TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Marraskuu 2021

#kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tämä tuote on ensisijaisesti suunnattu tietoturvasta vastaaville henkilöille. Lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen huolestuttava vakava

TRAFICOM

Kybersää marraskuu 2021

Tietomurrot ja -vuodot

- DVV on julkaissut Suomi.fi-verkkopalveluun sähköisen oppaan tietomurron tai tietovuodon kohteeksi joutuneelle organisaatiolle.
- Tanskalainen tuuliturbiineja valmistava ja operoiva yritys oli tietomurron kohteena.

Huijaukset ja kalastelut

- Tekstiviestihuijaukset ovat lisääntyneet räjähdysmäisesti.
- Pankkitunnusten lisäksi tietojenkalastelijoita kiinnostavat yliopistojen käyttäjätunnukset ja sähköpostit.

Haittaohjelmat ja haavoittuvuudet

- Aktiivisesti hyväksikäytetyn Log4j-komponentin haavoittuvuus vaatii ylläpitäjiltä välittömiä toimia.
- FluBot-haittaohjelmaa on levitetty ahkerasti Suomessa. Levitysviesteissä on käytetty postipaketti- sekä ääniviestiteemoja.

IoT ja automaatio

- IoT:n ja automaation kyberturvallisuuteen liittyvät strategiat ja ohjeistukset lisääntyvät ja kertovat kasvavasta tietoisuudesta aihepiirin tärkeydestä.

Verkkojen toimivuus

- Kuusi merkittävää toimivuushäiriötä, joissa korostuivat muutostyöt ja ohjelmistovirheet.
- Murrettuja palvelimia käytettiin palvelunestohyökkäyksiin.
- HUS kertoi joutuneensa palvelunestohyökkäyksen kohteeksi.

Vakoilu

- Iranilaiset toimijat ovat aiempaa kiinnostuneempia myös IT-alan toimijoista ja internetpalveluntarjoajista.
- Pohjoiskorealainen ryhmittymä pyrki taas vakoilemaan tietoturvatutkijoita.
- Erilaiset verkkolaitteet ovat kybervakoilun kohteina tai sen keinovalikoimassa jatkuvasti.

TRAFICOM

Kuukauden tunnuslukuja

2100+

Saimme yli 2100 ilmoitusta FluBot-haittaohjelman levitysyrityksistä.

25.11.

Julkaisimme varoituksen tekstiviestitse levitettävästä FluBot-haittaohjelmasta.

1700+

Kyberturvallisuuskeskuksen Tietoturvaseminaarissa oli kaikkien aikojen ennätysosallistujamäärä! Mukana oli yli 1700 katsojaa.

TRAFICOM

Julkaisimme varoituksen 4/2021 Varo tekstiviestitse levitettävää haittaohjelmaa

- Julkaisimme keltaisen varoituksen 25.11.2021.
- Tekstiviestitse leviävä FluBot-haittaohjelmakampanja on edelleen aktiivinen.
- Ilmoitusmäärät levitysyrityksistä ovat laskeneet marraskuun lopun jälkeen.
- Haittaohjelma voi varastaa tietoja laitteelta ja lähettää laitteesta haittaohjelmaa levittäviä huijaustekstiviestejä.
- Aiemmilla kerroilla haittaohjelma pyrki lähettämään tuhansia viestejä uusille uhreille. Operaattorit kertovat suodattaneensa miljoonia tekstiviestejä, joiden kautta on yritetty levittää haittaohjelmaa.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/varo-tekstiviestitse-levitettavaa-haittaohjelmaa

Julkaisimme punaisen varoituksen 5/2021 Log4j-komponentin haavoittuvuus on aktiivisen hyväksikäytön kohteena - päivitä välittömästi!

- Julkaisimme keltaisen varoituksen 10.12.2021. Varoitus muutettiin punaiseksi 13.12.2021, sillä ylläpitäjiltä vaaditaan nopeaa reagointia.
- Internetpalveluissa erittäin laajasti käytetyn, haavoittuvan Log4j-komponentin hyväksikäyttötapauksia havaitaan jatkuvasti lisää.
- Julkisten tietojen perusteella haavoittuvuus on koskenut isoa osaa internetin palveluita. Tarkennamme haavoittuvuustiedotettamme, kun lisätietoja julkaistaan.
- Kyberturvallisuuskeskus tiedotti haavoittuvuudesta 13.12. pidetyssä videoneuvottelussa, jonka tallenteen voi katsoa rajoitetun ajan täältä: https://youtu.be/wDp3BBuEChw
- Lue lisää:
  - https://www.kyberturvallisuuskeskus.fi/fi/varoitus_5/2021
  - https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_38/2021

Tietoturva 2021 virtuaaliseminaari keräsi ennätysyleisön!

- Liikenne- ja viestintävirasto Traficomin ja Huoltovarmuuskeskuksen järjestämä Tietoturva 2021 -seminaari järjestettiin myös tänä vuonna virtuaalisesti.
- Kyberturvallisuuskeskuksen CERT-toiminnon (Computer Emergency Response Team) juhlavuoden kunniaksi seminaari oli avoin kaikille tietoturvasta kiinnostuneille, ja seminaaria seurasi yli 1700 katsojaa.
- Tietoturvan suunnannäyttäjä -tunnustus jaettiin seminaarissa nyt kuudetta kertaa. Tunnustus myönnettiin LähiTapiolalle ansiokkaasta yhteiskunnallisesta aktiivisuudesta tietoturva-alalla.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturva-2021-seminaari-kerasi-ennatysyleison

TRAFICOM

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon. Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

2

Käyttäjätunnukset ovat organisaation arvokasta tietoa Käyttäjätunnusten kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle.

3

Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta. Suomessa tullaan näkemään yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet eurot ovat pikkuvaluuttaa.

Symbolit

Uusi

Päivitetty

4

Pilvi on organisaatioille uutta ja pilven tietoturvan ymmärtävät parhaiten hyökkääjät. Organisaatiot ovat siirtyneet vauhdilla pilvipalveluihin ja omaa ympäristöä ja sen kyvykkyyksiä ei ymmärretä tarpeeksi.

5

Toimitus- ja palveluketjujen tietoturva on yhä kriittisempää. Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä.

TRAFICOM

1. Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon

Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

- Haavoittuvuus tarkoittaa mitä tahansa heikkoutta, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamiseksi. Haavoittuvuuksia voi olla esimerkiksi tietojärjestelmissä, sovelluksissa, laitteissa, prosesseissa, kotiautomaatiossa tai niitä voi aiheutua ihmisten toiminnan seurauksena.
- Vuonna 2020 siirryttiin kiireen vilkkaa etätyö-moodiin. Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.
- Rikolliset kehittävät hyväksikäyttömenetelmiä nopeasti heti ohjelmistopäivitysten ilmestyttyä ja tunnistavat kohteet, joita ei ole päivitetty. Erityisesti tietoturvatuotteissa olevat haavoittuvuudet ovat vakavia, sillä ne on yleensä sijoitettu muutenkin hyökkäyksille alttiisiin tietojärjestelmien kohtiin.
- Valtiolliset toimijat ovat tyypillisesti ensimmäisten joukossa hyödyntämässä uusia haavoittuvuuksia kybervakoiluun ja vaikuttamiseen. Valtiollisilla toimijoilla on myös riittävät resurssit päivitysten takaisinmallintamista varten uusien hyökkäysten mahdollistamiseksi kriittisissä ohjelmistoissa.

CASE

Atlassian Confluence Server ja Data Center -tuotteista löydettyä haavoittuvuutta (CVE-2021-26084) hyväksikäyttämällä hyökkääjä pystyi suorittamaan etänä omaa ohjelmakoodiaan palvelimella ilman tunnuksia. Poikkeavan tapauksesta tekee se, että valmistaja julkaisi päivitykset ja ilmoitti alustavasti, ettei haavoittuvuus ollut kriittinen. Aluksi arvoitiin, että järjestelmään pääsemiseksi tarvitaan käyttäjätunnus. Kaksi päivää myöhemmin havaittiin, että tunnuksia ei tarvita lainkaan, vaan haavoittuvuuden hyväksikäyttö on helpompaa. Tästä syystä valmistaja muutti haavoittuvuuden arvion kriittiseksi.

TRAFICOM

2. Käyttäjätunnukset ovat organisaation arvokasta tietoa

Käyttäjätunnusten kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle tunnusten ollessa väärissä käsissä.

- Tunnuskalastelua tehdään monella eri tavalla ja eri laitteiden kautta. Sitä kohdistetaan organisaatioihin kuin yksityishenkilöihin. Se on helppoa ja yksinkertaista, jolla saadaan merkittävää hyötyä.
- Tunnuksia pyritään myös arvaamaan koneellisesti (password spray tai brute force) tai hyödyntämään erilaisia salansanatietovuotoja.
- Organisaation tietoturva tulee olla ratkaistuna niin, että teknisten kontrolleiden tulee estää ja havaita tunnusten väärinkäytökset. Siksi on tärkeää, että esimerkiksi kaksi- tai monivaiheinen tunnistautuminen on käytössä.
- Tunnusten ja oikeuksien käytöstä tulee kertyä riittävän tarkkaa lokia, jota analysoidaan poikkeamien varalta. Lokien tulee olla myös riittävän pitkään (esim. 6kk) käytössä jälkikäteen tehtävän selvittelyn vuoksi.

CASE

Microsoftin mukaan valtion tukemat hakkeriryhmät tavoittelevat käyttäjien salasanoja ja tunnuksia hyödyntäen nk. password spray menetelmää. Se on hyökkääjälle tehokas ja vähän resurssia vaativa keino. Microsoft arvioi, että yli kolmasosa tilien vaarantumisesta on password spary-hyökkäyksiä, vaikka tällaisten hyökkäysten onnistumisprosentti tilien kohdalla on 1 %, elleivät organisaatiot käytä teknisiä kontrolleja, joiden avulla voidaan estää ja havaita tunnusten käyttö. Havaintomme mukaan myös suomalaisiin organisaatioihin kohdistuu password spray-hyökkäyksiä

TRAFICOM

3. Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta

Suomessa tullaan näkemään yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet eurot ovat pikkuvaluuttaa.

- Erityisen merkittävä uhka on kiristyshaittaohjelmahyökkäykset, joiden kohteeksi voi joutua kuka tahansa pienestä konepajasta kansainväliseen high tech -jättiin.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan takia.
- Kiristyshyökkäysten uutena ilmiönä kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.
- Toiminta on aktiivista ja kehittyy jatkuvasti.

CASE

Palvelunestohyökkäyksillä kiristäminen nousi maailmalla ilmiönä loppu-vuodesta 2020 ja ilmiö rantautui myös Suomeen. Kyberturvallisuuskeskus on saanut ilmoituksia myös vuonna 2021 aiheeseen liittyen.

Yleisesti organisaatio vastaanottaa kiristysviestin sähköpostitse, joka on allekirjoitettu näennäisesti tunnettujen haitallisten toimijoiden nimissä. Kiristysviestin lähettämisen aikoihin on joissain tapauksissa tehty myös palvelunestohyökkäys viestin tehostamiseksi. Viestissä kerrotaan organisaation kohtaavan suuren palvelunestohyökkäyksen, mikäli lunnaita ei makseta. Ohjeemme on ja pysyy: älä maksa kiristäjille.

TRAFICOM

4. Pilvi on organisaatioille uutta ja pilven tietoturvan ymmärtävät parhaiten hyökkääjät

Organisaatiot ovat siirtyneet vauhdilla pilvipalveluihin ja omaa ympäristöä ja sen kyvykkyyksiä ei ymmärretä tarpeeksi.

- Pilvipalveluratkaisuiden hahmottaminen on vaikeaa, koska ympäristö on laaja. Siirtyminen pilveen on jäänyt puolitiehen ja tietojärjestelmien migraatio on jäänyt viimeistelemättä. Vanhoja palveluita voidaan edelleen hyväksikäyttää.
- Aivan kuten perinteisessä tietoverkossa, mikäli hyökkääjä onnistuu pääsemään pilven reunalle, voi sen kautta levittäytyä myös organisaation muihin verkon segmentteihin pilven ulkopuolellakin.
- Tarve kehittää yleisesti hyväksytyt tietoturvavaatimukset pilvipalveluille.
- Suomessa pilven tietoturvavaatimuksia on lähestytty esim. PITUKRI https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkkosivuiltamme-neuvoja-pilvipalveluiden-turvalliseen-kayttoon

CASE

Alkuvuonna 2021 laajamittainen Microsoft Exchange -sähköpostipalvelimien tietomurtoaalto pyyhkäisi myös Suomen yli. Tietomurtoaaltoa tutkittaessa paljastui, että kaikilla pilvipalveluiden käyttöön siirtyneillä organisaatioilla oli edelleen käytössään myös murrettavissa oleva perinteinen Exchange-sähköpostipalvelin. Osalla palvelin oli edelleen jossain marginaalisessa käytössä ja osalla se oli yksinkertaisesti unohdettu sulkea pilvimigraation lopuksi. Kaikkiin palvelimiin kuitenkin murtauduttiin. Tapaus on surullinen esimerkki siitä, kuinka loppumetreillä kesken jäänyt teknologiamuutos jättää ovet auki hyökkääjille.

TRAFICOM

5. Toimitus- ja palveluketjujen tietoturva on yhä kriittisempää

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä.

- Organisaatiot ostavat yhä enemmän palveluita ulkoisilta palveluntarjoajilta.
- Organisaatioiden olisi keskeistä ymmärtää omat alihankkijaketjunsa. On tärkeä ymmärtää kolmannen osapuolen tietoturvan taso. Esimerkiksi:
  - Konsultit ja heidän oman organisaation sisäiset järjestelmät.
  - Laitteistot ja palvelut joita voidaan käyttää joko osana omaa tuotetta tai palvelukokonaisuutena, tai ostettuna palveluna.
  - Organisaation tulee ymmärtää alihankinnanketju, myös alihankkija voi hankkia tuotteen/palvelun seuraavalta ketjussa olevalta palveluntarjoajalta.
- Organisaation tulisi kartoittaa, mistä osista sen eri palvelut muodostuvat, jotta ison kokonaisuuden voi hahmottaa. Erityisesti hankintavaiheessa tällaisen tekeminen on oleellista.
- On hyvä ymmärtää, että käytettävien palvelujen kautta voidaan murtautua organisaation, jos (kyber)turvallisuutta ei ole huomioitu.

CASE

Viime joulukuussa paljastunut Yhdysvaltojen hallintoon ja lukuisiin yrityksiin iskenyt SolarWinds-hyökkäys on merkittävä tietoturvatapaus. Tietomurron ja vakoilun mahdollistanut takaovi onnistuttiin levittämään tuhansiin organisaatioihin, joita oli myös Suomessa. Erilaiset toimitus- ja alihankintaketjut voivat mahdollistaa hyökkääjille keinon päästä huomaamattomammin varsinaiseen kohteeseensa tai saamaan samalla kertaa pääsyn laajaan kohdejoukkoon.

TRAFICOM

Tietomurrot ja -vuodot

Tietomurroissa ja -vuodoissa käsitellään suojauskeinoja sekä tietoomme tulleita trendejä tietomurroista ja –vuodoista. Onnistuneilla tietomurroilla voidaan aiheuttaa kohdeorganisaatiolle esimerkiksi merkittäviä taloudellisia tappioita sekä mainetappioita.

TRAFICOM

Tietomurrot ja -vuodot

- Tapahtuiko organisaatiossasi tietomurto tai tietovuoto?
  - Digi- ja väestötietovirasto on julkaissut Suomi.fi-verkkopalveluun sähköisen oppaan tietomurron tai tietovuodon kohteeksi joutuneelle organisaatiolle.
  - Oppaasta yritykset, yhteisöt ja muut organisaatiot saavat tietoa, kuinka toimia, jos epäilevät organisaationsa joutuneen tietomurron uhriksi tai jos organisaation hallussa olevia salassa pidettäviä tietoja on vuotanut julkisuuteen.
    - Ohjeet organisaatioille: https://www.suomi.fi/oppaat/tietomurto
    - Ohjeet yksityishenkilöille: https://www.suomi.fi/oppaat/tietovuoto

Analyysi

- Nyt julkaistu opas on jatkoa keväällä 2021 julkaistulle oppaalle, jossa ohjeistetaan, mitä yksityishenkilön tulee tehdä, jos epäilee henkilötietojensa joutuneen vääriin käsiin.
- Oppaat on julkaistu suomeksi, ruotsiksi ja englanniksi.

Tietomurrot ja -vuodot

- Tanskalainen Vestas tietomurron kohteena
  - Tuulivoimaloiden turbiineja valmistava ja operoiva Vestas joutui kiristyshaittaohjelman kohteeksi marraskuussa.
  - Vestaksen mukaan kyseessä oli heidän sisäisiä järjestelmiään koskenut kiristyshaittaohjelma, eivätkä asiakastiedot olleet vaarassa.
  - Koska Vestas ei maksanut vaadittuja lunnaita, rikollinen julkaisi varastetut tiedot Internetissä.
  - Tähän mennessä julkaistut asiat eivät ole olleet tietoturvamielessä kriittisiä.

Analyysi

- Kyberturvallisuuskeskus toimitti tietomurtoon liittyen neuvoja energiasektorin toimijoille.
- Viimeisimmässä suosituksessa painotimme monitoroinnin ja lokituksen tärkeyttä.
- Vestaksen julkisuuteen antamien tietojen mukaan tuuliturbiineihin ja niiden ohjaukseen tietomurrolla ei olisi suoraa vaikutusta.

Huijaukset ja kalastelut

Huijauksiin ja tietojenkalasteluun sisältyy käyttäjätunnusten ja salasanojen kalastelua, laskutuspetoksia, yrityshuijauksia, kiristyksiä ja muita vastaavia huijauksia. Lisäksi organisaatioihin voi kohdistua pankkitunnuskalastelua, maksukorttikalastelua ja muita geneerisiä yksittäisten uhrien huijauksia.

Huijaukset ja tietojenkalastelut

- Tekstiviestihuijauksia Postin nimissä
  - Sitkeä pankkitunnusten kalastelu on marraskuussa saanut seuraa suuresta määrästä huijaustekstiviestejä.
  - Postin ja kuriiripalveluiden nimissä tehtaillaan huijauksia, joilla joko kalastellaan maksukorttitietoja tai linkki johtaa tilausansaan.
  - Postin ja UPS:n nimissä tehtaillaan myös uskottavia sähköpostihuijauksia, joissa pyydetään maksamaan paketin tullimaksuja Paysafecard-palvelulla.
  - Pakettien saapumisilmoitukseksi väärennetty tekstiviesti voi johtaa monenlaisiin eri huijaustapoihin.
  - Samaa huijausmenetelmää käytetään myös haittaohjelmien levitykseen.

Puhelin pesukoneessa?

- Whatsapp-viestejä on käytetty uudenlaiseen huijaukseen.
- Tuntemattomasta numerosta tulee viesti, jossa väitetään että "Hei äiti/isä, puhelimeni joutui pesukoneeseen ja tässä on uusi numeroni".
- Huijari väittää olevansa huijattavan lapsi, jolla on uusi puhelinnumero ja koettaa sitten saada uhrin maksamaan tekaistun laskun ulkomaiselle pankkitilille.
- Huijarit osaavat olla uskottavia ja vakuuttavia viesteissään, mutta yritys on helppo todeta huijaukseksi soittamalla lapsen oikeaan numeroon ja kysymällä suoraan, onko numero vaihtunut.

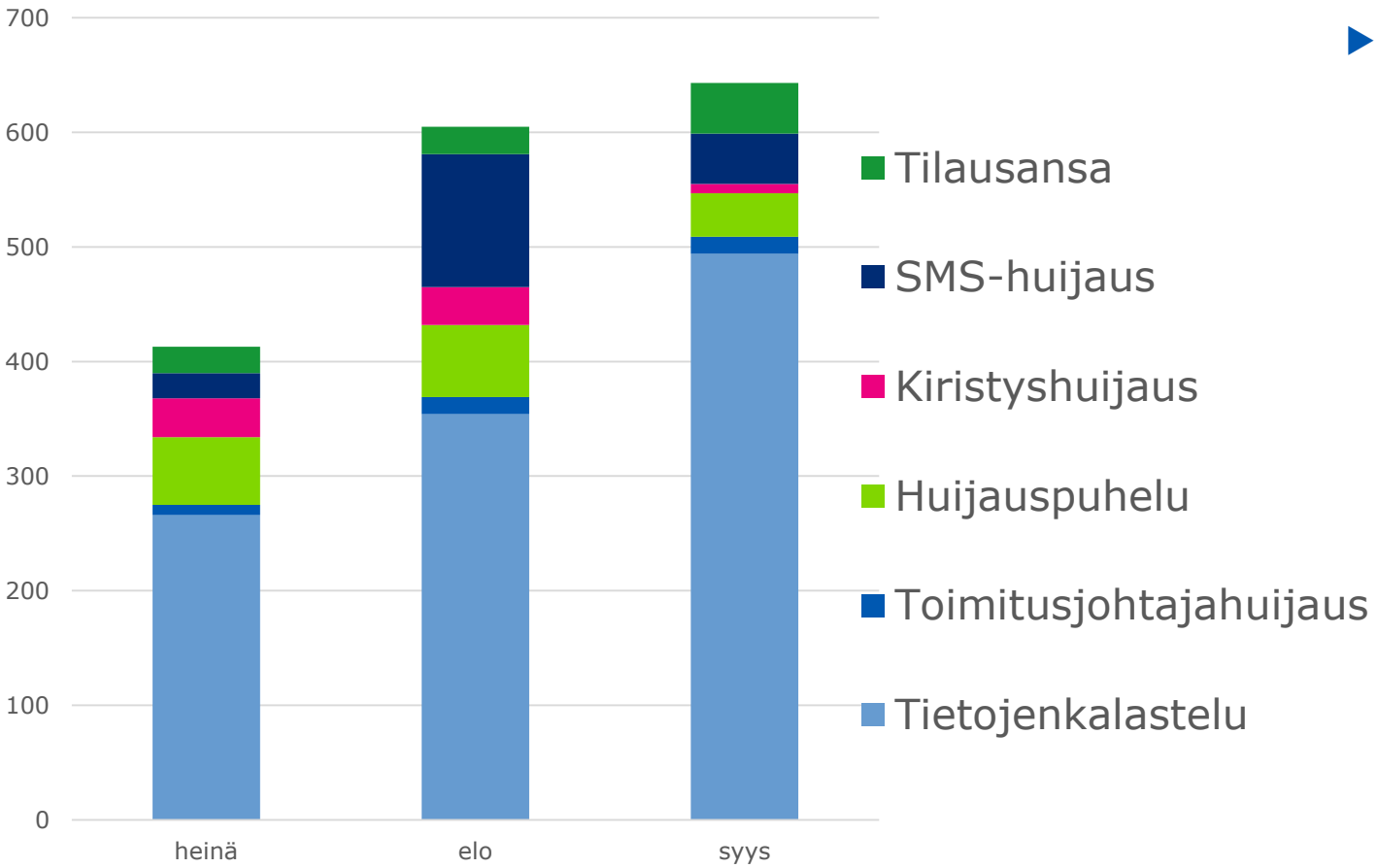
Huijaukset ja tietojenkalastelut

- Tietojenkalastelulla pyritään rahalliseen hyötyyn
  - Virtuaalivaluuttojen välitys- ja sijoituspalveluja käytetään tietojenkalastelun verukkeena aiempaa enemmän. Englanninkielisessä huijausviestissä väitetään, että tililläsi on rahaa, mutta tili pitää aktivoida. Aktivointilinkki johtaa tietojenkalastelusivulle.
  - Eri yliopistojen käyttäjätunnuksia on kalasteltu aktiivisesti marraskuussa. Pääsy yliopistojen sähköpostiin ja järjestelmiin on haluttua tavaraa esimerkiksi monilla kansainvälisillä rikollisfoorumeilla.

Some-tilejä kaapataan

- Sosiaalisen median käyttäjätilejä kaapataan aktiivisesti.
- Kaapattuja tilejä käytetään edelleen uusiin kaappauksiin.
- Huijari tekeytyy uhrin tuttavaksi, joka pyytää uhrilta puhelinnumeroa ja vahvistuskoodia. Niiden avulla käyttäjätilin voi kaapata.
- Kaapatun käyttäjätilin palauttaminen on työlästä ja hidasta. Jos tili kaapataan, ota mahdollisimman pian yhteyttä asiakaspalveluun ja ilmoita tili kaapatuksi.
- Suojautumisohjeet: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi

Käsiteltyjä huijaustapauksia Q3/2021



- Vuoden 2021 kolmannen neljänneksen ilmiöitä ovat:
  - Tietojenkalastelutapauksia on ilmoiteltu Kyberturvallisuus-keskukselle syksyn alettua merkittävästi kesää enemmän.
  - Tietojenkalasteluun pankkitunnusten kalastelu on aiheuttanut tasaista kasvua. Syyskuussa pankkikalasteluita ilmoitettiin 30 % enemmän kuin kesäkuukausina.
  - Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja järjestelmäpääsyn toivossa.

Haittaohjelmat ja haavoittuvuudet

Haittaohjelmissa ja haavoittuvuuksissa käsitellään aihealueen merkittävimmät julkaisut ja havainnot sekä annetaan toimenpidesuosituksia ja linkkejä lisätietoihin.

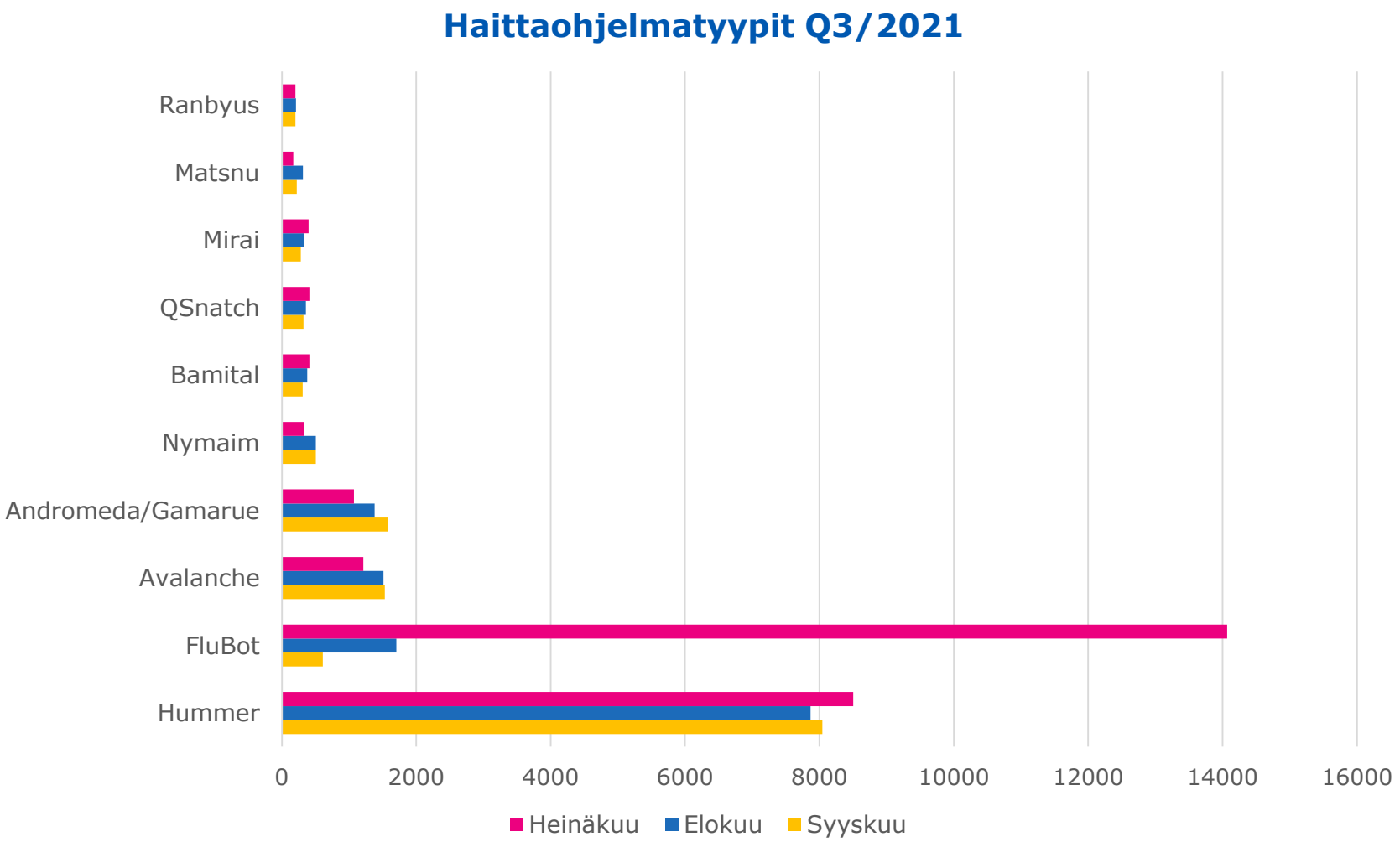
Haittaohjelmat

- FluBot-haittaohjelmaa levitetään jälleen
  - Kesäkuussa varoitimme FluBot-haittaohjelman levityksestä paketti- ja vastaaja-teemaisten viestien varjolla. Uudessa kampanjassa käytetään vastaajaviesti- ja pakettitoimitus-teemoja.
  - Norjassa estettiin marraskuun loppupuolella yli miljoona tekstiviestiä yhden päivän aikana FluBotiin liittyen.
  - Marraskuun loppupuolella haittaohjelmahavainnot alkoivat taas yleistyä myös Suomessa. Varoitimme ilmiöstä 112 Suomi -sovelluksessa.
    - 25.-30.11. välisenä ajanjaksona saimme 1089 ilmoitusta FluBot-tekstiviesteistä.
    - Kokonaisuudessaan uudesta kampanjasta on tullut Kyberturvallisuuskeskukselle yli 2100 ilmoitusta.
    - Suomalaiset operaattorit ovat kertoneet 3.12. kyvykkyydestään suodattaa tekstiviestiliikennettä.

Analyysi

- FluBotilla on kyvykkyys varastaa puhelimesta Gmail-sovelluksen tunnuksia.
- Tämän lisäksi haittaohjelma pyrkii varastamaan kryptovaluuttalompakko Binancen ja Coinbasen tietoja.
- FluBot-haittaohjelman poistaminen puhelimesta on erittäin hankalaa. Puhelin kannattaa palauttaa tehdasasetuksille, jos haittaohjelman poistamisen haluaa varmistaa.

Autoreporterin haittaohjelmahavainnot



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. Niistä voi lukea tarkempia tietoja kotisivuiltamme: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot

Katso lisää tilastoja:
https://www.traficom.fi/fi/tilastot/traficomin-haittaohjelmahavainnot

Kuukauden haavoittuvuusjulkaisut

- Palo Alto GlobalProtect -käyttöliittymissä kriittinen haavoittuvuus (34/2021)
- Hyväksikäytetty ja kriittinen Microsoft Exchange –haavoittuvuus (35/2021)
- Microsoft Windows –nollapäivähaavoittuvuus (36/2021)
- Grafana-ohjelmistossa kriittinen haavoittuvuus (37/2021)
- Kriittinen Log4shell-haavoittuvuus Apache Log4j -komponentissa (38/2021)

- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

Analyysi

- Päivitykset tulee asentaa viipymättä, sillä haavoittuvuuksien hyväksikäyttö on todella nopeaa.
- Päivityssyklien ulkopuoliset päivitykset tulee myös huomioida, muutoin järjestelmään voi jäädä kriittisiä haavoittuvuuksia pitkäksikin aikaa.
- Organisaation sisällä viestiminen on tärkeää, jotta työntekijät eivät lykkää omien päivitystensä asentamista tarpeettomasti.

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

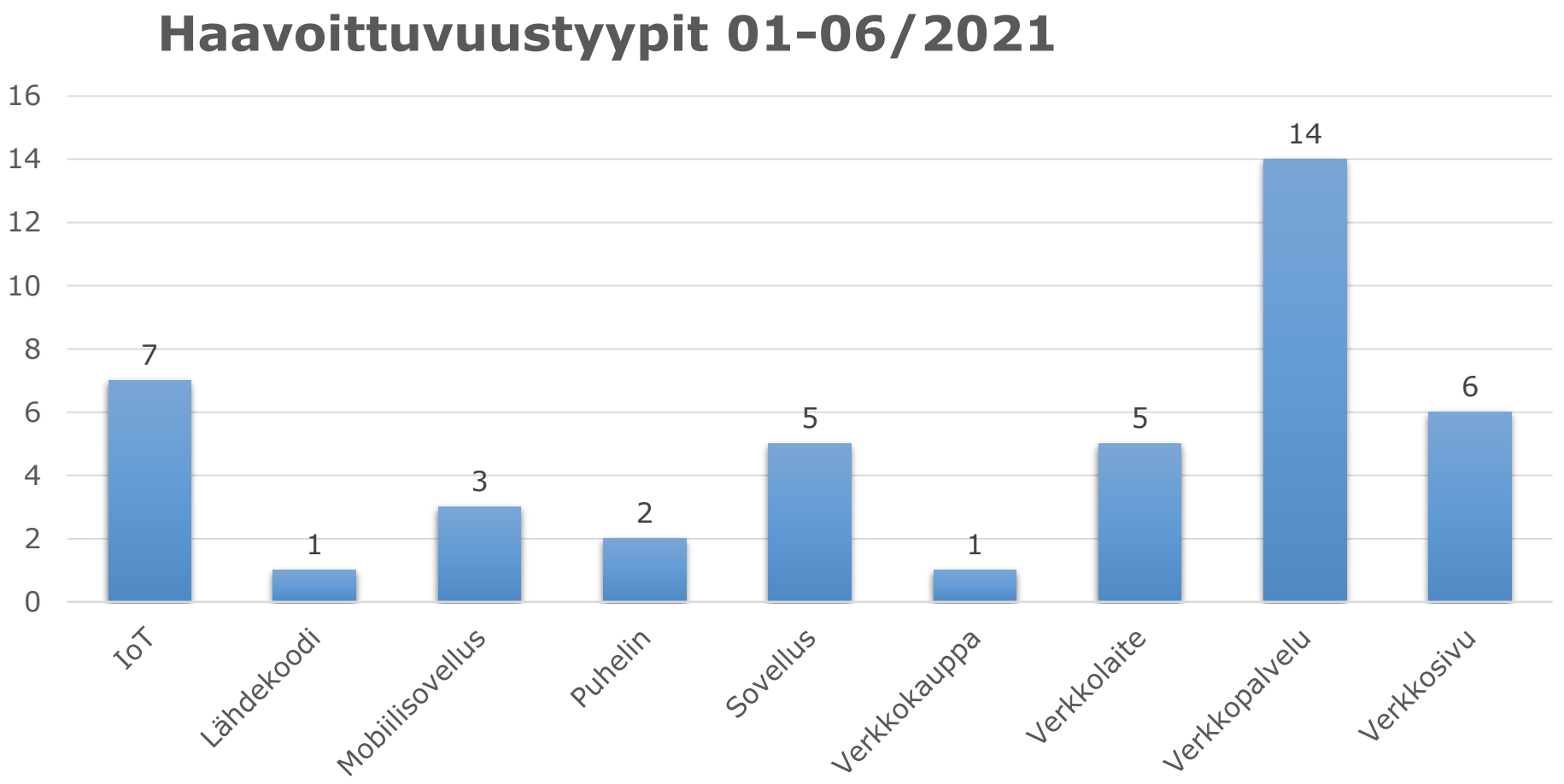
- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta
- **Haavoittuvuustiedotteita tänä vuonna 38 kpl (tilanne 14.12.2021)**
  - Mukana mm. Microsoft Exchange Server ja etäkäyttötoteutusten haavoittuvuudet
- **Tilaamalla haavoittuvuuskoosteen saat tietoa erilaisista haavoittuvuuksista**
  - Kaikista haavoittuvuuksista ei julkaista suomenkielistä haavoittuvuustiedotetta
  - Kooste julkaistaan lähes päivittäin ja sen voi tilata kotisivuiltamme https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat usein toistuva ongelma. Voi olla, että muutoin tietoturvallisesta tuotteesta löytyy kovakoodattu oletussalasana. Erilaisissa verkkopalveluissa voi myös olla parannettavaa salasanakäytännöissä esim. salasanan vaatimusten vai vaihto-ominaisuuksien osalta.
- IoT- ja verkkolaitteiden testaus on yleistä tietoturvatutkijoiden keskuudessa. Laitteiden turvallisuuden parantaminen on tärkeää verkossa ja kotona käytössä olevien laitteiden määrien jatkuvan kasvun vuoksi.
- Kyberturvallisuuskeskus saa haavoittuvuuksista ilmoituksia laidasta laitaan. Mikäli sinä tai organisaatiosi tarvitsette apua haavoittuvuuden löytyessä, haavoittuvuuden koordinoinnissa tai esimerkiksi CVE-tunnisteen haussa – olettehan yhteydessä Kyberturvallisuuskeskukseen.
- https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

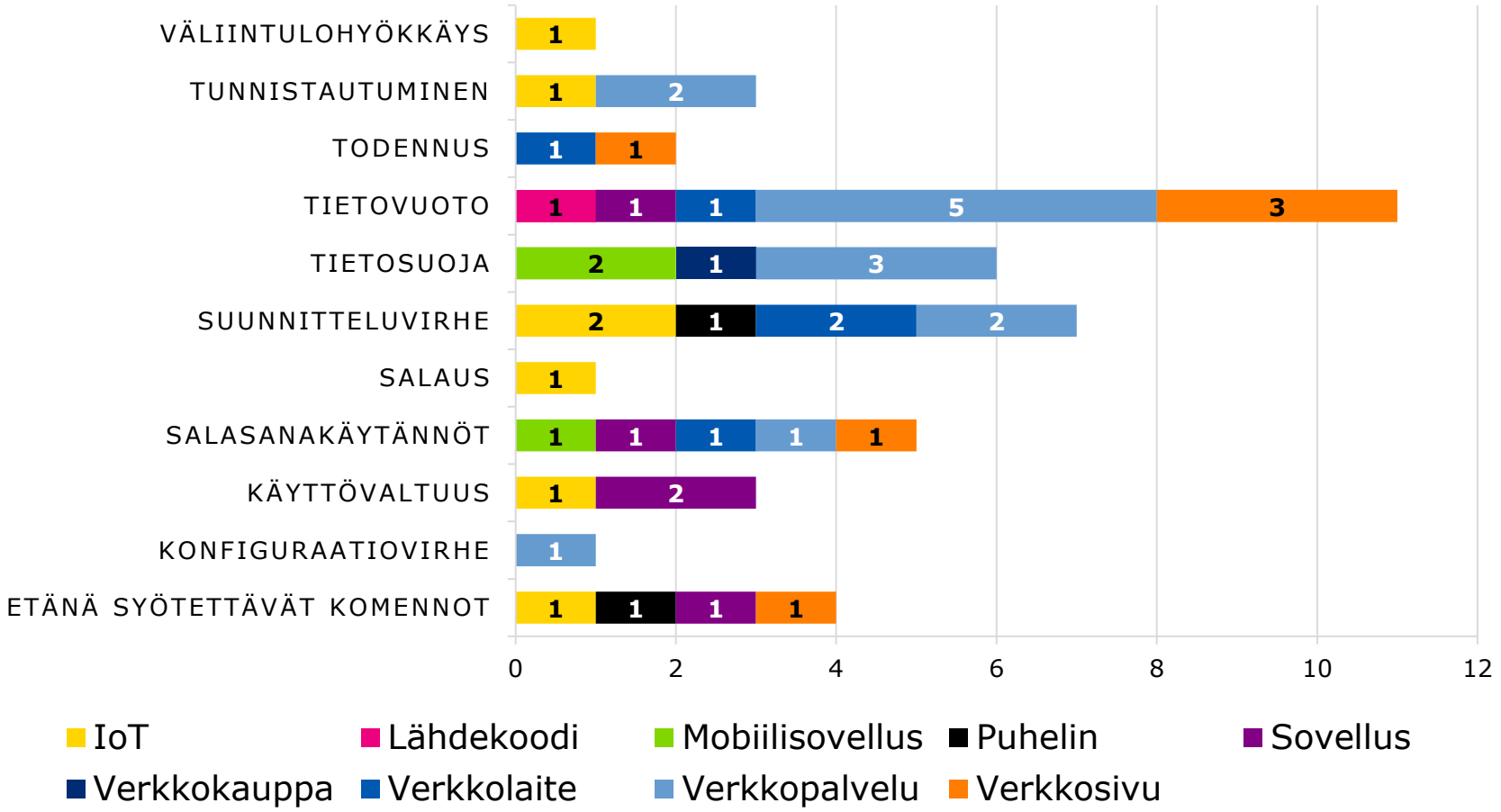
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

6kk



Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

6kk



Taulukossa on esitetty Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio-tapaukset vuodelta 2021.

Tutustu aiheeseen tarkemmin: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-haavoittuvuuskoordinaatio-pahkinankuoressa

Automaatio ja IoT

Automaatio-osiossa ilmiöseurantaryhmä seuraa alan uutisia ja ilmiöitä maailmalla ja kotimaassa. Automaatiojärjestelmiä käytetään ohjaamaan sekä monitoroimaan esimerkiksi erilaisia yksittäisiä tehtaan tai muun vastaavan tuotantolaitoksen palveluita tai laitteita.

TRAFICOM

Kansallisten kyberturvallisuus-strategioiden kehitys

- Suomen kanssa lokakuun alussa IoT-tietoturvamerkkien vastavuoroisesta tunnustamisesta sopimuksen tehnyt Singapore on julkaissut uuden Kyberturvallisuusstrategiansa
  - Strategia on rakennettu kolmen kantavan kokonaisuuden varaan. Nämä tähtäävät kriittisen infrastruktuurin resilienssin lisäämiseen, kyberavaruuden turvaamiseen ja kansainvälisen yhteistyön lisäämiseen.
  - https://www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021
- Myös muilla mailla on strategioita, jotka ottavat kantaa kriittisen infrastruktuurin automaatioon: Esimerkiksi Tanska on luonut toimialakohtaiset kyberturvallisuusstrategiat.

Analyysi

- Eri toimialojen digitalisointi ja sen vaikutukset huoltovarmuuskriittisen infrastruktuurin toimintaan ja siihen liittyviin riskeihin ovat luoneet kansallisia varautumistarpeita.
- Erilaiset kansallisen tason strategiat kuvaavat sitä, että valtiojohto on havahtunut kyberturvallisuuden merkittävyyteen yhteiskunnan kriittisten toimintojen järjestämisessä.

TRAFICOM

Verkkojen toimivuus

Verkkojen toimivuus -osassa käsitellään yleisten viestintäpalveluiden merkittäviä toimivuushäiriöitä Suomessa, muiden ICT-palveluiden huomattavia häiriöitä Suomessa ja maailmalla, sekä palvelunestohyökkäyksiä Suomessa ja maailmalla.

TRAFICOM

Verkkojen toimivuus

- Marraskuussa yleisissä viestintäpalveluissa oli 6 merkittävää toimivuushäiriötä.
  - Vakavuusluokat: A: 0, B: 0, C: 6
- Ohjelmistoviat ja muutostyöt korostuivat vikojen syinä.
  - Välillä korjaava ohjelmistopäivityskin voi osoittautua virheileväksi.
  - Vaikutuksina olivat kiinteän laajakaistan lisäksi mm. erilaiset verkossa olevat IoT- ja M2M-laitteet, jotka tarjoavat näkyvyyttä esimerkiksi erilaisiin kiinteistön mittareihin.
- Tänä vuonna merkittäviä verkkojen toimivuushäiriöitä on ollut 68. Lukema tulee olemaan hieman suurempi kuin viime vuonna.

Analyysi

- Yleisten viestintäpalveluiden toimivuus Suomessa on vuonna 2021 ollut keskimäärin hyvä.
- Kuukaudessa on keskimäärin vajaat kuusi merkittävää toimivuushäiriötä.
- Toimivuushäiriöt kotimaan verkossa ja globaaleissa palveluissa osoittavat meille, että 2020-luvulla merkittävän palvelukatkoksen aiheuttajana voi olla edelleen hajonnut laite, kaivinkoneen kauha tai työntekijä näppäimistöineen.

TRAFICOM

Palvelunestohyökkäykset

- Murretut palvelimet käytössä palvelunestohyökkäyksissä
  - Saimme muutaman ilmoituksen, joissa murrettua palvelinta on käytetty hyväksi palvelunestohyökkäyksissä.
  - Organisaatioiden tulisi tarkkailla myös lähtevää liikennettä, jotta vastaavanlaiset tilanteet havaittaisiin mahdollisimman nopeasti.
  - Verkossa oleva palvelin on hyökkääjille maukasta riistaa, mikäli sen päivitykset eivät ole ajan tasalla.
- HUS kertoi joutuneensa palvelunestohyökkäyksen kohteeksi marraskuun alussa
  - https://www.hus.fi/ajankohtaista/husin-verkkopalveluhairioiden-syy-selvinnyt
- Noin 40% meille ilmoitetuista hyökkäyksistä (Q3/2021) Suomessa oli kooltaan yli 1 Gbit/s. Ilmoitettujen hyökkäysten perusteella skaala ulottuu tänä vuonna jopa 260 Gbit/s tasolle asti.

Analyysi

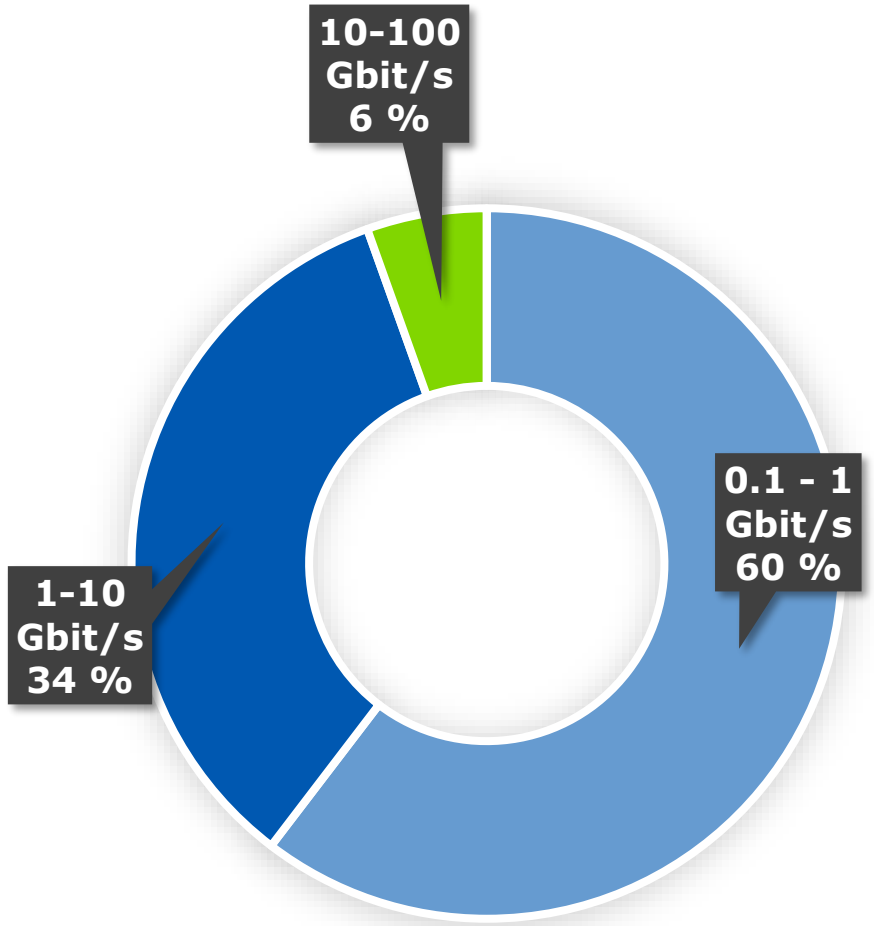
- Organisaatioiden tulisi tarkkailla ulospäin suuntautuvaa liikennettä kurkkaamalla konepellin alle.
  - Haittaohjelmat saatetaan havaita palvelimilla mm. prosessorikuorman kasvulla tai haitallisiin osoitteisiin liikennöinnistä, mutta palvelunestohyökkäykseen valjastetut palvelimet voivat vaatia liikenteen profiilien tarkkailua.
- Haavoittuvuuksien hallinta osoittautuu tärkeäksi myös palvelunestohyökkäysten kannalta.
  - Pidä palvelimet päivitettyinä, jotta ne eivät murrettuina osallistu toisten organisaatioiden häirintään.

TRAFICOM

Palvelunestohyökkäysten tunnuslukuja

3kk

- 99 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q3/2021.
- Noin 76% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q3/2021 - tilasto päivitetään kvartaaleittain.)

TRAFICOM

Vakoilu

Vakoiluosiossa käsitellään valtiollisten toimijoiden tai niihin liitettyjen ryhmien harjoittamaa kybervakoilua ja -vaikuttamista. Tavoitteena voi olla poliittinen tiedonhankinta, yritysvakoilu tai esimerkiksi tietojärjestelmien tuhoaminen.

TRAFICOM

Vakoilu

- Erilaisiin verkkolaitteisiin, kuten reitittimiin, murtautuminen kuuluu kybervakoilun keinovalikoimaan yhä tyypillisemmin.
- Esimerkiksi APT31-ryhmän uutisoitiin hyödyntäneen pienyritys-, koti- ja vastaavia reitittimiä vuonna 2021 toteuttamissaan operaatioissa.
  - SEKOIA.IO analysoi marraskuussa julkaisemassaan raportissa, että APT31 on siirtynyt aiemmin käyttämistään murretuista Pakedge-laitteista hyödyntämään myös muiden valmistajien laitteita.
- FBI puolestaan kertoi marraskuussa, että eräs APT-toimija ehti hyödyntää puolen vuoden ajan FatPipe MPVPN -verkkolaitteissa olevaa nollapäivähaavoittuvuutta.
  - FBI:n mukaan haavoittuvuuden avulla laitteelle asennettiin takaportti.

Analyysi

- Pienyritykset ja kodit eivät voi tuudittautua siihen, että niiden pienuus suojaa niitä APT-toimijoilta tai muilta rikollisilta.
- Myös tätä kuluttajaryhmää, ja erityisesti niiden verkkolaitteita, hyödynnetään yhtä lailla osana APT-operaatioita esimerkiksi hyökkäysinfrastruktuurin osana.

Vakoilu

- Iraniin liitetyt kyberoperaatiot olivat marraskuussa runsaasti esillä julkisuudessa.
- Microsoft kertoi muun muassa, että Iranin kiinnostus IT-sektoria kohtaan on noususussa ja Iraniin liittyviä havaintoja on tehty kuluneena vuonna merkittävästi aiempaa enemmän.
  - Toiminnan on havaittu kohdistuneen erityisesti Intiassa toimiviin IT-yrityksiin.
- Yhdysvallat ja Iso-Britannia puolestaan varoittivat iranilaisten hakkereiden hyödyntävän tunnettuja ja merkittäviä haavoittuvuuksia operaatioissaan.
  - Varoitus liittyi erityisesti Microsoft Exchange -sähköpostipalvelimen ja Fortinetin laitteisiin liittyviin haavoittuvuuksiin.
- FBI on myös ilmaissut huolensa iranilaisten toimijoiden kiinnostuksesta SCADA-järjestelmien tietoja kohtaan.
- Lisäksi marraskuussa uutisoitiin mm. Lyceum-nimellä tunnetun ryhmän kohdistavan toimiaan myös internetpalveluntarjoajiin ja valtionhallintoihin.
  - Aiemmin kohteena ovat olleet erityisesti teleoperaattorit ja energia-ala.

Analyysi

- Intia on IT-alalla merkittävä toimittaja-, alihankinta- ja IT-palveluiden keskittymä.
- Merkittäviä kohteita palvelevat IT-sektorin organisaatiot kiinnostavat kybervakoojia, sillä niiden kautta voidaan saada pääsy varsinaisen kohteen tietoihin.

Vakoilu

- Pohjois-Korean kybervakoiluoperaatioiden kohteena ovat jälleen olleet mm. valtionhallinto ja media.
  - Proofpointin mukaan Kimsuky-ryhmä on pyrkinyt vakoilemaan erilaisia korkean profiilin kohteita kohdistetuilla kalasteluviesteillä eri puolilla maailmaa.
  - Cisco Talos kertoi puolestaan eteläkorealaisten ajatushautomoiden vakoilusta haitallisten blogisivustojen kautta tarjoilluilla haittaohjelmilla.
- Lisäksi Pohjois-Koreaan linkitetty Lazarus-ryhmä pyrki vakoilemaan tietoturvatutkijoita saastutetulla versiolla ohjelmistosta, jota käytetään yleisesti tietoturvatutkinnoissa.
  - Haitallisilla kirjastoilla varustetun IDA Pro -ohjelman piraattiversion asentaminen johti muun muassa takaoven mahdollistavan ja näppäinpainalluksia ja ruutukaappauksia nauhoittavan haittaohjelman asentumiseen laitteelle.

Analyysi

- Vaikka Pohjois-Koreaan liitetyt kybervakoiluoperaatiot monilta osin keskittyvätkin maan lähialueille poliittisista ja maantieteellisistä syistä, on niillä pitkä historia myös kauemmas ulottuvista operaatioista.
- Viime aikaiset esimerkit tietoturvatutkijoiden vakoilusta ja jo pidempään pinnalla olleet pyrkimykset rikolliseen varainhankintaan ovat esimerkkejä myös muualla maailmassa läsnä olevista uhkista.

Tietoturva-alan kehitys

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.

TRAFICOM

Oikeudelliset asiat

- Muutoksia Liikenne- ja viestintävirastosta sekä sähköisen viestinnän palveluista annettuun lakiin.
  - Kyberturvallisuuskeskus nimetään Euroopan kyberturvallisuuden teollisuus-,teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta annetun EU-asetuksen mukaiseksi kansalliseksi koordinointikeskukseksi.
  - Kyberturvallisuuskeskus hoitaa kansallisena koordinointikeskuksena uusia EU-asetuksessa säädettyjä erityisesti kansallisen kyberturvallisuusyhteisön rakentamiseen, koordinointiin ja osaamisyhteisön kansallisen tason yhteyspisteenä toimimiseen liittyviä tehtäviä.
  - Muutokset tulivat voimaan 1.12.2021
  - Ks. lisää https://www.lvm.fi/-/kyberturvallisuuskeskuksesta-kansallinen-kyberturvallisuuden-koordinointikeskus-eu-verkostoon-1581944

TRAFICOM

Oikeudelliset asiat

- NIS2-direktiiviehdotuksen osalta yleisnäkemys hyväksytty televiestintäneuvostossa 3.12.
  - Ks. lisätietoa: https://www.consilium.europa.eu/fi/press/press-releases/2021/12/03/strengthening-eu-wide-cybersecurity-and-resilience-council-agrees-its-position/
- EU:n kilpailukykyministereistä koostuva neuvosto on hyväksynyt 25. marraskuuta 2021 digipalvelusäädöstä (Digital Services Act, DSA) koskevan neuvoston yleisnäkemyksen
  - Ks. lisätietoa: https://www.lvm.fi/-/eu-n-digipalvelusaados-lisaisi-internetin-palveluntarjoajien-vastuullisuutta-1592218
- Ajankohtaista tietosuojavaltuutetulta:
  - https://tietosuoja.fi/-/tietosuojavaltuutetun-toimistolta-ohjeistusta-sote-toimijoille-tietoturvaloukkausten-ilmoituskaytannoista
  - https://tietosuoja.fi/-/tietoturvaloukkausten-dokumentointivelvollisuuden-piiriin-kuuluvat-myos-tapahtuma-ajan-lokitiedot

TRAFICOM

Arjen kyberturvallisuus

Nasevia neuvoja tiliesi turvaamiseksi

- Verkkopalveluissa käytettäviä tilejä yritetään murtaa ja ottaa haltuun usein eri keinoin. Tähän artikkeliin on koostettu lyhyet ohjeet ennakkoon suojautumisen kannalta, sekä mitä tehdä murron tapahduttua.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi

Poistimme pankkitunnusten kaappausta koskevan varoituksen

- Poistimme 27.10. julkaistun pankkitunnusten kaappausta koskevan varoituksen. Verkkopankkitunnuksia kalastellaan kuitenkin yhä aktiivisesti muiden toimijoiden nimissä.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/poistimme-pankkitunnusten-kaappausta-koskevan-varoituksen

Laajoista kansalaisia koskevista tietoturvahäiriöistä ja -tilanteista tiedotetaan 112 Suomi -sovelluksen avulla

- 112 Suomi -sovellus toimii uutena viestintäkanavanamme yksityishenkilöille. Laajoista kansalaisia koskevista tietoturvahäiriöistä on tärkeää saada tieto jaettua mahdollisimman nopeasti ja laajasti. Kännykkä on tähän erinomainen väline
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/laajoista-kansalaisia-koskevista-tietoturvahairioista-ja-tilanteista-tiedotetaan-112

Vieraskynä: Päivittäminen hallussa? SeniorSurf tukee senioreita digitaidoissa

- SeniorSurf rohkaisee ikääntyneitä ihmisiä tarttumaan tietokoneisiin ja nettiin. Yhdistys toimii valtakunnallisesti ja on mukana senioreiden digiopastustoiminnassa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vieraskyna-paivittaminen-hallussa-seniorsurf-tukee-senioreita-digitaidoissa

Uutisia Kyberturvallisuuskeskuksesta

Kyberturvallisuuskeskus kartoittaa jälleen suojaamattomia automaatiojärjestelmiä

- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus etsii tietoverkoista suojaamattomia automaatiolaitteita. Työn tavoitteena on parantaa tilannekuvaa ja kyberturvallisuutta Suomessa. Saatuja tuloksia verrataan aikaisempien vuosien tuloksiin.
- Selvitys toteutetaan lähettämällä yhteydenavauspyyntöjä suomalaisissa verkoissa olevien tietokoneiden ja verkkolaitteiden tiettyihin tietoliikenneportteihin ja analysoimalla niistä tulevia vastausviestejä viikoilla 43-44.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kartoitus2021

Onnea LähiTapiola Tietoturvan suunnannäyttäjä -tunnustuksesta!

- Tietoturvan suunnannäyttäjä -tunnustus jaettiin Tietoturva 2021 -virtuaaliseminaarissamme 24.11.
- LähiTapiola on nostanut esiin tietoturvaa aktiivisesti ja positiivisesti. Se on myös ollut tärkeä yhteiskunnallinen tietoturvavaikuttaja.
- Lue lisää tunnustuksesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/onnea-lahitapiola-tietoturvan-suunnannayttaja-tunnustuksesta

Traficomin Kyberturvallisuuskeskus julkaisi Suomen ensimmäisen tekoälyselvityksen

- Selvitys tarkastelee tekoälyä kyberturvallisuuden ja riskienhallinnan näkökulmasta. Se kannustaa tekoälypohjaisten palvelujen tai tuotteiden kehittäjiä tekemään nämä kolme asiaa jo nyt: menemään kehitystyön kyberturvallisuus ja riskienhallinta edellä, hahmottamaan koneoppimismallin koko elinkaari ja panostamaan datan laatuun.
- Kyberturvallisuuskeskus esitteli myös uuden työkalun tekoälyn kyberturvallisuuden riskienhallintaan.
- https://www.traficom.fi/fi/ajankohtaista/miten-rakennetaan-kyberturvallinen-tekoalyratkaisu-traficomin-kyberturvallisuuskeskus

TRAFICOM

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

TRAFICOM