



TRAFFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Kesäkuu 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

Kybersää kesäkuu 2022

Tietomurrot ja -vuodot

- ▶ O365-tietomurtoja on tapahtunut myös kesäkuussa normaaliin tapaan.
- ▶ Kiinassa tehtiin tietomurto poliisin tietokantaan ja miljardin ihmisen tiedot päätyivät väärin käsiin.

Automaatio ja IoT

- ▶ Valveutunutkaan käyttäjä ei aina pysty suojaamaan äylaitteitaan, jos haavoittuvuus onkin valmistajan pilvipalvelussa.
- ▶ Automaatioympäristöistä löytyy koko ajan haavoittuvuuksia ja niitä myös hyödynnetään entistä enemmän kyberoperaatioissa.

Huijaukset ja kalastelut

- ▶ Verkkopankkitunnuksia kalastellaan liki kaikkien suomalaisten pankkien nimissä.
- ▶ Poliisihallituksen nimissä levitetään huijausviestejä.

Verkkojen toimivuus

- ▶ Verkoissa on havaittu kuusi merkittävää häiriötä, jotka eivät kuitenkaan aiheuttaneet suuria vaikutuksia.
- ▶ Palvelunestohyökkäysten osalta tilanne on Suomessa rauhallinen.

Haaitaohjelmat ja haavoittuvuudet

- ▶ Haavoittuvuus Microsoftin työkalussa mahdollistaa hyökkäykset haitallisten Microsoft Office -dokumenttien avulla.

Vakoilu

- ▶ Soft Cell -kampanja on laajentanut kohdistustaan teleoperaattoreiden lisäksi finanssisektoriin ja valtionhallintoihin.
- ▶ APT-toimijat hyödyntävät Follina-haavoittuvuutta.
- ▶ Koti- ja pienyritysreitittimet ovat edelleen APT-toimijoiden kohteena.

Kuukauden tunnuslukuja



Suurin Suomessa nähty palvelunestohyökkäys huhti-kesäkuun aikana oli liikennemäärältään 119 Gbit/s.



Suomalaiset menettivät nettihuijauksissa vuonna 2021 noin 47 miljoonaa euroa, kertoo Kuluttajaliiton Varo, varmista ja varoita -kampanja.



Hyvää kesää! Kyberturvallisuudesta huolehtiminen kuuluu myös lomakaudelle.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1 

Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen. Digitaalisuus läpileikkaa koko organisaation toimintaa ja muutokset kansainvälisessä turvallisuustilanteessa vaikuttavat merkittävästi organisaation jatkuvuuteen ja riskienhallintaan.

2 

Puutteellinen tiedonvaihto heikentää kyberturvallisuuden kokonaistilannekuvaa. Organisaation kohtaama kyberuhka saattaa kohdata toisia organisaatioita seuraavana päivänä.

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.

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.

Symbolit

Uusi



Päivitetty



1. Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen

Digitaalisuus läpileikkaa koko organisaation toimintaa ja muutokset kansainvälisessä turvallisuustilanteessa vaikuttavat merkittävästi organisaation jatkuvuuteen ja riskienhallintaan.

- ▶ Sota Ukrainassa vaikuttaa myös Suomessa. Esimerkiksi talouden äkilliset muutokset ja energian hinnannousu näkyvät vaikeasti ennakoitavina kehityskulkuina. Muutokset saattavat tapahtua nopeasti ja heijastua myös digitaalisen maailman toimivuuteen.
- ▶ Epävarmuustekijöillä voi olla isoja vaikutuksia organisaatioiden toimintaan. Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön aiheuttamat uhkat kriittisille prosesseille.
- ▶ Kansainvälinen tilanne vaikuttaa väistämättä myös digitaaliseen maailmaan ja kyberuhkilta varautumiseen. On tärkeää, että organisaatioiden johto ja asiantuntijat tarkastelevat kyberturvallisuuden suojauskäytäntöjään sekä ylläpitävät niitä aktiivisesti. Tutustu johdon ja asiantuntijoiden ohjeeseen.⁽¹⁾

CASE

Nato-jäsenhakemuksen seurauksena Suomeen voidaan kohdistaa erilaista kybervaikuttamista sekä informaatiovaikuttamista verkossa.

Vaikuttaminen voi näkyä esimerkiksi palvelunestohyökkäyksinä.

Palvelunestohyökkäyksillä saadaan näkyvyyttä, mutta niiden vaikutukset eivät useimmiten ole laajoja ja pitkävaikutteisia. Tällä hetkellä Suomen kyberturvallisuustilanne on vakaa ja verkot toimivat normaalisti.

2. Puutteellinen tiedonvaihto heikentää kyberturvallisuuden kokonaistilannekuvaa

Kyberturvallisuus on organisaatioiden rajat ylittävää. Organisaation kohtaama kyberuhka saattaa kohdata toisia organisaatioita seuraavana päivänä. Tiedonvaihto on tärkeää eri toimijoiden välillä kokonaistilannekuvan rakentamiseksi.

- ▶ Jokainen organisaatio on tärkeä pala kokonaisturvallisuuden ketjussa, joka rakennetaan yhteistyöllä eri toimijoiden välillä.
- ▶ Omien sidosryhmien tunteminen on keskeistä. Jos organisaatio on kyberhyökkäyksen kohteena on tärkeä ymmärtää, miten tilanne voi vaikuttaa sidosryhmiin tai toisinpäin. Yhteistyö verkostoissa onkin keskiössä.
- ▶ Tiedonvaihtoverkostojen tarkoitus on mahdollistaa tietoturva-asioiden luottamuksellinen käsittely osallistujien kesken sekä organisaatioiden tietoturvaosaamisen lisääminen ja kokonaistilannekuvan kehittäminen.
- ▶ Avoin ja ajankohtainen tiedonjako vähentää uhkien vaikutuksia ja kustannuksia. Toisilta oppiminen on myös kustannustehokasta, kun muiden ei tarvitse keksiä uudelleen toisaalla jo käytössä olevaa ratkaisua.
- ▶ Ilmoita Kyberturvallisuuskeskukselle, joka kokoaa kybertilannekuvaa Suomesta!

CASE

ISAC-tiedonvaihtoryhmät (ISAC=Information Sharing and Analysis Centre) ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä. ISAC-ryhmissä käsitellään luottamuksellisesti kyberturvallisuuteen liittyviä asioita, kuten uhkia, ilmiöitä ja hyviä käytäntöjä. Ryhmät kehittävät myös edustamansa toimialan ja yhteiskunnan kyberturvallisuutta esimerkiksi toteuttamalla toimialaansa liittyviä riskianalyyskejä, tutkimuksia ja ohjeistusta.⁽²⁾

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 tietoturvaluotteissa 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.⁽³⁾

OHJE

Jos käyttöoikeudet joutuvat väärin käsiin, tulee toimia nopeasti.

1. Lukitse tunnus välittömästi!
2. Sulje kirjautunut murtaaja 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

- ▶ Miljardin käyttäjän tiedot varastettiin Shanghain poliisin tietokannasta.
 - ▶ Kyseessä on Kiinan suurin yksittäinen tietovuototapaus.
 - ▶ Tietojen joukossa ovat ainakin henkilöiden nimi, syntymäpaikka, rikosrekisteri, osoite sekä henkilötunnus.

Analyysi

- ▶ Vuodettuja tietoja voidaan hyödyntää esimerkiksi laskutuspetoksessa tai identiteettivarkaudessa.
- ▶ On tärkeää varmistaa, että tileillä on käytössä monivaiheinen tunnistautuminen sekä vahvat yksilölliset salasanat.
- ▶ Tietovuodon uhri ei voi aina itse vaikuttaa tilanteeseensa. Jos palvelu on tietomurron kohteena, voivat tiedot päätyä väärin käsiin, vaikka omasta tietoturvasta olisi huolehdittu ohjeiden mukaan.



Tietomurrot ja -vuodot

- ▶ Office 365 -kalasteluviestejä käytetään jälleen murtautumiseen.
 - ▶ Ilmoituksia onnistuneista tietomurroista ja niiden yrityksistä tehdään Kyberturvallisuuskeskukselle edelleen tasaisella tahdilla.
 - ▶ Kaapattuja sähköpostitilejä käytetään uusien kalasteluviestien lähettämiseen. Murretulta tililtä voidaan varastaa myös tietoja, kuten sähköpostiviestejä.

Analyysi

- ▶ Monivaiheisen tunnistautumisen käyttöönotto estää suurimman osan tunnuskalastelun avulla tehdyistä tietomurroista.
- ▶ Monipuoliset suojaukset, lokitietojen seuranta, päätelaitteiden hallinta ja henkilöstön kouluttaminen ovat avaintekijöitä suojautumisessa.
- ▶ Tietomurron jälkeen luottamuksellista tietoa voi paljastua ja päätyä rikollisten käsiin.
- ▶ Tiliä ja sieltä saatuja tietoja voidaan käyttää rikolliseen toimintaan, kuten laskutuspetoksiin, tietojen kalasteluun ja haittaohjelmien levittämiseen.



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.



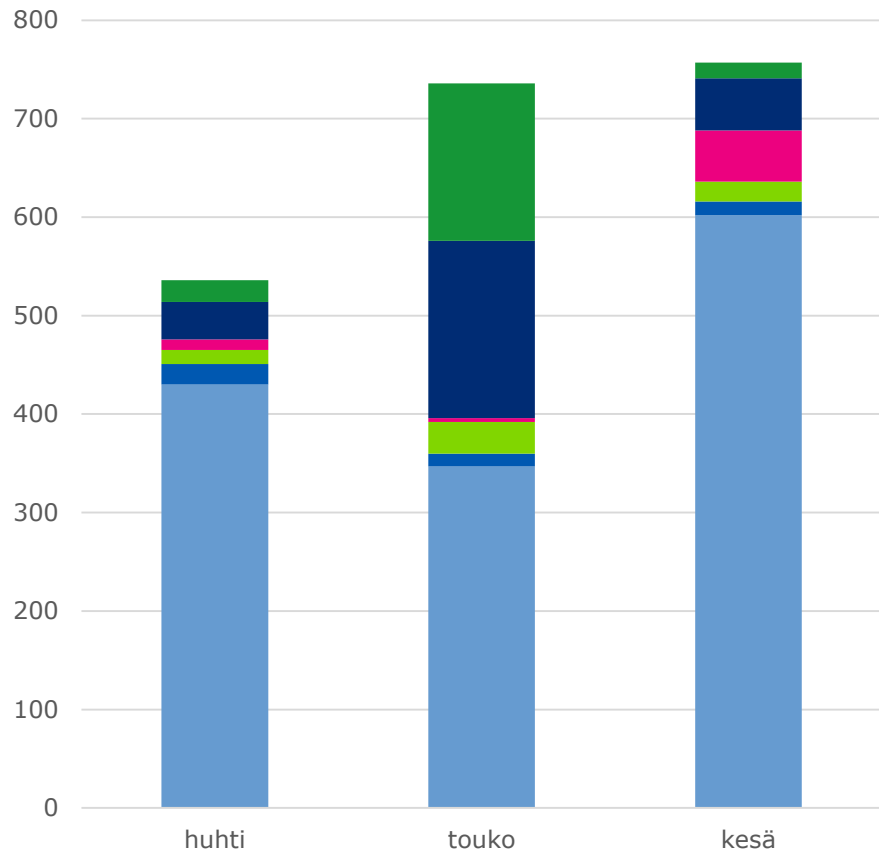
Huijaukset ja kalastelut

- ▶ Verkkopankkitunnusten kalastelu jatkuu
 - ▶ Liki kaikkien suomalaisten pankkien nimissä kalastellaan edelleen verkkopankkitunnuksia.
 - ▶ Kalastelua tehdään niin sähköpostitse kuin tekstiviestitse levitettävien viestien avulla.
 - ▶ Kalastelussa on hyödynnetty myös suomalaisia .fi-verkkotunnuksia.
- ▶ Poliisihallituksen nimissä leviävä huijausviesti
 - ▶ Sähköpostitse levitettävässä huijauksessa käytetään poliisihallituksen nimeä.
 - ▶ Vastaanottajalle lähetettävässä viestissä teemana on esimerkiksi haastehakemus.
 - ▶ Aiemmin vastaavissa kampanjoissa on pyydetty maksamaan valheellinen sakko.

Analyysi

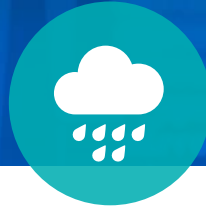
- ▶ Kuluttajaliiton Varo, varmista ja varoita -kampanja kertoo, että suomalaiset menettivät vuonna 2021 huijauksissa 47 miljoonaa euroa.
- ▶ Huijaukset kehittyvät jatkuvasti, mutta niiden tunnistaminen ja muiden varoittaminen estävät vahinkoja.
- ▶ Jos epäilet omien pankkitietojen joutumista väärin käsiin, ole välittömästi yhteydessä pankkiisi lisävahinkojen estämiseksi.

Käsiteltyjä huijaustapauksia Q2/2022



- Tilausansa
- SMS-huijaus
- Kiristyshuija us
- Huijauspuhe lu
- Toimitusjoht ajahuijaus
- Tietojenkala stelu

- ▶ Vuoden 2022 toisen neljänneksen ilmiöitä ovat:
 - ▶ Pankkitunnusten kalastelu ja tilausansat ovat jatkuneet aktiivisina.
 - ▶ Toukokuun SMS-huijausten piikki johtui taustakuva- ja pelipalveluaiheisista tilausansoista
 - ▶ Huijauspuheluiden määrä on pysynyt edelleen matalana.
 - ▶ Toimitusjohtajahuijausten määrä ei lisääntynyt lomakauden alusta huolimatta.



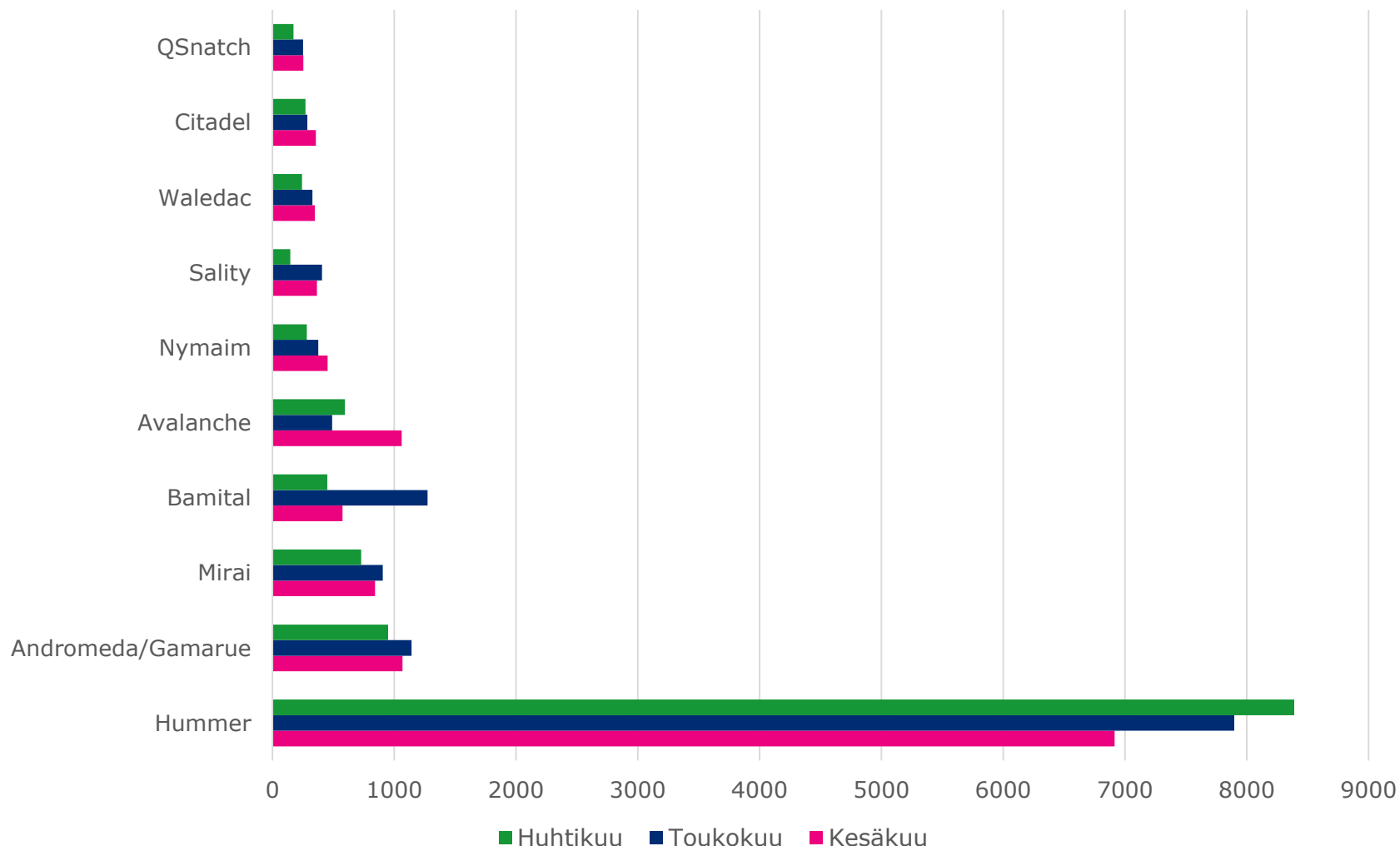
Haittaohjelmat ja haavoittuvuudet

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

Autoreporterin haittaohjelmahavainnot



Haittaohjelmatyypit Q2/2022



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 tarkemmin kotisivuiltamme.⁽⁴⁾

Katso lisää:

<https://tieto.traficom.fi/fi/tilastot/traficomin-haittaohjelmahavainnot>

13.7.2022



Haavoittuvuus

- ▶ Haavoittuvuus Microsoftin työkalussa mahdollistaa hyökkäykset haitallisten Microsoft Office -dokumenttien avulla.⁽⁵⁾

- ▶ Kyseessä on haavoittuvuus, joka on saanut tunnisteiden CVE-2022-30190. Se tunnetaan myös nimeltä Follina.
- ▶ Haavoittuvuuden korjaava päivitys julkaistiin 14.6.2022.
- ▶ Myös valtiolliset toimijat ovat hyödyntäneet aktiivisesti haavoittuvuutta. Lisätietoja Vakoilu-osuudessa.

Analyysi

- ▶ Organisaatioissa kannattaa varautua haavoittuvuuksiin, joihin ei ole tarjolla korjausta, mutta joita käytetään silti aktiivisesti hyväksi.
- ▶ Mikäli haavoittuvuuden vaikutuksia joudutaan rajoittamaan tilapäisillä keinoilla, tulee myös keinojen vaikutukset arvioida ennen niiden käyttöönottoa liiketoiminnan jatkuvuuden turvaamiseksi.



Kuukauden haavoittuvuusjulkaisut

- ▶ Ei haavoittuvuusjulkaisuja.
- ▶ Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

```
elif _operation == "MIRROR_X":
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

#selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
#mirror_ob.select = 0
base = bpy.context.selected_objects[0]
for data in bpy.data.objects:
    data.select = 1
```





Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- ▶ **Kyberturvallisuuskeskus vastaanottaa vuositasolla n. 50 haavoittuvuuskoordinaatiotapausta.**
 - ▶ Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
- ▶ **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta.**
 - ▶ Vastaanotamme ilmoituksia myös anonyymeilta ilmoittajilta.
- ▶ **Haavoittuvuustiedotteita tullut tänä vuonna 11 kpl (tilanne 10.7.2022).**
 - ▶ 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

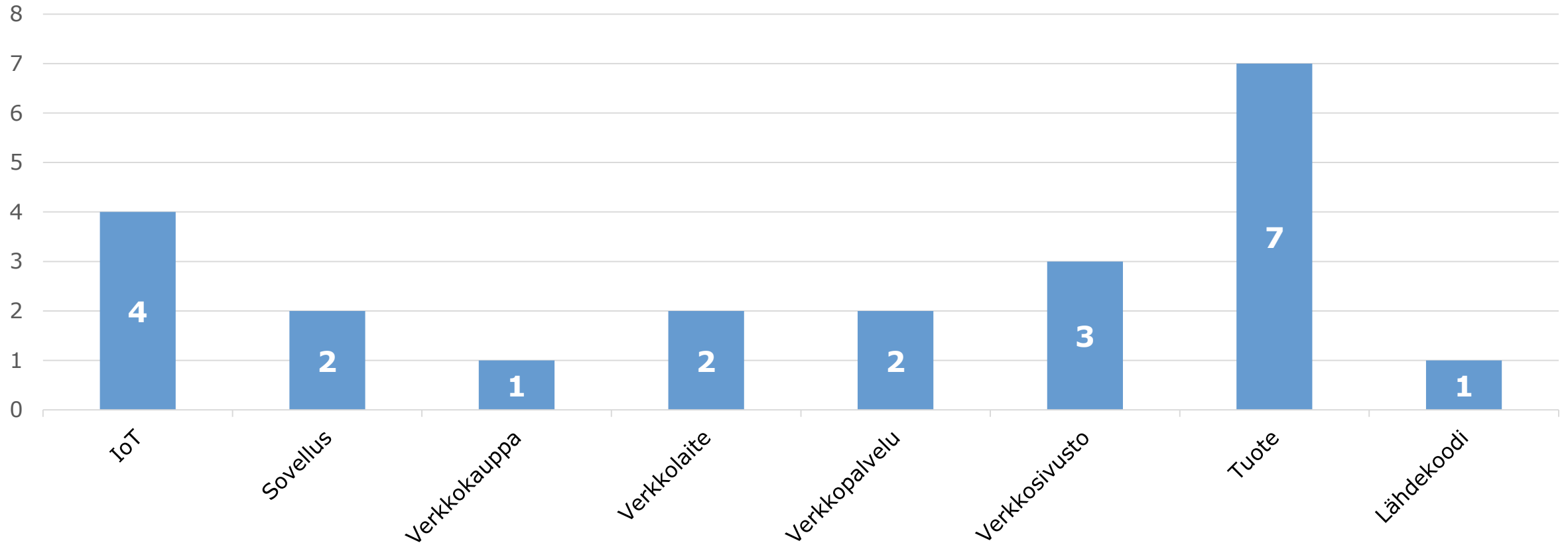
- ▶ Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- ▶ Vanhentuneet tai heikot salasanakäytännöt ovat usein toistuva ongelma. Voi olla, että muutoin tietoturvallisesta tuotteesta löytyy oletussalasana. Erilaisissa verkkopalveluissa voi myös olla parannettavaa salasanakäytännöissä esim. salasanan vaatimusten tai salasanan vaihtominaisuuksien 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

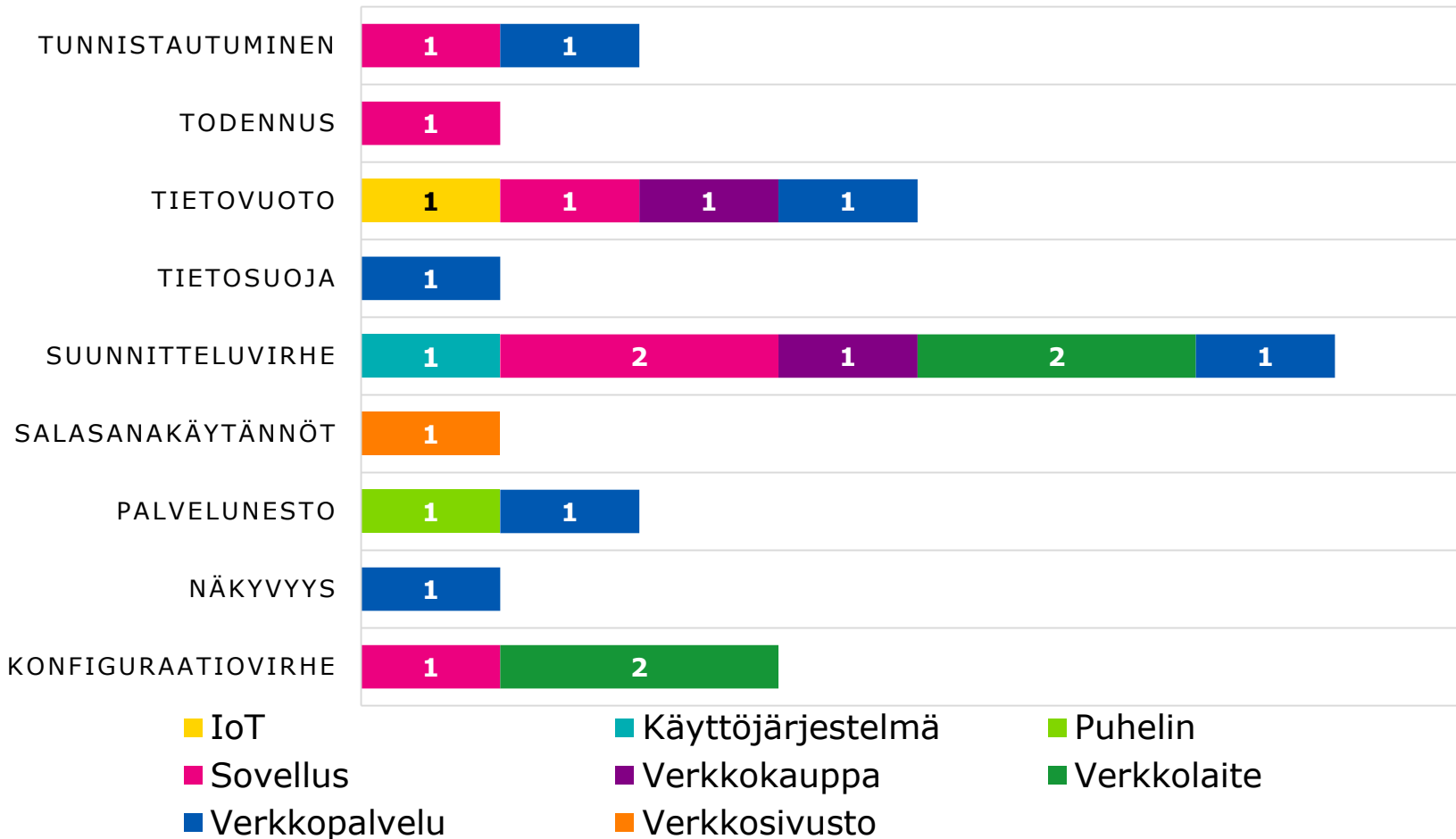


Haavoittuvuustyytit 01-06/2022





Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio



Taulukossa on esitetty Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio-tapaukset vuoden 2022 ensimmäiseltä vuosipuolikkaalta.

Haavoittuvuuskoordinaatiota on esitelty laajemmin verkkosivuillamme. [\(6\)](#)



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

► Haavoittuvuus älyporealtaassa

- Tietoturvatutkija hankki Jacuzzi-älyporealtaan, joka kytkeytyy valmistajan pilvipalveluun. Palvelun hallintakäyttöliittymä sekä muiden asiakkaiden tietoja paljastui heti ja tutkija sai täyden pääsyn pilvipalvelun kautta valmistajan kaikkien älyporealtaiden hallintaan.⁽⁷⁾
- Valmistaja ei useista yrityksistä huolimatta vastannut asiasta ilmoittaneelle tutkijalle, joskin haavoittuvuus korjattiin lopulta.⁽⁸⁾
- Porealtaiden hallintaan päässyt tietoturvatutkija sai pääsyn siellä näkyviin tietoon – sisältäen asiakkaiden henkilötietoja. Potentiaalinen hyökkääjä saattaisi pystyä myös muuttamaan porealtaan sähkönkulutuksen asetuksia.

Analyysi

- Älyominaisuudet helpottavat kuluttajalaitteiden käyttöä. Varjopuolena on, että tietoturvaan ei panosteta aina riittävästi.
- Kuluttajan tulisi pohtia, ovatko älyominaisuudet hänen kannaltaan tarpeellisia. Lisäksi on tärkeää huomioida, mitä tietoja syöttää palveluihin ja mitä niiden mahdollinen vuotaminen tarkoittaisi. Pilvipalveluissa sijaitseva haavoittuvuus voi yllättää valveutuneenkin kuluttajan.
- Valmistajien tulisi mahdollistaa havaituista tietoturvaongelmista ilmoittaminen.⁽⁹⁾
- Esimerkiksi Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskuksen myöntämä Tietoturvamerkki kertoo siitä, että merkillä varustettu tuote tai palvelu on jo lähtökohtaisesti suunniteltu tietoturvalliseksi ja täyttää Traficom asettamat tietoturvavaatimukset.



Automaatio

► OT:ICEFALL-haavoittuvuuskokonaisuus

- Tietoturvayritys Forescout julkaisi laajan raportin löytämistään 56 uudesta haavoittuvuudesta, jotka koskettavat kymmenen eri valmistajan automaatiolaitteita.⁽¹⁰⁾
 - Haavoittuvuudet sisältävät mm. turvattomia protokollia sekä mahdollisuuksia komentojen suorittamiseen etänä ilman tunnistautumista.⁽¹¹⁾
 - Haavoittuvuuskokonaisuudella voi olla vaikutuksia monella eri toimialalla. Raportin mukaan mahdollisia hyökkäyksiä voidaan tehdä esim. tuulivoimapuistoihin, maakaasuverkostoihin sekä yleisemmin valmistavan teollisuuden ympäristöihin.
- Löydöksiä vastaan on esitetty myös kritiikkiä, sillä osa löydöksistä on tiedossa olevia standardin ominaisuuksia. Tutkijat raportoivat myös vanhoja ohjelmistoversioiden haavoittuvuuksia, vaikka valmistaja on korjannut ne jo useita vuosia sitten.⁽¹²⁾

Analyysi

- Automaatioympäristöjen ominaispiirteitä ovat esimerkiksi laitteiden pitkät elinkaaret sekä mahdollisuus asentaa tietoturvapäivitykset ainoastaan muutamia kertoja vuodessa olevilla huoltokatkosten aikana. Ympäristöt on aiemmin suunniteltu niin, että ne ovat ns. omia julkisesta tietoverkosta eristettyjä ympäristöjään.
- Tästä syystä automaatioympäristöissä on usein korjaamattomia haavoittuvuuksia, vaikka niiden ulkopuolelta tapahtuva hyödyntäminen ei olekaan todennäköistä.
- Pilvipalveluita hyödyntävät analytiikka- ja IoT-palvelut ovat muuttamassa tilannetta myös automaatioympäristöjen osalta. Aiemmin "eristetty" ympäristö kytkeytyykin nyt Internetiin. Silloin päivittämättömien haavoittuvuuksien merkitys kasvaa.
- Suosittelemme organisaatioita tutustumaan OT:ICEFALL-löydöksiin sekä pohtimaan niiden vaikutuksia omaan toimintaan ja automaatioympäristöihin. Jos päivittäminen ei ole mahdollista, voidaanko haavoittuvuuden muodostamaa riskiä rajoittaa jollakin muulla tavalla?



Automaatio

► Hyökkäys Iranin terästeollisuuteen

- Aiemmin Iranin polttoaineenjakeleua vastaan suunnattuun kyberhyökkäykseen liitetty Predatory Sparrow -ryhmä ilmoitti hyökänneensä 27.6.2022 kolmea iranilaista terästeollisuuden yhtiötä vastaan. Hyökkääjän jakamassa videossa näkyy terästehtaan kaapatulta valvontakameralta, kuinka masuuni laskee sulan teräksen tuotantolinjalle ja tehtaan lattialle.
- Tietoturvyhtiö Check Point ilmoitti löytäneensä hyökkäyksessä käytetyn Chaplin-haittaohjelman, jolla on yhteneväisyyksiä viime vuonna Iranin rautateitä vastaan suunnattuun Meteor-haittaohjelmaan.
- Iranin kyberoperaatioiden seuraamiseen erikoistunut Certfa Labs uskoo, että kyseessä olisi toimitusketjua hyödyntänyt hyökkäys. Sen mukaan Iranin terästeollisuuden laajasti käyttämä järjestelmätoimittaja Irida olisi toiminut hyökkäyksen tunkeutumisreittinä.
- Myöhemmin Israelin puolustusministeri määräsi tutkittavaksi, miten tieto armeijan Yksikkö 8200:n mahdollisesta osuudesta hyökkäykseen oli päässyt vuotamaan paikallisten televisiokanavien uutisiin.

Analyysi

- Kriittisen infrastruktuurin sekä teollisuuden automaatiojärjestelmillä ohjataan fyysisen maailman tapahtumia. Silloin oleellista on varmistaa tuotantoprosessin, ihmisten, ympäristön sekä omaisuuden turvallisuus.
- Kevään 2022 aikana on havaittu aiempaa enemmän myös automaatioympäristöihin kohdistettuja kyberhyökkäyksiä ja niiden yrityksiä. Näissä tapauksissa huolestuttavaa on, että ne vaarantavat myös ihmisten turvallisuuden.
- Tämän tyyppisistä hyökkäyksistä on tulossa vain yksi työkalu joidenkin valtioiden geopoliittisen vaikuttamisen työkalupakkiin. Toisaalta jotkin valtiot katsovat, että esimerkiksi kyberhyökkäys niiden kriittistä infrastruktuuria vastaan saattaa oikeuttaa jopa sotilaalliset vastatoimet.



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 verkot toimivat Suomessa kohtalaisen hyvin.
 - ▶ Kesäkuussa oli kuusi merkittävää häiriötä.
 - ▶ Vakavuusluokat: A: 0, B: 1, C: 5
 - ▶ Vikojen syyt johtuivat pääosin muutostöistä ja erilaisista laitevioista.
- ▶ Otto-automaateissa laaja häiriö [\(13\)](#)
 - ▶ Häiriön aiheutti palveluntoimittajan tietoliikennekatko.
 - ▶ Pahimmillaan tietoliikennekatko sulki 8.6. lähes kaikki Otto-pankkiautomaatit.

Analyysi

- ▶ Yleisten viestintäpalveluiden toimivuus oli Suomessa vuonna 2021 keskimäärin hyvä.
- ▶ Kuukaudessa tapahtuu 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.



ICT-palveluiden toimivuus

- ▶ Kanadalainen teleoperaattori Rogers kärsi tietoliikennehäiriöstä.⁽¹⁴⁾
 - ▶ Katkokset johtuivat muutostyöstä, joka aiheutti reitittimien toimintahäiriön.
 - ▶ Laajalla katkolla oli hetkellisesti vaikutuksia mm. valtionhallinnon, terveydenhuollon ja finanssialan toimijoihin.
- ▶ Häiriö kotimaan turvapuhelimissa
 - ▶ Yle uutisoi 7.7. turvapuhelimissa ilmenneestä häiriöstä mm. Oulun ja Pohjois-Karjalan seudulla.⁽¹⁵⁾
 - ▶ Vastaavanlainen katko on tapahtunut myös aiemmin tänä keväänä.

Analyysi

- ▶ Rogersin kaltaiset tietoliikennehäiriöt osoittavat, kuinka tärkeää testaaminen on muutostöiden yhteydessä.
 - ▶ Yhtä tärkeää on myös palautumisen harjoittelu, mikäli kaikki ei jostain syystä menekään niin kuin pitäisi.
- ▶ Kesäkuussa häiriöitä ilmeni myös mm. Cloudflare- ja Microsoft 365 -palveluissa.
 - ▶ Katkokset suuremmilla palveluntarjoajilla osoittavat, että mikä tahansa palvelu voi olla hetkellisesti saavuttamattomissa.



Palvelunestohyökkäykset

- ▶ Kesäkuussa tiedossamme olevien palvelunestohyökkäysten vaikutukset jäivät pieniksi.
 - ▶ Vastaanotimme kourallisen ilmoituksia, joiden perusteella suojautumistoimenpiteet ovat olleet riittäviä hyökkäysten estämiseksi.
- ▶ Toistaiseksi olemme saaneet lukea vain muihin maihin kohdistuneista palvelunestohyökkäyksistä.
 - ▶ Killnet-ryhmittymä ilmoitti tehneensä palvelunestohyökkäyksiä Liettuaan ja Norjaan kesäkuun lopulla. [\(16\)](#) [\(17\)](#)

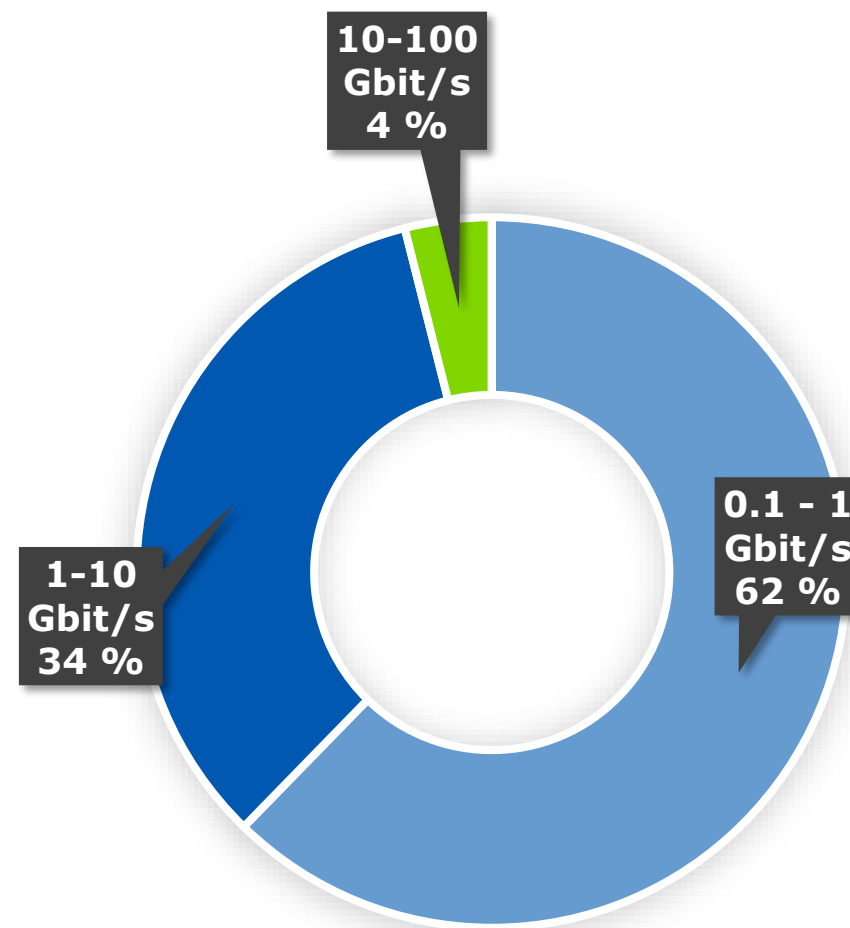
Analyysi

- ▶ Kyberturvallisuuskeskus ottaa vastaan ilmoituksia tietoturvapoikkeamista.
- ▶ Tilannekuvamme kannalta on tärkeää, että ilmoitatte meille myös palvelunestohyökkäyksistä, joilla ei välttämättä ole ollut vaikutuksia palveluidenne toimintaan.
- ▶ Erilaisten ilmoitusten perusteella tiedämme, millaisia hyökkäyksiä Suomessa tällä hetkellä tapahtuu ja pystymme ohjeistamaan organisaatioita hyökkäyksiin varautumisessa.

Palvelunestohyökkäysten tunnuslukuja



- ▶ 119 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q2/2022.
- ▶ Noin 79% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- ▶ Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q2/2022 - 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

- ▶ Tietoturvayhtiö Palo Alton Unit 42:n tutkijat ovat tunnistaneet uuden GALLIUM-ryhmän käyttämän etäkäytön mahdollistavan haittaohjelman, jota kutsutaan nimellä PingPull.⁽¹⁸⁾
 - ▶ GALLIUM tunnetaan myös nimellä Operaatio Soft Cell tai Softcell, joka oli merkittävä teleoperaattoreihin kohdistunut vakoilukampanja.
 - ▶ Tietoturvayhtiöt ovat arvioineet GALLIUM:in olevan todennäköisesti Kiinan valtion tukema APT-ryhmä.⁽¹⁹⁾
- ▶ PingPullin ominaisuuksiin kuuluu mm. se, että se pystyy käyttämään myös ICMP-protokollaa komentokanavana. Tällä voidaan tehdä haittaohjelmasta vaikeammin havaittava.
- ▶ Aiemmin erityisesti teleoperaattoreihin toimintaansa kohdistanut GALLIUM on Palo Alton mukaan laajentanut viimeisen vuoden aikana kohdistustaan myös finanssisektoriin ja valtionhallintoon.
- ▶ Maantieteellisesti APT-toimijan kohteet ovat Kaakkois-Aasiassa, Euroopassa ja Afrikassa.

Analyysi

- ▶ Organisaation havainnoinnissa pitäisi huomioida myös ICMP-protokollan käyttäminen mahdollisena komentokanavana.
- ▶ Uhkatoimijoiden operaatioiden kohdistus ja kohdetoimialat voivat muuttua tai laajentua ajan myötä, joten organisaatioiden kannattaa päivittää uhka-arvioitaan säännöllisesti.



Vakoilu

- ▶ APT-ryhmät hyödyntävät uusia löydettyjä haavoittuvuuksia ketterästi. Tästä tuoreena esimerkkinä on Microsoft Support Diagnostic Tool -työkalun (MSDT) niin kutsuttu Follina-haavoittuvuus (CVE-2022-30190).
 - ▶ Follina-haavoittuvuudesta lisää tämän katsauksen Haavoittuvuudet-osiossa.
- ▶ Esimerkiksi tietoturvayritys Malwarebytesin tutkijoiden mukaan venäläinen APT-ryhmä on pyrkinyt saamaan jalansijaa ukrainalaisiin kohteisiin kyseisen haavoittuvuuden avulla.⁽²⁰⁾
 - ▶ Haavoittuvuutta hyödyntäviä haitallisia .docx-liitteitä on lähetetty kohteille sähköpostitse.
 - ▶ Tavoitteena on ollut varastaa käyttäjän evästetietoja tai salasanoja, jotka käyttäjä on tallentanut selaimeensa.
 - ▶ Myös Ukrainan CERT eli CERT-UA on raportoinut kyseisestä kampanjasta.
- ▶ Follinaa on tietävästi pyritty hyödyntämään myös eurooppalaisiin valtionhallintoihin ja Yhdysvaltojen paikallishallintoihin lähetetyssä kalastelukampanjassa.⁽²¹⁾
 - ▶ Asiasta kesäkuun alussa kertonut Proofpoint on todennut epäilevänsä taustalla olevan valtiollinen toimija.⁽²²⁾

Analyysi

- ▶ Follina-haavoittuvuuden kohdalla nopean päivittämisen sijaan korostui nopeiden rajoitustoimenpiteiden toteuttaminen, sillä korjaavaa päivitystä ei ollut heti saatavilla.
- ▶ Uusien kriittisten haavoittuvuuksien tultua julki rajoitustoimenpiteiden tai nopean päivittämisen lisäksi on syytä varmistua siitä, ettei haavoittuvuutta ole ehditty hyödyntämään järjestelmiin tunkeutumisessa.



Vakoilu

- ▶ Teleoperaattori Lumen Technologiesin (ent. CenturyLink) Black Lotus Labs -yksikkö on tunnistanut kehittyneen koti- ja pienyritysreitittimiin kohdistuvan haittaohjelman, jota kutsutaan nimellä ZuoRAT.⁽²³⁾
 - ▶ Monivaiheinen ZuoRAT mahdollistaa hyökkääjälle mm. etenemisen ja muiden järjestelmien murtamisen samassa lähiverkossa. Yhtiön mukaan haittaohjelma vaikuttaa olevan muokattu versio Miraista.
 - ▶ Kampanja on Black Lotus Labsin mukaan jatkunut todennäköisesti jo vuosia ja kohdistunut ainakin 80 kohteeseen. Yhtiö on saanut viitteitä siitä, että haittaohjelmasta olisi tehty versioita useiden eri reititinvalmistajien laitteille.
 - ▶ Yhtiö ei nimennyt mitään yksittäistä ryhmää kampanjan taustalla olevaksi toimijaksi.
- ▶ Yhdysvaltojen tietoturaviranomainen CISA varoitti puolestaan yhdessä NSA:n ja FBI:n kanssa Kiinan valtion tukemien APT-ryhmien koti- ja pienyritysreitittimiin kohdistamasta toiminnasta sekä teleoperaattoreihin kohdistetusta kybervakoilusta.⁽²⁴⁾ ⁽²⁵⁾

Analyysi

- ▶ Valtaosalta koti- ja pienreitittimiin kohdistuvista tietomurroista voitaisiin välttyä huolehtimalla laitteiden päivittämisestä, oletussalasanoiden vaihtamisesta sekä siitä, että laitteiden hallintakäyttöliittymät eivät olisi avoinna Internetiin.
- ▶ Reitittimeen kohdistuva tietomurto ei vaaranna vain laitteen haltijan tai käyttäjän tietoturvaa. Murrettua laitetta voidaan hyödyntää myös muihin kohdistuvassa kybervakoilussa, tietomurroissa ja näiden valmistelussa.



Tietoturva-alan kehitys, sääntely ja standardit

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



Oikeudelliset asiat

- ▶ Teletoinnin tietoturvaan annetun määräyksen (67 A/2015 M) ajantasaistaminen
 - ▶ Liikenne- ja viestintävirasto käynnistää määräyshankkeen, jossa ajantasaistetaan 4.3.2015 voimaan tullutta Viestintäviraston määräystä teletoinnin tietoturvaan.
 - ▶ Määräys koskee yleistä teletointia ja sen tarkoituksena on:
 1. edistää yleisten viestintäverkkojen ja -palvelujen tietoturvaa,
 2. turvata sähköisen viestinnän luottamuksellisuutta ja yksityisyyden suojan toteutumista sekä
 3. varmistaa, että tietoturvan toteuttaminen teleyrityksissä on kattavaa, suunnitelmallista ja tehokasta.
 - ▶ Tarkoituksena on huomioida 5G-tekniikan uudet arkkitehtuuriratkaisut, matkaviestinverkkojen uudet käyttötapaukset sekä niihin liittyvät tietoturva-vaatimukset. Päivitystarvetta on lisännyt myös verkon monimuotoistuminen, uusien rajapintojen avaaminen, virtualisointi, pilvipalvelujen käyttö sekä laitetilojen monimuotoistuminen.
 - ▶ Vastaukset pyydetään toimittamaan Liikenne- ja viestintävirastolle lausuntopalvelu.fi-verkkosivuston kautta viimeistään 31.8.2022.
 - ▶ <https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=e80c3ac0-6941-4bba-bdcf-62c826646465>



Oikeudelliset asiat

- ▶ Apulaistietosuoja-valtuutetun päätös rekisteröityjen sijaintitietojen käsittelyä koskevassa asiassa (Dnro 6813/171/21)
- ▶ Päätöksen taustalla Pohjois-Savon sairaanhoitopiirin tekemä tietoturvaloukkausilmoitus, jonka mukaan sijaintitietojen keräämisen sallivat asetukset ovat olleet päällä työntekijöiden Windows 10 -työasemissa, vaikka tietoja ei ole ollut tarkoitus kerätä. Kannettavia tietokoneita on käytetty esimerkiksi etätyössä.
- ▶ Tietosuoja-valtuutetun toimisto pyysi asiasta selvitystä Pohjois-Savon sairaanhoitopiirin ICT-palvelut tuottavalta Istekki Oy:ltä sekä Valtion tieto- ja viestintätekniikkakeskus Valtorilta. Molemmat kertoivat, että sijaintitietojen kerääminen on oletusarvoisesti päällä Windows 10 -käyttöjärjestelmässä, eivätkä asiakkaat ole ohjeistaneet muuta.
- ▶ Rekisterinpitäjälle annettiin huomautus ja velvoite poistaa kaikki kerätyt tiedot. Sijaintitietoasetus on ollut perusteetta oletusarvoisesti päällä työntekijöiden kannettavissa tietokoneissa, eikä rekisterinpitäjä ole huolehtinut siitä, että näin ei ole. Rekisterinpitäjällä ei ole ollut lain edellyttämää tarvetta työntekijöiden sijaintitietojen käsittelylle.
- ▶ Apulaistietosuoja-valtuutetun päätöksen mukaan rekisterinpitäjän on kolmannen osapuolen ohjelmistoa tai valmisohjelmistoa käyttäessään varmistettava, että toiminnot, joille ei ole laillista perustetta tai jotka eivät vastaa käsittelyn aiottuja tarkoituksia poistetaan käytöstä.
- ▶ Apulaistietosuoja-valtuutetun päätökset koskevat arviolta kymmenien tuhansien julkisen sektorin työntekijöiden sijaintitietojen käsittelyä.
- ▶ <https://finlex.fi/fi/viranomaiset/tsv/2022/20221463>
- ▶ <https://tietosuoja.fi/-/apulaistietosuoja-valtuutettu-sijaintitiedon-keräämisen-ei-pida-olla-automaattisesti-paalla-tyontekijoiden-tietokoneissa-ilman-perustetta>



Oikeudelliset asiat

- ▶ Tekijänoikeus ja yksityisyydensuoja: Korkeimman oikeuden ennakkopäätös (KKO:2022:47)
- ▶ Yhtiö vaati teleyrityksen velvoittamista luovuttamaan sille yhteystiedot 34 teleliittymästä, joista oli yhtiön mukaan tekijänoikeuksien suojan kannalta merkittävässä määrin saatettu yleisön saataviin yhtiön tekijänoikeudella suojattua aineistoa ilman yhtiön suostumusta. Markkinaoikeus määräsi teleyrityksen luovuttamaan yhteystiedot viidestä teleliittymästä hyläten hakemuksen muilta osin.
- ▶ Kysymys erityisesti siitä, oliko tekijänoikeudella suojattua aineistoa saatettu yleisön saataviin tekijänoikeuslain 60 a §:ssä tarkoitetuin tavoin tekijän oikeuksien suojan kannalta *merkittävässä määrin*. Lisäksi arvioitavana yhtiön tiedonsaantioikeudet suhteessa teleliittymän käyttäjän yksityisyyden ja henkilötietojen suojaan.
- ▶ Markkinaoikeuden arvion mukaan muutamina vuorokausina tehdyt havainnot tai vähäinen määrä tätä pitemmällä ajanjaksolla tehtyjä havaintoja eivät tyypillisesti osoittaneet merkittävässä määrin -kriteerin täyttymistä.
- ▶ Tapauksessa tekijänoikeudella suojattuja teoksia jaettiin tiedostoina vertaisverkossa BitTorrent-tekniikkaa hyödyntäen. Käyttäjien määrä vaihteli muutamasta kymmenestä yli tuhanteen ja kyseessä oli elokuvateatterilevityksessä olleet elokuvat.
- ▶ Korkein oikeus katsoi, että markkinaoikeuden määräämän lisäksi käyttäjän ja tilaajan yhteystiedot on luovutettava myös niistä teleliittymistä, joiden osalta markkinaoikeus on hylännyt hakemuksen.
- ▶ Ratkaisun perusteena se, että tekijänoikeudella suojatun aineiston yleisön saataviin saattaminen on ollut laajamittaista ja tekijän oikeuksien suojan kannalta haitallista myös suojatun aineiston laadun ja teleliittymän käyttäjän toiminnan kannalta. Luovutuksen kohteena ovat pelkästään IP-osoitteiden haltijoiden ja käyttäjien yhteystiedot, joiden perusteella ei yleensä ole tehtävissä tarkkoja päätelmiä käyttäjän yksityiselämästä.
- ▶ <https://korkeinoikeus.fi/fi/index/ennakkopaatokset/kko202247.html>

Arjen kyberturvallisuus

Varo, varmista ja varoita

- ▶ Varo, varmista ja varoita: Nettihuijaukset ja tietojenkalastelu muuttavat muotoaan, mutta niiltä on mahdollista suojautua. Tutustu viranomaisten ja yritysten yhteiskampanjan materiaaleihin ja pysy turvassa.
- ▶ Lue lisää: <https://www.kuluttajaliitto.fi/varo-varmista-varoita/>

Kyberturvallisuuskuukausi on tulossa

- ▶ Lokakuussa vietettävä Euroopan kyberturvallisuuskuukausi tuo tullessaan jälleen liudan hyödyllisiä materiaaleja. Tänä vuonna teemoina ovat tietojenkalastelu ja kiristyshaittaohjelmat.
- ▶ Lue lisää: <https://cybersecuritymonth.eu/>

SuomiAreenassa keskustellaan kyberistä

- ▶ Kyberturvallisuus on vahvasti esillä tämän vuoden SuomiAreenassa! Teemoina keskusteluissa mm. informaatiovaikuttaminen, kyberrikollisuus, huijaukset ja tietojenkalastelu.
- ▶ Lue lisää: <https://www.suomiareena.fi/pori/ohjelma/>

Laskutushuijaukset lisääntyvät kesäisin - näin suojaudut huijauksilta

- ▶ Yritysten rahaliikenteeseen kohdistuvat huijaukset lisääntyvät kesän lomakauden aikana. Pitäkää huolta siitä, että organisaationne maksukäytännöt ovat kaikkien työntekijöiden tiedossa.
- ▶ Lue lisää: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/laskutushuijaukset-lisaantyyvat-kesaisin-na-in-suojaudut-huijauksilta>



Uutisia Kyberturvallisuuskeskuksesta

Lausu ja vaikuta!

- ▶ Liikenne- ja viestintäministeriö pyytää lausuntoja valtioneuvoston asetusluonnoksesta tietoturvan kehittämisen tueksi, eli niin kutsutuksi tietoturvaseteliksi.
- ▶ Ehdotetulla uudella määräaikaisella tuella organisaatiot voisivat konkreettisesti parantaa järjestelmiensä tietoturvaa sekä kehittää omaa tietoturvaosaamistaan. Kybervarautumistason nostaminen eniten tukea tarvitsevilla sektoreilla parantaisi yhteiskunnan kykyä suojautua mm. hybridiuhkilta.
- ▶ Lausuntoaika päättyy 22.7.2022.
- ▶ <https://www.lvm.fi/-/tietoturvaseteli-lausuntokierrokselle-tukea-organisaatioiden-tietoturvan-kehittamiseen-1783637>

Vastaa kyselyyn Kyberturvallisuuskeskuksen uutis- ja haavoittuvuuskoosteista!

- ▶ Tiesitkö, että voit saada Kyberturvallisuuskeskuksen tietoturva-asiantuntijoiden laatimat uutis- ja haavoittuvuuskoosteet ajankohtaisista tietoturvailmiöistä sähköpostiisi joka päivä?
- ▶ Pyydämme apuasi koostettamme kehittämiseen niin nykyisiltä lukijoilta kuin teiltä, jotka ette vielä koostettamme tilaa.
- ▶ Vastaa kyselyymme 31.8.2022 mennessä!
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vastaa-kyselyyn-kyberturvallisuuskeskuksen-uutis-ja-haavoittuvuuskoosteista>

Kyber- ja informaatiovaikuttaminen, saman kolikon kaksi puolta

- ▶ Informaatio- ja kyberturvallisuus kytkeytyvät tiiviisti toisiinsa. Ne ovat olennainen osa toimivaa yhteiskuntaa. Niihin liittyy myös uhkia, jotka koskettavat meitä kaikkia.
- ▶ Jotta pystymme toimimaan ja osallistumaan yhteiskuntaamme, valvomaan etujamme ja oikeuksiamme, on tärkeää ymmärtää erilaisia uhkia, joihin voimme törmätä arjessamme.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyber-ja-informaatiovaikuttaminen-saman-kolikon-kaksi-puolta>

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>

Lähdeluettelo

1) Kyberturvallisuuden vahvistaminen suomalaisissa organisaatiossa - ohje johdolle ja asiantuntijoille

<https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuden-vahvistaminen-suomalaisissa-organisaatiossa-ohje-johdolle-ja-asiantuntijoille>

2) Kyberturvallisuuskeskus, ISAC-tiedonvaihtoryhmät <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat>

3) Kyberturvallisuuskeskus – monivaiheinen tunnistautuminen suojaaa käyttäjätilejäsi

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suoja-kayttajatilejasi>

4) Autoreporterin haittaohjelmahavainnot

<https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot>

5) Uusi haavoittuvuus Microsoftin työkalussa mahdollistaa hyökkäykset haitallisten Microsoft Office -dokumenttien avulla

https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_10/2022

6) Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio pähkinäkuoressa

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-haavoittuvuuskoordinaatio-pahkinankuoressa>

Lähdeluettelo

7) Hypponen's Law: If it's smart, it's vulnerable

<https://blog.f-secure.com/hypponens-law-smart-vulnerable/>

8) Hacking into the worldwide Jacuzzi SmartTub network

<https://eaton-works.com/2022/06/20/hacking-into-the-worldwide-jacuzzi-smarttub-network/>

9) Haavoittuvuudet - miten niistä ilmoitetaan oikein

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein>

10) OT:ICEFALL: 56 Vulnerabilities Caused by Insecure-by-Design Practices in OT

<https://www.forescout.com/blog/ot-icefall-56-vulnerabilities-caused-by-insecure-by-design-practices-in-ot/>

11) OT:ICEFALL report: The legacy of "insecure by design" and its implications for certifications and risk management

<https://www.forescout.com/resources/ot-icefall-report/>

12) Does Disclosing OT:ICEFALL Vulnerabilities Help Secure OT?

<https://www.isssource.com/56-vulnerabilities-in-oticefall-research/>

13) Otto-automaateista 90 prosenttia oli keskiviikkona poissa käytöstä – syytä selvitetään

<https://yle.fi/uutiset/3-12482724>

Lähdeluettelo

13) Rogers CEO apologizes for massive service outage, blames maintenance update

<https://www.cbc.ca/news/business/rogers-outage-interac-debit-restored-1.6515869>

14) Häiriö Oulun kaupungin turvpuhelinten verkkoyhteysissä on ohitse

<https://yle.fi/uutiset/3-12527845>

15) Venäläinen hakkeriryhmä teki taas kyberiskun Liettuaan

<https://yle.fi/uutiset/3-12043017/64-3-89275>

16) Venäläiset hakkerit iskivät Norjaan ja uhkailivat Naton Stoltenbergiä

<https://yle.fi/uutiset/3-12043017/64-3-89487>

17) GALLIUM Expands Targeting Across Telecommunications, Government and Finance Sectors With New PingPull Tool

<https://unit42.paloaltonetworks.com/pingpull-gallium/>

18) Chinese 'Gallium' Hackers Using New PingPull Malware in Cyberespionage Attacks

<https://thehackernews.com/2022/06/chinese-gallium-hackers-using-new.html>

Lähdeluettelo

19) Russia's APT28 uses fear of nuclear war to spread Follina docs in Ukraine

<https://blog.malwarebytes.com/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine/>

20) Windows zero-day exploited in US local govt phishing attacks

<https://www.bleepingcomputer.com/news/security/windows-zero-day-exploited-in-us-local-govt-phishing-attacks/>

21) Twitter: @ThreatInsight [Twiitti]

<https://twitter.com/threatinsight/status/1532830739208732673>

22) ZuoRAT Hijacks SOHO Routers To Silently Stalk Networks

<https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/>

23) People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices

<https://www.cisa.gov/uscert/ncas/alerts/aa22-158a>

24) US: Chinese govt hackers breached telcos to snoop on network traffic

<https://www.bleepingcomputer.com/news/security/us-chinese-govt-hackers-breached-telcos-to-snoop-on-network-traffic/>