisuudelle.[11]

Päivittämättömiä verkon reunalaitteita hyväksikäytetään edelleen runsaasti tietomurroissa. Organisaatioiden tulisi huolehtia siitä, että kyseiset tuotteet on otettu käyttöön tietoturvasta huolta pitäen ja päivitykset ovat aina ajan tasalla.[12]

Kansallinen koordinointikeskus (NCC-FI) järjestää maksuttoman kaksiosaisen Digitaalinen Eurooppa -ohjelman kyberturvallisuushakujen esittely- ja hakemuskoulutuksen 18.6. & 28.6.2024. Ilmoittaudu mukaan![13]

Toukokuun kyberturvallisuuden yleiskuva

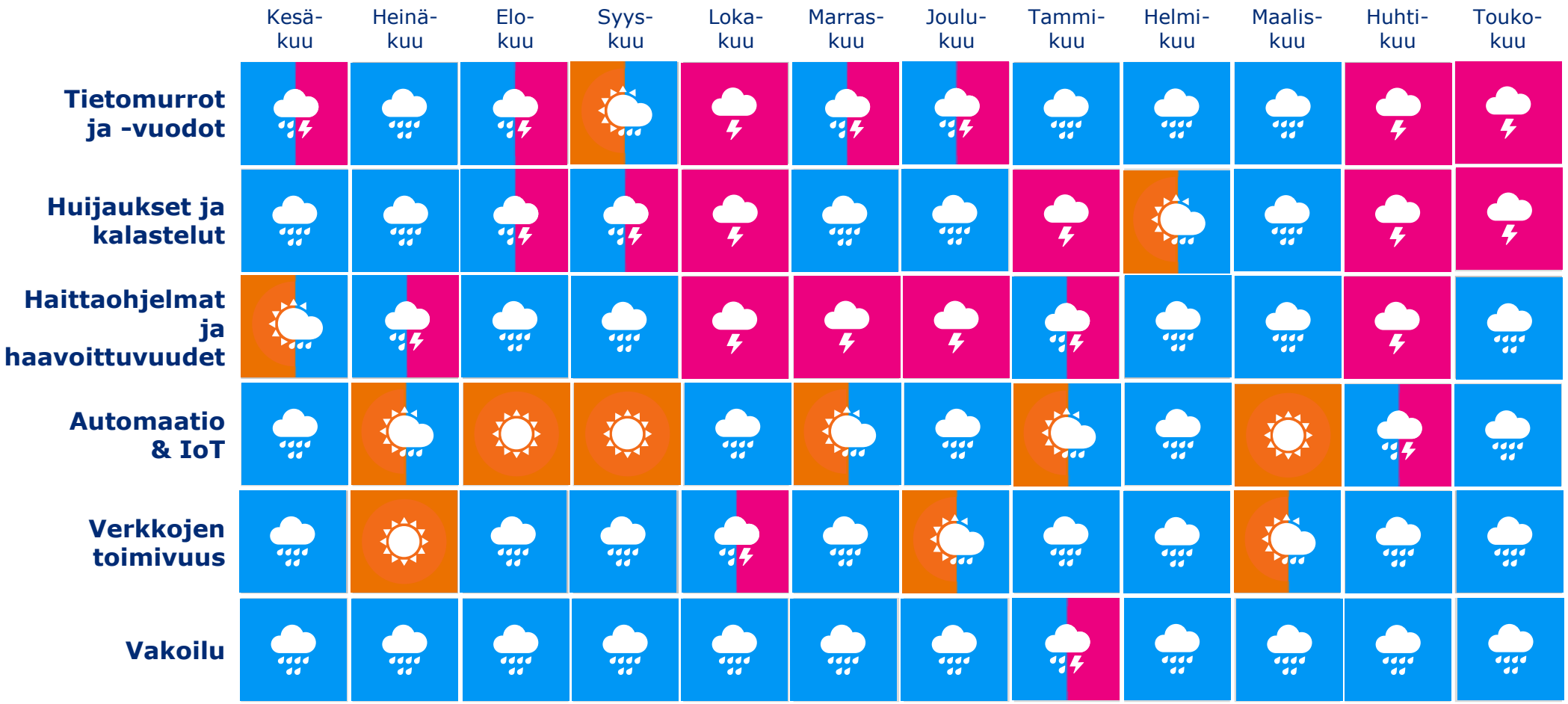
- Toukokuussa 2024 suljettu 911 S5 -bottiverkko tarjosi rikollisille pääsyn vaarantuneisiin IP-osoitteisiin ja niihin liittyviin yksityishenkilöiden ja yritysten omistamiin laitteisiin. Joukossa oli myös tuhansittain suomalaisia IP-osoitteita.[14]
  - Ilmaiset, laittomat VPN-palvelut oli pakattu piraattivideopeleihin ja ohjelmistoihin, joita uhrit latasivat laitteilleen. Kun lataus oli valmis, VPN-sovellus ja välityspalvelimen takaovi asentuivat uhrien tietämättä heidän laitteisiinsa, ja heistä tuli tietämättään osa 911 S5 -bottiverkkoa.
- Menneen kuukauden aikana Suomessa tapahtuneet tietomurrot ja -vuodot ovat olleet poikkeuksellisen laajoja.
- Microsoft Planner aikataulutus- ja tehtävienjakosovelluksen teemaa käytetään kalastelussa jakamalla sieltä PDF-tiedosto, jossa on linkki kalastelusivulle.
  - Kyberturvallisuuskeskukselle ilmoitettiin 53 Microsoft 365 -sähköpostitunnusten kalastelua. Niistä 25 oli johtanut Microsoft 365 -sähköpostitilin tietomurtoon.

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

Tekoäly

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:
Toimitusketjujen tietoturva

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä. Valtaosa organisaatioista on enemmän tai vähemmän riippuvaisia ulkoistetuista digitaalisista palveluista. Organisaatioissa pitäisi aina olla tietoisuus, miten asiat on sovittu palveluntarjoajien kanssa.

- Toimitusketjuhyökkäyksen havainnointi ja hallinta ovat tärkeitä paitsi oman toiminnan jatkuvuuden kannalta, myös koska niillä on suuri merkitys organisaation maineelle ja luottamukselle verkostossa. Toimitusketjuhyökkäyksen uhrina ovat sekä toimittaja että asiakas. Tilanteen hallinta vaatii usein avoimuutta ja yhteistyötä osapuolilta.
- Kyberturvallisuuskeskuksen tekemän selvityksen mukaan yhdellä organisaatiolla on keskimäärin 35 toimittajaa, joista sen omat toiminnot ovat riippuvaisia.[15]
- Enisan kesällä 2023 julkaiseman raportin mukaan organisaatiot ymmärtävät toimitusketjujen turvallisuuden tärkeyden, mutta toimitusketjujen turvaamiseksi ei siitä huolimatta osoiteta tarpeeksi resursseja.[16]
  - Raportin mukaan organisaatioilla ei useinkaan ole riittävän kattavaa haavoittuvuuksien hallintajärjestelmää.
- Kyberturvallisuuskeskus toteutti vuonna 2023 Huoltovarmuuskeskuksen rahoittaman Ketjutonttu-kampanjan, jossa osallistujille tarjottiin maksuton toimitusketjujen tietoturvan tarkastus. Kampanjan tulosraportin mukaan joka seitsemännellä toimittajalla oli korjattavaa tietoturvassaan.[15]
  - Seuraavia puutteita havaittiin: alidomainin haltuunottoriski, vanhentuneet palvelimet ja palvelut sekä altistuneet verkkopalvelut (tietokannat, etähallinnat, tiedostonjaot).

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

- **Avaruustilannekeskuksen perustaminen**[17]
  - Liikenne- ja viestintäministeriö (LVM) pyytää sidosryhmiä lausumaan hallituksen esitysluonnoksesta laeiksi Ilmatieteen laitoksesta annetun lain sekä Puolustusvoimista annetun lain muuttamisesta.
  - LVM:n ohjausryhmä selvitti, miten Suomen kansallista avaruustilannekuvatoimintaa tulisi kehittää. Ohjaustyhmä suosittaa, että Suomeen perustettaisiin kansallinen avaruustilannekeskus, joka aloittaisi toimintansa vuoden 2025 alusta.
  - Kuten kyberturvallisuuteen liittyvissä valtion toimenpiteissä, Suomen kansallisen avaruustilannekeskuksen perustamisen lähtökohtana on pyrkimys minimoida ja hallita kansalliseen turvallisuuteen liittyviä uhkia.
  - Keskuksen on tarkoitus tuottaa ja ylläpitää koordinoitua avaruustilannekuvaa, jotta Suomessa voitaisiin hyvissä ajoin havaita, tunnistaa ja ennakoida avaruudesta ja avaruustoiminnasta yhteiskunnan turvallisuudelle ja häiriöttömälle toiminnalle aiheutuvia uhkatilanteita.
  - Lausuntoja voi antaa 27.5.-30.6.2024.

Oikeudelliset asiat

- **Kyberturvallisuuslaki (NIS2) etenee eduskunnassa**[18, 19]
  - Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi annettiin 23.5.2024.
  - 30.5.2024 asia on siirtynyt liikenne- ja viestintävaliokuntaan mietinnön antamista varten, sekä perustuslakivaliokuntaan ja hallintovaliokuntaan lausunnon antamista varten.

- **Tietosuojavaltuutetun toimisto selvittää Helsingin kaupunkiin kohdistunutta tietoturvaloukkausta**[20]
  - Asiaa tutkitaan tietosuojalainsäädännön noudattamisen näkökulmasta, eli onko kaupunki huolehtinut asianmukaisesti tietosuojavaatimuksista, ja ovatko sen suojatoimet olleet puutteelliset.

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 - 20/2024
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-202024
2) Kyberturvallisuuskeskuksen viikkokatsaus - 22/2024
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-222024
3) Kyberturvallisuuskeskuksen viikkokatsaus - 21/2024
   https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-212024
4) Urgent Warning from Multiple Cybersecurity Organizations on Current Threat to OT Systems
   https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3761830/urgent-warning-from-multiple-cybersecurity-organizations-on-current-threat-to-o/
5) Defending Ot Operations Against Ongoing Pro-russia Hacktivist Activity
   https://media.defense.gov/2024/May/01/2003454817/-1/-1/0/DEFENDING-OT-OPERATIONS-AGAINST-ONGOING-PRO-RUSSIA-HACKTIVIST-ACTIVITY.PDF
6) Rekomendacje dla wzmocnienia ochrony systemów OT https://cert.pl/posts/2024/05/rekomendacje-ot/

Lähdeluettelo

7) APT28 campaign targeting Polish government institutions https://cert.pl/en/posts/2024/05/apt28-campaign/
8) Germany warns of consequences for alleged Russian cyber attack https://www.reuters.com/technology/cybersecurity/germany-warns-consequences-alleged-russian-cyber-attack-2024-05-03/
9) German foreign minister summons Russia over 2023 cyber-attacks https://www.lemonde.fr/en/europe/article/2024/05/03/german-foreign-minister-summons-russia-over-2023-cyber-attacks_6670339_143.html
10) Kyberuhkien lieventäminen rajallisilla resursseilla - ohje kansalaisyhteiskunnalle julkaistu https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberuhkien-lieventaminen-rajallisilla-resursseilla-ohje-kansalaisyhteiskunnalle
11) Mitä NIS2-direktiivissä esitetyt kyberhygieniakäytännöt ovat? https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mita-nis2-direktiivissa-esitetyt-kyberhygieniakaytannot-ovat
12) Riskialttiit verkon reunalaitteet aktiivisten murtoyritysten kohteena https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/riskialttiit-verkon-reunalaitteet-aktiivisten-murtoyritysten-kohteena

Lähdeluettelo

13) Info- ja koulutuswebinaari 18.6. & 28.6.2024: Digitaalinen Eurooppa -ohjelman heinäkuun 2024 kyberturvallisuushaut https://www.kyberturvallisuuskeskus.fi/fi/info-ja-koulutuswebinaari-186-2862024-digitaalinen-eurooppa-ohjelman-heinakuun-2024
14) 911 S5 -bottiverkossa tuhansia suomalaisia IP-osoitteita mukana https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/911-s5-bottiverkossa-tuhansia-suomalaisia-ip-osoitteita-mukana
15) Tonttu-projektit - uusien menetelmien toteutettavuustestaus https://www.kyberturvallisuuskeskus.fi/fi/tonttu
16) Good Practices for Supply Chain Cybersecurity https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity/
17) Hallituksen esitys eduskunnalle laeiksi Ilmatieteen laitoksesta annetun lain ja Puolustusvoimista annetun lain muuttamisesta https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=dfad9649-383c-4a03-826a-d782ddd66800&proposalLanguage=da4408c3-39e4-4f5a-84db-84481bafc744

Lähdeluettelo

18) Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_57+2024.aspx

19) Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_57+2024.pdf

20) Tietosuojavaltuutetun toimisto selvittää Helsingin kaupunkiin kohdistunutta tietoturvaloukkausta https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-selvittaa-helsingin-kaupunkiin-kohdistunutta-tietoturvaloukkausta