TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Kesäkuu 2021

#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

Kybersää kesäkuu 2021

Tietomurrot ja -vuodot

- Tietovuoto voi tapahtua myös tahattomasti tai ilman, että ulkopuolinen toimija aiheuttaa sen.
- Varmuuskopioiden kanssa pitää olla huolellinen, avainasemassa on tiedon monistaminen.

Huijaukset ja kalastelut

- Pankkien nimissä tehtiin jälleen aktiivisesti tietojen kalastelua. Verkkohuijausten taloudelliset menetykset ovat poliisin mukaan olleet tänä vuonna miljoonia euroja.
- FluBot-kampanja oli erittäin aktiivinen kesäkuussa.

Haittaohjelmat ja haavoittuvuudet

- Norjalainen Axiell AS on joutunut kiristyshaittaohjelman uhriksi.
- Kaseya-toimitusketjuhyökkäys vaikutti satoihin organisaatioihin.
- Tekstiviestien linkkien avulla leviävät haittaohjelmat ovat olleet hyvin aktiivisia.

Automaatio ja IoT

- Boschin IP-kameroista on kriittinen haavoittuvuus. Päivitys on saatavilla.
- Useat tahot ovat julkaisseet ohjeita, joiden tavoitteena on saada organisaatiot järjestelmällisemmin varautumaan kyberuhkiin.

Verkkojen toimivuus

- Kesäkuussa 14 merkittävää toimivuushäiriötä yleisissä viestintäpalveluissa.
- Myrskyt ja huoltokatkot nostivat toimivuushäiriöiden määrää edellisiin kuukausiin (huhtikuussa 2 kpl ja toukokuussa 3 kpl) verrattuna.
- Kiristysviestejä palvelunestohyökkäysteemalla

Vakoilu

- Länsimaiset tietoturvaviranomaiset tiedottivat laajamittaisen bruteforce-kampanjan yhdistämisestä Venäjän sotilastiedusteluun.
- Aasian maat olivat runsaasti edustettuina kybervakoilua koskevissa uutisissa.

Kuukauden tunnuslukuja

~1400

HAAVOITTUVIA ZYXEL-LAITETTA SUOMESSA. ZYXELIN 24.6 JULKAISEMAN HAAVOITTUVUUDEN TEKEE KRIITTISEKSI SE, ETTÄ VERKKOLAITTEET OVAT SAATAVILLA INTERNETISTÄ, MIKÄ TEKEE NIISTÄ MYÖS HYÖKKÄÄJILLE HALUTTUJA KOHTEITA.

YLI 1600

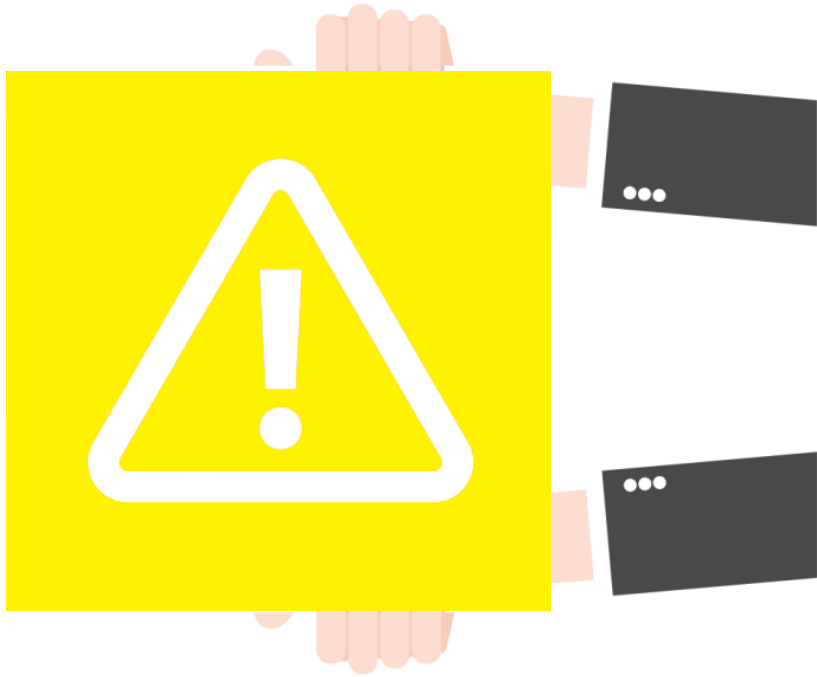
SAAMAMME ILMOITUKSET FLUBOT HAVAINNOISTA. SUURIN OSA ILMOITTAJISTA OLI YKSITYISHENKILÖITÄ. FLUBOT ON ANDOIRD-LAITTEILLE SUUNNATTU HAITTAOHJELMA, JOKA LEVIÄÄ TEKSTIVIESTISTSE. JULKAISIMME FLUBTOISTA VAROITUKSEN KESÄKUUSSA!

10.6.2021

JULKAISTIIN KYBERTURVALLISUUDEN KEHITTÄMISOHJELMA. SIINÄ MÄÄRITETÄÄN KESKEISET TOIMENPITEET KYBERTURVALLISUUDEN PARANTAMISEKSI KOKO YHTEISKUNNASSA.

Julkaisimme 2/2021 Tekstiviestitse levitettävät Android-haittaohjelmat

- Julkaisimme keltaisen varoituksen 4.6.2021. Varoitus päätettiin poistettiin 22.6., koska tilanne ei enää ollut niin akuutti. **Nyt varoitus on aktivoitu uudelleen, sillä tapausmäärät ovat merkittävästi nousseet.**
- Haittaohjelma on kohdistettu kaikille, joilla on käytössään Android-laite ja matkapuhelinliittymä.
- Uusi viestityyppi kertoo, että henkilö on saanut vastaajaviestin ja viesti sisältää linkin sivustolle. Sivun latauslinkki tarjoaa .apk-sovelluksen asentamista, joka sisältää haittaohjelman Android-laitteille (esim. FluBot).
- Aikaisemmin suomenkielinen, pakettitoimituksesta kertova huijaustekstiviesti sisälsi linkin sivustolle, jonka kautta haittaohjelmaa levitettiin.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/tekstiviestitse-levitettavat-android-haittaohjelmat



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

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

3

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

Symbolit

Uusi

Päivitetty

4

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

5

Etätyö tuli jäädäkseen – niin myös riskit. Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.

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.

- 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

Microsoft tiedotti 2.3. Exchange-sähköpostipalvelimien kriittisistä haavoittuvuuksista ja niiden aktiivisesta hyväksikäytöstä. Kyberturvallisuuskeskus havaitsi suomessa aluksi lähes 300 haavoittuvaa Exchange-palvelinta. Mukana oli myös palvelimia, joihin oli jo murtauduttu haavoittuvuutta hyväksi käyttäen. Suomalaisten organisaatioiden haavoittuvat Exchange-palvelimet oli päivitetty huhtikuun alkuun mennessä. Organisaatioiden kyky reagoida kriittisiin haavoittuvuuksiin, päivityksiin sekä tietomurtojen tutkintaan nousi tärkeäksi osaksi Exchange-haavoittuvuuksien hoidossa.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

2

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.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

3

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.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

4

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.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

5

Etätyö tuli jäädäkseen – niin myös riskit Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.

- Vuonna 2020 siirryttiin kiireen vilkkaa etätöihin. Osa toimijoista rakensi etätyöjärjestelynsä kiireessä kirjavien viritysten varaan. Näiden väliaikaisten ratkaisujen kuntoon laittamisessa kestää vielä pitkään.
- Laaja siirtymä etätyöhön näkyi maaliskuussa 2020 suojattomien laitteiden määrän selvänä kasvuna Suomen verkoissa. Verkkoon avoimilla laitteilla ja laitteiden suojattomilla etäyhteyspalveluilla tarkoitetaan tässä yhteydessä esimerkiksi avoimia etätyöpöytäyhteyksiä ja tiedostonjakopalveluja (esim. RDP, VNC ja SMB).
- Kesän 2021 jälkeen organisaatioissa ollaan todennäköisesti hybridiratkaisussa, jossa osa tekee töitä etänä ja osa toimistolla. Tässä tulee huomioida myös se, että koronan alussa tehdyt nopeat etätyöratkaisut tarkastellaan ja varmistetaan niiden tietoturvallisuus, jotta tietoturva huomioidaan ja voidaan taata pysyvämmässä mallissa.

CASE

Suojelupoliisin tiedote: Ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun. Suojelupoliisi on havainnut, että suomalaista infrastruktuuria hyödyntävä kybervakoilu on lisääntynyt. Erityisesti autoritaaristen valtioiden tiedustelupalvelujen kybervakoiluoperaatioissa on käytetty hyväksi kymmeniä suomalaisten yksityishenkilöiden ja yritysten verkkolaitteita ja palvelimia liittämällä ne osaksi operaatiossa käytettävää infrastruktuuria.

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

- Tietovuoto ei johdu aina ulkopuolisesta toimijasta
  - Tietovuoto voi tapahtua myös esimerkiksi inhimillisen virheen seurauksena tai järjestelmän suunnitteluvirheen vuoksi
  - Tietovuodon juurisyyn selvittäminen on tärkeää, järjestelmätestaus on tärkeää tehdä huolellisesti ennen järjestelmien käyttöönottoa
  - Hyvin suunnittelulla viestinnällä ja tiedottamisella on mahdollista välttää myöhempiä PR-tappioita

ANALYYSI

- LinkedIn:n kesäkuussa kertoma 700 miljoonan käyttäjän tietovuoto ei ollut tietomurrosta aiheutunut tietovuoto
- Järjestelmän paremmalla suunnittelulla oltaisiin kenties voitu välttää tietojen massamainen keräämismahdollisuus

Tietomurrot ja -vuodot

- Tietomurron seurauksena tuhottiin tiedot ja vaadittiin lunnaita tietojen palautuksesta
  - Tämän tyyppisessä toiminnassa ei käytetä kiristyshaittaohjelmaa
  - Verkkokovalevykin on mahdollista murtaa ja tiedot voivat hävitä myös sieltä
  - Tietojen palauttaminen voi olla mahdollista tällaisissa tapauksissa, mutta siitä ei ole mitään takeita
  - Katso lisää esimerkiksi Pienyritysten kyberturvallisuusoppaastamme https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

ANALYYSI

- Varmuuskopiointi tulee tehdä säännöllisesti ja avainasemassa on tiedon monistaminen
- Tietoja pitäisi olla useammassa paikassa ja mielellään offline
- Mikäli alkuperäinen tietue on tuhottu ja siirretty varmuuskopiointiratkaisuun, ei kyseessä ole enää varmuuskopiointi

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

- Tekstiviestien käyttö on yleistynyt huijausviesteissä huomattavasti
  - Aikaisemmin eri kuljetuspalveluiden nimissä on lähetetty huijaus- ja kalasteluviestejä, mutta kesäkuussa yleistyivät myös viestit, joissa kerrotaan vastaajaan saapuneesta viestistä.
  - Näissä erityisesti kesäkuussa on näkynyt viestit, joissa yritetään levittää Flubot haittaohjelmaa.

ANALYYSI

- Tällä hetkellä suurin ilmoittajajoukko on yksityishenkilöt Flubotin osalta.
- Organisaation näkökulmasta on tärkeää tiedostaa, että FluBot varastaa käyttäjän puhelimesta tietoja, mikäli käyttäjä asentaa haitallisen .apk-tiedoston Android-puhelimelle. Tällaisissa tapauksissa on tärkeä tietää, mitä tietoja puhelimessa on ollut ja tehdä riskiarvio, minkälaiset vaikutukset tietovuodolla voisi olla.
- Ennaltaehkäisy on tärkeää ja organisaation on hyvä tiedottaa mm. FluBot-ilmiöstä, jotta henkilöt eivät lataa haittaohjelmaa puhelimelleen ja näin ollen välttyvät myös puhelimen nollaukselta.

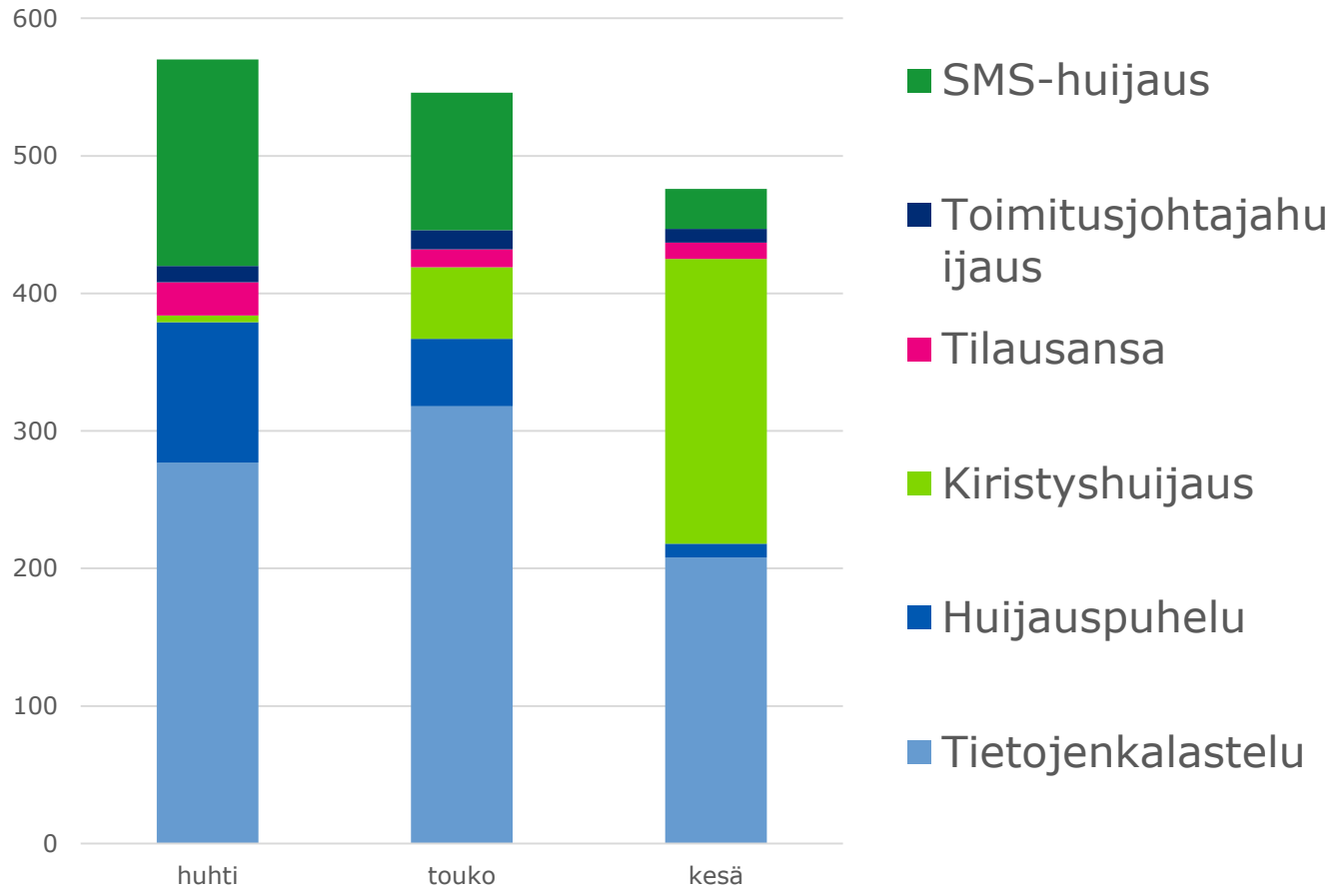
Huijaukset ja kalastelut

- Pankkikalasteluja tehtiin myös kesäkuussa ahkerasti niin tekstiviestitse kuin sähköpostin välityksellä
- Pankkikalastelua tehdään entistä taitavammin.
  - Pankkitietoja, maksukorttitietoja, henkilötietoja ja kirjautumistietoja kalastellaan hyvin monenlaisilla eri verukkeilla.
  - Tyypillisin kalasteluviesti väittää, että uhrin tunnus tai tili jäädytetään tai sopimus on päättymässä, klikkaa tästä jos haluat jatkaa tiliä. Toinen yleinen kalasteluviesti vetoaa virhetilanteeseen tai muuhun ongelmaan, joka pitää korjata klikkaamalla.

ANALYYSI

- Poliisi kertoi kesäkuussa, että se on saanut yli 300 ilmoitusta joko pankki- tai kuljetusalan nimissä tehdyistä verkkohuijauksista. Rikoshyöty näistä on ollut yli 4 miljoonaa euroa.
- Poliisin ja meidän saamat ilmoitukset tapauksista kertovat siitä, että tällaiset verkkohuijaukset kohdistuvat erityisesti yksilöön. Yksittäistapauksessa tuhansien eurojen menetys on tuntuva yksilölle.

Käsiteltyjä huijaustapauksia Q2/2021



- Vuoden toisen neljänneksen 2021 ilmiöitä ovat:
  - Kiristyshuijaukset esiintyivät kausittain aalloissa. Tämä näkyy päivitetyssä tilastossa, jossa kesäkuun pornokiristysaalto, näkyy kiristyshuijausten määrän merkittävässä kasvussa.
  - Pankkikalastelu on toinen, jota esiintyy aalloissa ja erittäin aktiivisesti.
- 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

- Norjalainen Axiell AS on joutunut kiristyshaittaohjelman uhriksi
  - Axiell Norge AS tarjoaa ohjelmistoja mm. kirjastoille, kouluille ja museoille
  - Axiell Norge AS toimittaa Mikromarc-nimistä ohjelmistoa, johon haittaohjelmatapaus vaikuttaa
  - Palveluja on käytössä myös Suomessa, joten kiristyshaittaohjelmalla oli vaikutusta suomalaisten kirjastojen, koulujen ja museoiden palveluihin
  - 30.6.: Axiellin kaikki suomalaiset käyttäjät saivat taas palvelut käyttöönsä

ANALYYSI

- Kiristyshaittaohjelmalla voidaan lamauttaa yrityksen liiketoiminta
- Kiristyshaittaohjelma voi osua kaikenlaisiin toimijoihin ja sektoreihin
- Toimitusketjut voivat olla hyvinkin pitkiä ja monimutkaisia ja riippuvuudet voivat tulla yllätyksenä

Haittaohjelmat

- Useat keskitettyä palvelunhallintaa (MSP) tarjoavat tahot sekä niiden asiakkaat ovat olleet Kaseya-toimitusketjuhyökkäyksen kohteena
  - Hyökkäyksessä on hyödynnetty nollapäivähaavoittuvuutta Kaseyan VSA-komponentissa
  - Kiristyshaittaohjelma on päässyt aktivoituvaan useissa koneissa
  - Hyväksikäytetty nollapäivähaavoittuvuus oli Kaseyalla tiedossa, mutta sitä ei ehditty päivittää ennen REvilin tekemään kyberhyökkäystä
  - Ruotsissa lähes kaikki Coop-ketjun myymälät joutuivat sulkemaan ovensa kiristyshaittaohjelman vuoksi, koska myyntipäätteet olivat poissa käytöstä
  - Ruotsissa vaikutuksia oli myös huoltoasemien ja apteekkipalveluiden toimintaan

ANALYYSI

- Ruotsin tilanteen juurisyynä oli se, että Kaseyan tuotteita käyttävä palveluntarjoaja toimittaa kassajärjestelmäpalveluita Coop-myymälöille.
- Kassajärjestelmätoimittajalla ei ollut tietoturvaongelmia, mutta sen ostama Kaseya-palvelu johti ongelmiin. Toimitusketjuhyökkäykseen on teknisesti vaikea varautua, kun siihen liittyy useampia toimijoita pidemmässä ketjussa.

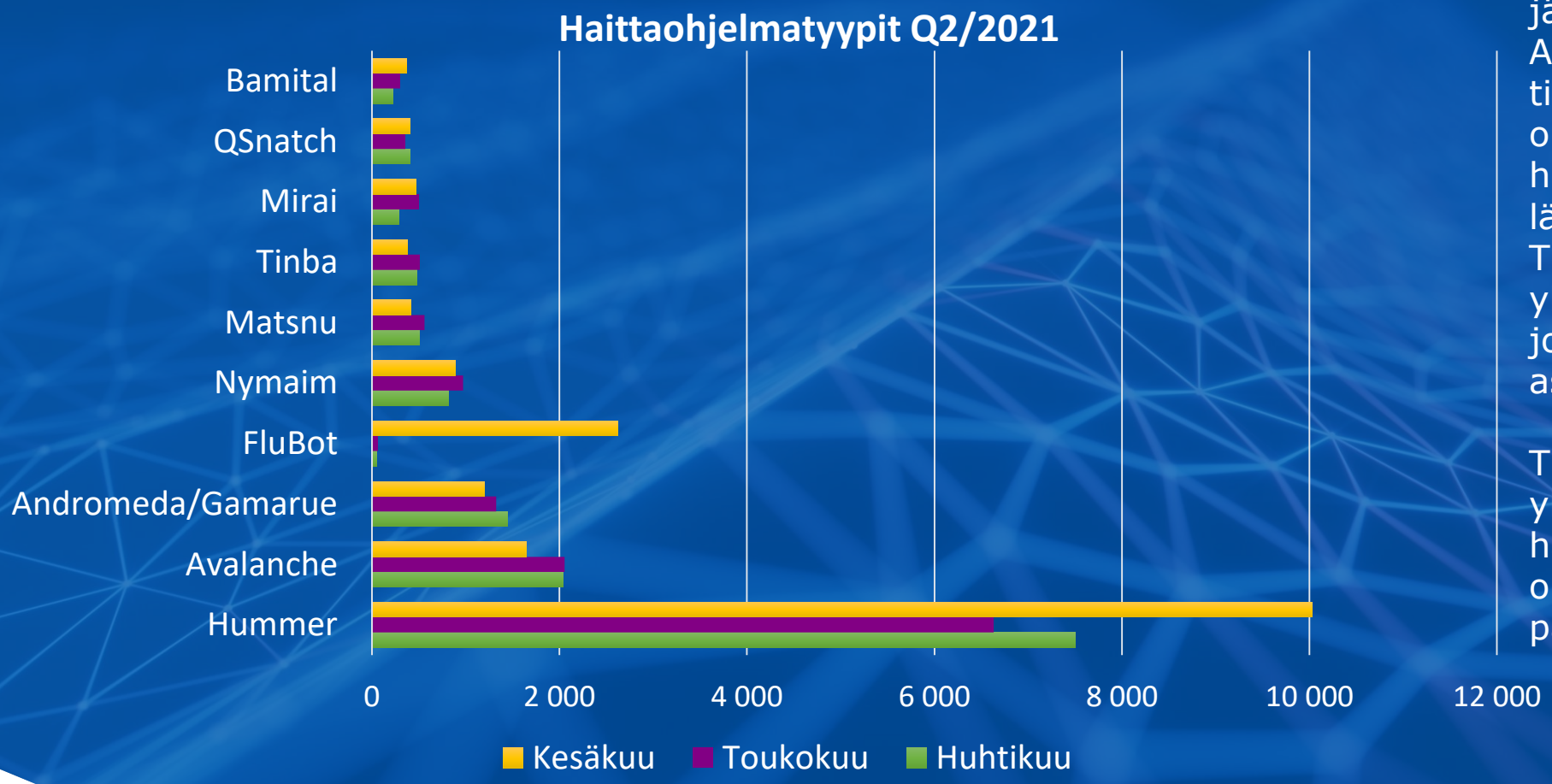
Haittaohjelmat

- Kyberturvallisuuskeskukselle on tullut paljon ilmoituksia aktiivisesti levitettävistä haittaohjelmista
  - Aiemmin olemme kertoneet Fakecop/Fakespy-haittaohjelman levityksestä ja viimeisimpänä FluBotista, mutta saamme ilmoituksia myös muista haittaohjelmista kuten QakBotista
  - QakBot on tietoja varastava troijalainen, joka kykenee myös levittämään muita haittaohjelmia saastuneisiin laitteisiin
  - Haittaohjelmaa levitetään samalla mallilla kuin 2020 Suomeen iskenyttä Emotet-haittaohjelmaa: jollakin tavalla varastettuun postikeskusteluun tulee väärennetystä lähteestä uusi viesti ja pyyntö ladata tiedosto
  - Emotetista poiketen QakBotia levitetään myös kalastelun uhriksi joutuneiden käyttäjien tileiltä varastettujen postien kautta. Emotet-haittaohjelmaa levitettiin käytännössä pelkästään Emotetilla saastuneilta laitteilta varastettujen tietojen pohjalta

ANALYYSI

- Haittaohjelmien tavoitteena voi olla tietojen varastaminen saastuneelta laitteelta ja haittaohjelmaa edelleen levittävien tekstiviestien lähetys
- Omien käyttäjätilien suojaaminen monivaiheisella tunnistautumisella ja salasanojen vaihtaminen haittaohjelman saastuttaneella laitteella käytetyistä palveluista (mm. sähköposti ja sosiaalinen media) on tärkeää, jotta haittaohjelman varastamat tiedot eivät päädy huijareiden käyttöön.

Autoreporterin haittaohjelmahavainnot



Torjumme haittaohjelmia yhteistyössä teleyritysten kanssa Autoreporter-järjestelmän avulla. Autoreporter-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.

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

Haavoittuvuudet

- Zyxel on tiedottanut haavoittuvuudesta 24.6. ja julkaissut korjaavan päivityksen
  - Zyxel on julkaissut 6.7. korjaavan päivityksen ja ohjeet, joilla voidaan lieventää haavoittuvuutta ja sen vaikutuksia
  - Haavoittuvuuden hyväksikäyttö on tietojemme mukaan alkanut jo 22.6.
  - Suomalaisilta organisaatioilta on löydetty kymmeniä murrettuja laitteita
  - Tunkeutumisen laajentamista ei ole havaittu

ANALYYSI

- Haavoittuvuuden tekee kriittiseksi se, että verkkolaitteet ovat saatavilla internetistä, mikä tekee niistä myös hyökkääjille haluttuja kohteita
- Hyökkääjät ovat haavoittuvuutta hyväksikäyttämällä ohittaneet tunnistautumisen ja muodostaneet SSL VPN-tunnelin tuntemattomien käyttäjien nimissä

Kuukauden haavoittuvuusjulkaisut

- Kriittinen haavoittuvuus etäkäytettävissä Zyxelin tuotteissa (18/2021)
- Kriittinen taustatulostuspalvelun haavoittuvuus Windows-versioissa (19/2021)

- Lue lisää: www.kyberturvallisuuskeskus.fi/haavoittuvuudet

ANALYYSI

- Päivitykset tulee asentaa viipymättä, haavoittuvuuksien hyväksikäyttö on todella nopeaa
- Päivityssyklien ulkopuoliset päivitykset tulee myös huomioida, muutoin järjestelmään voi jäädä kriittisiä haavoittuvuuksia pitkäksikin aikaa

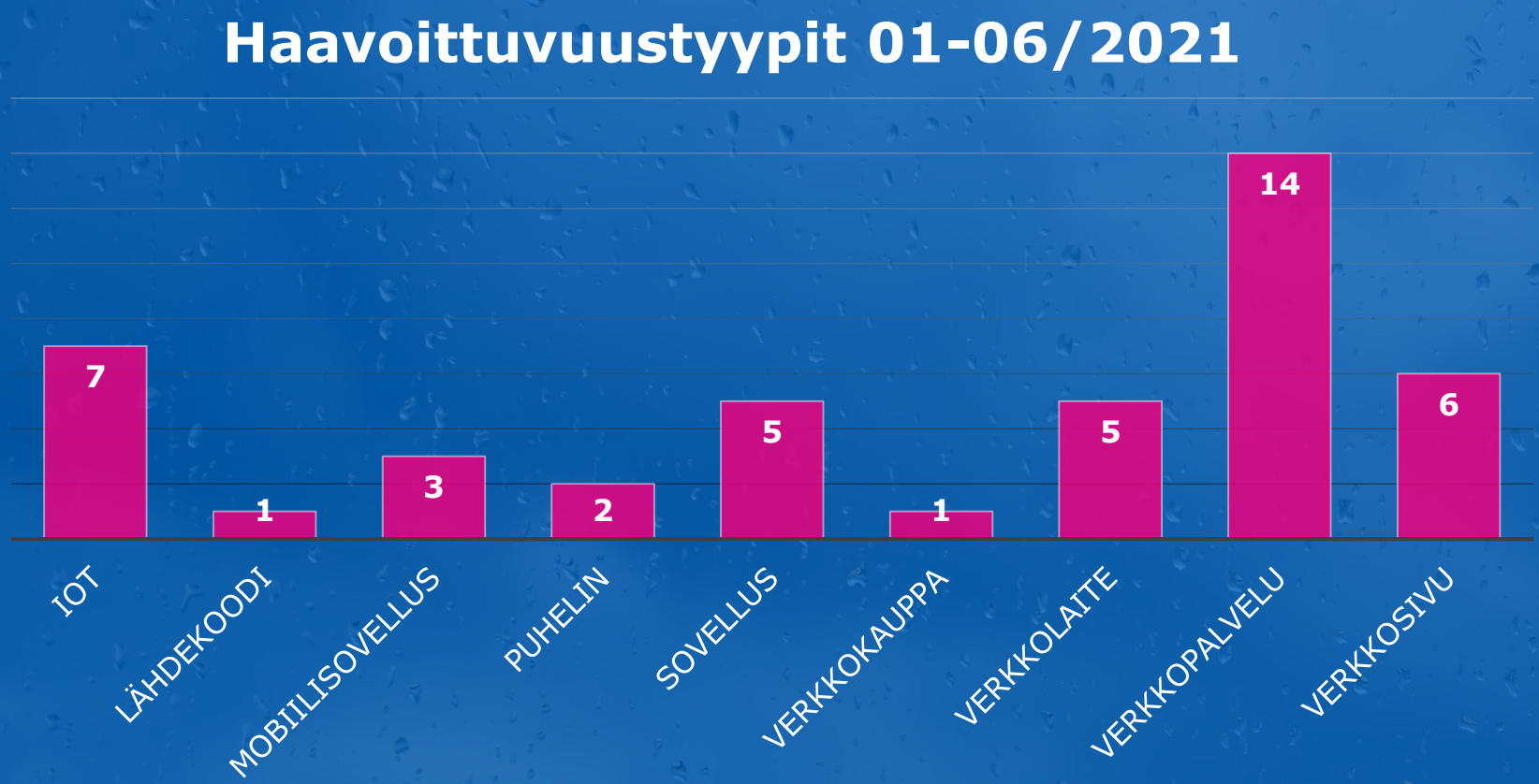
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- Kyberturvallisuuskeskus vastaanottaa vuositasolla noin 50kpl 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 19 kpl (tilanne 7.7.2021)
  - Mukana mm. Microsoft Exchange Server ja etäkäyttötoteutusten haavoittuvuudet
- Tilaamalla haavoittuvuuskoosteen saat tietoa erilaisista haavoittuvuuksista
  - Kaikista haavoittuvuuksista ei julkaista suomenkielistä haavoittuvuustiedotetta
  - Kooste julkaistaan lähes päivittäin
  - 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 myös toistuva ilmiö. Voi olla, että muutoin tietoturvallisesta tuotteesta löytyy kovakoodattu oletussalasana. Erilaisissa verkkopalveluissa voi myös olla parannettavaa salasanakäytännöissä esimerkiksi 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 löytämisen johdosta, sellaisen koordinoinnissa tai esimerkiksi CVE-tunnisteen haussa – olettehan yhteydessä Kyberturvallisuuskeskukseen.
- https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

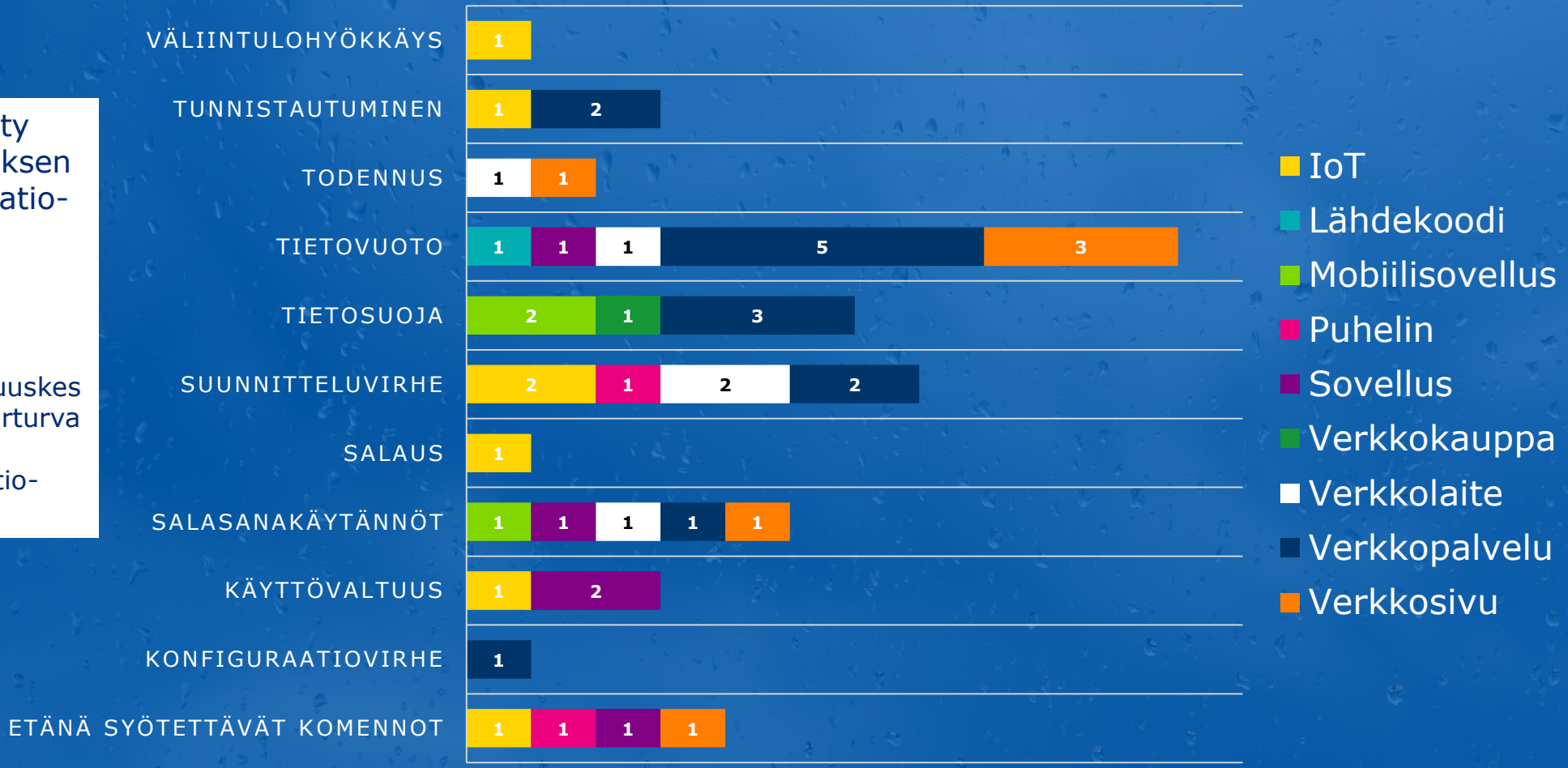
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio



Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

Taulukossa on esitetty Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio-tapauksia.

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.

Automaatio & IoT

- Liikenne- ja viestintävirasto Traficomin teettämän Kuluttajatutkimuksen mukaan kuluttajien tietoisuus älylaitteisiin liittyvistä riskeistä on noussut vuosi vuodelta. Traficomin vuonna 2019 julkaisema Tietoturvamerkki parantaa osaltaan kuluttajien mahdollisuutta tehdä tietoturvallisempia valintoja älylaiteostoksissaan.
  - Keväällä 2021 teettämän Kuluttajatutkimuksen mukaan hieman aiempaa suurempi osuus kuluttajista on tietoisia siitä, että nettiin kytkettävät turvattomat älylaitteet voivat jakaa tietoja luvatta ulkopuolisille.
  - Aiemmin Traficomin Kyberturvallisuuskeskus on vastannut yksin älytuotteiden tietoturvatarkastuksista. Haluamme laajentaa voimakkaasti merkittyjen tuotteiden saamista kauppoihin ja helpottaa yritysten tuotetarkastusprosessia.
  - Keväästä 2021 lähtien Traficom on antanut kaupallisille yrityksille mahdollisuuden tehdä Tietoturvamerkin saamisen edellytyksenä olevat tekniset tarkastukset. Traficom kuitenkin edelleen myöntää itse Tietoturvamerkin ja vastaa siitä, että sen vaatimukset toteutuvat

ANALYYSI

- Hyvän tietoturvallisuuden edellytyksenä on paitsi turvallisen käytön mahdollistava laite, myös osaava käyttäjä. Turvallinenkin laite voi muuttua turvattomaksi, jos sitä käytetään väärin. Siksi jokaisen tulisi perehtyä käyttämiensä laitteiden tai palveluiden tietoturvaan niin, että pystyy käyttämään niitä turvallisesti.

Automaatio & IoT

- Kesän alussa on julkaistu useita ohjeita ja artikkeleita koskien automaatiojärjestelmien että IoT:n tietoturvaa, alla muutamia:
  - Standardeilla kyberhyökkäyksiä vastaan kuvaa standardien merkitystä kyberturvallisuuden edistämisessä. https://sfs.fi/standardeilla-kyberhyokkayksia-vastaan/
  - Kuuntelevien IoT laitteiden osalta Yhdysvaltojen armeija suositteli työntekijöitään välttämään työntekoa niiden lähettyvillä, mutta veti suosituksensa pois. Laitteet kannattaa huomioida riskiarvioinneissa.
  - Ohjelmoitavan logiikan (PLC) turvalliselle toteuttamiselle julkaistiin 20 parasta käytäntöä https://www.plc-security.com/content/Top_20_Secure_PLC_Coding_Practices_V1.0.pdf
  - Automaation tietoturvakirjasta on julkaistu uudistettu painos (maksullinen) https://www.automaatioseura.fi/uutiset/uusi-kirja-automaation-tietoturvasta/

ANALYYSI

- On tärkeää tuntea oma toimintaympäristö ja prosessit, jotta eri osa-alueille voidaan määrittää hyväksyttävä riskitaso, dokumentointi ja mahdollisesti tarvittavat kehitystoimenpiteet.

Automaatio & IoT

- Bosch julkaisi tiedotteen IP-kameroista löydetyistä haavoittuvuuksista (BOSCH-SA-478243-BT). Tuotteisiin on päivitys saatavilla.
  - Hyökkääjä voi muuttaa kameran asetuksia ja saada haltuunsa arkaluontoista tietoa.

- Terveydenhuoltoalalle kohdistuvien hyökkäysten määrä on merkittävässä kasvussa.
  - Covid-19 epidemia lisää hyökkääjien kiinnostusta
  - Paljon laitekantaa, joiden käyttöön ei ole enää tietoturvapäivityksiä tarjolla
  - Lisää: https://threatpost.com/healthcare-prey-ransomware-cyberattacks/167525/

ANALYYSI

- Myös IoT laitteiden osalta muistettava perusasiat: päivittäminen, salasanat ja varmistaminen, etteivät laitteet ole avoinna internetiin.

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

- Kesäkuussa 14 merkittävää toimivuushäiriötä yleisissä viestintäpalveluissa.
  - Myrskyt ja huoltokatkot nostivat toimivuushäiriöiden määrää edellisiin kuukausiin (huhtikuussa 2 kpl ja toukokuussa 3 kpl) verrattuna.
  - Kesäkuun alkupuolella operaattorilla oli valtakunnallinen häiriö muutamien tuntien ajan, joka vaikutti muiden operaattoreiden liittymistä tuleviin puheluihin.
  - Muutostyöt aiheuttivat kesäkuussa kuusi toimivuushäiriötä, joten muutostöiden suunnittelu ja testaus korostuvat häiriöiden välttämiseksi.

ANALYYSI

- Yleisten viestintäpalveluiden toimivuus Suomessa on ollut alkuvuoden 2021 aikana hyvä. Merkittäviä toimivuushäiriöitä on ollut 37 kappaletta. Kesäkuun 14 merkittävää toimivuushäiriötä nostavat hieman ennustettavaa kokonaislukemaa vuoden 2021 saldoksi.
- Historiallisesti alkuvuosi on keskimäärin rauhallisempi ja kesän alkaessa myrskyt saattavat aiheuttaa nousua toimivuushäiriömäärissä.

ICT-palveluiden toimivuus

- Fastly-palveluntarjoajalla tunnin katko palveluissa 8.6.
- Katko johtui ohjelmistovirheestä, joka havaittiin vasta asiakkaan tekemästä käyttäjäasetusmuutoksesta.
- Vaikutuksia useisiin palveluihin, kuten Reddit, Amazon verkkokauppa, BBC, CNN ja The New York Times.

ANALYYSI

- Suurissa pilvipalveluissa on viime aikoina ollut kuukausittain maailmanlaajuisesti vaikuttaneita häiriöitä. Niiden toistumiseen kannattaa varautua esimerkiksi häiriötilanteiden toimintatapoja suunnittelemalla ja harjoittelemalla.
- On syytä muistaa, että vaikka asioihin on varauduttu hyvin - voi esimerkiksi inhimillinen virhe suurella toimijalla aiheuttaa maailmanlaajuisen palvelukatkon.

Palvelunestohyökkäykset

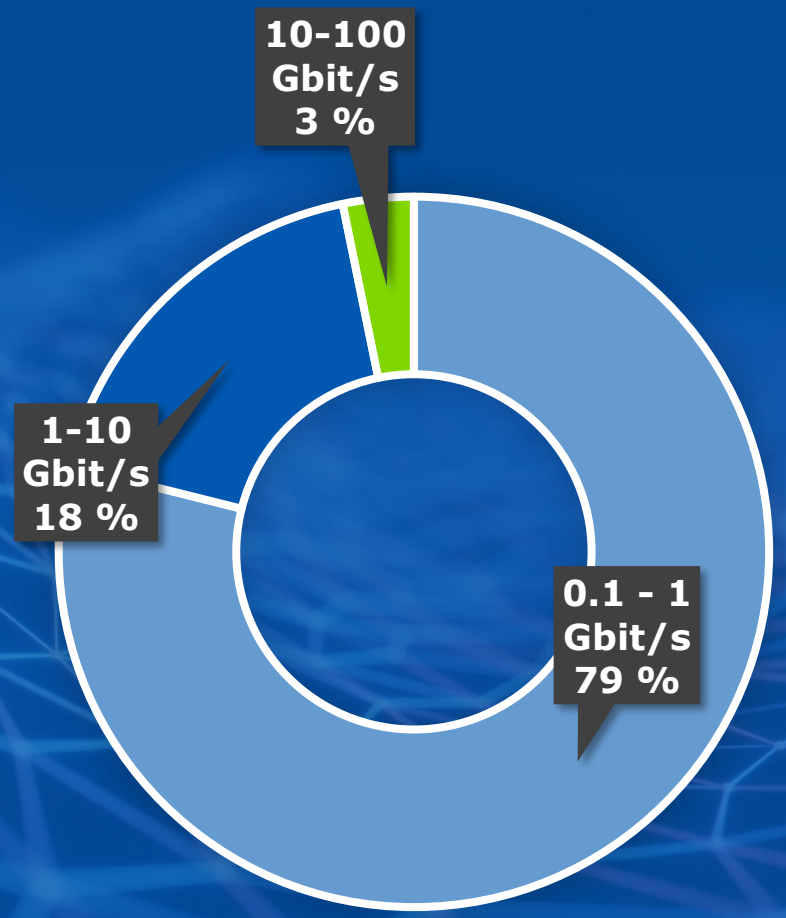
- Kesäkuussa saimme vain muutamia ilmoituksia palvelunestohyökkäyksiin liittyen
- Saimme taas tietoomme kiristysviesteistä palvelunestohyökkäyksiin liittyen.
  - Toistaiseksi uhattuja suurempia hyökkäyksiä ei ole nähty, mutta kiristysviestin lähettämisen lisäksi kiristäjä on voinut tehostaa viestiä uhattua pienemmällä palvelunestohyökkäyksellä.
  - Mainittu pienempi hyökkäys voi hyvinkin tarkoittaa kymmenien gigatavujen kokoista hyökkäystä.

ANALYYSI

- Organisaatioiden tulee tietää mitkä palvelut ovat heille tärkeitä, ja mitkä tulisi suunnitella toimimaan myös mahdollisen palvelunestohyökkäyksen aikana.
- Noin 25% hyökkäyksistä (Q2/2021) Suomessa oli kooltaan yli 1Gbit/s. Viime kuussa meille ilmoitettujen hyökkäysten perusteella skaala ulottuu siis jopa 260Gbit/s tasolle asti.

Palvelunestohyökkäysten tunnuslukuja

- 260 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q2/2021.
- Noin 72% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



SUOMEEN KOHDISTUNEIDEN PALVELUNESTOHYÖKKÄYSTEN VOLYYMIT (Q2/2021 - 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

- Yhdysvaltalais- ja brittiviranomaisten mukaan Venäjän sotilastiedustelu on pyrkinyt saamaan haltuunsa kirjautumistunnuksia sarjalla bruteforce-kampanjoita.
  - Tiedustelu- ja kyberturvallisuusviranomaisten mukaan toimija tunnetaan myös nimillä APT28 ja Fancy Bear.
  - Laajamittainen kampanja on kohdistunut tiedoksiannon mukaan sekä valtionhallinnon että yksityisen sektorin toimijoiden pilvi-infrastruktuuriin ja -palveluihin eri puolilla maailmaa.
  - Ensimmäiset havainnot kampanjasta on tehty vuoden 2019 puolivälin tienoilla, ja havaintoja on tehty edelleen vuoden 2021 alkupuolella.

ANALYYSI

- Haltuun saatuja kirjautumistunnuksia voidaan hyödyntää eri tavoin muun muassa erilaisiin tietoihin käsiksi pääsemiseksi, jalansijan saamiseksi organisaatioon tai lateraalisen leviämisen mahdollistamiseksi. Niitä on tiedotteen mukaan käytetty myös yhdessä tunnettujen haavoittuvuuksien kanssa haitallisen koodin suorittamiseksi kohdejärjestelmissä.

Vakoilu

- SolarWinds-haavoittuvuuskokonaisuudesta on paljastunut uusia tietoja.
- Tanskalaisjulkaisun haltuunsa saamien dokumenttien mukaan SolarWinds-uhrien joukossa oli muun muassa Tanskan keskuspankki.
  - Murto ei kuitenkaan keskuspankin tutkimusten mukaan olisi edennyt ensimmäistä vaihetta pidemmälle. Ensimmäisen vaiheen tietomurto kohdistui maailmalla tuhansiin organisaatioihin. Järjestelmät ehtivät olla avoimina hyökkääjälle kuukausien ajan ennen kuin se huomattiin.
- Microsoft puolestaan kertoi hyökkääjän toteuttaneen uusia hyökkäyksiä, joiden seurauksena tietomurron uhreiksi on joutunut ainakin kolme uutta tahoa.

ANALYYSI

- Maailmanlaajuisessa kybervakoilukampanjassa hyökkääjä onnistui ujuttamaan SolarWindsin hallintatyökaluun omaa haitallista koodiaan. Yhdysvallat on syyttänyt SolarWinds-murroista Venäjän ulkomaantiedustelupalvelua (SVR), jonka kybervakoilutoiminta tunnetaan myös nimillä APT29, Cozy Bear ja The Dukes.
- Kesäkuussa kerrottiin myös saman ryhmittymän murtautuneen vuonna 2017 Alankomaiden poliisin järjestelmiin. Murron motiivina uskotaan olleen Ukrainassa vuonna 2014 alas ammutun matkustajakoneen tapauksen tutkinta. Kone oli matkalla Amsterdamista Kuala Lumpuriin.

Vakoilu

- Kesäkuun kybervakoilu-uutisointi painottui kesäkuussa pitkälti Aasiaan.
  - Pohjoiskorealaisten hakkereiden kerrotaan murtautuneen eteläkorealaisen sukellusvenevalmistajan järjestelmiin varastaakseen tietoja muun muassa ydinkäyttöisestä sukellusveneestä.
  - Pakistaniin liitettyjen hakkereiden arvioidaan pyrkineen tunkeutumaan muun muassa intialaisten sähkönsiirtotoimijoiden järjestelmiin.
  - Check Pointin tutkijat kertoivat Afganistaniin kohdistuvasta kybervakoilukampanjasta, jonka toteuttajana arvioidaan olevan kiinankielinen ryhmittymä. Saman operaation aiempia kohteita ovat tiettävästi olleet myös Kirgisia ja Uzbekistan.
  - Lisäksi mongolialaisen varmenteiden myöntäjän verkkosivujen kautta jaettiin takaoven sisältävää sovellusta. Asian havainnut tietoturvatalo Avast ei kertomansa mukaan ole pystynyt tunnistamaan hyökkäyksen taustalla ollutta tahoa.

ANALYYSI

- Maantiede heijastuu edelleen voimakkaasti kybervakoiluun, vaikka internet onkin tuonut myös eri puolilla maailmaa olevat uhrit helpommin saavutettaviksi hyökkääjille.

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

- Traficomin määräys viestintäverkkojen ja -palvelujen varmistamisesta sekä viestintäverkkojen synkronoinnista uudistettiin ja se tuli voimaan 1.7.2021
- Keskeisimmät muutokset:
  - Matkaviestinverkon tukiasemien varateholähteiden varmistusaikavaatimuksia muutettiin.
  - Laitetilojen kulunvalvonnan ja lukitusten vaatimuksia tiukennettiin.
  - Tärkeysluokan 2 laitetilojen rakennevaatimuksia kevennettiin.
  - Lisäksi yksityiset radiotoiminnan harjoittajat rajattiin pois määräyksen soveltamisalasta.

ANALYYSI

- Uudistusten myötä matkaviestinverkkojen uusien verkkotekniikoiden toimintavarmuus paranee sähkönsyötön häiriötilanteissa.
- Lisäksi viestintäverkon toimintavarmuus ja fyysinen suojaaminen paranee päivitettyjen lukitus- ja kulunvalvontavaatimusten myötä

Oikeudelliset asiat

- Liikenne- ja viestintävirasto Traficomin Sijaintitietopalvelun valmistelu etenee - verkkotietietojen toimittamisen rajapintakuvaukset julkaistu
  - Sijaintitietopalvelu tarjoaa sähköisessä muodossa tiedot verkkojen fyysisestä infrastruktuurista sekä ja kaapeleiden, putkien ja niihin verrattavien aktiivisten verkon osien sijainneista.
  - Lisätietoa ja linkki rajapintakuvauksiin: https://www.traficom.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-traficomin-sijaintitietopalvelun-valmistelu-etenee

TAUSTAA

- Yhteisrakentamislain mukaan Liikenne- ja viestintävirasto Traficomin tehtävänä on huolehtia siitä, että verkkoinfrastruktuurin rakentajien on mahdollista saada tarvitsemansa tiedot helposti ja tietoturvallisesti keskitetystä tietopisteestä. Tätä varten on päätetty kehittää Sijaintitietopalvelu.
- Palvelun käyttö alkaa 1.10.2022, jolloin verkkojen sijaintitiedot tulee olla viimeistään toimitettuna palveluun digitaalisessa muodossa.

Oikeudelliset asiat

Komissio antoi 3.6.2021 ehdotuksen nk. eIDAS-asetuksen (EU) 910/2014 muuttamisesta.

- Ehdotetaan EU-tasoista sähköistä mobiililompakkoa luonnollisille ja oikeushenkilöille. EUid:llä voisi tunnistautua julkisiin ja yksityisiin palveluihin myös rajat ylittävästi ja tehdä yhteentoimivia sähköisiä allekirjoituksia.
- Ehdotetaan myös joitakin uusia luottamuspalveluja, esim. sähköisten henkilötietojen välitystä (nk. attribuuttipalvelu)
- Asetusehdotuksen valmistelutyöstä vastaa valtiovarainministeriö
- Lainsäädäntötyön rinnalla käynnistyy syksyllä 2021 komission johdolla jäsenvaltioiden asiantuntijoiden Toolbox-työ, jossa valmistellaan EUid:n teknistä arkkitehtuuria ja toimintamallia.
  - Ks. C(2021) 3968 final COMMISSION RECOMMENDATION of 3.6.2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework.
- Traficom osallistuu valmisteluun sekä kansallisessa että kansainvälisessä yhteistyössä.

- Komission ehdotus COM(2021) 281: https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation

Valtiovarainministeriö on asettanut 23.6.2021 kansallisessa digitaalisen identiteetin hankkeessa lainsäädäntöryhmän ja vaikutusarviointiryhmän valmistelemaan digitaalista henkilöllisyyttä koskevia lainsäädäntömuutoksia

- Työssä huomioidaan eIDAS-asetuksen muutokset.
- https://vm.fi/-/digitaalista-henkilollisyystodistusta-koskevien-lainsaadantomuutosten-valmistelu-aloitetaan

Arjen kyberturvallisuus

Android haittaohjelman levitystä tekstiviestitse

- Julkaisimme kesäkuussa varoituksen, koska FluBot-nimistä Android-haittaohjelmaa levitettiin erittäin aktiivisesti tekstiviestien avulla kesäkuun alkupuolella. Varoituksen julkaisun jälkeen saimme haittaohjelman levityksestä enimmillään noin 900 ilmoitusta päivässä. Nyt ilmoitusmäärät uusista levitysyrityksistä ovat laskeneet merkittävästi.

- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/poistimme-android-haittaohjelmia-koskevan-varoituksen

CERT-FI 20 vuotta: Kansainvälinen yhteistyö antoi innon ja hyvät eväät tietoturvauralle

- Kansainvälisyys on lähes sisäänrakennettu CERT-työn ominaisuus. Ilman kansainvälisiä verkostoja esimerkiksi tieto huijauskampanjoista ei liiku ajoissa sinne, missä sitä tarvittaisiin. Kun havaintoja ja oppeja voidaan luottamuksellisesti jakaa, siitä hyötyvät kaikki

- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/cert-fi-20-vuotta-kansainvalinen-yhteistyo-antoi-innon-ja-hyvat-evaat

Poliisi varoittaa valesivuista – suomalaiset menettäneet miljoonia euroja pankkien nimissä tehdyissä petoksissa

- Poliisi varoittaa rikosilmiöstä, jossa rikolliset kalastelevat verkkopankkitunnuksia pankkien verkkosivuja muistuttavien valesivustojen avulla.

- Jos epäilee, että rikolliset ovat saaneet haltuunsa verkkopankkitunnuksen, niin pitää ottaa välittömästi yhteys omaan pankkiin.

- https://www.ts.fi/uutiset/paikalliset/5351657/Poliisi+varoittaa+valesivuista++suomalaiset+menettaneet+miljoonia+euroja+pankkien+nimissa+tehtyissa+petoksissa

Kuluttajat: 5G on nopea, hyvä ja tulevaisuuteen liittyvä – monelle silti tuntematon

- Traficom seuraa viestintäverkkojen ja -palvelujen kehitystä Suomessa ja julkaisee niistä tietoja käyttäjien saataville viestintämarkkinoiden seuraamiseksi ja ennakoimiseksi.

- https://www.traficom.fi/fi/ajankohtaista/kuluttajat-5g-nopea-hyva-ja-tulevaisuuteen-liittyva-monelle-silti-tuntematon

Uutisia Kyberturvallisuuskeskuksesta

Evästekäytäntöihin selvyyttä - valmisteilla oleviin ohjeistuksiin pyydetään kommentteja

- Sähköisten palvelujen tarjoajien tulee lain mukaan pyytää käyttäjältä suostumus palvelussa käytettävien muiden kuin välttämättömien evästeiden käyttöön.
- Liikenne- ja viestintävirasto Traficom on valmistellut ohjeistuksia evästeiden ja niiden kaltaisten tekniikoiden käyttämisestä lainsäädännön edellyttämällä tavalla.
- Ohjeistusluonnokset ovat nyt julkisesti kommentoitavana ennen niiden viimeistelyä ja julkaisua: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=5450870c-1703-49e6-b48c-f89bb6ca3319

130 valkohattuhakkeria 30 maasta testasi 5G-teknologian kyberturvallisuutta

- Hackathonin haastekumppaneita olivat Cisco, Ericsson, Nokia sekä PwC Finland ja Aalto-yliopisto.
- Suomessa yhteistyö julkisen sektorin, yritysten, tutkimuslaitosten, korkeakoulujen ja muiden organisaatioiden välillä on tiivistä ja ketterää. Tämä toimintatapa on ainutlaatuinen ja mahdollistaa kyberturvallisuuden tehokkaan kehittämisen. Hackathonissa testattiin yhteistyössä 5G-pohjaisia palveluja, joita tullaan käyttämään lähitulevaisuudessa.
- https://www.traficom.fi/fi/ajankohtaista/130-valkohattuhakkeria-30-maasta-testasi-5g-teknologian-kyberturvallisuutta-viime

Suunnittelulla on merkittävä rooli onnistuneessa kyberharjoituksessa

- Huoltovarmuuskeskuksen Elintarvikehuoltosektorin poolisihteerit Markus Lassheikki, Jyri Valmu ja Lauri Kulonen toimivat tarkkailijoina Kyberturvallisuuskeskuksen Elintarvike-tiedonvaihtoryhmän kyberharjoituksessa. Laajaa huoltovarmuussektorin osaamistaan hyödyntämällä he tarkastelevat kyberharjoittelun etuja niin tiedonvaihtoryhmille kuin laajemmalle joukolle organisaatioita.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suunnittelulla-merkittava-rooli-onnistuneessa-kyberharjoituksessa

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