TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Tammikuu 2022

#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

17.2.2022

Kybersää Tammikuu 2022

Tietomurrot ja -vuodot

- Facebook Messengerin kautta tehdään aktiivisesti Facebook-tunnusten kalastelua
- Tammikuu on ollut muutoin rauhallinen kuukausi tietomurtoilmoitusten suhteen

Huijaukset ja kalastelut

- Laskuksi ja turvaposti-ilmoitukseksi väärennetyillä viesteillä on kalasteltu satoja tunnuksia ja kaapattu tilejä
- Netin myyntipalstoilla huijataan syöttämään luottokorttitietoja varkaille

Haittaohjelmat ja haavoittuvuudet

- Log4shell-haavoittuvuudesta annettu kriittinen varoitus on poistettu kahden kuukauden voimassaolon jälkeen
- FluBot-varoitus on poistettu, koska operaattoreiden suodatustoimenpiteet ovat toimineet hyvin

Automaatio

- Yli puolet terveydenhuollon IoT-laitteista haavoittuvia
- Tesla-autoista löytyi haavoittuvuuksia. Vastuullinen ilmoittaminen haavoittuvuuksista ei ole itsestään selvää.
- Automaation tietoturva -kirjaan julkaistiin lisämateriaalia

Verkkojen toimivuus

- Tammikuussa yleisissä viestintäpalveluissa oli viisi merkittävää toimivuushäiriötä.
- Useita palvelunestohyökkäyksiä tammikuun loppupuolella
- Taas uusia ennätyslukemia Suomessa: palvelunestohyökkäys oli kooltaan 379Gbit/s

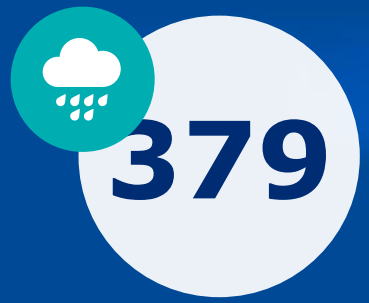
Vakoilu

- Myös suomalaisdiplomaatteja on vakoiltu mobiililaitteiden vakoiluun tarkoitetulla Pegasus-ohjelmalla
- Ukrainan ja Venäjän välisen konfliktin kiristyminen on näkynyt kyberhyökkäyksinä alueella

TRAFICOM

17.2.2022

Kuukauden tunnuslukuja



379Gbit/s palvelunestohyökkäys on toistaiseksi volumetrisesti suurin Suomessa nähty. Lyhyt hyökkäys piti sisällään 33 miljoonaa pakettia sekunnissa

Myös suomalaisdiplomaatteja on vakoiltu mobiililaitteiden vakoiluun tarkoitetulla Pegasus-ohjelmalla

Varoitukset Flubot-haittaohjelmasta sekä Log4shell-haavoittuvuudesta poistettiin

TRAFICOM

Poistimme varoituksen 4/2021 Varo tekstiviestitse levitettävää haittaohjelmaa

- Julkaisimme keltaisen varoituksen Flubotista 25.11.2021
- Flubotin huijausviesteissä viitataan ääniviestiin tai vastaamattomaan puheluun, jonka saa kuultavakseen linkistä. Linkin takaa ei kuitenkaan löydy viestejä, vaan sieltä tarjotaan puhelimeen asennettavaksi haittaohjelma tai tietojenkalastelua
- Varoitus poistettiin, koska haittaohjelman leviäminen on laantunut
- Kyberturvallisuuskeskus antaa noin 1-5 varoitusta vuoden aikana, eikä varoituksia anneta kevein perustein
- Katso lisää: https://www.kyberturvallisuuskeskus.fi/fi/varo-tekstiviestitse-levitettavaa-haittaohjelmaa

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

- Julkaisimme keltaisen varoituksen 10.12.2021. Varoitus muutettiin punaiseksi 13.12.2021
- Haavoittuvaa Log4j-komponenttia on käytössä todella laajasti suosituissa sovelluksissa
- Varoitus poistettiin, koska haavoittuvuuden kohteena olleet ohjelmistot on pitkälti päivitetty
- Kyberturvallisuuskeskus antaa noin 1-5 varoitusta vuoden aikana, eikä varoituksia anneta kevein perustein
- Katso lisää: https://www.kyberturvallisuuskeskus.fi/fi/varoitus_5/2021

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen. Ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia kyberturvallisuudessa.

2

Johtaminen ja riskienhallinta. Toimintaympäristön nopeat muutokset koettelevat organisaatioiden riskienhallintaa kyberturvallisuudessa. Johdon vastuulla on varmistaa riskienhallinnan vaikuttavuus.

3

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.

Symbolit

Uusi

Päivitetty

4

Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille! Tarve kyberturvallisuuden osaajille monipuolistuu uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää entisestään tarvetta osaajille.

5

Käyttöoikeudet ovat avaimet organisaatioon. Käyttöoikeuksien kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle tunnusten ollessa väärissä käsissä.

TRAFICOM

17.2.2022

1. Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen

Digitaalisuus läpileikkaa koko organisaation toimintaa ja erilaiset tapahtumat voivat vaikuttaa merkittävästi organisaation jatkuvuuden- ja riskienhallintaan.

- Muutokset kansainvälisten ilmiöiden kehityksessä näkyvät vaihtelevilla voimakkuuksilla Suomessa
- Esimerkiksi pitkittynyt koronaviruspandemia, talouden äkilliset muutokset, luonnonilmiöt, energian hinnannousu, sekä ennakoimaton kansainvälinen turvallisuustilanne näkyvät vaikeasti ennakoitavina kehityskulkuina, ja muutokset saattavat tapahtua nopeastikin
- Epävarmuustekijöillä voi yksistään olla isoja vaikutuksia organisaatioiden toimintaan. Yhdessä nämä ilmiöt voivat näkyä digitaalisessa toimintaympäristössä nopeasti ja aiheuttaa vaikeasti ennakoitavia tapahtumia myös kyberturvallisuuden toimintaympäristössä
- Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön aiheuttamat uhkat kriittisille prosesseille

CASE

Toimitusketjut häiriintyivät koronapandemian alkaessa vakavasti. Esimerkiksi puolijohteiden saatavuus on ollut jo pidemmän aikaa huono eikä sirupula näytä helpottamisen merkkejä vielä lähikuukausina. Organisaatiot saattavat joutua odottamaan uusia laitteita kuukausikaupalla ja siten joutua käyttämään elinkaaren päässä olevia laitteita pidempään ja uusien suojausratkaisujen rakentamisessa kestää suunniteltua pidempään. Laitekaupoilla kannattaakin olla tarkkana, sillä saatavuushäiriöt ja hintojen nousu houkuttelevat markkinoille myös halpoja kopioita.

2. Johtamisella riskienhallintaa

Monen organisaation riskienhallinta ei pysy digitalisaation vauhdissa. Digitaalisia ratkaisuja otetaan käyttöön sokkona ilman riskien ymmärtämistä ja arviointia. Lopputulos saattaa olla riskialtis niin kansalaisen, organisaation itsensä kuin koko yhteiskunnan kannalta.

Organisaation riskienhallinta on viime kädessä johdon vastuulla. Johdon tulee seurata riskienhallinnan toteutumisesta vähintään:

- **Toimintaympäristön määrittely**. Organisaation tulee tunnistaa sen kriittiset prosessit ja mitä uhkia toimintaympäristö muodostaa
- **Riskien arviointi.** Organisaation on edellisen vaiheen pohjalta tunnistettava ja arvioitava riskit, sekä miten ne vaikuttavat kriittisiin prosesseihin
- **Riskien käsittely.** Kun riskit on arvioitu, organisaation tulee toteuttaa riittävät hallintatoimenpiteet riskien vaikutusten vähentämiseksi
- **Seuranta ja katselmointi.** Organisaation tulee seurata riskienhallintatoimenpiteiden vaikuttavuutta. Toimintaympäristön muutoksia ja omaa varautumista riskeihin tulee jatkuvasti seurata ja katselmoida

CASE

Esimerkkiskenaariossa organisaatio ei ole analysoinut toimintaympäristöään, eikä siten ole kyennyt arvioimaan sen vaikutuksia kriittisiin prosesseihinsa. Puutteellinen digitaalinen ratkaisu otetaan käyttöön tiedostamatta uhkaa. Riski, joka olisi ollut tunnistettavissa, realisoituu. Organisaation kriittinen prosessi pysähtyy, aiheuttaa mittavan mainehaitan sekä taloudelliset menetykset. Myös asiakkaiden tiedot ovat vaarantuneet. Riskin hallintatoimenpiteiden kustannukset olisivat olleet murto-osan asian korjaamisesta aiheutuneista kuluista.

3. 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.

4. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisäävät entisestään tarvetta erilaisille osaajille. Yritykset eivät etsi pelkkiä koodareita. Tulevaisuudessa laaja-alaisemmalle digitalisaation, kyberturvallisuuden ja datan osaamiselle on entistä enemmän kysyntää.

- **Osaamisen saaminen riittävälle tasolle kestää vielä pitkään.** Organisaatioiden kyberturvallisuus vaarantuu, mikäli osaavaa henkilöstöä ei ole tarpeeksi saatavilla
  - Arviomme mukaan lyhyen aikavälillä tarvitaan erityisesti teknisiä osaajia, jotka osallistuvat tietoturvatutkintaan sekä ennaltaehkäisevään työhön
  - Pitkällä aikavälillä osaajatarve monipuolistuu ja esimerkiksi hallinnollisia osaajia tarvitaan lisää
- Osaajapula ei ole kiinni pelkästään määrästä, vaan myös laadusta! Osaaminen ei saisi henkilöityä liikaa, jotta jatkuvuus voidaan turvata kaikissa tilanteissa. Organisaation tietoturvan hallinta tulee osallistaa ja kouluttaa osaksi kaikkien työntekijöiden päivittäistä toimintaa
- Johdon tulee ymmärtää ja varmistaa riittävä osaaminen organisaatiossa kyberturvallisuusosaajien kysynnän kasvaessa. On tärkeää miettiä, millaista asiantuntemusta tarvitaan nyt ja tulevaisuudessa, sekä miten se hankitaan

CASE

2020 vuoden digibarometrin teemana oli kyberturvallisuus. Suomen tilanne on tutkimuksen mukaan kohtuullisen hyvä, mutta verrokkimaat uhkaavat karata etumatkalle. Erityisesti suurimmilla yrityksillä vaikuttaa olevan kirittävää. Kaikkiaan suomalaisissa yrityksissä esimerkiksi tietovuodot olivat yleisempiä kuin Euroopassa keskimäärin. Barometrissa selvitettiin Suomen kyberturva-alan osaamisvajetta. Kyselyn mukaan noin 60 prosenttia on kokenut osaajapulaa ja työvoiman saatavuus koettiin merkittävimmäksi yksittäiseksi alan kasvua hidastavaksi tekijäksi. (Digibarometri 2020)

5. Käyttöoikeudet ovat avaimet organisaatioon

Käyttöoikeuksien 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 sekä organisaatioihin että yksityishenkilöihin. Tunnuksia ja niihin liittyviä salasanoja yritetään lisäksi aktiivisesti murtaa automaattisin työkaluin. Jos avaimet viedään, tulee asiaan reagoida välittömästi!
- On hyvä pohtia, millaiset käyttöoikeudet omilla työntekijöillä tai ulkoistetuilla palveluntarjoajilla on yrityksen hallussa olevaan tietoon. Organisaation käyttäjillä tulee olla mahdollisimman rajoitetut, kuten perustason, käyttöoikeudet. Pääkäyttäjä-tason oikeuksien käyttö tulee olla erityisen suojattua ja kontrolloitua
- Organisaation tietoturva tulee olla ratkaistuna niin, että teknisten kontrolleiden tulee estää ja havaita tunnusten väärinkäytökset. Siksi on tärkeää, että esimerkiksi monivaiheinen tunnistautuminen (MFA) on käytössä
  - Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/suojautuminen-microsoft-office-365-tunnusten-kalastelulta-ja-tietomurroilta ja https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

OHJE

Jos käyttöoikeudet joutuvat vääriin käsiin, tulee toimia nopeasti.

1. Lukitse tunnus välittömästi!
2. Sulje kirjautunut murtaja pois organisaation palveluista.
3. Selvitä, mitä on tapahtunut ja tee toipumissuunnitelma.
4. Ota yhteys Kyberturvallisuuskeskukseen.
5. Kun voidaan varmistua, että rikollinen on häädetty, tulee käyttäjän vaihtaa salasana ja tunnuksen voi avata uudelleen

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.

Tietomurrot ja –vuodot

- Aktiivista Facebook-tunnusten kalastelua Facebook Messengerin kautta
- Kyberturvallisuuskeskus sai tammikuun aikana useita kymmeniä ilmoituksia kalasteluyrityksistä tai onnistuneista Facebookin tilikaappauksista
- Huijausyrityksessä murretulta tililtä lähetetään viesti, jonka tavoitteena on saada vastaanottajan Facebook-tili haltuun uhrin puhelinnumeron ja kaksivaiheisen tunnistautumisen vahvistuskoodin avulla
- Paras suojautumiskeino tältä huijaukselta on valppaus myös tutuilta saapuvien Facebook-viestien kanssa
  - https://www.kyberturvallisuuskeskus.fi/fi/ttn_20012022

Analyysi

- Tutulta kontaktilta tulevaan viestiin luotetaan herkemmin kuin täysin tuntemattomalta tulevaan
- Kun kaappari on saanut tilin haltuunsa, uhrin kontakteille tehtailtujen huijausten onnistumisprosentti on paljon suurempi kuin satunnaisiin osoitteisiin lähetettyjen huijausten
- Facebook-tilikaappausten avulla on varastettu rahaa uhrien tileiltä tuhansia euroja yhdellä kertaa

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 kalastelut

- Turvapostikin voi olla väärennetty
  - Turvaposti ei aina tuo turvaa, jos huijari väärentää viestinsä näyttämään turvapostilta
  - Tuoreessa tietojenkalastelukampanjassa on lähetetty turvaposti-ilmoitukseksi väärennettyjä sähköposti-laskuja, joiden linkki johtaa tietojenkalastelusivuun
  - Sivut on pystytetty avoimen lähdekoodin verkkosivupalveluntuottajan ilmaisen kokeilujakson avulla suomalaiselle kuntasektorille räätälöityinä
  - Uskottava kalastelu on saanut satoja uhreja suomalaiselta palvelu- ja kuntasektorilta
  - Kaapatut sähköpostitilit on otettu rikollisten käyttöön ja niiltä on lähetetty tuhansia uusia kalasteluviestejä

Analyysi

- Turvapostiksi väärennetty huijausviesti tehoaa paremmin kuin tavallinen sähköposti tai tekstiviesti
- Jo pelkkä ajatus turvapostista tuudittaa vastaanottajan uskomaan, että viestiin voi luottaa
- Kuluttaja käyttää turvapostipalveluita harvoin, ja ne ovat juuri riittävän monimutkaisia mahdollistaakseen huijaamisen väärennetyllä viestillä
- Kuluttaja luottaa turvapostiin enemmän kuin tekstiviestiin tai tavalliseen sähköpostiin. Kaikkia niitä voidaan valitettavasti väärentää tavalla tai toisella

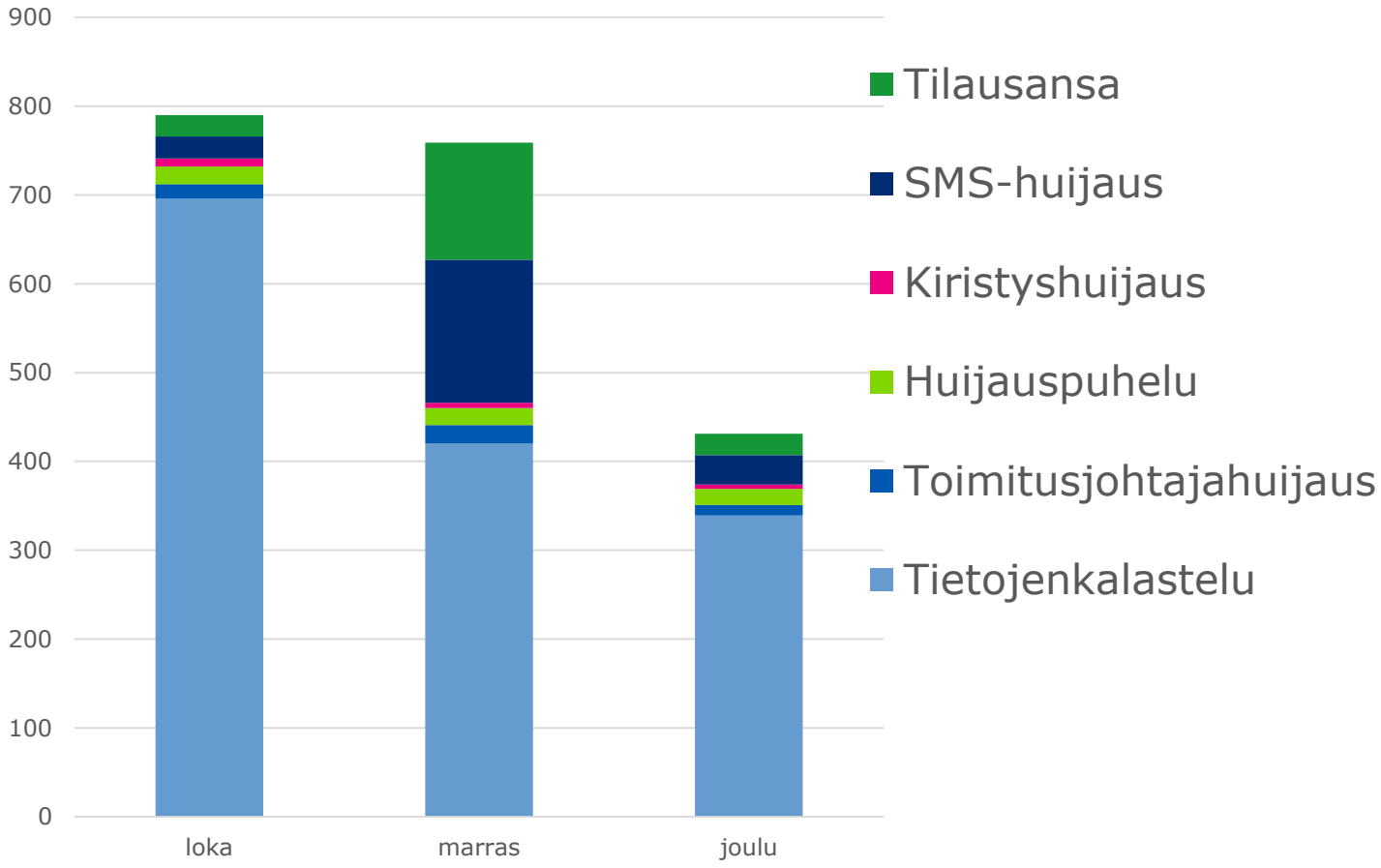
Huijaukset ja kalastelut

- Huijareita internetin myyntipalstoilla
  - Kyberturvallisuuskeskukselle ilmoitettujen huijausyrityksien määrät ovat kaksinkertaistuneet joulukuun 2021 jälkeen
  - Huijausyrityksessä tarkoituksena on saada myyjän pankkitiedot huijarin haltuun
  - Erilaisilla myyntialustoilla, kuten Tori.fi ja Facebook Marketplace on liikkunut viime aikoina kuriiriteemaisia huijauksia
  - Huijauksen uhrit ovat menettäneet satoja tai tuhansia euroja

Huijaukset etenevät seuraavasti:

1. Myyjä on laittanut esineen myyntiin
2. Ostajaehdokas ottaa yhteyttä pikaviestinsovelluksessa (usein WhatsApp), ja kyselee tuotteen kunnosta
3. Ostaja tarjoutuu ostamaan tuotteen kuriiripalvelun avulla
4. Ostaja lähettää linkin kuriiripalvelun verkkosivuille, josta voi lunastaa rahat ja varata ajan
5. Kuriiripalvelun sivustolle täytyy syöttää luottokorttitiedot maksun suorittamista varten, myyjä syöttää tiedot
6. Myyjän syöttämät tiedot ovat nyt rikollisen hallussa

Käsiteltyjä huijaustapauksia Q4/2021



- Vuoden 2021 viimeisen neljänneksen ilmiöitä ovat:
  - Haittaohjelman aiheuttamat hujaustekstiviestit näkyivät korostetusti kaikkien operaattoreiden SMS-liikenteessä marraskuusta alkaen.
  - Joulukuun loppua kohti operaattoreiden suodatustoimet saivat huijaus-SMS-viestit kuriin.
  - Pankkitunnusten kalastelu on jatkunut tasaisen laajana koko kvartaalin.

Haittaohjelmat ja haavoittuvuudet

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

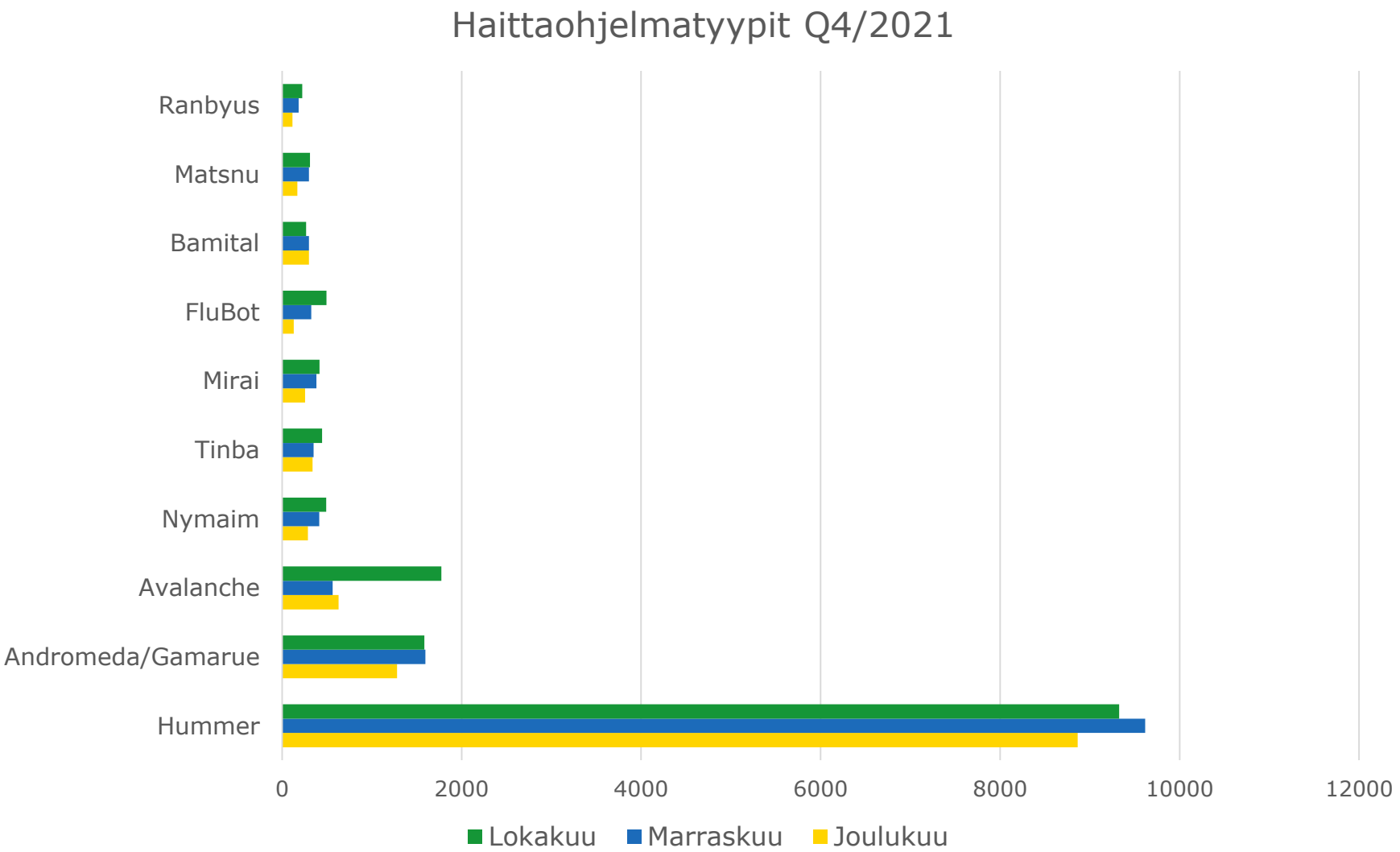
Haittaohjelmat

- Androidin FluBot-haittaohjelman varoitus poistettiin
  - FluBot-haittaohjelmaepidemia on saatu taltutettua toistaiseksi Suomessa, mutta haittaohjelman käyttämä infrastruktuuri on yhä verkossa olemassa
  - Viranomaiset ja teleoperaattorit ovat varautuneet haittaohjelman aktivoitumiseen, mutta tällä hetkellä syytä varoitukseen ei enää ole
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/androidin-flubot-haittaohjelman-varoitus-poistettu
- Qbot-haittaohjelman levitystä sähköpostitse
  - Tietoja varastava haittaohjelma pyrkii myös laajemmalle ympäristöön
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-1
    - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnetko-tunkeutumisen-laajentamisen-osa-2

Analyysi

- Teleoperaattoreiden käyttöönottamat suodatustoimet ovat pitäneet haittaohjelman lähettämät tekstiviestit aisoissa ja ongelma on rauhoittunut
- Vuoden ensimmäisellä viikolla operaattorit ovat raportoineet vain joitakin kymmeniä suodatettuja viestejä päivässä, kun pahimmillaan marraskuun lopussa puhuttiin miljoonista haitallisista viesteistä

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:
https://www.traficom.fi/fi/tilastot/traficomin-haittaohjelmahavainnot

Haavoittuvuus

- Log4shell-haavoittuvuuden hyväksikäytöistä ei Suomessa ole merkittäviä havaintoja
  - Suomessa käytettyjen palveluiden Log4j-haavoittuvuudet on pyritty korjaamaan ensi tilassa.
  - Hyväksikäyttöyrityksiä on kyllä havaittu säännöllisesti, mutta ne eivät ole johtaneet onnistuneisiin tietomurtoihin
  - Kansainvälisestikin tilanne on ollut Suomea vastaava – odotettiin suurempaa hyökkäysaktiviteettia, mutta tilanne on ollutkin rauhallinen
  - Log4jshell-haavoittuvuuden hyväksikäyttömenetelmät tulevat kuitenkin jäämään hyökkääjien työkalupakkiin vuosien ajaksi

Analyysi

- Punainen varoitus on poistettu keskiviikkona 9.2, melkein 2kk voimassaolon jälkeen
- Julkaisimme aiheesta Tietoturva Nyt! –artikkelin, jossa muistuttaa päivitystarpeiden seuraamisesta myös jatkossa
- Seuraamme haavoittuvuutta edelleen aktiivisesti ja viestimme heti, jos tilanteessa tapahtuu muutoksia
  - https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/poistimme-varoituksen-log4j-komponentin-haavoittuvuudesta

Kuukauden haavoittuvuusjulkaisut

- Kriittinen haavoittuvuus Windowsin http.sys-protokollapinossa (1/2022)
- Kriittinen haavoittuvuus Unix polkit-komponentissa (2/2022)
  - Polkitin pkexec-komentokäskyssä on vuodesta 2009 alkaen ollut ohjelmistovirhe, joka liittyy komentoriviparametrien hallintaan muistissa. Virheen avulla käyttäjä voi korottaa käyttövaltuuksiansa pääkäyttäjätasolle.
- Kriittinen SAP-haavoittuvuus tulisi päivittää välittömästi (3/2022)
- Kriittinen haavoittuvuus Adobe Commerce- ja Magento-verkkokauppa-alustoissa (4/2022)

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

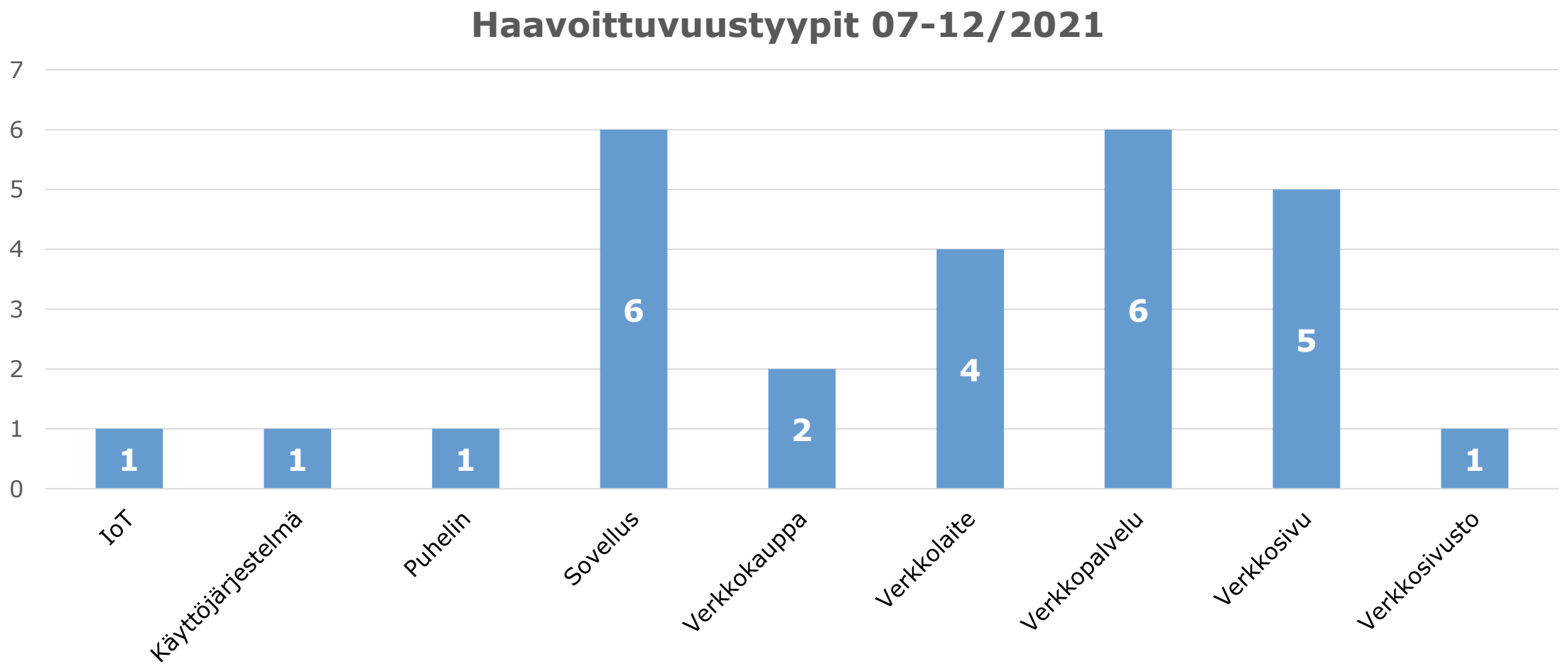
- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta
- **Haavoittuvuustiedotteita tänä vuonna 4 kpl (tilanne 15.2.2022)**
  - 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

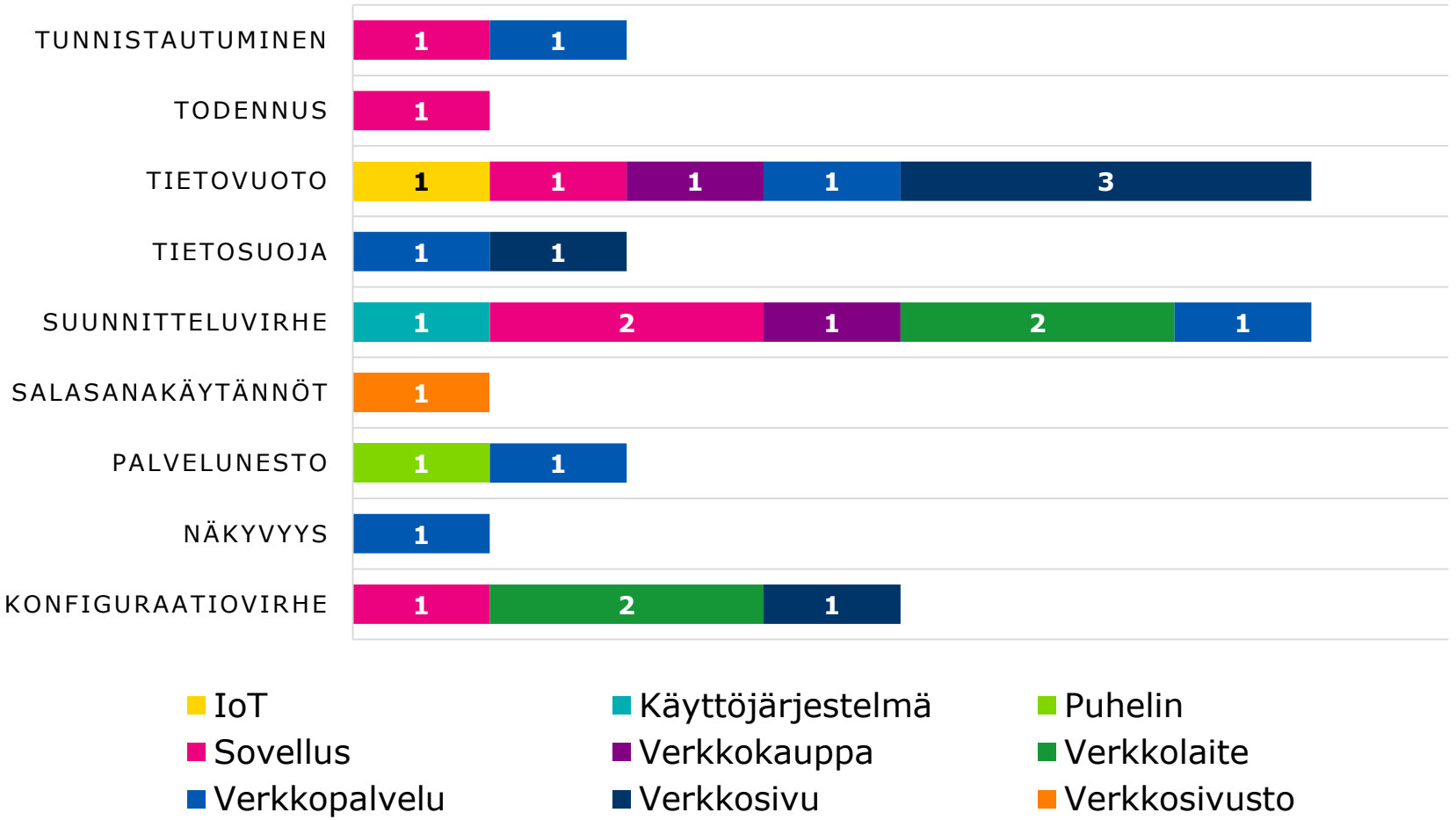
- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot
- Vanhentuneet tai heikot salasanakäytännöt ovat usein 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



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.

IoT

- Haavoittuvat IoT-laitteet yleisiä terveydenhuollossa
  - Terveydenhuollon älykkäiden laitteiden tietoturvaan erikoistuneen Cynerio-yrityksen mukaan yli puolessa terveydenhuollon yksiköissä käytetyistä laitteista on kriittisiä kyberturvallisuusriskejä. Riskejä on monen laatuisia turvattomien tietoliikenneprotokollien käytöstä tunnettuihin ohjelmistohaavoittuvuuksiin
  - Myös monissa lääkinnällisiin laitteisiin liittyvissä tietokoneissa on käytössä vanhentuneita käyttöjärjestelmiä, joissa on tunnettuja haavoittuvuuksia
  - Haavoittuvien ohjelmistojen korjaaminen ei monista syistä onnistu nopeasti eikä kattavasti, joten verkkojen segmentointi on tärkeä keino riskien hallitsemiseksi
  - https://www.csoonline.com/article/3648592/outdated-iot-healthcare-devices-pose-major-security-threats.html

Analyysi

- Digitekniikka on laajasti käytössä terveydenhuollossa ja monesti se on olennaisen tärkeää potilaan hoidolle. Mikä tahansa häiriö terveydenhuollon digitaalisessa tekniikassa haittaa hoitotyötä ja voi pahimmillaan vaarantaa potilaan terveyden.
- Mikä tahansa verkkoon kytketty haavoittuva laite on hyökkääjille mahdollisuus laajentaa hyökkäystä. Haavoittuvat laitteet voivat myös paljastaa henkilötietoja salakuuntelijalle.
- Laitteiden kyberturvallisuus tulee huomioida jo hankintavaiheessa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja

IoT

Tesloja hakkeroinut nuori löysi autoista lisää ongelmia

- Hän pystyi etsimään autojen tarkan sijainnin sekä kytkemään niidenturvajärjestelmät pois päältä
- Lisäksi hän pystyi estoitta avaamaan ajopelien ovet ja ikkunat, käynnistämään ne sekä soittamaan musiikkia
- https://www.bloomberg.com/news/articles/2022-01-25/teen-tesla-hacker-accessed-owners-email-addresses-to-warn-them

Analyysi

- Hakkeri ilmoitti haavoittuvuudesta Teslalle, mutta valitettavasti myös julkaisi sen ensin Twitterissä
- Vastaavia haavoittuvuuksia on havaittu aikaisemminkin kriittisissä toteutuksissa. Autot ovat kuitenkin käyttöympäristönsä vuoksi alttiimpia hyökkäyksille kuin monet muut kohteet
- Kyberturvallisuuskeskus on koonnut toimintaohjeita valkohattuhakkereille julkaisuun https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vinkkeja-valkohatuille-parempaan-ja-helpompaan-yhteistyohon

Automaatio

- Automaation tietoturva – Kriittisen tuotannon turvaaminen - kirjaan julkaistu lisämateriaalia
  - Suomen Automaatioseuran kirjaan on julkaistu tarkentavaa ja täydentävää ilmaista lisämateriaalia.
  - Aiheina tällä hetkellä GDPR, OSINT ja tekoäly.
  - https://www.automaatioseura.fi/julkaisut-kirjakauppa/automaation-tietoturva-julkaisut/liitteet/

Analyysi

- Automaatiojärjestelmät ovat tärkeitä yhteiskunnan arjen toiminnan kannalta: niillä hallitaan mm. vesi- ja sähköverkkoja ja teollisuuslaitoksia.
- Kirjaan julkaistut lisämateriaalit lisäävät automaatiojärjestelmien käyttäjien tietämystä järjestelmien kyberturvallisuuden hallinnasta ja parantavat näin yhteiskunnan häiriönsietoa.
- Kyberturvallisuuskeskuksen yhteenveto automaatiojärjestelmien kyberturvallisuutta koskevista aineistoista: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/materiaaleja-kriittisen-infran-turvaamiseen

Verkkojen toimivuus

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

Verkkojen toimivuus

- Tammikuussa yleisissä viestintäpalveluissa oli 5 merkittävää toimivuushäiriötä
  - Vakavuusluokat: A: 0, B: 1, C: 4
- Kaikki viat johtuivat jonkinlaisista ohjelmisto- tai laitevioista
  - Verkoissa on useampia komponentteja, jotka voivat hajota. Tässä kuussa kaksi erillistä vikaa aiheutti korttivika, yhden ohjelmistovika ja viimeiset kaksi sähkövika
- Kazakstanissa sammutettiin internet mielenosoitusten vuoksi
  - Valtio katkaisi yhteydet muutamaan otteeseen vaikuttaakseen tilanteeseen muiden toimien ohessa
  - https://therecord.media/massive-internet-outages-continue-to-sow-confusion-amid-kazakhstan-protests/

Analyysi

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

Palvelunestohyökkäykset

- Useita palvelunestohyökkäyksiä tammikuun loppupuolella
  - Tiistaina 25. päivä n. 30Gbit/s palvelunestohyökkäys pyyhkäisi useammalla sektorilla ja vastaanotimme kourallisen ilmoituksia aiheeseen liittyen
  - Saamiemme ilmoitusten perusteella kyseessä oli sama UDP-paketteja syöksevä palvelunestohyökkäys
  - Hyökkäykset olivat lyhyitä, mutta onnistuivat kuitenkin aiheuttamaan minuuttien palvelukatkoja palveluntarjoajille
- Uusi volumetrinen Suomen ennätys
  - Saimme tiedoksi joulukuulta toistaiseksi suurimman palvelunestohyökkäyksen Suomessa
  - Hyökkäys oli kooltaan 379Gbit/s ja lyhyt hyökkäys piti sisällään 33 miljoonaa pakettia sekunnissa
  - Palveluntarjoajan mitigointipalvelut kestivät hyökkäyksen ja palveluvaikutuksilta vältyttiin

Analyysi

- Organisaatioiden on hyvä varautua 25.1. mainitun esimerkin voimin palvelunestohyökkäyksiin mitigointipalvelulla, joka kestää kymmenien gigatavujen kokoiset hyökkäykset
  - Organisaation tietoliikenneyhteyksien on myös kestettävä tämän kokoiset hyökkäykset; mikäli yhteys on 10G ja hyökkäys 30Gbit/s - voi hyökkäys aiheuttaa väliaikaisen putkitukoksen
- Andorran internetyhteydet menivät käytännössä kokonaan poikki Andorra Telecomiin kohdistuneen palvelunestohyökkäyksen takia
  - Artikkelin mukaan hyökkäyksen koko oli hetkellisesti 100 Gbit/s –suuruusluokkaa
  - https://therecord.media/ddos-attacks-on-andorras-internet-linked-to-squid-game-minecraft-tournament/

Palvelunestohyökkäykset

- Saimme tammikuussa tiedoksi muutamia palvelunestohyökkäyksiä, joilla häirittiin esimerkiksi erilaisia kirjautumispalveluja
  - Hyökkääjä saattaa luoda massoittain erilaisia kirjautumisyrityksiä - tai yrittää palauttaa samalla tekniikalla massoittain salasanoja laajojen sähköpostiosoitelistojen avulla
  - Tämän kaltainen hyökkäys saattaa tukottaa palvelun ja aiheuttaa harmaita hiuksia, kuinka palvelunestohyökkäys saataisiin rajattua ja kokonaan torjuttua ollessaan aktiivisena
- Osuuspankin palveluissa usean tunnin kestänyt katkos sunnuntaina 9.1
  - Osuuspankki ajoi verkkosivupohjaisen verkkopankkipalvelun alas varotoimenpiteenä hyökkäyksen havaitsemisen jälkeen
  - Häiriön aiheutti sovellukseen kohdistuva volumetrinen hyökkäys, jossa palveluun kohdistettiin suuri määrä sovelluskyselyitä
  - https://yle.fi/uutiset/3-12263848

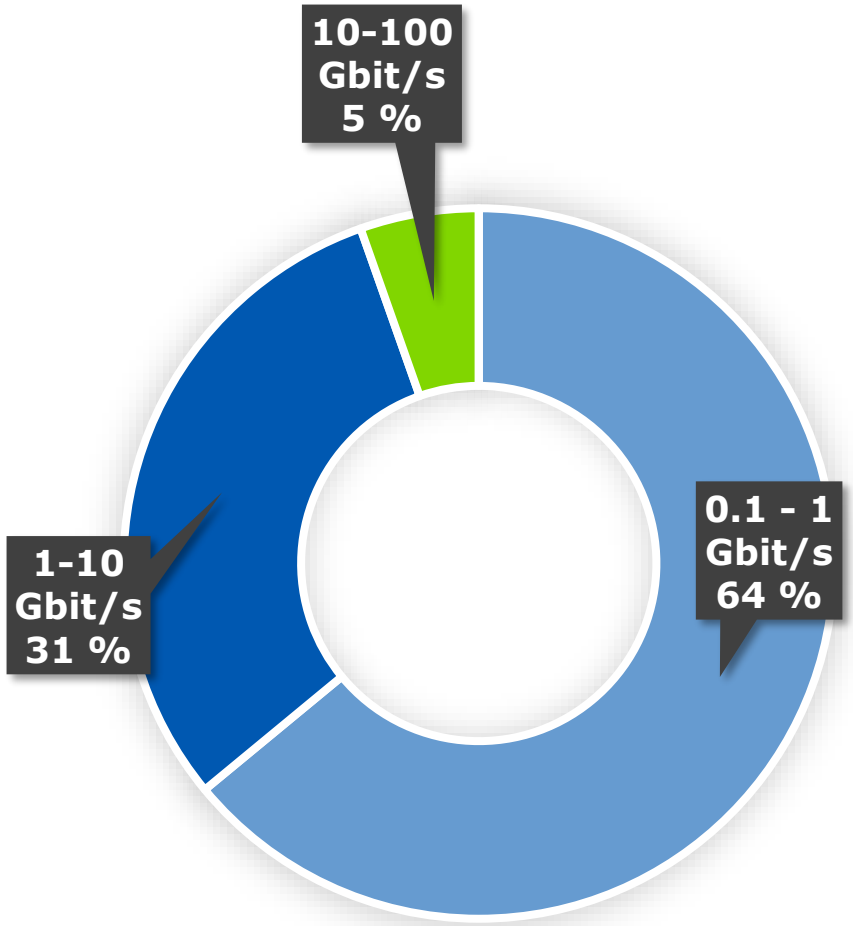
Analyysi

- Palvelunestohyökkäys häiritsi Nobel-palkintojen jakoa joulukuussa
  - https://www.bleepingcomputer.com/news/security/nobel-foundation-site-hit-by-ddos-attack-on-award-day/
- Iso-Britannian kansallinen kyberrikosyksikkö on aloittanut kampanjan jolla pyritään lisäämään nuorten tietoisuutta tilattujen DDoS hyökkäysten rikosseuraamuksista
  - Kouluverkkoihin kohdistuneet hyökkäykset ovat kasvaneet voimakkaasti viimevuosina.
  - https://www.nationalcrimeagency.gov.uk/news/rise-in-school-cyber-crime-attacks-sparks-nca-education-drive

Palvelunestohyökkäysten tunnuslukuja

3kk

- 379 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q4/2021
- Noin 74% hyökkäyksistä oli pituudeltaan alle 15 minuuttia
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q4/2021 - tilasto päivitetään kvartaaleittain.)

Vakoilu

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

Vakoilu

- Ulkoministeriö kertoi selvittäneensä suomalaisdiplomaatteihin kohdistuneen vakoilutapauksen. Diplomaatteja oli vakoiltu NSO Groupin Pegasus-haittaohjelmalla
  - Ulkoministeriö ei kertonut vakoilun ajankohtaa mutta sanoo, että tapausta on selvitetty syksyn ja talven 2021–2022 aikana. Myös Kyberturvallisuuskeskus on tukenut selvitystyötä
  - Vakoilun kohteena oli Suomen ulkomailla työskentelevä, niin sanottu lähetetty henkilökunta
- Pegasus on NSO Groupin kehittämä valtioiden ja viranomaisten työkaluksi suunniteltu ohjelma. Sen käyttö poliittisten vastustajien, aktivistien ja toimittajien vakoiluun nousi laajasti julkisuuteen kesällä 2021
  - Ohjelma mahdollistaa käyttäjän Apple iOS- tai Android-puhelimen vakoilun edistynein menetelmin. Vakoilu oli mahdollista ilman käyttäjän toimenpiteitä ja käyttäjän huomaamatta
  - Julkisuudessa on raportoitu lukuisista valtioista, jotka ovat hyödyntäneet Pegasusta

Analyysi

- Korkean profiilin henkilöiden mobiilipäätelaitteet tulee suojata vastaavalla tavoin kuin muukin tietotekniikka
- Autoritääriset valtiot pystyvät hyödyntämään erityisesti matkaviestintäverkkoja haluamiensa kohteiden vakoiluun
- Tämä pitää huomioida matkustusturvallisuudessa, esimerkiksi hyödyntämällä vain matkustuksen aikaiseen käyttöön tarkoitettuja mobiilipäätelaitteita

Vakoilu

- Ukrainassa on havaittu erilaisia kyberhyökkäyksiä tammikuussa Ukrainan ja Venäjän välisen konfliktin kiristyttyä
- Useille Ukrainan valtionhallinnon verkkosivuille tunkeuduttiin ja sivuilla julkaistiin uhkailevia viestejä
- Ukrainalaisiin organisaatioihin on lisäksi kohdistunut haittaohjelmahyökkäys, jonka tarkoituksena on estää kohdejärjestelmän toiminta ja tuhota tiedostoja
  - Haittaohjelma on nimetty WhisperGateksi
  - Haittaohjelma näyttäytyy kiristyshaittaohjelmana, mutta sitä analysoimalla on pystytty toteamaan, että tosiasiallinen tarkoitus on tietojen tuhoaminen ja toiminnan haittaaminen ilman mahdollisuutta tietojen palauttamiseen lunnaita vastaan

Analyysi

- Merkkejä tilanteen laajenemisesta Ukrainan ulkopuolelle ei toistaiseksi ole
- Organisaatioiden, joilla on toimintaa tai liittymäpintoja Ukrainaan, on syytä varautua siihen, että Ukrainassa tapahtuneet kyberhyökkäykset aiheuttavat heille seurannaisvaikutuksia

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.

Oikeudelliset asiat

Työryhmä selvittämään keinoja viranomaisten yhteistoiminnan tehostamiseksi kyberturvallisuuden häiriötilanteissa

- Liikenne- ja viestintäministeriö on 28.1.2022 asettanut työryhmän arvioimaan lainsäädäntötarpeita ja tukemaan säädösvalmistelua, joka koskee keskeisten viranomaisten yhteistoimintaa kyberturvallisuuden häiriötilanteissa
- Tavoitteena edistää keskeisten viranomaisten mahdollisimman tehokasta yhteistoimintaa laajamittaisissa kyberturvallisuuden häiriötilanteissa
- Työn esikuvana toimii poliisin, tullin ja rajavartiolaitoksen yhteistoiminnasta (PTR) annettu laki
- Työryhmän toimikausi on 1.2.2022-31.3.2023
- Lisätietoja: https://www.lvm.fi/-/tyoryhma-selvittamaan-keinoja-viranomaisten-yhteistoiminnan-tehostamiseksi-kyberturvallisuuden-hairiotilanteissa-1645662

Traficomin kyberturvallisuuskeskus mukana eurooppalaisen digitaalisen identiteetin valmistelun kansallisessa koordinaatioryhmässä

- Valtiovarainministeriö asettanut eurooppalaisen digitaalisen identiteetin valmistelun kansallisen koordinaatioryhmän ajalle 27.1.2022-31.7.2023
- Työryhmän tavoitteena on pyrkiä vaikuttamaan Suomen tavoitteiden mukaisesti eurooppalaisen digitaalisen identiteetin valmisteluun EU:n toimielimissä ja yhteistyössä muiden jäsenvaltioiden kanssa
- Eurooppalainen digitaalinen identiteetti on EU-kansalaisille, EU:ssa asuville henkilöille sekä yrityksille tarkoitettu väline tunnistautumista tai tiettyjen henkilötietojen vahvistamista varten
  - Voidaan käyttää sekä julkisissa että yksityisissä sähköisissä ja muissa palveluissa
- Lisätietoja: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_fi

Oikeudelliset asiat

Belgian tietosuojaviranomainen: IAB Euroopan mainosmekanismi yleisen tietosuoja-asetuksen vastainen

- Belgian tietosuojaviranomainen katsoi 2.2.2022 antamassaan päätöksessä, että IAB Euroopan (Interactive Advertising Bureau Europe) sähköiseen mainontaan ja käyttäjien valintojen hallinnointiin kehittämä Transparency and Consent Framework –mekanismi rikkoo useita EU:n yleisen tietosuojasetuksen kohtia
- Kyseinen mekanismi on laajasti käytössä eri palveluntarjoajien internetsivustoilla EU:n alueella
- Ratkaisu ei sido Traficomia evästeiden käyttöä valvovana viranomaisena, mutta Traficom arvioi sen merkitystä valvomansa sääntelyn kannalta
- Lisätietoja: https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

Saksalainen tuomioistuin: Kolmannen osapuolen fonttien ja sisältöelementtien käyttö internetsivulla edellyttää suostumusta

- Saksalainen tuomioistuin katsoi 20.1.2022 antamassaan ratkaisussa, että kolmannen osapuolen tarjoamien fonttien tai muiden sisältöelementtien käyttö internetsivulla edellyttää käyttäjän suostumusta
- Käyttäjän suostumusta tulee pyytää EU:n yleisen tietosuoja-asetuksen nojalla, koska käyttäjää koskevia tietoja välitetään kolmannen osapuolen palvelimelle osana fonttien tai muiden elementtien lataamista
- Ratkaisu ei sido Traficomia evästeiden käyttöä valvovana viranomaisena, mutta Traficom arvioi sen merkitystä valvomansa sääntelyn kannalta
- Lisätietoja: https://rewis.io/urteile/urteil/lhm-20-01-2022-3-o-1749320/

Oikeudelliset asiat

Itävallan ja Ranskan tietosuojaviranomaiset: Google Analyticsin käyttö vastoin EU:n yleistä tietosuoja-asetusta

- Itävallan tietosuojaviranomainen ja Ranskan tietosuojaviranomainen CNIL ovat 13.1.2022 ja 10.2.2022 antaneet päätökset, joiden mukaan Google Analyticsin tapa käsitellä henkilötietoja ja tietojen siirto EU-alueen ulkopuolelle ovat vastoin EU:n yleistä tietosuoja-asetusta
- Viranomaisten mukaan siltä osin kuin EU-kansalaisia koskevia henkilötietoja siirretään Googlen Yhdysvalloissa sijaitseville palvelimille, Yhdysvaltojen tiedusteluviranomaisilla on tarvittaessa pääsy dataan, jolloin EU:n yleisen tietosuoja-asetuksen mukainen yksityisyydensuoja ei toteudu
- Ratkaisujen taustalla on EU-tuomioistuimen ”Schrems II”-ratkaisu 16.7.2020, joka kumosi EU:n ja Yhdysvaltojen välillä tapahtuvaa tiedonsiirtoa koskevan Privacy Shield –sopimuksen
- Itävallan ja Ranskan ratkaisut eivät sido Traficomia evästeiden käyttöä valvovana viranomaisena, mutta Traficom arvioi niiden merkitystä valvomansa sääntelyn kannalta
  - Itävallan tapaus: https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal
  - Ranskan tapaus: https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply

Arjen kyberturvallisuus

Euroopan laajuinen 112-päivä

- Viime perjantaina vietettiin Euroopan laajuisesti 112-päivää. Tämän vuoden teemana on "Turvallisuuden tunne tehdään yhdessä". Tietoturva onkin verrattavissa kodin turvallisuuteen. Nappaa talteen vinkit oman turvallisuuden parantamiseksi
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvavinkit-kuuluvat-112-paivaan

Mediataitoviikko

- Viime viikolla vietettiin mediataitoviikkoa, joka on mediakasvatuksen oma teemaviikko, ja tarjoaa mediataitojen kanssa työskenteleville inspiraatiota oman työn kehittämiseen
- Käy tutustumassa Traficomin Kyberturvallisuuskeskuksen kaikenikäisille tarkoitettuihin oppaisiin: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mediataitoviikko-tarjoaa-tekemista-kaikenikaisille

Kuluttajaliitto muistuttaa verkkohuijauksista: varo, varmista ja varoita

- Suomalaisilta viety tänä vuonna jo kymmeniä miljoonia nettihuijauksilla
- Lue vinkit suojautumiseen Kuluttajaliiton sivuilta: https://www.kuluttajaliitto.fi/varo-varmista-varoita/

Aktiivista Facebook-tunnusten kalastelua Facebook Messengerin kautta

- Huijausyrityksessä murretulta tililtä lähetetään viesti, jonka tavoitteena on saada vastaanottajan Facebook-tili haltuun uhrin puhelinnumeron ja kaksivaiheisen tunnistautumisen vahvistuskoodin avulla
- Lisätietoja: https://www.kyberturvallisuuskeskus.fi/fi/ttn_20012022

Uutisia Kyberturvallisuuskeskuksesta

Traficomin Kyberturvallisuuskeskus järjesti webinaarin kuntatoimijoille

- Kyberturvallisuuskeskus tekee tiiviisti yhteistyötä huoltovarmuuskriittisten organisaatioiden kanssa
- Seminaarin aamupäivä oli suunnattu hallinnon toimijoille ja iltapäivä kuntien teknisille asiantuntijoille
- Seminaarin tallenne on nähtävillä Youtubessa https://www.youtube.com/watch?v=V-ghgg0QZJw

Kyberturvallisuuskeskuksen CERT -toiminnon PGP-avaimet vaihtuivat

- Kyberturvallisuuskeskuksen CERT-toiminnon yleinen avain (NCSC-FI Incident Response), tiedotteiden allekirjoittamiseen käytetty avain (NCSC-FI Advisory Signing Key) ja uutiskoosteen allekirjoittamiseen käytetty avain (NCSC-FI Newsfeed Signing Key) vaihtuvat. Uudet avaimet ovat saatavilla keskuksen www-sivuilla ja yleisillä avainpalvelimilla
- Linkki uutiseen https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/cert-toiminnon-pgp-2022

Uudistuksia Kyberturvallisuuskeskuksen lomakkeissa

- Myös yksityishenkilöille tietoturvaloukkausten ilmoittamiseen tarkoitetut lomakkeet ovat päivittyneet
- Lue lisää https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/uudistuksia-kyberturvallisuuskeskuksen-lomakkeissa

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