TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Heinäkuu 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 heinäkuu 2021

Tietomurrot ja -vuodot

- Useita ilmoituksia murretuista .fi-verkkosivustoista
- Sosiaalisen median tilien kanssa tulee olla tarkkana, rikolliset käyttävät myös niitä ahkerasti hyväkseen

Huijaukset ja kalastelut

- Pankkihuijausten aalto on jatkunut vilkkaana.
- Pankkitunnuksia ja maksutietoja kalastellaan aktiivisesti kaikkien pankkien nimissä sekä sähköpostitse että tekstiviesteillä.

Haittaohjelmat ja haavoittuvuudet

- FluBot-haittaohjelmaepidemia on laantumassa, haittaohjelmamäärät aaltoilevat kuukaudesta toiseen
- Heinäkuussa tuli ilmi useita kriittisiä haavoittuvuuksia, jotka tulisi päivittää mahdollisimman nopeasti

Automaatio

- IoT-tuotteiden kehittäjien keskeisin huolenaihe on tietoturva
- ISOn ensimmäinen IoT:n tietoturvaa ja tietosuojaa käsittelevä standardi on kansainvälisellä lausuntokierroksella ja siihen voi tutustua ja kommentoida maksutta

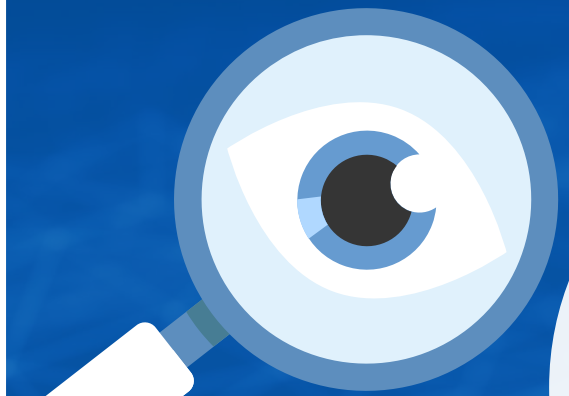
Verkkojen toimivuus

- Erilaiset muutostyöt ja konfigurointivirheet tuottivat häiriötilanteita
- Myös VoLTE-palveluissa oli erilaisia häiriöitä
- Palvelunestohyökkäysten vähäinen ilmoitusmäärä piti kuitenkin sisällään arvokkaita esimerkkejä muille organisaatioille.

Vakoilu

- Länsimaat syyttävät Kiinaa laajamittaisesta kybervakoilusta
- Israelilaisen NSO Groupin valvontaohjelmistoa on käytetty toimittajien ja aktivistien vakoilemiseen
- APT29/NOBELIUM vakoilee aktiivisesti valtionhallintoja

Kuukauden tunnuslukuja



1

AKTIVOIMME FLUBOT VAROITUKSEMME UUDELLEEN, KOSKA TEKSTIVIESTITSE LEVITETTÄVÄT ANDROID-HAITTAOHJELMAT VAIVAAVAT SUOMALAISIA EDELLEEN.

1

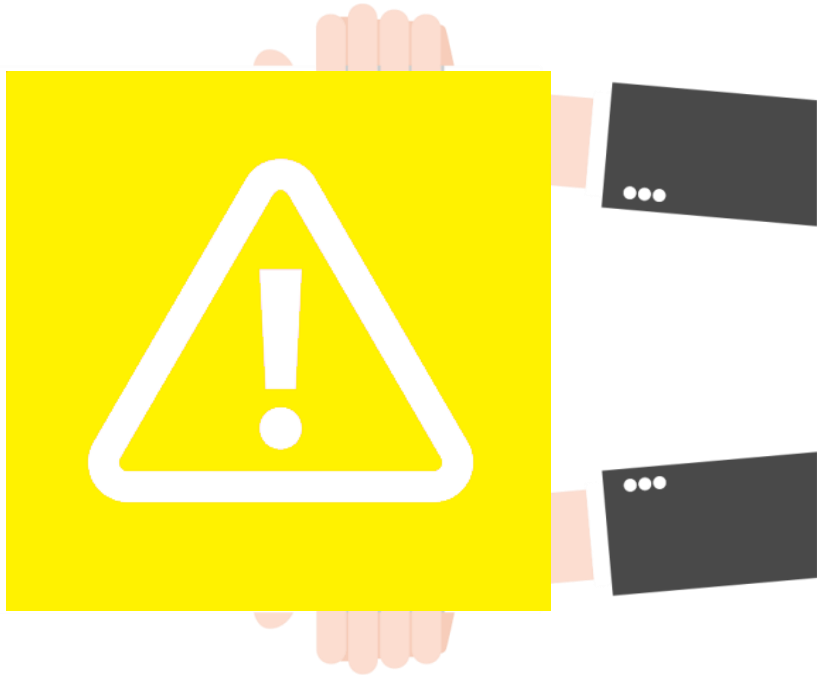
EU, ISO-BRITANNIA, YHDYSVALLAT JA NATO SYYTTÄVÄT JULKAISTUSSA JULKILAUSUMASSA KIINAN VALTIOTA USEIDEN KYBERHYÖKKÄYKSIÄ TEKEVIEN RYHMIEN TUKEMISESTA

1

ISON ENSIMMÄINEN IOT:N TIETOTURVAA JA TIETOSUOJAA KÄSITTELEVÄ STANDARDILUONNOS ISO/IEC DIS 27400 CYBERSECURITY — IOT SECURITY AND PRIVACY — GUIDELINES ON NYT KANSAINVÄLISELLÄ LAUSUNTOKIERROKSELLA

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. **Heinäkuussa varoitus aktivoitiin uudelleen, sillä tapausmäärät ovat jälleen ollut nousussa.**
- 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).
- FluBot-ilmoituksia tulee aaltomaisesti, välillä haittaohjelmaa jaetaan aktiivisesti ja välillä tilanne rauhoittuu.
- 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

- Useita ilmoituksia murretuista .fi-verkkosivustoista
  - Kyberturvallisuuskeskus on saanut ryppään ilmoituksia useista murretuista suomalaisista verkkosivustoista
  - Tietomurroissa käytettiin mahdollisesti yhden palveluntarjoajan jaetulla palvelimella ajetussa verkkosivujen julkaisujärjestelmässä olevia korjaamattomia haavoittuvuuksia
  - Murrettuja sivustoja on käytetty myös tietojen kalasteluun

ANALYYSI

- Verkkosivujen tietomurron mahdollistava haavoittuvuus jaetulla palvelimella voi altistaa kaikki samassa ympäristössä olevat käyttäjät ja asiakkaat.
- Palveluntarjoajien on hyvä seurata haavoittuvuusilmoituksia ja pitää jaetuilla palvelimilla sijaitsevat järjestelmät päivitettyinä. Tämä koskee etenkin järjestelmiä, joita asiakkaat eivät voi itse päivittää.
- Palveluntarjoajien ja asiakkaiden on hyvä sopia ja olla selvillä mitä kaikkea sopimuksiin kuuluu ja kuka on vastuussa järjestelmien päivityksistä.

Tietomurrot ja -vuodot

- Ilmoituksia Instagram- ja Facebook-tilien tietomurroista
  - Tilin palautus ei aina etene aina sujuvasti ja siihen voi kulua huomattavan kauan aikaa
  - Organisaatioiden tulisi tietää ketkä ovat nimettyjä tilin ylläpitäjiä ja ovatko he paikalla esimerkiksi lomakaudella
  - Ilmoitukset koskevat myös organisaatioiden tilejä, joten on syytä tarkastaa niiden salasanat ja tunnistautumistavat ajan tasalle - monivaiheisen tunnistautumisen on syytä olla käytössä
  - Tileillä olevien tietojen menettämisestä voi aiheutua merkittävää haittaa, kiusallisia tilanteita tai kuluja

ANALYYSI

- Tunkeutumisen tapahduttua, yritä ottaa tili takaisin haltuun kyseisen palvelun automaattityökalujen kautta
- Monessa palvelussa on automaattisia varoitustoimintoja käytössä salasanojen vaihdoista ja uusista kirjautumisista
- Ota yhteyttä palvelun ylläpitoon tilin palauttamisprosessin aloittamiseksi, jos automaattityökalut eivät toimi
- Tee asiasta myös rikosilmoitus, jotta tekijä saadaan teoistaan vastuuseen

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.

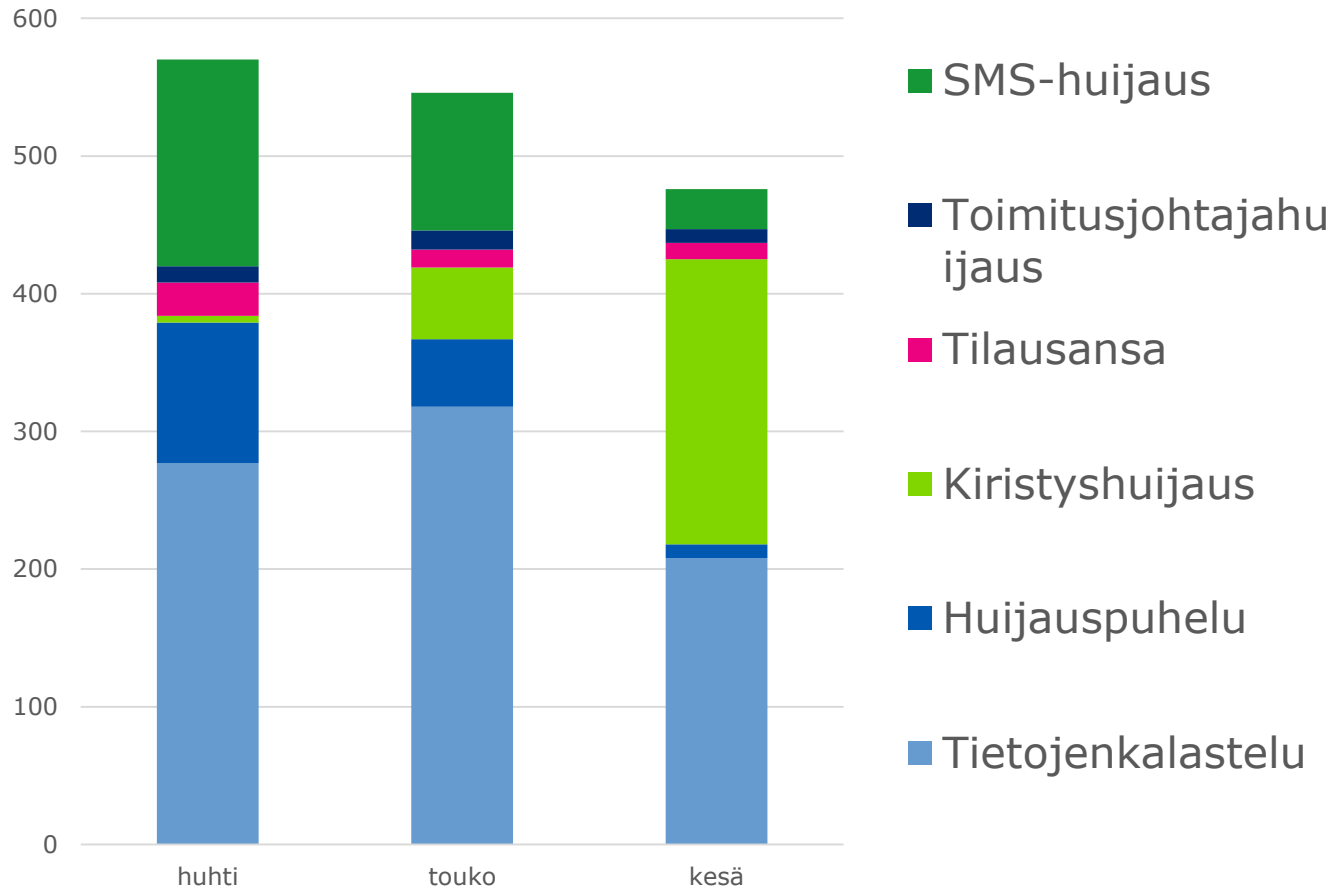
Huijaukset ja kalastelut

- Tunnusten ja maksutietojen kalastelua
  - Pankkitunnuksia kalasteltiin kaikkien Suomessa toimivien liikepankkien nimissä.
  - Erityisesti OP:n nimissä kalastelukampanjaa levitettiin tekstiviesteinä.
  - Pankkitunnusten lisäksi kalasteltiin paljon myös Netflixin ja Amazonin käyttäjätunnuksia.
  - Myös AppleID-tunnusten kalastelu on taas nostanut päätään. Apple Pay ja Google Pay -palveluiden käyttäjiä koetettiin huijata tekaistuilla aktivointiviesteillä.
  - Toimitusjohtajahuijauksia on loppukesästä raportoitu vähemmän kuin alkukesällä.

ANALYYSI

- Kesäkuinen ärhäkkä suomenkielisten kiristyshuijausten kampanja jatkui heinäkuussa kevyempänä englanninkielisten huijausviestien aaltona
- Murrettuja Office 365 -tilejä käytettiin kalasteluviestien levitykseen.

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

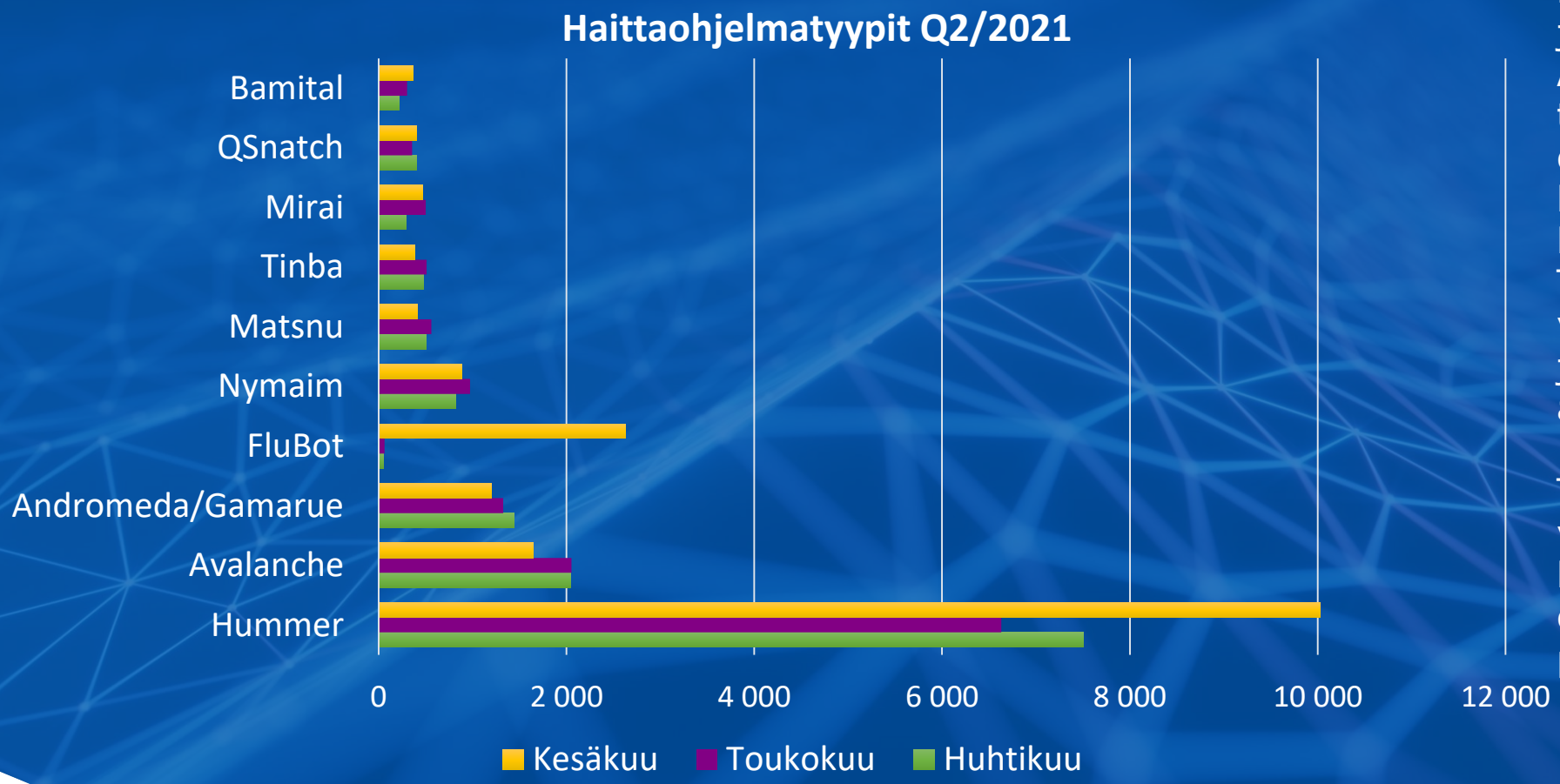
- FluBot-haittaohjelmaepidemia on laantumassa
  - Ilmoitusmäärät Android-haittaohjelmaa (FluBot) levittävistä tekstiviesteistä ovat vähentyneet merkittävästi
  - Vaikka liikkeellä on nyt enemmän vastaaja-teemaisia viestejä, voi pakettiteemaa hyödyntäviä viestejä näkyä edelleen
  - Havaintoja haittaohjelmasta tulee Kyberturvallisuuskeskukselle edelleen ja haittaohjelmia levittävien viestin kanssa tuleekin yhä olla tarkkana

ANALYYSI

- Olemme tehneet yhteistyötä operaattoreiden kanssa ja operaattorit ovat mm. välittäneet liittymien omistajille viestejä saastuneesta puhelimesta
- Haittaohjelma on kohdistettu kaikille, joilla on käytössään Android-laite ja matkapuhelinliittymä
- Tekstiviestit saapuvat myös muihin laitteisiin, mutta .apk-asennuspaketti ei toimi esimerkiksi iPhonella

Autoreporterin haittaohjelmahavainnot

3kk



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

Haavoittuvuus

- Heinäkuussa Microsoft korjasi Print Spooler - palvelusta löytyneitä haavoittuvuuksia
  - Microsoft julkaisi haavoittuvuuden CVE-2021-34481, joka mahdollistaa käyttövaltuuksien korottamisen paikallisesti haavoittuvuuden avulla
  - Haavoittuvuuteen ei ole toistaiseksi korjausta, vaan suosituksena on asentaa edelliset päivitykset ja poistaa Print Spooler käytöstä
  - Aiemmin julkaistu haavoittuvuustiedote: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_19/2021

ANALYYSI

- Haavoittuvuus koskettaa organisaatioita ja heidän IT-ylläpitäjiään. Yksityishenkilöiltä ei vaadita toimenpiteitä tämän haavoittuvuuden suhteen.

Haavoittuvuus

- Uusi NTLM PetitPotam-hyökkäys mahdollistaa Windows toimialueen ohjauskoneen (domain controller) haltuun ottamisen
  - Kyseessä ei ole varsinainen haavoittuvuus, vaan olemassa olevan ominaisuuden toiminallisuuden hyväksikäyttö
  - Microsoftin tiedote asiasta: https://msrc.microsoft.com/update-guide/vulnerability/ADV210003

- Applelta korjaus kriittiseen iOS- ja iPadOS-haavoittuvuuteen
  - Haavoittuvuutta on Applen mukaan saatettu jo aktiivisesti hyödyntää ja päivitykset tulisi suorittaa viipymättä.

ANALYYSI

- Kyberturvallisuuskeskuksen haavoittuvuustiedotteiden lisäksi kannattaa seurata myös haavoittuvuuksista lähetettävää uutiskoostetta. Vastaanottajaksi voi rekisteröityä kotisivujemme kautta.

Kuukauden haavoittuvuusjulkaisut

- Kriittinen haavoittuvuus SolarWinds Serv-U tuotteessa (20/2021)
- Microsoft korjasi kuukausittaisessa päivityksessään useita kriittisiä haavoittuvuuksia (21/2021)
- NicheStack TCP/IP-toteutuksesta löytyi useita haavoittuvuuksia (22/2021)

- 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 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 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 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

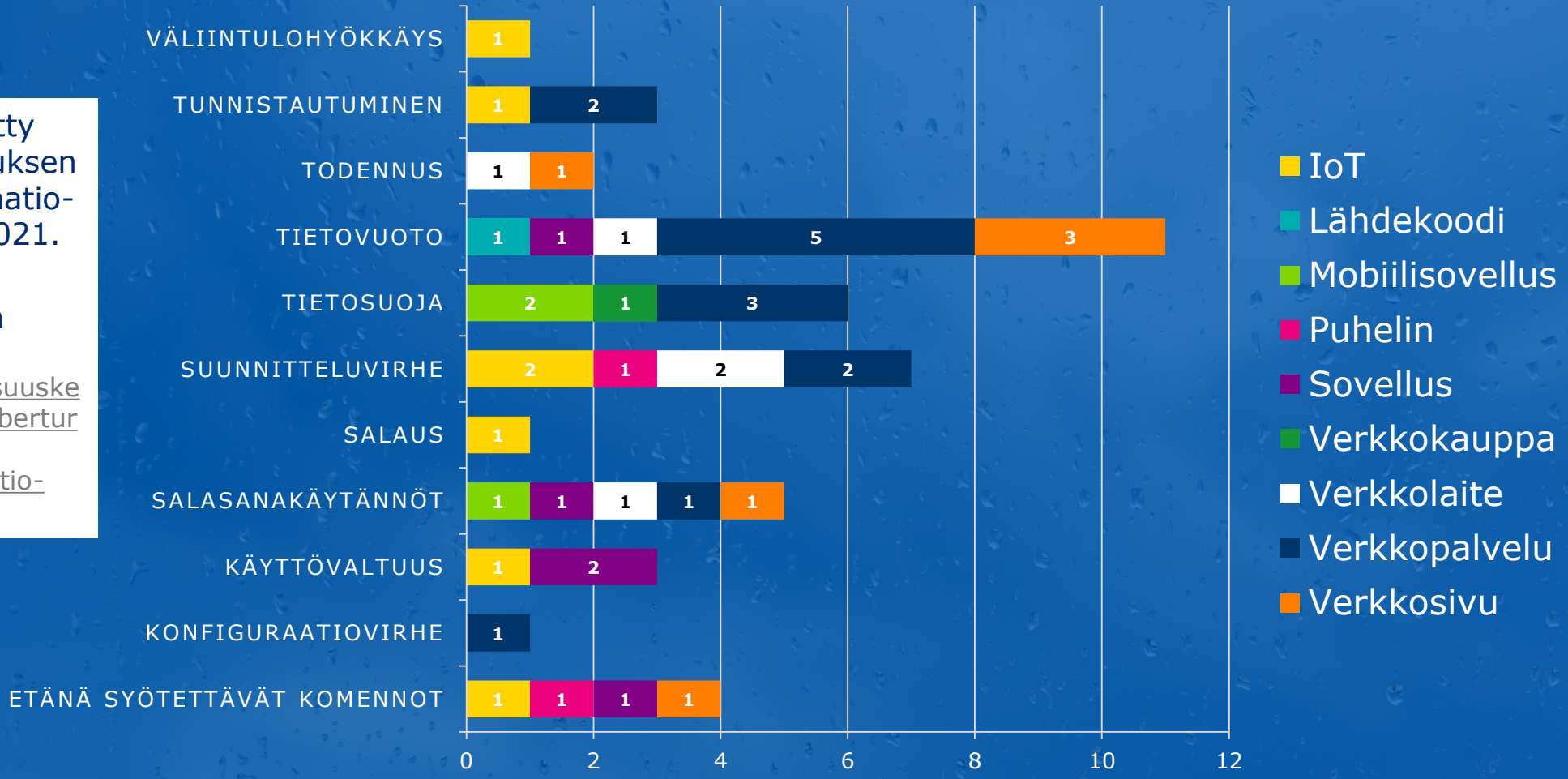
6kk

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.

IoT

- "Käyttäjän tunnistuksen ohittava haavoittuvuus muun muassa Buffalo-merkkisissä reitittimissä
  - https://medium.com/tenable-techblog/bypassing-authentication-on-arcadyan-routers-with-cve-2021-20090-and-rooting-some-buffalo-ea1dd30980c2
  - Tietoturvatutkija löysi haavoittuvuuden tutkimalla laitetta fyysisen kytkennän kautta. Kun haavoittuvuus on kerran löydetty, voidaan sitä hyödyntää jatkossa myös verkon yli.
  - Sama haavoittuvuus esiintyy useiden muidenkin valmistajien nimellä myytävissä kuluttajien käyttöön tarkoitetuissa verkkolaitteissa. Kuluttajaelektroniikassa laitteen myyjä ei välttämättä ole sen valmistaja ja että laiteohjelmistossa oleva haavoittuvuus voi koskea monia muitakin laitteita."

ANALYYSI

- Reitittimien häiriöt jäävät usein helposti huomaamatta, koska niissä ei ole antivirustuotteita eikä mikään varoita tunkeutumisesta. Lisäksi verkko voi hidastella monista harmittomistakin syistä
- Tehdasasetusten palauttaminen (resetointi) saattaa auttaa riippuen siitä, mikä ongelmat aiheuttaa ja miten palauttaminen on reitittimessä toteutettu
- Kuluttajamarkkinoille suunnatuista IoT-tuotteista löytyy toistuvasti vastaavia ohjelmistohaavoittuvuuksia. Tietoturvan parantaminen edellyttää asian tiedostamista ja paremman tietoturvatason aktiivista vaatimista

IoT

- ISOn ensimmäinen IoT:n tietoturvaa ja tietosuojaa käsittelevä standardiluonnos ISO/IEC DIS 27400 Cybersecurity — IoT security and privacy — Guidelines on nyt kansainvälisellä lausuntokierroksella
- Standardi
  - Sisältää ohjeistuksen IoT-ratkaisujen riskienhallintaan, periaatteisiin, tietoturvan hallintakeinoihin ja tietosuojaan.
  - Määrittää IoT-maailman keskeiset käsitteet, kuten IoT-laite, ekosysteemi, valmistaja ja palveluntarjoaja
  - On luettavissa ja sitä voi kommentoida maksutta Suomen Standardisoimisliitto SFS:n lausuntopalvelussa osoitteessa https://lausunto.sfs.fi/Home/Details/13898
  - On saatavissa myös liittymällä jäseneksi SFS:n standardisoimisryhmään SR 307 Tietoturvatekniikat. Standardiin tulleet kommentit käsitellään ja Suomen kanta muodostetaan ryhmän kokouksessa.
    - Osallistuminen on osallistujille maksutonta ja ryhmään voi ilmoittautua SFS:n verkkosivulla osoitteessa: https://sfs.fi/osallistu-ja-vaikuta/miten-voin-osallistua-standardisointiin/liity-sfsn-standardisointiryhmaan/
    - Lisätietoja antaa ryhmän vetäjä Elina Huttunen elina.huttunen@sfs.fi

IoT

- Tietoturva esineiden internetin kehittäjien yleisin huolenaihe
  - Elektroniikan ja teollisuusautomaatiotuotteiden jakeluyritys Newarkin tekemän kyselytutkimuksen mukaan esineiden internetin tuotteiden kehittäjien yleisin huolenaihe on edelleen tuotteiden tietoturva ja yksityisyydensuoja (security). Niin vastanneiden osuus on laskenut hieman vuodesta 2018, mistä voi päätellä alan tietoturvaratkaisuiden parantuneen ja yleistyneen.
  - Esineiden internetin soveltaminen teollisuuteen sai eniten mainintoja alan suuntaa seuraavien vuosien aikana määrittävänä sovelluskohteena. Toisena oli kotiautomaatio.
  - Kehittäjät kaipaavat alalle kattavampia ja parempia standardeja. Kolme eniten esineiden internetin hyötyjä lisäävää asiaa vastaajien mielestä olivat laitteiden yhteentoimivuutta parantavat standardit, avoimet standardit ja kehitystyön helpottaminen.
  - Lue lisää: https://www.newark.com/iot-trends-2021

ANALYYSI

- Esineiden internet on arkipäiväistynyt, mutta ala kehittyy edelleen voimakkaasti. Kansainvälisiä standardeja kehitetään erityisesti tietoturvan osalta.
- Kyselyyn vastanneet arvioivat koronapandemian lisäävän esineiden internetin soveltamista erityisesti terveydenhuoltoalalla. Melko harva kuitenkin näkee terveydenhuoltoalaa esineiden internetin kehittämistä määrittävänä alana. Tämä ero voi kertoa ehkä siitä, että koronaepidemian vaikutukset arvioidaan lyhytkestoisiksi alan kehityksen kannalta, tai siitä, että esineiden internetin kehittämismahdollisuuksia työvoimavaltaisella terveydenhuoltoalalla pidetään rajallisina.

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

- Heinäkuussa 8 merkittävää toimivuushäiriötä yleisissä viestintäpalveluissa
  - Heinäkuun häiriöt koostuivat luonnonilmiöiden sijaan normaaleista vikatilanteista, jotka vaativat erilaisia korjaus- tai konfigurointitöitä.
  - Erilaiset muutostyöt ja konfigurointivirheet aiheuttivat muutaman häiriön.
  - Myös erilaiset sähkönjakelukeskeytykset tai häiriöt voivat vaikuttaa palveluiden saatavuuteen riippuen siitä, kestääkö akusto katkon ja onko varavoimaa saatavilla.
  - VoLTE, eli Voice over LTE –palvelussa oli häiriöitä eri operaattoreilla.

ANALYYSI

- Yleisten viestintäpalveluiden toimivuus Suomessa on ollut alkuvuoden 2021 aikana hyvä. Merkittäviä toimivuushäiriöitä on ollut 45 kappaletta.
- Historiallisesti alkuvuosi on keskimäärin rauhallisempi ja kesän alkaessa myrskyt saattavat aiheuttaa nousua toimivuushäiriömäärissä.

ICT-palveluiden toimivuus

- Valtorilla oli merkittävä häiriö palveluissa kuitukatkon vuoksi 16.7.
  - Kaivuutöiden yhteydessä kauha katkaisi pää- ja varayhteydet.
  - Valtori kertoo, että varayhteys on nyt geohajautettu eli siirretty maantieteellisesti eri paikkaan kuin pääyhteys.
  - https://valtori.fi/-/telian-runkoverkkohairion-16.7.-korjaustoimet-varayhteys-siirretty-uudelle-reitille
- Akamailla oli ongelmia DNS-palveluissa 22.7.
  - https://www.bleepingcomputer.com/news/security/akamai-dns-global-outage-takes-down-major-websites-online-services/

ANALYYSI

- Suurissa pilvipalveluissa on viime aikoina ollut kuukausittain maailmanlaajuisesti vaikuttaneita häiriöitä. Niiden toistumiseen kannattaa varautua esimerkiksi häiriötilanteiden toimintatapoja suunnittelemalla ja harjoittelemalla.
- Traficom tarjoaa fi-verkkotunnusvälittäjille maksuttoman mahdollisuuden tarjota hajautettua toissijaista nimipalvelua fi-verkkotunnuksille ja niiden käyttäjille
- https://www.traficom.fi/fi/hajautettu-nimipalvelu-valittajien-kayttoon

Palvelunestohyökkäykset

- Heinäkuussa saimme vain kolme ilmoitusta palvelunestohyökkäyksiin liittyen.
- Näistä kaksi oli kokoluokaltaan suuria hyökkäyksiä, mutta organisaatioilla oli käytössään mitigointipalvelut niitä torjumaan.
  - Ilmoitetuista hyökkäyksistä suurin oli kokoluokaltaan 139 Gbps/s ja toiselta organisaatiolta suurin ilmoitettu lukema oli 105 Gbps/s
  - Vaikka organisaatio olisi hankkinut operaattorilta mitigointipalvelun, voi tämän kokoluokan hyökkäyksen alkuvaiheessa tapahtua vähintäänkin pieni katkos yhteyksissä.
- Yksi tietoomme tullut hyökkäys kesti 20 tuntia ja vaati operaattorin toimia, jotta hyökkäys saatiin torjuttua. Hyökkäys onnistui tukkimaan palomuurin ja täten vaikutti yrityksen toimintaan.

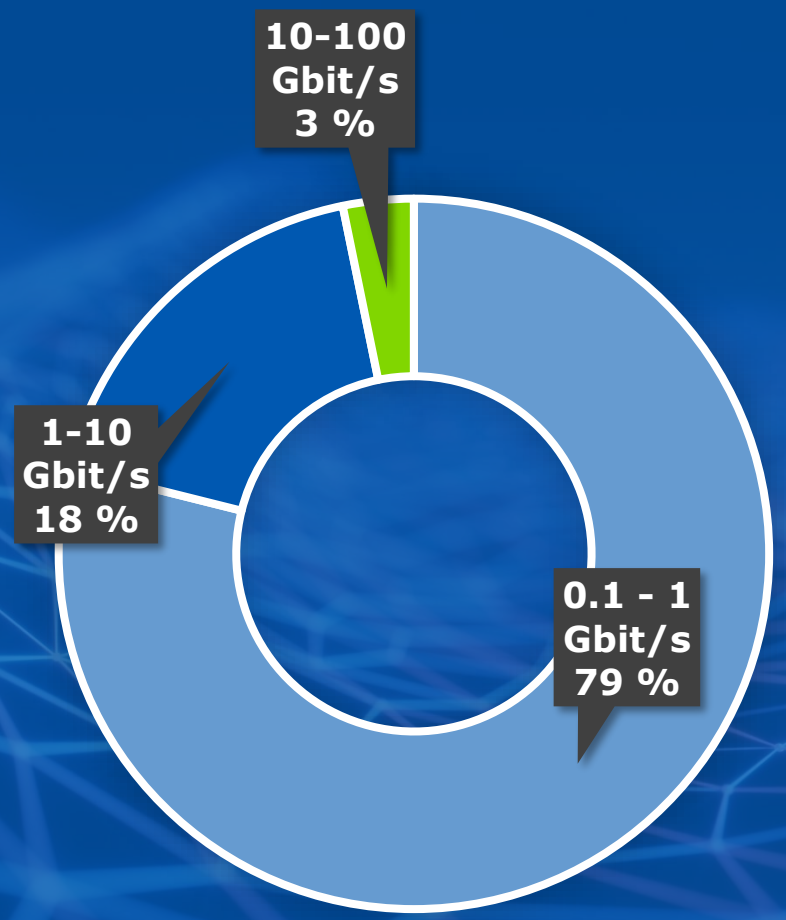
ANALYYSI

- 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 1 Gbit/s. Viime kuussa meille ilmoitettujen hyökkäysten perusteella skaala ulottuu siis jopa 260 Gbit/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.

3kk



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

- EU, Iso-Britannia, Yhdysvallat ja NATO syyttävät Kiinan valtiota useiden kyberhyökkäyksiä tekevien ryhmien tukemisesta
  - Ryhmä HAFNIUM on vastuussa maailmanlaajuisesta Microsoft Exchange –sähköpostipalvelimien murtokampanjasta
  - Ryhmä APT31 on murtautunut lukuisiin eurooppalaisiin organisaatioihin, mukaan lukien Suomen eduskunta
  - Ryhmä APT40 on murtautunut lukuisiin yrityksiin Euroopassa ja muualla
  - https://www.consilium.europa.eu/fi/press/press-releases/2021/07/19/declaration-by-the-high-representative-on-behalf-of-the-eu-urging-china-to-take-action-against-malicious-cyber-activities-undertaken-from-its-territory/

ANALYYSI

- Länsimaiden mukaan ryhmät ovat Kiinan turvallisuusministeriön MSS alihankkijoita ja toimivat suoraan Kiinan valtion ohjauksessa
- Jatkuvan kybervakoilun uskotaan liittyvän läheisesti Kiinalle tärkeään *Belt & Road Initiative* -hankkeeseen

Vakoilu

- Useat tiedotusvälineet ja Amnesty International julkaisivat selvityksen, jossa epäillään ainakin kuuden valtion hallituksen käyttäneen israelilaisyritys NSO Groupin toimittamaa Pegasus-ohjelmaa erityisesti toimittajien ja ihmisoikeusaktivistien vakoiluun.
  - Pegasus-ohjelma mahdollistaa pääsyn kaikkeen iPhone- ja Android-laitteiden dataan sekä äänen ja kuvan tallentamisen.
  - Ohjelman käyttämien nollapäivähaavoittuvuuksien ansiosta se voidaan asentaa täysin käyttäjän huomaamatta lähettämällä käyttäjän numeroon haitallinen viesti
  - Julkaisun lähteenä olevassa tietovuodossa oli yli 50 000 puhelinnumeroa jotka kuuluvat poliitikoille, yritysjohtajille, toimittajille, ihmisoikeusaktivisteille ja virkamiehille ympäri maailmaa. Puhelinnumeroiden käyttötarkoitus ei ole selvillä

ANALYYSI

- 37 tutkitusta laitteesta on löydetty merkkejä Pegasus-ohjelmasta
- Paljastus nostaa esiin ongelmat sekä viranomaisille myydyn valvontateknologian väärinkäytössä että löydettyjen ohjelmistohaavoittuvuuksien ilmoittamisessa
- Israelin hallinto on aloittanut tutkinnan NSO Groupin liiketoimista, koska ne ovat puolustusministeriön vientituotteiden valvonnan alaisia

Vakoilu

- APT29/NOBELIUM on tehnyt tänä vuonna jo useita kohdistettuja hyökkäyksiä erityisesti valtionhallintoja kohtaan
  - Toukokuussa APT29/NOBELIUM teki laajamittaisen Spearphishing-kampanjan käyttäen normaalien mainossähköpostin lähettämiseen tarkoitettuja alustoja, mukaan lukien Googlen Firebase
    - Googlen tietoturvatutkijat raportoivat heinäkuussa, että hyökkäyksissä oli käytetty myös Applen selainohjelmiston nollapäivähaavoittuvuutta
  - APT29/NOBELIUM väitetään myös tunkeutuneen kesällä 2021 Yhdysvaltain republikaanipuolueen alihankkijan järjestelmiin

ANALYYSI

- APT29/NOBELIUM on liitetty useissa lähteissä Venäjän tiedustelupalveluun.
- Saman tekijän uskotaan olleen joulukuussa 2020 tapahtuneen laajamittaisen Solarwinds-yhtiöön ja heidän asiakkaisiinsa kohdistuneen toimitusketjuhyökkäyksen takana.
- Viimeaikaiset tapaukset osoittavat, että APT29/NOBELIUM toimii aktiivisesti käyttäen useita eri menetelmiä tavoitteidensa saavuttamiseksi

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

- Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat antaneet yhteisen lausunnon komission tekoälyä koskevasta asetusehdotuksesta
  - Keskeisenä huolenaiheena epäoikeudenmukaisen syrjinnän riski henkilöiden tunnistamisessa ja luokittelussa
  - Tekoälyn käyttö kehotetaan kieltämään tilanteissa, joissa on kyse henkilöiden biometrisestä etätunnistuksesta julkisissa tiloissa sekä ihmisen ominaisuuksien automaattisesta tunnistamisesta. Ominaisuudet voivat olla sekä biometrisiä että käyttäytymiseen liittyviä signaaleja, kuten kasvot, kävelytapa, sormenjäljet, DNA, ääni ja näppäimistön käytön tunnistettavat kaavat.
  - Lisäksi suositellaan sellaisten tekoälyjärjestelmien kieltämistä, joissa biometriikkaa käytetään sosiaaliseen pisteyttämiseen tai henkilöiden luokittelemiseksi ryhmiin esimerkiksi etnisen alkuperän, sukupuolen tai poliittisen tai sukupuolisen suuntautumisen perusteella.
  - https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

Oikeudelliset asiat

- Hallituksen esitys laiksi yksityisyyden suojasta työelämässä annetun lain 4 §:n muuttamisesta
  - Lakia ehdotetaan muutettavaksi siten, että työntekijän suostumusta hänen henkilötietojensa keräämiselle muualta kuin häneltä itseltään ei tarvita silloin, kun työnantaja kerää työntekijän henkilötietoja työsuhteen aikana työnantajalle laissa säädettyjen oikeuksien tai velvollisuuksien toteuttamista varten.
  - Tavoitteena on sääntelyn selkeyttäminen suhteessa työnantajan lakisääteisten oikeuksien ja velvollisuuksien toteuttamiseen liittyvään henkilötietojen keräämiseen ja tietosuoja-asetukseen.
  - Työnantaja voisi ehdotetun säännöksen mukaan kerätä ilman suostumusta esimerkiksi työntekijän työn suorittamiseen ja suoriutumiseen sekä lainsäädännön ja työnantajan ohjeiden noudattamiseen liittyviä työntekijää koskevia henkilötietoja.
  - Hallituksen esitysluonnoksesta pyydetään lausuntoa viimeistään maanantaina 6.9.2021. Ehdotettu laki on tarkoitettu tulemaan voimaan mahdollisimman pian.
  - https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1ddf35b0-2d2a-459c-abca-d14fd6e8f2d6

Arjen kyberturvallisuus

Vieraskynä: Aikuisen tukea tarvitaan, jotta lapsi voi kulkea turvallisesti digiliikenteessä

- Kuinka lasta voi opastaa liikkumaan netissä turvallisesti? Aiheesta kirjoittaa kehityspsykologian asiantuntija Katariina Leivo Suojellaan lapsia ry:stä.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vieraskyna-aikuisen-tukea-tarvitaan-jotta-lapsi-voi-kulkea-turvallisesti

Uusi puhelin koulujen alun kunniaksi

- Tietoturvasta huolehtiminen on tärkeä kansalaistaito myös lapsille. Taitojen omaksuminen alkaa heti, kun lapsi saa älylaitteen käteensä, ja kehitys jatkuu läpi elämän.
- Tutustukaa ohjeisiin yhdessä: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tekemista-lapsille

Etenkin iäkkäät menettävät nyt rahojaan verkkorikollisille - menetykset yhteensä jo 2,1 miljoonaa

- Vuosi 2021 on ollut verkkorikollisten kulta-aikaa. Rikolliset ovat onnistuneet varastamaan suomalaisten verkkopankki- ja luottokorttitunnuksia ja siirtäneet suuria summia uhriensa pankkitileiltä. Rikoshyöty heinäkuussa jo yli 5 miljoonaa euroa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/etenkin-iakkaat-menettavat-nyt-rahojaan-verkkorikollisille-menetykset-yhteensa-jo-21

CERT-FI 20 vuotta: Oi, muistathan Heartbleedin ja NotPetyan!

- CERT-FI sulautui osaksi Kyberturvallisuuskeskusta 1.1.2014. Vuonna 2013 valmistauduttiin uuden organisaation perustamiseen ja uusia tietoturva-asiantuntijoita tarvittiin. Samana vuonna taloon astelivat herrat Kurittu ja Karinen.
- Tutustu tarinaan ja tekijöihin kyberturvallisuuden kulisseissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/cert-fi-20-vuotta-oi-muistathan-heartbleedin-ja-notpetyan

Uutisia Kyberturvallisuuskeskuksesta

Liikenne- ja viestintävirasto Traficomin Sijaintitietopalvelun valmistelu etenee - verkkotietietojen toimittamisen rajapintakuvaukset julkaistu

- Liikenne- ja viestintävirasto Traficomin Sijaintitietopalvelun käyttöönottovaihe alkaa 1.4.2022, jolloin verkkotoimijat voivat alkaa toimittaa palveluun verkkojensa sijaintitietoja. Sijaintitietojen toimittamiseksi on nyt julkaistu sähköisten rajapintojen tekniset kuvaukset. Palvelun käyttö alkaa 1.10.2022, jolloin verkkojen sijaintitiedot tulee olla viimeistään toimitettuna palveluun digitaalisessa muodossa.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/liikenne-ja-viestintavirasto-traficomin-sijaintitietopalvelun-valmistelu-etenee

CERT-FI 20 vuotta: Kun verkkomato Conficker maailmaa mullisti

- Vuonna 2008 maailmalla riehui Conficker-verkkomato. Suomeen se rantautui alkuvuodesta 2009 ja pamautti Autoreporter-ilmoitukset ennennäkemättömiin lukemiin. Conficker osasi levitä internetissä, yritysten sisäverkossa, tartuttaa USB-massalaitteita ja päivittää itseään. Uinuvan uhkan tapausta muistelee Thomas Grenman, Telia Cygaten tietoturvakonsultti, joka tuolloin seurasi verkkomadon liikkeitä CERT-FI:n tietoturvapäivystäjänä.
- Lue koko tarina: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/cert-fi-20-vuotta-kun-verkkomato-conficker-maailmaa-mullisti

Lausuntopyyntö: Radioamatöörimääräystä muutetaan väliaikaisesti

- Radioamatöörimääräyksen 6 K/2019M 6 §:ää muutetaan väliaikaisesti 100 päivän ajaksi siten, että 15.9.-23.12.2021 välisenä aikana radioamatööriaseman kutsumerkissä saa alussa käyttää kirjaintunnuksen OH sijaista kirjaintunnusta OF. Muutos perustuu siihen, että vuosi 2021 on Suomen Radioamatööriliitto ry:n 100-vuotisjuhlavuosi.
- HUOM! Lausuntoaika päättyi 4.8.2021
- Tutustu: https://www.traficom.fi/fi/ajankohtaista/lausuntopyynto-radioamatoorimaaraysta-muutetaan-valiaikaisesti

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