TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Heinäkuu 2022

#kybersää

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

rauhallinen huolestuttava vakava

TRAFICOM

11.8.2022

Kybersää heinäkuu 2022

Tietomurrot ja -vuodot

- Haavoittuvia tai päivittämättömiä web-palvelimia murretaan jatkuvasti.
- Suomen Tietotoimisto STT ja Wärtsilä olivat tietomurron ja sitä seuranneen kiristyshaittaohjelman kohteena.

Huijaukset ja kalastelut

- Poliisin nimiä ja logoja on käytetty huijausviesteissä, joissa uhkaillaan oikeustoimilla ja vaaditaan lunnaita.
- Pankkitunnuksia kalastellaan hyvin monenlaisilla eri huijausviesteillä sekä tekstiviesteillä että sähköpostilla.

Haittaohjelmat ja haavoittuvuudet

- Heinäkuussa ei tehty juurikaan ilmoituksia haittaohjelmatartunnoista.
- Samban vakava ja Vmwaren kriittinen haavoittuvuus vaativat pikaista päivittämistä.

Automaatio ja IoT

- Kyberrikolliset pyrkivät löytämään uusia ja luovia tapoja päästäkseen käsiksi eristettyihin automaatiojärjestelmiin.
- Salasananmurto-ohjelma voikin sisältää troijalaisen!

Verkkojen toimivuus

- A-vika (yli 300 000 käyttäjään vaikuttava häiriö) Yle TV1-kanavalla arki-iltana.
- Vain kaksi merkittävää viestintäverkkojen häiriötä.
- Palvelunestohyökkäysten tilanne Suomessa oli rauhallinen.

Vakoilu

- Iranin hallintoon liitetty toimija tuhosi Albanian valtiohallinnon tietojärjestelmiä.
- Pohjois-Korean hallintoon liitetyt hyökkääjät ovat aktiivisia.
- Venäjän tiedustelupalveluun liitetty toimija jatkaa tunkeutumisyrityksiään.

TRAFICOM

11.8.2022

Kuukauden tunnuslukuja

1

Verkot toimivat heinäkuussa hyvin vakaasti. Yksi A-luokan vika (yli 300 000 käyttäjään vaikuttava häiriö) vaikutti arki-iltana hetkellisesti Yle TV1 -kanavan toimivuuteen.

15.7

Valmiuslain (706/2022) poikkeusolomääritelmää on täydennetty 15.7.2022. Siinä otetaan aikaisempaa kattavammin huomioon erilaiset hybridiuhat uudessa 3 §:n 6 kohdassa.

30 MILJARDIA

Sertifiointiorganisaatio TÜV SÜD ennustaa IoT-laitteiden määrän nousevan 30 miljardiin vuoteen 2025 mennessä. TÜV on alkanut tarjota sertifiointimerkkiä laitteen kyberturvallisuuden tason osoittamiseksi.

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.

Symbolit

Uusi

Päivitetty

4

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

5

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

TRAFICOM

11.8.2022

1. Talouden ja politiikan ilmiöt heijastuvat myös kyberturvallisuuteen

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

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

CASE

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

2. 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 riskianalyysejä, tutkimuksia ja ohjeistusta.(1)

3. Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon

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

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

CASE

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

4. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

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

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

CASE

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

5. Käyttöoikeudet ovat avaimet organisaatioon

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

- Tunnuskalastelua tehdään monella eri tavalla ja eri laitteiden kautta. Sitä kohdistetaan sekä organisaatioihin että yksityishenkilöihin. Tunnuksia ja niihin liittyviä salasanoja yritetään lisäksi aktiivisesti murtaa automaattisin työkaluin. Jos avaimet viedään, tulee asiaan reagoida välittömästi!
- On hyvä pohtia, millaiset käyttöoikeudet omilla työntekijöillä tai ulkoistetuilla palveluntarjoajilla on yrityksen hallussa olevaan tietoon. Organisaation käyttäjillä tulee olla mahdollisimman rajoitetut, kuten perustason, käyttöoikeudet. Pääkäyttäjä-tason oikeuksien käyttö tulee olla erityisen suojattua ja kontrolloitua.
- Organisaation tietoturva tulee olla ratkaistuna niin, että teknisten kontrolleiden tulee estää ja havaita tunnusten väärinkäytökset. Siksi on tärkeää, että esimerkiksi monivaiheinen tunnistautuminen (MFA) on käytössä.[(2)] [(3)]

OHJE

Jos käyttöoikeudet joutuvat vääriin käsiin, tulee toimia nopeasti.

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

Tietomurrot ja -vuodot

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

Tietomurrot ja -vuodot

- Web-palvelimien tietomurrot.
  - Haavoittuvia tai päivittämättömiä web-palvelimia murretaan jatkuvasti.
  - Murrettuja palvelimia voidaan käyttää väärin useilla eri tavoilla esimerkiksi palvelunestohyökkäyksiin, tietojen kalasteluun tai haittaohjelmien levittämiseen.

Analyysi

- Ympäristöjen koventamisen ja palveluiden turvaamisen lisäksi myös käyttöoikeuksien rajaaminen ja käyttäjätilien turvaaminen on tärkeää.
- Monivaiheisen tunnistautumisen käyttöönotto voi ehkäistä aiheetonta pääsyä järjestelmiin.
- Tietomurtojen seurauksena tapahtuu myös kiristyshaittaohjelmahyökkäyksiä.[(3)] [(4)]

Tietomurrot ja -vuodot

- Kaksi suomalaista organisaatiota kiristyshaittaohjelman kohteena.
  - Suomen Tietotoimisto STT ja Wärtsilä ovat kertoneet julkisuuteen joutuneensa tietomurron ja sitä seuranneen kiristyshaittaohjelman kohteeksi.
  - Hyökkäysten tekijäksi on ilmoittautunut sama LV Group- kyberrikollisryhmittymä.
  - Poliisi tutkii STT:n asiaa tietomurtona ja tietojärjestelmän häirintänä.(5)
  - Myös Wärtsilä on ollut tietomurron seurauksena yhteydessä viranomaisiin.

Analyysi

- Riski kiristyshaittaohjelman kohteeksi joutumisesta on kasvanut viime vuosina merkittävästi.
- Lunnaiden maksamista ei voida suositella. On mahdollista, että tietoa ei saada takaisin, vaikka lunnaat päätyisikin maksamaan.
- Kiristyshaittaohjelmahyökkäys on aina kriisi organisaatiolle.
- Kyberturvallisuuskeskus on julkaissut organisaatioiden johdolle ohjeen kiristyshaittaohjelmien varalta.(6)

Huijaukset ja kalastelut

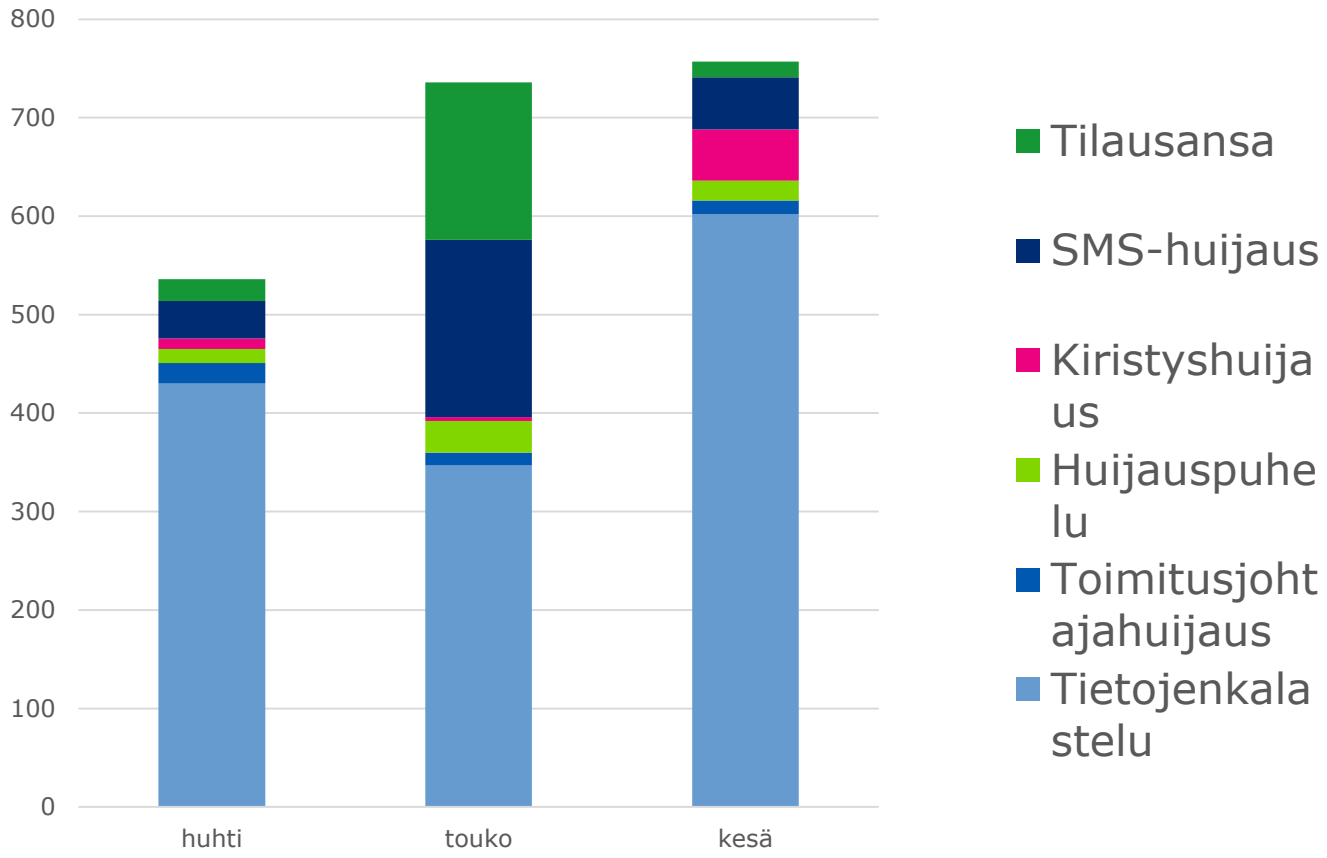
Huijauksiin ja tietojenkalasteluun sisältyy käyttäjätunnusten ja salasanojen kalastelua, laskutuspetoksia, yrityshuijauksia, kiristyksiä ja muita vastaavia huijauksia. Lisäksi organisaatioihin voi kohdistua pankkitunnuskalastelua, maksukorttikalastelua ja muita geneerisiä yksittäisten uhrien huijauksia.

Huijaukset ja kalastelut

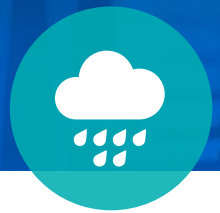
- Heinäkuussa oli liikkeellä pankkitunnusten kalastelua vaihtelevilla teemoilla.
  - Tekstiviestejä käytetään pankkitunnuskalasteluun yhä useammin.
  - Huijausviestien aiheita yhdistää linkki väärennetylle pankkitunnistautumissivulle, jolla rikollinen kalastelee pankkitunnukset.
  - Huijausviestejä on lähetetty pankkien lisäksi myös verottajan, kelan, vakuutusyhtiöiden, teleoperaattoreiden ja eri viranomaisten nimissä.
  - Huijari yhdistelee eri teemoja luovasti ja mielikuvituksellisesti: uusimmissa huijausviesteissä Valtioneuvosto lupailee veronpalautuksia.
  - Kyberturvallisuuskeskus julkaisi 9.8.2022 tiedotteen veronpalautusteemaisista huijauksista.(7)

- **Poliisin nimeä on käytetty huijauksiin**
  - Sähköpostissa on liikkunut huijausviestejä, joita on väärennetty näyttämään lähetetyiksi Poliisihallituksesta, Keskusrikospoliisista, tai oikeuslaitokselta.
  - Viesteissä väitetään vastaanottajan syyllistyneen erilaisiin vakaviin rikoksiin ja syytteistä vapautumiseksi vaaditaan rahalunnaita.
  - Uhkauksen tehosteena on virallisen näköinen dokumenttiliite värikkäine leimoineen ja poliisin logoineen.
  - Vastaavia huijauksia on nähty muuallakin Euroopassa.

Käsiteltyjä huijaustapauksia Q2/2022



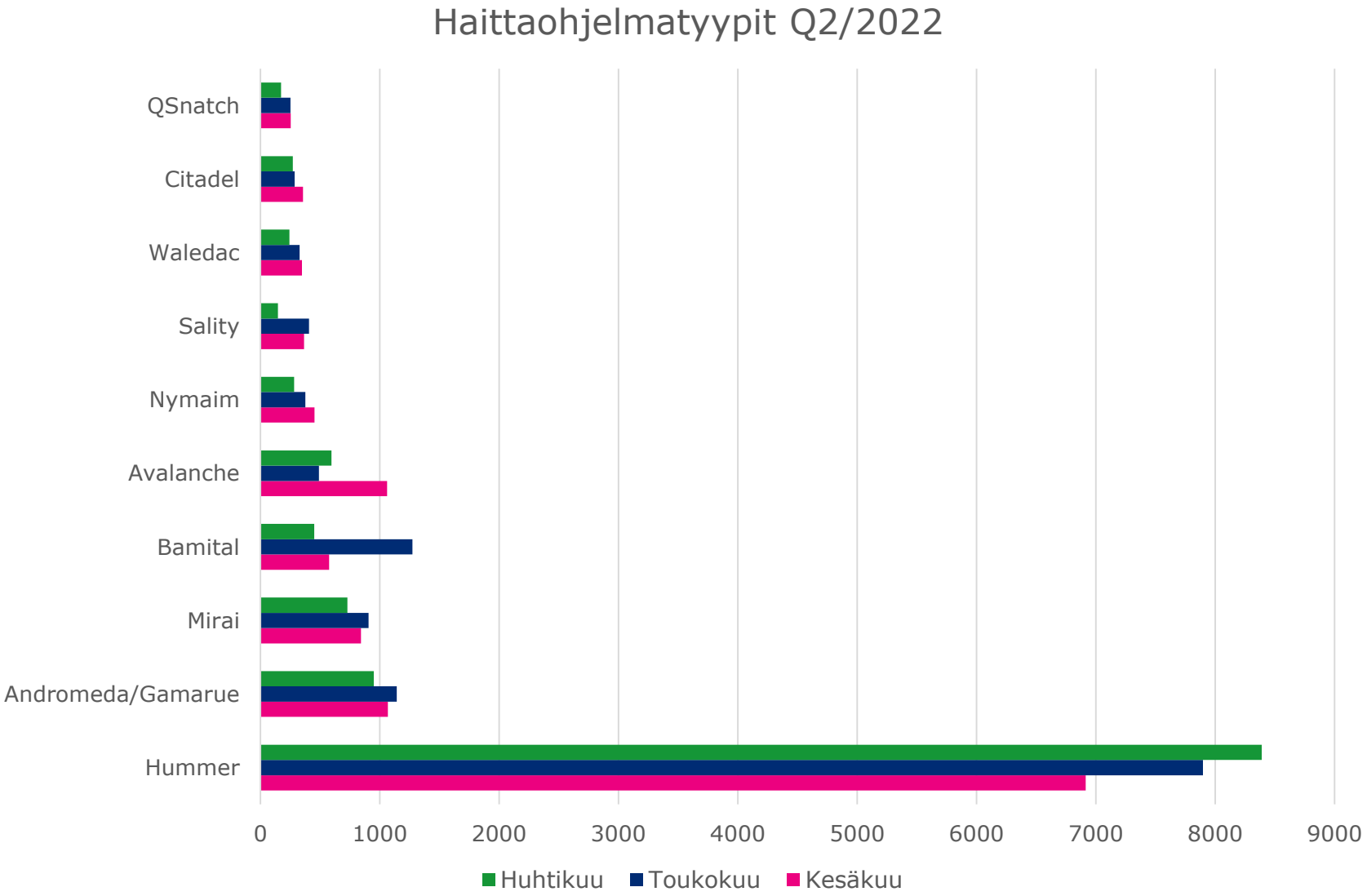
- Vuoden 2022 toisen neljänneksen ilmiöitä ovat:
  - Pankkitunnusten kalastelu ja tilausansat ovat jatkuneet aktiivisina.
  - Toukokuun SMS-huijausten piikki johtui taustakuva- ja pelipalveluaiheisista tilausansoista.
  - Huijauspuheluiden määrä on pysynyt edelleen matalana.
  - Ilmoitettujen toimitusjohtajahuijausten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



Haittaohjelmat ja haavoittuvuudet

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

Autoreporterin haittaohjelmahavainnot



Torjumme haittaohjelmia yhteistyössä teleyritysten kanssa Autoreporter-järjestelmän avulla. Järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta. Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen.

Tilastossa kerromme 10 yleisintä ja nimettyä haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla.(8)

Kuukauden haavoittuvuusjulkaisut

- Vakava haavoittuvuus Samba-palvelinohjelmistossa (12/2022).
  - Haavoittuvuus vaatii toimia palveluiden ylläpitäjiltä, ja on suositeltavaa päivittää eri ympäristöjen Sambat mahdollisimman pian uuteen korjattuun versioon.
- Kriittiseksi luokiteltu VMware-päivityspaketti korjaa haavoittuvuuksia useista tuotteista (13/2022).
- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

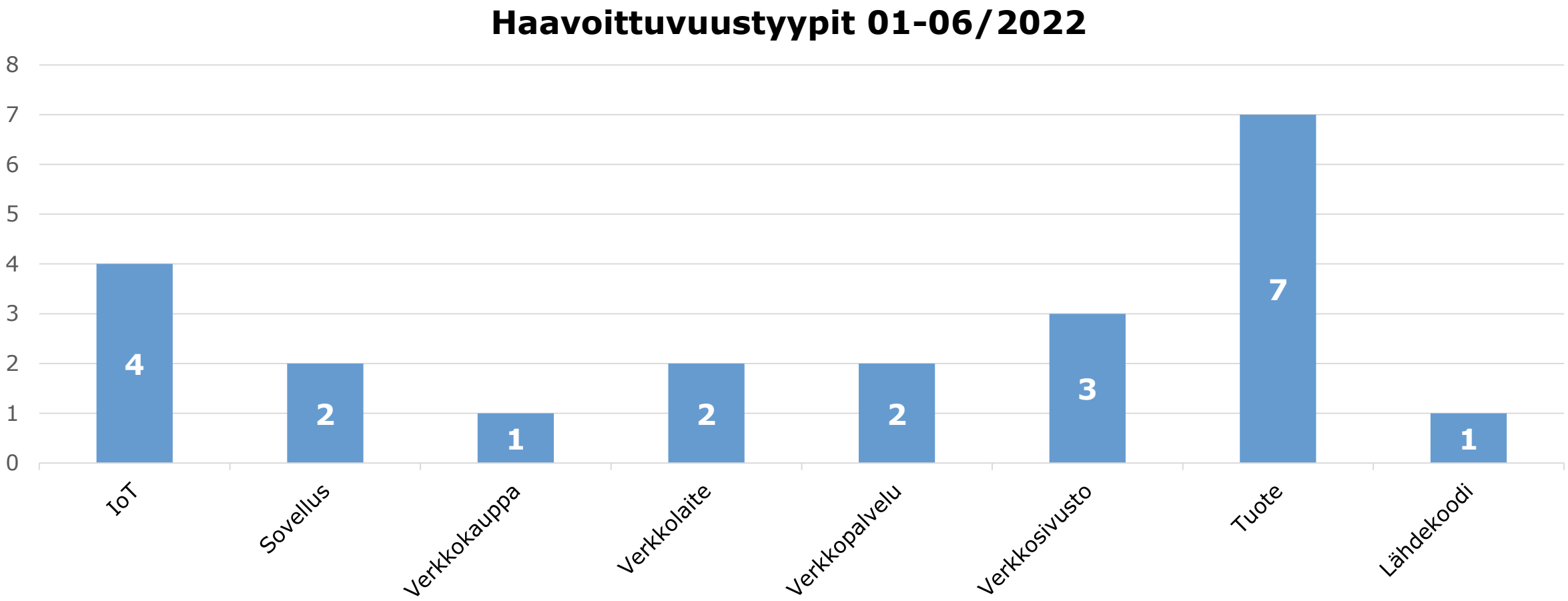
- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta.**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn.
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta.**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta.
- **Haavoittuvuustiedotteita tänä vuonna 13 kpl (tilanne 11.8.2022).**
  - Mukana mm. Microsoft Exchange Server ja etäkäyttötoteutusten haavoittuvuudet.
- **Tilaamalla haavoittuvuuskoosteen saat tietoa erilaisista haavoittuvuuksista.**
  - Kaikista haavoittuvuuksista ei julkaista suomenkielistä haavoittuvuustiedotetta.
  - Kooste julkaistaan lähes päivittäin ja sen voi tilata kotisivuiltamme: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

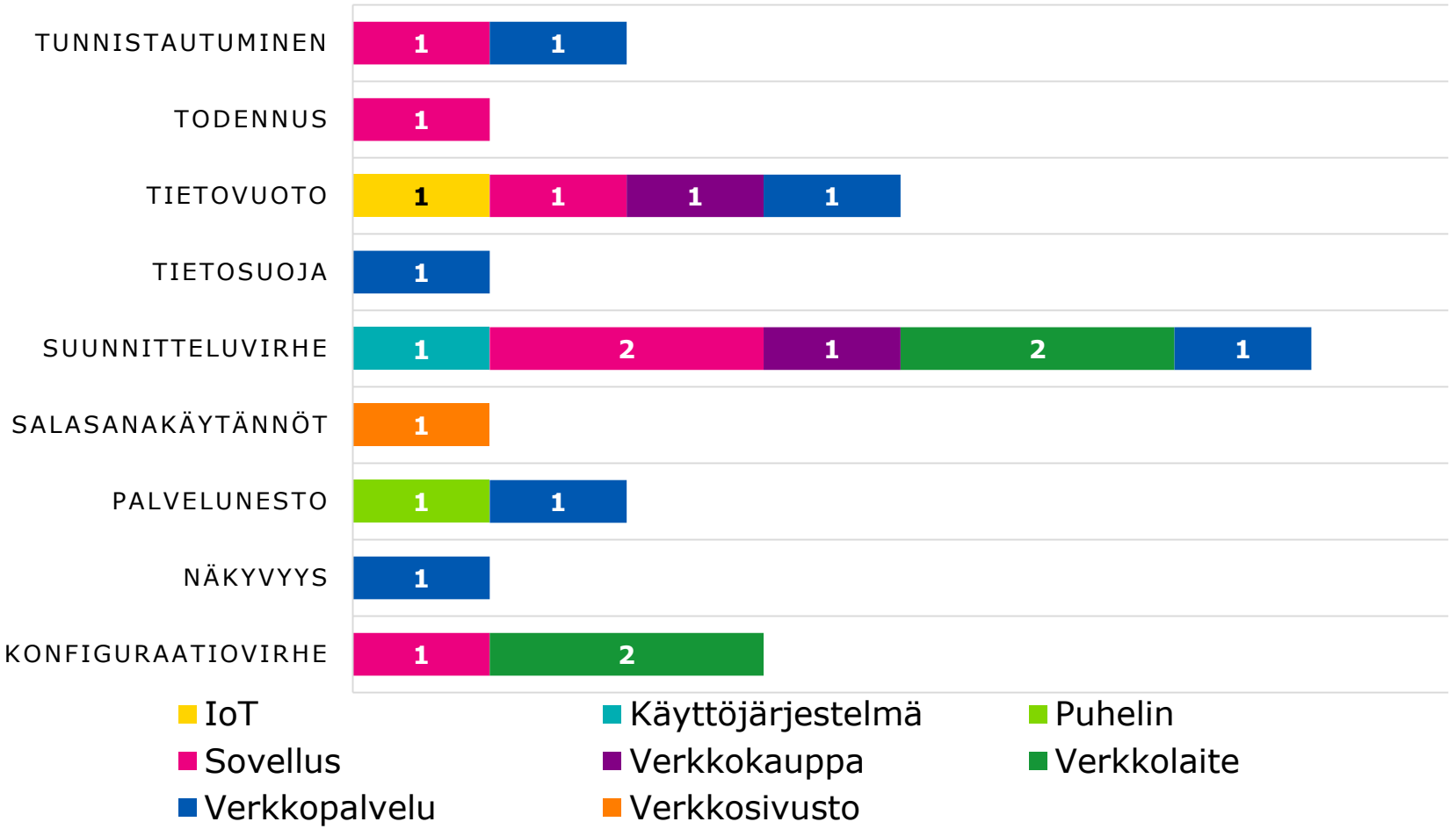
- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat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

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

6kk



Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio



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

Haavoittuvuuskoordinaatiota on esitelty laajemmin verkkosivuillamme.(9)

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

- Saksalainen standardointiorganisaatio TÜV SÜD ennustaa IoT-laitteiden määrän nousevan 30 miljardiin vuoteen 2025 mennessä. Se tarkoittaa samalla laitteisiin liittyvien kyberriskien kasvamista mahdollisten haavoittuvuuksien ja suunnitteluvirheiden lisääntyessä.
- TÜV SÜD kertoo valmistajille, että kyberturvallisuus on tärkeää kuluttajien laitteissa ja ilman riittävää suojausta valmistajat saattavat joutua ongelmista vastuuseen.
- TÜV SÜD:n mukaan riittävä suojaus saadaan noudattamalla kyberturvallisuusstandardeja ja -määräyksiä sekä kansallisia lakeja.
- TÜV on alkanut tarjota Cybersecurity Certified -sertifiointimerkkiä (TÜV CSC), jolla osoittaa laitteen kyberturvallisuuden tasoa.(10) (11) (12)

Analyysi

- Tuotteiden turvallisuus nähdään kilpailuetuna, ja yhä useammat tuotevalmistajat haluavat erottua joukosta hankkimalla tuotteilleen tietoturvasertifikaatin.
- Traficomin, Singaporen CSA:n ja Saksan BSI:n tietoturvamerkit käyttävät samoja ETSI EN 303 645 -standardiin perustuvia tietoturvavaatimuksia kuin TÜV SÜD:n CSC.
- Laitetta ostaessa kannattaa valita tietoturvasertifioitu tuote, jos mahdollista. Sertifiointi etenee ja yhä useammasta tuotteesta löytyy tietoturvasertifikaatti.

IoT

- Uusiin ja vanhoihin rakennuksiin lisätään IoT-järjestelmiä ja antureita energiankulutuksen vähentämiseksi ja käyttökustannuksien leikkaamiseksi.
- Kaikki älylaitteet, kuten älytermostaatit tulee ottaa hallitusti käyttöön muokkaamalla niiden oletusasetukset tarkoituksenmukaisiksi.(13)
- Nozomi Networks julkaisi rakennusautomaation tietoturvahaasteita kuvaavan raportin.(14)
  - Turvattomasti liitetyt tai konfiguroidut laitteet lisäävät kyberhyökkäysten pinta-alaa ja tarjoavat mahdollisuuksia pahantekoon.
  - Rakennusautomaatiolaitteiden suuri määrä ja monimuotoisuus, selkeä järjestelmien omistajan puute ja riittämätön resursointi tuovat lisähaasteita laitteiden turvaamiseen.

Analyysi

- Energian hinnannousu on kannustanut ihmisiä ja taloyhtiöitä ottamaan käyttöön älykotiratkaisuja, joilla seurata sähkön kulutusta ja säästää energiaa.
- Rakennusautomaatiojärjestelmät muodostavat toistuvasti suurimman osan Kyberturvallisuuskeskuksen havaitsemista suojaamattomista automaatiojärjestelmistä.(15)
- Rakennusautomaatiojärjestelmien omaisuuden hallinta on käytännössä välttämätöntä, jotta kaikki laitteet saadaan pidettyä turvallisina ja käyttökykyisinä.
- Omaisuudenhallintajärjestelmään on hyvä lisätä tieto laitteen ohjelmistopäivityksistä, haavoittuvuuksista sekä laitteiden fyysisestä ja loogisesta sijainnista.
- Kyberturvallisuuskeskukselta löytyy vinkkejä rakennusautomaatiojärjestelmien suojaamiseen.(16)

Automaatio

- Tietoturvayhtiö Dragos julkaisi artikkelin automaatioympäristöihin suunnatusta haittaohjelmasta.(17)
  - Useilla sosiaalisen median tileillä mainostetaan ohjelmia, joiden väitetään osaavan murtaa unohtuneita automaatioympäristöjen salasanoja.
  - Tämän tyyppisille ohjelmille saattaa olla tarvetta esimerkiksi silloin, kun vuosia sitten jo pois lähteneen työtekijän tekemiin automaatio-ohjelmiin pitäisi tehdä muutoksia ja salasana on unohtunut.
  - Kyberrikolliset ovat oivaltaneet tämän muodostavan yhden pääsyn automaatioympäristöihin. Rikolliset ovat jakaneet muokattua salasananmurto-ohjelmaa, joka on myös saastutettu Sality-haittaohjelmalla.
  - Haittaohjelmatartunnan jälkeen salasanaa murtaneen automaatioinsinöörin työasema liittyy botnetin osaksi muodostaen suuren riskin kyseille automaatioympäristölle.

Analyysi

- Kyberrikolliset pyrkivät löytämään uusia ja luovia tapoja tavoitteidensa saavuttamiseksi.
- Vaikka automaatioympäristö olisikin hyvin suojattu verkosta tulevia hyökkäyksiä vastaan, rikollinen voi saavuttaa tavoitteensa kohdistamalla toimintaa suoraan automaatioinsinöörien tyypillisiin tehtäviin
- Tuntemattomista lähteistä ladattaviin sovelluksiin tulisi aina suhtautua suurella varoivaisuudella. Vaikka tietoturva-asiantuntija ei haksahtaisi, niin ei tietoturva-taustainen henkilö voi nähdä tämän tyyppisen sovelluksen vain näppäränä ratkaisuna käsillä olevaan ongelmaan.
- Organisaatioiden olisi hyvä muistuttaa työntekijöitä internetistä ladattavien sovellusten vaaroista.
- Kaikkien organisaatiossa käytettävien sovellusten tulisi kulkea hyväksymisprosessin läpi, jossa tarkasteltaisiin myös niiden tietoturvavaikutukset.

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 verkot toimivat vakaasti.
  - Poikkeamien vakavuusluokat: A: 1, B: 0, C: 1
- A-vika (yli 300 000 käyttäjää) vaikutti arki-iltana hetkellisesti Yle TV1 -kanavan toimivuuteen.
  - Laitevian aiheuttama katkos vaikutti Uuttamaata lukuun ottamatta koko Suomeen.(18)
- Kiinteän laajakaistan kuitupäätelaitteissa ongelmia.
  - Suomessa eri operaattoreilla edelleen käytössä olevissa yli viisi vuotta vanhoissa Inteno FG500 -laitteissa on havaittu palvelunestotilan aiheuttava ohjelmistovirhe.(19)
  - Valmistaja, operaattorit ja Kyberturvallisuuskeskus tekevät yhteistyötä ongelman korjaamiseksi.
  - Tällä hetkellä uusien päätelaitteiden saatavuus voi olla heikko.

Analyysi

- Heinäkuussa ei raportoitu yhtäkään tavanomaista merkittävää häiriötä, joka olisi vaikuttanut mobiili- tai internetyhteyksiin.
- Yleensä erilaiset huoltokatkot, sähkökatkot, muutostyöt tai luonnonilmiöt aiheuttavat joitakin merkittäviä häiriöitä kuukausitasolla.
- Kuukaudessa tapahtuu keskimäärin noin kuusi merkittävää toimivuushäiriötä.

ICT-palveluiden toimivuus

- Meripelastuksen hälytysnumerossa oli häiriö 20.7.
  - Asiasta tiedotettiin kansalaisia myös 112-sovelluksessa.
  - Vika koski koko Suomea ja haittasi puheluita meripelastuksen hätänumeroon kaikilla merialueilla.(20)
- Microsoft Teams -palvelussa ongelmia 21.7.(21)
  - Vian syy johtui konfiguraatiomuutoksesta, joka aiheutti yhteyskatkoksen Teamsin infrastruktuurissa.

Analyysi

- Teamsin katkos tapahtui kesälomakaudella ja Euroopan kannalta suotuisasti yöaikaan.
  - Katkos laajalti käytetyssä palvelussa kesken työpäivän vaikuttaisi monien organisaatioiden työskentelyyn.
  - The Registerin artikkelissa mainitaan australialaisen organisaation viestineen Twitterissä, että he ovat viasta johtuen poikkeuksellisesti tavoitettavissa vain sähköpostitse.
  - Tapaus osoittaa, kuinka australialaisen hevosurheiluun liittyvän organisaationkin on syytä varautua erilaisiin poikkeustilanteisiin IT-palveluissa.

Palvelunestohyökkäykset

- Heinäkuu oli palvelunestohyökkäysten osalta rauhallinen.
  - Vastaanotimme yksittäisiä ilmoituksia, joissa vaikutukset onnistuttiin torjumaan, tai vaikutukset olivat pieniä.
- Kansainvälisistä aktiviteeteistä huolimatta Suomea kohtaan ei kohdistunut merkittäviä hyökkäyksiä heinäkuussa.
  - Kerroimme viime kybersäässä, kuinka Killnet-ryhmittymä on tehnyt palvelunestohyökkäyksiä Liettuaan ja Norjaan kesäkuun lopulla.
  - Organisaatiot Suomessa ovat suojautuneet volumetrisiin hyökkäyksiin hankkimalla suodatuskyvykkyyttä palveluntarjoajilta.
  - Muistutamme myös tarkistamaan, kuinka organisaationne on suojautunut sovellustason palvelunestohyökkäyksiltä.

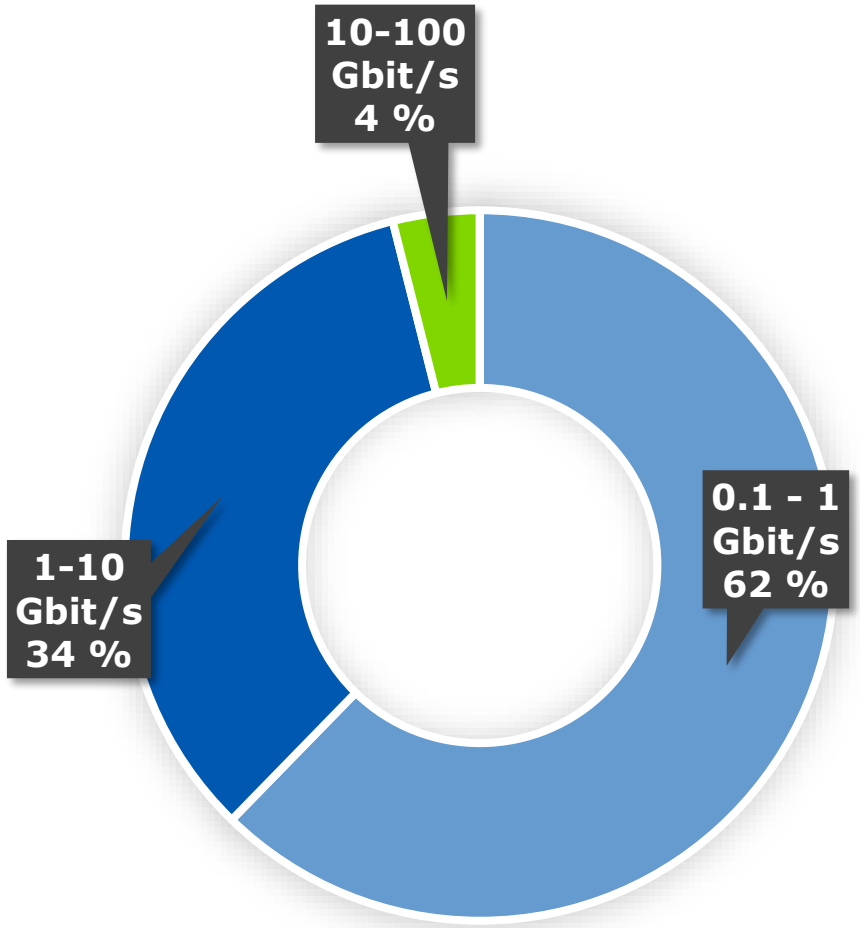
Analyysi

- 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. Siten pystymme ohjeistamaan organisaatioita hyökkäyksiin varautumisessa.

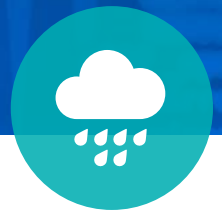
Palvelunestohyökkäysten tunnuslukuja

3kk

- 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

- Iranin hallintoon liitetty toimija hyökkäsi Albanian valtionhallinnon digitaalisiin palveluihin kiristyshaittaohjelmalla.(22)
  - Palvelut ovat olleet käyttökelvottomia useita viikkoja.
  - Albanialaiseksi tekeytyvä valepersoona on ottanut vastuun hyökkäyksestä. Todellisuudessa hyökkäyksen uskotaan olevan Iranin hallinnon tekemä.
- Hyökkäyksen uskotaan liittyvän Albaniassa järjestettyyn iranilaisten toisinajattelijoiden konferenssiin.
- Albanian valtiohallinnon järjestelmät yhdistettiin toukokuussa yhteiselle alustalle, mikä omalta osaltaan mahdollisti häiriöiden laaja-alaisuuden.

Analyysi

- On täysin poikkeuksellista, että valtiollinen toimija aiheuttaa toiminnan estämiä häiriöitä NATO-maan valtiohallinnon tietojärjestelmiin.
- Tapaus osoittaa huolestuttavan eskalaation Iranin hallinnon valmiudessa tehdä tietoja tuhoavia kyberhyökkäyksiä.

Vakoilu

- Pohjois-Korean hallintoon liitetyt hyökkääjät ovat aktiivisia.
  - Hyökkääjiä on useita eri ryhmiä ja ne käyttävät eri haittaohjelmia. Uhreja on ollut myös useissa Euroopan maissa.(23)
  - Osassa tunkeutumisista on hyödynnetty aiemmin tuntemattomia haitallisia selainten lisäosia nimeltä SHARPEXT.(24)
  - Osassa hyökkäyksistä tavoitteena on ollut kiristyshaittaohjelmien levittäminen.(25)
- Lunnaiden maksaminen EU sanktioiden kohteena oleville tahoille, kuten Pohjois-Korean hallintoon liitetyille hyökkääjille, saattaa johtaa EU lainsäädännön perusteella seuraamuksiin maksajalle.

Analyysi

- Myös muihin maihin kuin Venäjään liitetyt hyökkääjät jatkavat tunkeutumisiaan aktiivisesti.
- Erityisesti Pohjois-Koreaan ja Iraniin liitetyistä ryhmistä on ollut havaintoja viime aikoina.

Vakoilu

- Venäjän tiedustelupalveluun liitetty toimija jatkaa tunkeutumisyrityksiään.(26)
  - Tietoturvayritys Palo Alton mukaan uhkatoimija Cloaked Ursa, joka tunnetaan myös nimillä Nobelium, Cozy Bear ja APT29, on jatkanut eri maiden valtionhallintoihin kohdistuneita tunkeutumisyrityksiään.
  - Tunkeutumisyrityksissä on hyödynnetty DropBox ja Google Drive -palveluita haittaohjelmien jakamiseen.
- EU julistaa paheksuvansa vahvasti Venäjän vihamielisiä toimia kybertoimintaympäristössä.(27)

Analyysi

- Venäjän tiedustelu- ja turvallisuuspalveluihin liitetyt tunkeutujat jatkavat hyökkäyksiään aktiivisesti. Useat länsimaihin kohdistuvat operaatiot eivät liity Venäjän hyökkäykseen Ukrainaan, vaan ovat jatkoa aiempaan vihamieliseen toimintaan.
- Venäjä-mielisten haktivistiryhmien toiminta puolestaan on lisääntynyt helmikuussa alkaneen hyökkäyksen jälkeen. Näillä hyökkäyksillä voi olla myös ennalta-arvaamattomia seurannaisvaikutuksia.

Vakoilu

- Kaupallinen kybervakoilupalvelutarjoaja KNOTWEED on käyttänyt nollapäivähaavoittuvuuksia hyökkäyksissään.(28)
  - Microsoft julkaisi kattavan selvityksen itävaltalaisen kybervakoilupalvelutarjoajan DSIRF käyttämästä Subzero työkalusta. Microsoft käyttää yrityksestä nimitystä KNOTWEED.
  - Yrityksellä oli käytössään useita Windows- ja Adobe-tuotteisiin suunnattuja nollapäivähaavoittuvuuksia hyödyntäviä hyväksikäyttömenetelmiä. Haavoittuvuudet on korjattu heinäkuun korjauspäivityksissä.
- EU komission virkamiesten puhelimista on löytynyt viitteitä Pegasus-haittaohjelmasta.(29)
  - Pegasus on israelilaisen NSO-yrityksen käyttämä mobiililaitteisiin tunkeutumiseen käytetty haittaohjelma.
  - Pegasus on liitetty vuoden aikana useisiin vakoilutapauksiin Euroopassa, mukaan lukien Suomi. Nyt julkaistu havainto liittyy viime vuonna julkisuuteen nousseeseen kokonaisuuteen.
  - Komissio on ilmaissut huolensa näiden tuotteiden väärinkäytöstä.

Analyysi

- Useat yritykset myyvät haittaohjelmia eri valtioiden viranomaisille. Näiden haittaohjelmien käyttöön viranomaisten toimesta on paljastunut useita kyseenalaisia käyttötapauksia.
- Vastaavia tuotteita ja palveluita on tarjolla myös kaupallisille yrityksille. Näiden palvelujen käyttöä koskevat samat eettiset ja moraaliset kysymykset kuin haittaohjelmien käyttöön viranomaisten toimesta.

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

- Valmiuslain muutos (706/2022) tuli voimaan 15.7.2022.
  - Lain poikkeusolomääritelmää on täydennetty siten, että siinä otetaan aikaisempaa kattavammin huomioon erilaiset hybridiuhat (uusi 3 §:n 6 kohta).
  - Huomattava osa lain toimivaltuussäännöksistä voi tulla sovellettavaksi uuden määritelmän mukaisissa poikkeusoloissa, minkä lisäksi lakiin tehtiin muita muutoksia.(30)
  - Oikeusministeriö on lisäksi käynnistämässä valmiuslain kokonaisuudistuksen, jonka tavoitteena on saattaa laki vastaamaan nykyaikaista käsitystä yhteiskunnan kokonaisturvallisuudesta ja sitä uhkaavista tekijöistä.(31)

Oikeudelliset asiat

- Ajankohtaista Tietosuojavaltuutetulta.
  - Sijoituspalvelujen tarjoajalle huomautus tietosuojasäännösten vastaisesta käytännöstä tunnistamiseen tarvittavien tietojen pyytämisessä.(32)
  - Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat antaneet yhteisen lausuntonsa komission eurooppalaista terveysdata-avaruutta koskevasta ehdotuksesta.(33)

Arjen kyberturvallisuus

Tietoturvamerkki – turvallisen arjen puolesta

- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen myöntämä Tietoturvamerkki kertoo, että merkillä varustettu tuote tai palvelu on suunniteltu tietoturvalliseksi ja täyttää Traficomin asettamat tietoturvavaatimukset.
- Merkkiä käytetään älykkäissä kuluttajalaitteissa, jotka yhdistetään internetiin eli ns. IoT-laitteissa.
- Lue lisää: https://tietoturvamerkki.fi/fi/

Muista etätyön tietoturvallisuus lomilta palatessa

- Pienillä arjen kyberteoilla kotona työskentely on turvallista kaikille.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/etatyon-tietoturva-ohjeita-tyontekijoille

Koulut alkavat – lapsille tarjolla tietoturva-asiaa pelin muodossa

- Spoofy on vuonna 2019 julkaistu alakouluikäisille sopiva mobiilipeli. Peli valmentaa lapsia suojautumaan esimerkiksi nettikiusaamiselta ja huijausviesteiltä.
- Peli opettaa hauskalla ja innostavalla tavalla myös salasanoihin, yksityisyyteen sekä netin käytöstapoihin liittyviä digitaalisen turvallisuuden perustaitoja.
- Tutustu Spoofy-peliin: https://www.spoofy.fi/ ja muihin lasten materiaaleihin https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tekemista-lapsille

Uutisia Kyberturvallisuuskeskuksesta

Onnistunut kyberharjoitus alkaa huolellisella valmistautumisella

- Vuoden 2022 kyberharjoitusteemaisten artikkeleiden sarja jatkuu.
- Kyberharjoitusten valmisteluun liittyvässä artikkelissa käydään läpi, mitä tulisi ottaa huomioon ennen harjoittelun aloittamista.
- Tutustu artikkeliin ja ohjeisiin täältä: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/onnistunut-kyberharjoitus-alkaa-huolellisella-valmistautumisella

Tietoturvamerkki-seminaari 29.9.2022

- Kuluttajille suunnattujen älylaitteiden tietoturvaan tulee uusia vaatimuksia 1.8.2024 alkaen.
- Kyberturvallisuuskeskus järjestää 29.9.2022 klo 13 tilaisuuden, jossa keskuksen asiantuntijat kertovat uudesta 1.8.2024 voimaan tulevasta älylaitteiden tietoturvaa koskevasta sääntelystä.
- Tilaisuudessa kuulemme myös Euroopan komission, Googlen, Polar Electron ja SOK:n asiantuntijoiden näkemyksiä Security by designista ja vastuullisuudesta.
- Seuraa tapahtuman sivua, johon ilmestyy ilmoittautumislinkki lähempänä tapahtumaa: https://www.kyberturvallisuuskeskus.fi/fi/tietoturvamerkki-seminaari-2992022

Digi- ja väestötietovirasto kokoaa digituen verkostotyön ja kehittämisen sanaston

- Tarkoituksena on tunnistaa digituen verkostotyön ja kehittämisen keskeinen sanasto sekä luoda käsitteille selkeät kuvaukset.
- Sanastolla pyritään kohti selkeämpää kieltä. Sanasto julkaistaan yhteistoimivuusalustalla osoitteessa, jossa se on kaikkien vapaassa käytössä.
- Tarkoituksena on, että sanastoa voidaan jatkossa päivittää vastaamaan ajankohtaisia tarpeita.
- Tutustu tiedotteeseen: https://dvv.fi/-/digituen-verkostotyon-ja-kehittamisen-sanaston-kokoaminen-alkaa-

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) ISAC-tiedonvaihtoryhmät https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

2) Suojautuminen Microsoft Office 365 -tunnusten kalastelulta ja tietomurroilta https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/suojautuminen-microsoft-office-365-tunnusten-kalastelulta-ja-tietomurroilta

3) Opas tietomurtojen havaitsemiseen https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/opas-tietomurtojen-havaitsemiseen

4) Verkkopalvelun ohjelmistoalustan valinta ja palvelun turvallinen ylläpito https://www.kyberturvallisuuskeskus.fi/fi/verkkopalvelun-ohjelmistoalustan-valinta-ja-palvelun-turvallinen-yllapito-ohje-12011

5) Poliisi aloitti esitutkinnan STT:hen kohdistuneesta verkkohyökkäyksestä https://yle.fi/uutiset/3-12558950

6) Toiminta kiristyshaittaohjelmatilanteessa - johdon ohje https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/toiminta-kiristyshaittaohjelmatilanteessa-johdon-ohje

7) Veronpalautukset tulevat ja rikolliset yrittävät saada niistä osansa https://www.kyberturvallisuuskeskus.fi/fi/ttn_08082022

8) Autoreporterin haittaohjelmahavainnot https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot

Lähdeluettelo

9) Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-haavoittuvuuskoordinaatio-pahkinankuoressa

10) TÜV SÜD CyberSecurity Certified (CSC) Certification https://www.tuvsud.com/en/-/media/global/pdf-files/infographics/tuvsud-infographic-cybersecurity-certified-csc-certification.pdf

11) Internet of Things (IoT) for a connected world - IoT cyber security threats and regulations https://www.tuvsud.com/en/-/media/global/pdf-files/whitepaper-report-e-books/tuvsud-internet-of-things-for-a-connected-world.pdf

12) TÜV SÜD Cybersecurity certified (csc) certification https://www.tuvsud.com/en/services/product-certification/ps-cert/tuv-sud-csc-certification-scheme

13) Smart thermostat swarms are straining the US grid https://www.theregister.com/2022/07/13/smart_thermostat_strain/

14) Solving Cybersecurity for Building Management Systems https://www.nozominetworks.com/downloads/US/Nozomi-Networks-Solving-Cybersecurity-for-BMS-ebook.pdf

15) Noin 1000 automaatiolaitetta on yhä suojaamatta suomalaisissa verkoissa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/noin-1000-automaatiolaitetta-yha-suojaamatta-suomalaisissa-verkoissa

Lähdeluettelo

16) Kuka sammutti valot? Puutteellinen rakennusautomaatiolaitteiden suojaus verkossa altistaa kyberuhille https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kuka-sammutti-valot-puutteellinen-rakennusautomaatiolaitteiden-suojaus-verkossa

17) The Trojan Horse Malware & Password "Cracking" Ecosystem Targeting Industrial Operators https://www.dragos.com/blog/the-trojan-horse-malware-password-cracking-ecosystem-targeting-industrial-operators/

18) Yle TV1:n HD-kanavan toistossa oli laaja katkos keskiviikkoiltana – syynä laitevika https://yle.fi/uutiset/3-12526746

19) Savolainen tietoverkkoyhtiö epäilee asiakkaiden yhteysongelmien syyksi kyberhyökkäystä – koskee myös muita operaattoreita https://yle.fi/uutiset/3-12536783

20) Meripelastuksen hälytysnumeron vika korjattu https://yle.fi/uutiset/3-12543484

21) Microsoft Teams outage widens to take out M365 services, admin center https://www.theregister.com/2022/07/21/teams_outage/

22) Likely Iranian Threat Actor Conducts Politically Motivated Disruptive Activity Against Albanian Government Organizations https://www.mandiant.com/resources/likely-iranian-threat-actor-conducts-politically-motivated-disruptive-activity-against?1

23) New Attack Campaign Observed Possibly Linked to Konni/APT37 (North Korea) https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/

Lähdeluettelo

24) SharpTongue Deploys Clever Mail-Stealing Browser Extension “SHARPEXT” https://www.volexity.com/blog/2022/07/28/sharptongue-deploys-clever-mail-stealing-browser-extension-sharpext/

25) North Korean threat actor targets small and midsize businesses with H0lyGh0st ransomware https://www.microsoft.com/security/blog/2022/07/14/north-korean-threat-actor-targets-small-and-midsize-businesses-with-h0lygh0st-ransomware/

26) Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/

27) Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia’s aggression against Ukraine https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/

28) Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits https://www.microsoft.com/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/

Lähdeluettelo

29) EXCLUSIVE EU found evidence employee phones compromised with spyware –letter https://www.reuters.com/technology/exclusive-eu-found-evidence-employee-phones-compromised-with-spyware-letter-2022-07-27/

30) HE 63 2022 https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_63+2022.aspx

31) Valmiuslaki uudistuu https://oikeusministerio.fi/valmiuslaki-uudistuu

32) Sijoituspalvelujen tarjoajalle huomautus tietosuojasäännösten vastaisesta käytännöstä tunnistamiseen tarvittavien tietojen pyytämisessä https://tietosuoja.fi/-/sijoituspalvelujen-tarjoajalle-huomautus-tietosuojasaannosten-vastaisesta-kaytannosta-tunnistamiseen-tarvittavien-tietojen-pyytamisessa

33) Lausunto: Eurooppalaisen terveysdata-avaruuden on varmistettava sähköisten terveystietojen vahva suoja https://tietosuoja.fi/-/lausunto-eurooppalaisen-terveysdata-avaruuden-on-varmistettava-sahkoisten-terveystietojen-vahva-suoja