TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Joulukuu 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

12.1.2023

Kybersää joulukuu 2022

Tietomurrot ja -vuodot

- Sosiaalisen median tilien kaappaukset ovat edelleen arkipäivää.
- Microsoftin Exchange haavoittuvuutta käytetään aktiivisesti kiristyshaittaohjelmien järjestelmään saamisessa.

Huijaukset ja kalastelut

- Pankkikalasteluissa .fi-verkkotunnukset ovat harvinaisia poikkeuksia. Suurin osa huijauksista käyttää edelleen kansainvälisiä verkkopäätteitä.
- Toimitusjohtajahuijauksia on yritetty ahkerasti, mutta onneksi suurin osa jää yritykseksi.

Haittaohjelmat ja haavoittuvuudet

- Kiristyshaittaohjelmista ilmoitettu entistä enemmän.
- Joulukuun aikana julkaistiin useita haavoittuvuustiedotteita, joissa kerrottiin lukuisista korjauksista eri tuotteiden kriittisiin haavoittuvuuksiin.

Automaatio ja IoT

- Lääkinnällisten implanttien toiminnan ja ylläpidon jatkuvuus on eettisesti tärkeää. Valmistajan konkurssi voi vaarantaa myös potilaiden kyberturvallisuuden.

Verkkojen toimivuus

- Joulukuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä.
- Palvelunestohyökkäyksiä tehdään aiempaa enemmän.
- 25% vuoden 2022 palvelunestohyökkäysten ilmoituksista tehtiin joulukuussa.

Vakoilu

- Käyttäjän varoittamiseksi suunniteltuja mekanismeja pyritään kiertämään vakoilukampanjoissa.
- VPN-ratkaisujen ja muiden verkkoliikenteeseen liittyvien tuotteiden haavoittuvuudet ovat keskeisiä APT-toimijoiden hyödyntämiä tunkeutumisreittejä.

TRAFICOM

12.1.2023

Kuukauden tunnuslukuja

-25%

Verkot toimivat vakaasti vuonna 2022. Toimintahäiriöitä oli vuoden aikana noin 25% vähemmän kuin aiempina vuosina keskimäärin.

-39%

Ilmoitukset tietojenkalastelusta vähenivät loka-joulukuun välillä 39%. Silti kalasteluhuijarit ovat edelleen hyvin kiinnostuneita erityisesti pankkitunnuksista.

1/4

Palvelunestohyökkäysten määrä jatkoi kasvuaan. Joulukuussa ilmoitettiin neljäsosa koko vuoden 2022 palvelunestohyökkäyksistä.

Top 5 kyberuhat - lähitulevaisuudessa (6kk-2v)

1

Talouden ja politiikan ilmiöt vaikuttavat voimakkaasti kyberturvallisuuteen. Digitaalisuus läpileikkaa koko organisaation toimintaa. Muutokset kansainvälisessä turvallisuustilanteessa vaikuttavat merkittävästi organisaatioiden jatkuvuuteen ja riskienhallintaan.

2

Suomeen kohdistunut kyberympäristön uhkataso on edelleen kohonneella tasolla. Lisääntyneen haitallisen liikenteen ja kohonneen uhkatason vuoksi organisaatioiden varautumisen merkitys korostuu.

3

Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista. Esimerkiksi käyttäjäoikeuksien hallinta, ohjelmistojen ajantasaisuuden ylläpito ja hyvä tietoturvakulttuuri ovat kyberturvallisuuden kivijalkaa.

Symbolit

Uusi

Päivitetty

4

Puutteellinen tiedonvaihto heikentää kyberturvallisuuden kokonaistilannekuvaa. Organisaation kohtaama kyberuhka saattaa kohdata toisia organisaatioita seuraavana päivänä. Tehokas tiedonvaihto parantaa kaikkien kyberturvallisuutta.

5

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.

TRAFICOM

12.1.2023

1. Talouden ja politiikan ilmiöt vaikuttavat voimakkaasti kyberturvallisuuteen.

Muutokset kansainvälisessä turvallisuustilanteessa on hyvä huomioida myös organisaatioiden jatkuvuuden- ja riskienhallinnassa. Nyt on hyvä hetki päivittää riskienhallintasuunnitelmat vastaamaan muuttunutta turvallisuustilannetta.

- Venäjän hyökkäys Ukrainaan heijastuu myös kyberturvallisuuteen. Esimerkiksi sodan aiheuttamat muutokset talouteen, energian hinnan nopea nousu ja informaatioympäristön herkkyys näkyvät vaikeasti ennakoitavina kehityskulkuina, jotka ulottuvat myös digitaaliseen maailmaan.
  - Energiamarkkinoiden vaihteleva ja ennakoimaton tilanne voi vaikuttaa myös kyberturvallisuuteen. Kriittiseen infrastruktuuriin vaikuttaminen voi näkyä myös kyberympäristön häiriöinä Euroopassa.
  - Mahdollinen sähkön sääntely voi aiheuttaa vaikutuksia myös kyberturvallisuuteen ja ICT-palveluiden toimivuuteen.
  - Epävarmuustekijöillä voi olla isoja vaikutuksia organisaatioiden päivittäiseen toimintaan. Organisaatioiden tulee huomioida omassa riskienhallinnassaan ja jatkuvuussuunnittelussaan toimintaympäristön muutokset ja sen aiheuttamat uhkat kriittisille prosesseille.

CASE

Suomen NATO-jäsenyysprosessin aikana Suomea kohtaan voidaan kohdistaa erilaista kyber-vaikuttamista sekä verkossa tapahtuvaa informaatio-vaikuttamista. Vaikuttaminen voi näkyä esimerkiksi palvelunesto-hyökkäyksinä. Palvelunesto-hyökkäyksillä saadaan hetkellisesti näkyvyyttä, mutta niiden vaikutukset eivät useimmiten ole laajoja tai pitkävaikutteisia.

2. Suomeen kohdistunut kyberympäristön uhkataso on edelleen kohonneella tasolla

Kyberhyökkäykset ovat lisääntyneet maailmanlaajuisesti kuluvan vuoden aikana. Samalla niitä kohdistuu kasvavassa määrin myös Suomeen. Merkittävät poliittiset ratkaisut tai suurten organisaatioiden päätökset saattavat aktivoida ja motivoida hyökkääjiä.

- Merkittävä uhka organisaatioille ovat kiristyshaittaohjelmat, joiden määrä kasvaa jatkuvasti. Kuluneen kesän aikana usea organisaatio Suomessa on joutunut kiristyshaittaohjelman uhriksi.
- Erityisesti huoltovarmuuden kannalta kriittisten organisaatioiden joutuessa kiristyshaittaohjelman uhriksi yhteiskunnan elintärkeät toiminnot voivat vaarantua.
- Suojelupoliisi on todennut kansallisen turvallisuuden katsauksessaan kriittiseen infrastruktuuriin kohdistuvan tiedustelun ja vaikuttamisen uhkan pysyvän kohonneena lähitulevaisuudessa.
- Vaikka tavanomaisten kyberhyökkäysten määrä on kokonaisuudessaan kasvanut, myös mm. kohdennetut tietojenkalasteluviestit ja murtautumisyritykset ovat lisääntyneet.
- Tutustu Kyberturvallisuuskeskuksen tiedotteeseen kohonneesta kyberuhkatasosta.(1)

OHJE

Kesän ja syksyn aikana merkittäviä organisaatioita on joutunut kiristyshaittaohjelmien uhriksi Suomessa. Vaikutukset eivät ole olleet organisaatioita lamauttavia, ja toimintaa on kyetty jatkamaan.

Oikeanlaiset suojaustoimet, varautuminen ja hyvä jatkuvuudenhallinta pienentävät hyökkäysten vaikutuksia sekä riskiä joutua uhriksi. Lisäksi ne helpottavat organisaation palautumista takaisin normaaliin tilaan.

3. Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.

Organisaation kyberturvallisuuden kivijalka rakennetaan arkisilla kyberturvallisuuden toiminnoilla. Edelleen suurin osa tietoturvapoikkeamista olisi vältettävissä tavanomaisilla keinoilla, kuten ohjelmistopäivityksillä, hyvillä salasanakäytänteillä ja tietoturvakulttuurilla.

- Käyttöoikeuksien kontrollointi on organisaatioissa tärkeää. Erilaisia hyökkäyskeinoja voidaan hyödyntää tunnusten haltuun saamiseksi, jolla voi olla merkittävä vaikutus organisaation toiminnalle tunnusten ollessa väärissä käsissä.
- Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon saatetaan jättää auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu. Kun suojaustoimet ja ylläpito ovat puutteellisia, koko organisaatio altistuu tietoturvapoikkeamille.
- Tietojen kalastelu on edelleen helppo ja yleinen tapa rikolliselle pyrkiä organisaatioon sisälle. Tietoisuuden lisääminen organisaatiossa auttaa tunnistamaan epäilyttävän toiminnan.
- Kyberturvallisuuskeskus tarjoaa organisaatioille runsaasti käytännön ohjeita kyberturvallisuuden parantamiseksi.(2)

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. Puutteellinen tiedonvaihto heikentää kyberturvallisuuden kokonaistilannekuvaa.

Kyberturvallisuus on organisaatioiden rajat ylittävää. Organisaation kohtaama kyberuhka saattaa kohdata toisia organisaatioita seuraavana päivänä. Hyvän tiedonvaihdon ylläpitäminen 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 Suomen kansallista kyberturvallisuuden tilannekuvaa. Myös muut viranomaiset vastanottavat toimialaansa liittyviä ilmoituksia.(3)

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.

5. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

Uusi sääntely ja kyberturvallisuuden sulautuminen osaksi yritysten päivittäisiä toimintoja lisää 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 määrästä vaan 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.

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

- Sosiaalisen median tilien murrot edelleen yleisiä.
  - Saamme kuukausittain merkittävä määrä ilmoituksia, joissa henkilö saa viestin sosiaalisessa mediassa kilpailun tai muun vastaan nimissä. Viesteissä pyydetään ensin puhelinnumeroa, jonka jälkeen puhelimeen saapuvaa tarkastusnumeroa.
  - Ylläkuvattu ketju mahdollistaa tunkeutujan pääsyn tilille, sekä tiliin liittyvien sähköpostiosoitteiden ja puhelinnumeroiden muuttamisen ja tilin lopullisen haltuun saamisen.
  - Kaapattuja tilejä käytetään jatkohuijausten tekemiseen, sekä erilaisiin luottokorttinumeroiden sekä taloudellisesti hyödynnettävien tietojen kalasteluun.

Analyysi

- Tänä päivänä tallennamme merkittävän määrän omaa historiaamme sosiaaliseen mediaan.
- Myös yhä useamman henkilön toimeentulo on suoraan sosiaaliseen mediaan liittyvää.
  - Tilin hallinnan menetyksen myötä, voivat kadota myös vuosien aikana kertyneet muistot kuvien ja viestien muodossa.
  - Mieti kirjaudutko sosiaalisen median tilin avulla muihin palveluihin – mitä jos sosiaalisen median tilisi tunnukset vuotavat toisen palvelun kautta.
  - Ota käyttöön kaksivaiheinen tunnistautuminen aina kun sen on mahdollista.
  - Ota tärkeimmistä tiedoista aina varmuuskopiot.

Tietomurrot ja –vuodot

- Yrityssähköpostien vaarantuminen ja kalastelu hienoisessa nousussa.
  - Joulukuussa saimme jälleen useita ilmoituksia murretuista yrityssähköposteista tulleista kalasteluviesteistä. Viestit ovat usein hyvin kohdennettuja joko organisaatio- tai henkilötarkkuudella.
  - Kalasteluiden avulla yritetään saada haltuun tunnukset jotta päästään ympäristöön sisään ja siellä käyttöön otetaan kiristyshaittaohjelma.
  - Maailmalla on havaittu useita tapauksia, joissa juuri organisaation käyttämän Exchange sähköpostipalvelinten päivittämättömyys on mahdollistanut kiristyshaittaohjelmatartunnat.

Analyysi

- Yrityssähköpostien vaarantumisen on raportoitu ulkomailla aiheuttaneen useita kiristyshaittaohjelmatartuntoja.
- Ota käyttöön monivaiheinen tunnistautuminen!
- Lisää aiheesta Viikkokatsauksessa 47/2022.(4)
- Olemme julkaisseet kaksi opasta kotisivuillamme:
  - Suojautuminen tietomurroilta.(5)
  - Toimintaohje tietomurtotilanteisiin.(6)

Tietomurrot ja –vuodot

- Elokuussa 2022 Lastpass salasananhallintaohjelmistoon kohdistunut tietomurto sai jatkohyökkäyksen marras-joulukuun 2022 taitteessa.[7]
  - Jatkohyökkäyksen yhteydessä yrityksen järjestelmistä saatiin haettua käyttäjätilien metatiedot, käyttäjien salatut salasanatietueet sekä salattujen tietojen yhteydessä olleet salaamattomat metatiedot.[8]
  - On kuitenkin hyvä muistaa, että salasananhallintaohjelmistot ovat parempi vaihtoehto kuin samojen salasanojen kierrättäminen eri palveluiden välillä
    - Salasanojen muuttaminen ja uusiminen on myös helpompaa kun käyttäjällä on selkeä lista käytössää olevista palveluista ja niiden käyttäjätunnuksista ja salasanoista.
- Joulukuussa ulkomaalainen toimija julkaisi raportin tunnettujen yritysten vuodettujen sertifikaattien käytöstä kiristys- ja tietojentuhoajahaittaohjelmien allekirjoittamiseksi.
  - Yritysten tietoturvasta vastaavien henkilöiden tulisikin seurata aktiivisesti erilaisten etähallintajärjestelmien käyttöä, sekä tietoja sertifikaattien vuodoista.

Analyysi

- Avoin tiedottaminen parantaa toipumista luotettavuuden näkökulmasta
- Tietovuotoja tulee ilmi jatkuvasti. Tunnetut ja isotkin organisaatiot ovat olleet vuosien aikana tietomurtojen uhreina
  - Viime aikoina mm. Twitter ja Uber ovat tulleet julkisuuteen niiden kohtaamien tietovuotojen takia.
- Tiedot voivat vuotaa myös palveluntarjoajien/-toimittajien heikkouksien ja virheiden vuoksi osana toimitusketjua.
- Tutustu ohjeisiimme salasanan hallintasovelluksen käyttöönottoon.[9]

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

- Pankkikalastelu on jatkuva ilmiö. Tekstiviestitse levitettiin taas suuri määrä huijausviestejä, joissa oli linkki pankkitunnuskalastelusivustoihin.
  - Eri pankkien nimissä on pystytetty varta vasten räätälöityjä kalastelusivuja, kuten identiteetti-op.fi, turvallisuus-op.fi ja jopa petos-op.fi.
  - Tällaisia suomalaisiin .fi-tunnuksiin pystytettyjä huijaussivuja nähtiin muutamia, mutta edelleen hallitseva enemmistö huijaussivuista on kansainvälisissä .net- ja .info-verkkotunnuksissa.
  - Pankkikalastelu näyttää vaihtelevan säännöllisesti Nordean, Dansken, OP:n ja muiden pankkien kesken. Myös verottajan ja viranomaisten nimissä tehty kalastelu pitää pintansa.

Pidä kiinni laskutuskäytännöistä

- Eri organisaatioiden henkilöstöä on lähestytty johtajien nimissä ja yritetty perinteisiä toimitusjohtajahuijauksia.
- Huijarit käyttävät erilaisia viestiväleineitä WhatsApp-viesteistä sähköpostiin ja puheluihin.
- Toimitusjohtajahuijauksilla tavoitellaan rahakasta laskutuspetosta ja isoa pottia. Vaikka vain harva yritys onnistuisi, silti se kannattaa huijarille.
- Organisaation omia hyväksymisprosesseja kannattaa noudattaa tarkasti. Jos poikkeuksiin ryhdytään, ne on varmistettava huolellisesti, ettei huijarin petos onnistu.

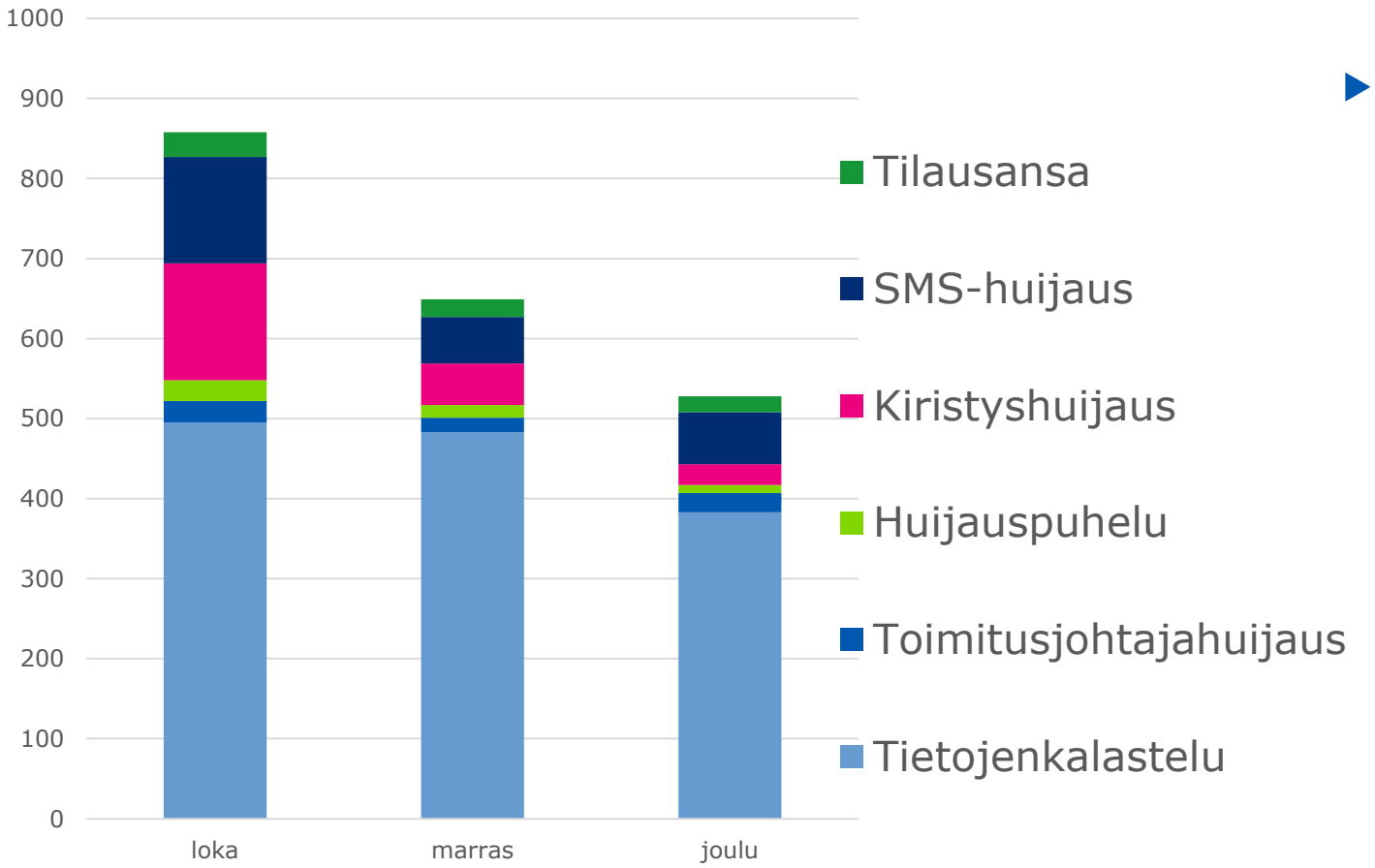
Huijaukset ja kalastelut

- Operaattorit tunnistavat hälärihuijauksia.
  - Muutamia hälärihuijauksia on pitkästä aikaa ilmoitettu Kyberturvallisuuskeskukselle.
  - Hälärihuijauksissa puhelin soi kerran tai pari ja katkeaa sitten, jotta uhri soittaisi takaisin kalliiseen ulkomaan puhelinnumeroon tai satelliittipalvelun numeroon.
  - Hälärihuijauksissa soittajan numeroita ei voi väärentää ja suomalaiset teleoperaattorit pystyvät tunnistamaan hälärihuijauksiin käytettyjä numeroita.
  - Osa huijauksista kuitenkin ehtii päästä läpi ennen kuin operaattorit tunnistavat puhelut huijauksiksi siitä, että samoista numeroista tulee suuri määrä lyhyitä hälärisoittoja.
  - Huijausten uhriksi voi silti joutua eikä tuntemattomiin hälärisoittoihin kaukomaista pidä soittaa takaisin. Viime aikoina on nähty hälärisoittoja mm. Sri Lankasta ja Lesothosta.

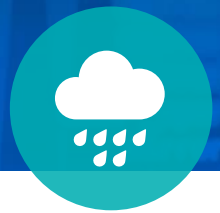
Poliisihuijauksia sinne tänne

- Poliisihuijausviestejä on taas roiskittu ympäriinsä.
- Suomalaisia on koetettu huijata myös Ranskan, Viron ja Liettuan poliisiviranomaisten nimissä.
- Sama poliisiaiheinen huijauskampanja näkyy eri muodoissaan monissa Euroopan maissa eivätkä huijarit ole turhan tarkkoja siitä, mihin viestejä levitetään.

Käsiteltyjä huijaustapauksia Q4/2022



- Vuoden 2022 viimeisen neljänneksen ilmiöitä olivat:
  - Vuoden vaihdetta kohden huijausten kokonaismäärä näytti rauhoittuvan. Silti kalasteluhuijarit ovat edelleen hyvin kiinnostuneita erityisesti pankkitunnuksista.
  - Suurin osa tekstiviestihuijauksista kalastelee pankkitunnuksia.
  - Poliisiaiheisia kiristyshuijauksia saadaan edelleen samaan tapaan kuin muuallakin Euroopassa.



Haittaohjelmat ja haavoittuvuudet

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

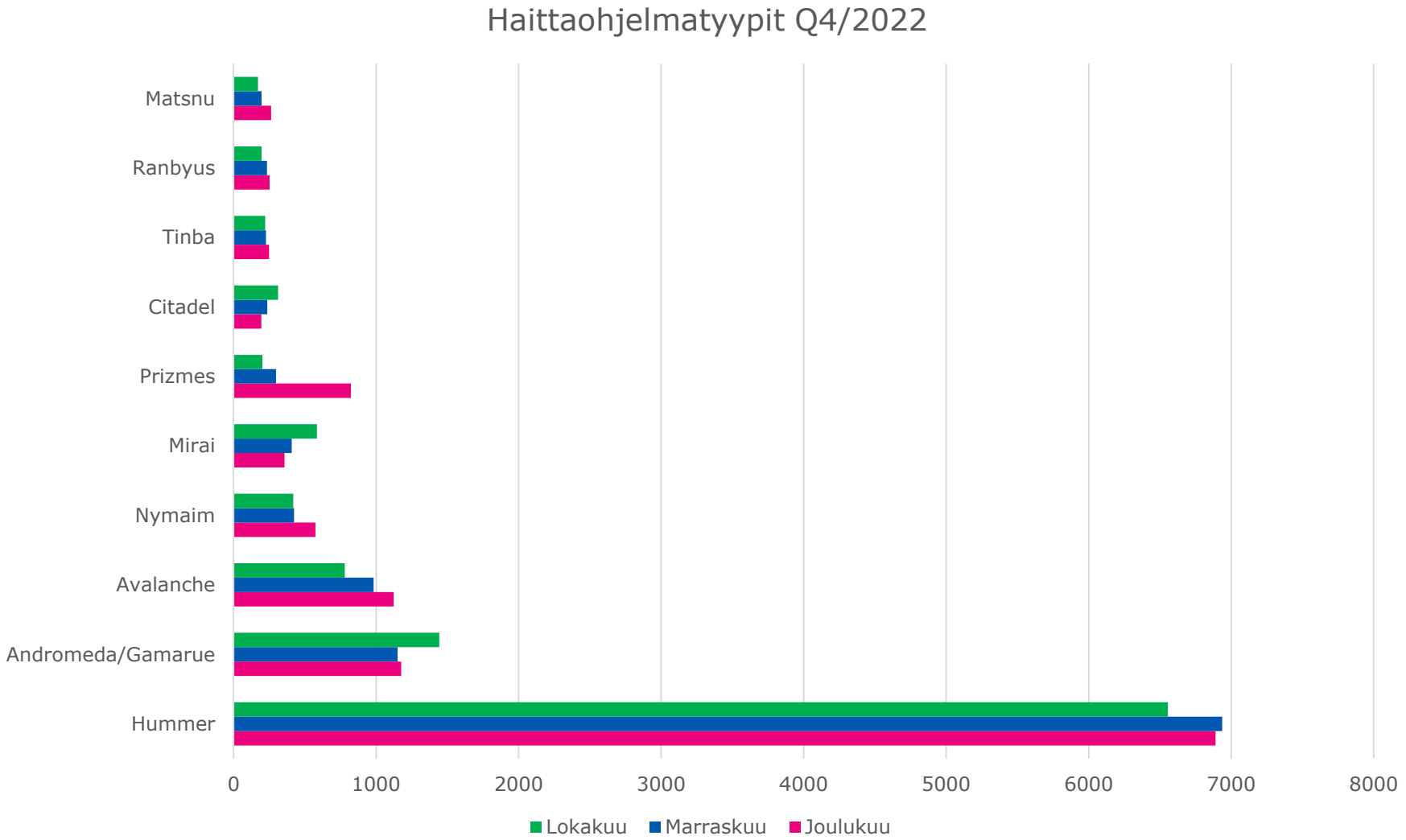
Haittaohjelmat

- Kiristyshaittaohjelmista ilmoitettu entistä enemmän joulukuussa ja loppuvuonna 2022.
  - Vuoden 2022 aikana useampi suomalainen organisaatio on joutunut kiristyshaittaohjelman uhriksi ja myös ilmoittanut siitä viranomaisille.
  - Kiristyshaittaohjelmia levittävät tahot eivät keskity vain suuriin yrityksiin, vaan kaiken kokoiset organisaatiot voivat joutua hyökkäyksen.
  - Kiristyshaittaohjelmahyökkäyksen kohteeksi joutuminen on aina vakava tilanne organisaatiolle. Tutustu Kyberturvallisuuskeskuksen toimintaohjeisiin kiristyshaittaohjelmatilanteiden varalta.(10)

Analyysi

- Lunnaiden maksu tilanteen selvittämiseksi ei ole oikea ratkaisu.
  - Maksaminen ei välttämättä takaa tietojen palauttamista tai edes estä kiristyksen tai muiden hyökkäysten jatkumista.
- Hyökkääjän tavoitteena voi olla myös pelkkä tietojen tuhoaminen, jolloin kiristys on vain hämäystä.
  - Tällöin dataa ei ole mahdollista palauttaa edes lunnaita maksamalla. Kiristyshaittaohjelmahyökkäys voi johtaa myös tietojen vuotamiseen.

Autoreporterin haittaohjelmahavainnot



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

Tilastossa kerromme 10 yleisintä ja nimettyä haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Niistä voi lukea tarkempia tietoja kotisivuiltamme.(11)

Kuukauden haavoittuvuusjulkaisut

- Kaksi haavoittuvuutta Linux Debian Cacti Web-rajapinnan palvelussa (23/2022).
- Useita kriittisiä haavoittuvuuksia Neutrinolabsin xrdp etätyöpöytäprotokollan toteutuksessa (24/2022).
- Kriittinen haavoittuvuus Fortinetin FortiOS-ohjelmistossa (25/2022).
- Kriittinen haavoittuvuus Citrix Gateway ja Citrix ADC –ohjelmistoissa (26/2022).
- Useita kriittisiä haavoittuvuuksia VMwaren virtualisointiohjelmistoissa (27/2022).
- Apple julkaisi kriittisen haavoittuvuuden korjaavan päivityksen tuotteisiinsa (28/2022).

- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

TRAFICOM

12.1.2023

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

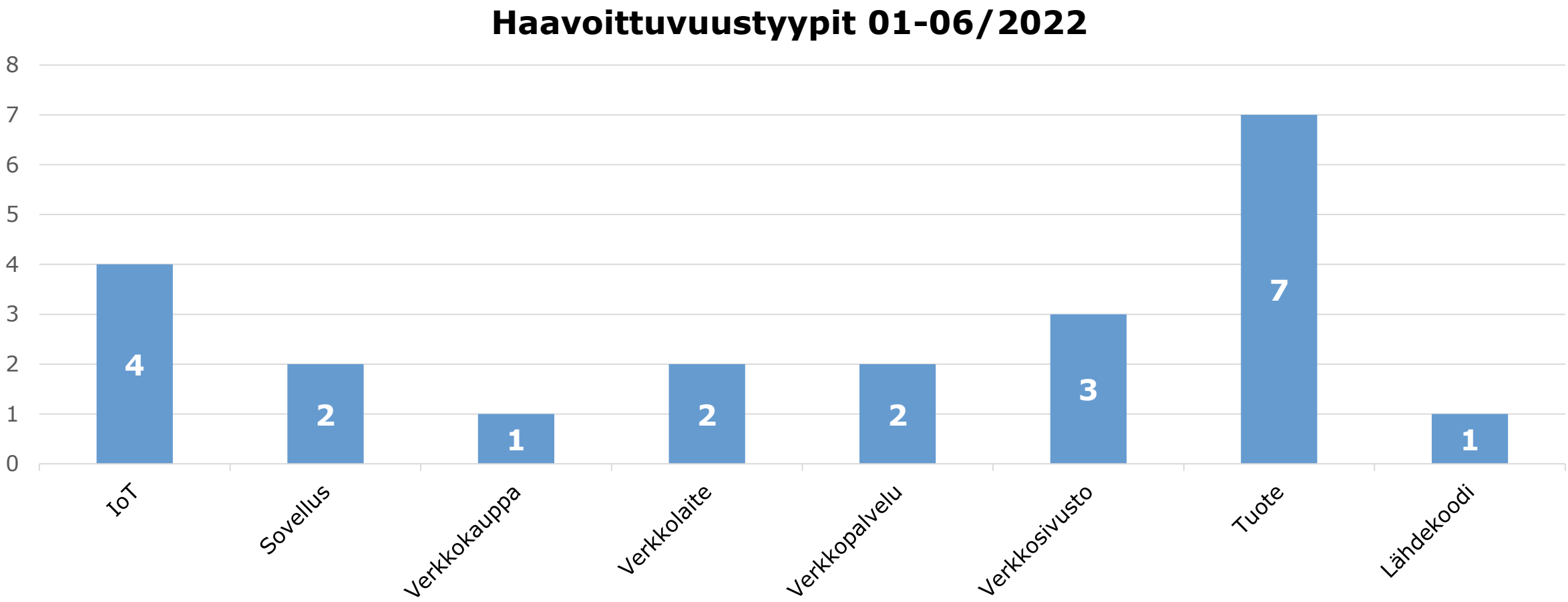
- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta.**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn.
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta.**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta.
- **Haavoittuvuustiedotteita vuonna 2022 28 kpl (tilanne 5.1.2023).**
  - 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

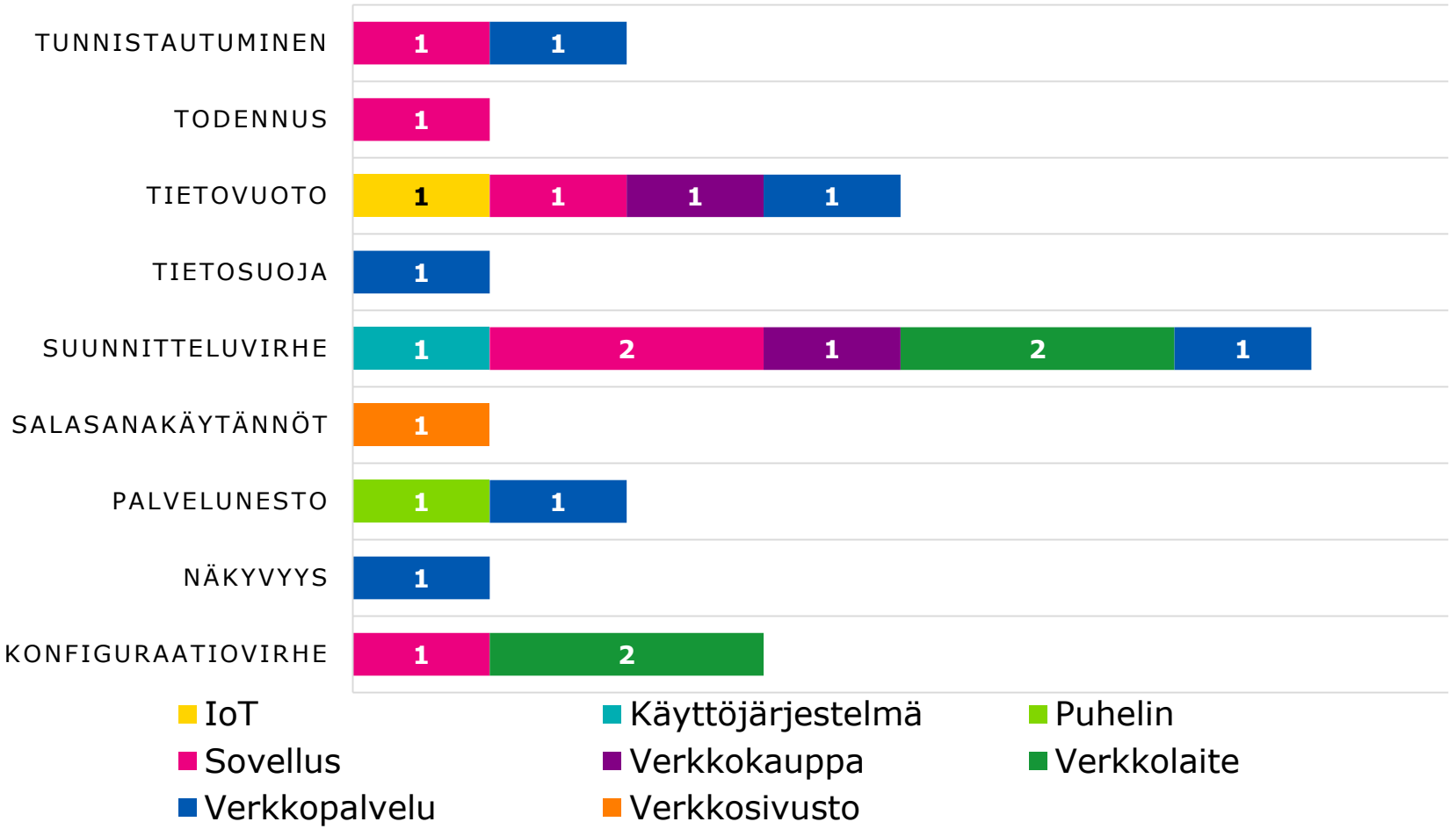
- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat 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.(12)

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

- Lääkinnällisten implanttien toiminnan ja ylläpidon jatkuvuus on eettisesti tärkeää.(13)
- Useat kehon sisälle sijoitettavat lääkinnälliset laitteet tarvitsevat ohjelmistoja toimiakseen, kuten sydämentahdistimet ja kuulokojeet.
  - Tyypillisesti asetusten muuttamiseen tarvitaan laitteen valmistajan omistama tietokoneohjelmisto.
  - Myös implantissa itsessään on monesti pieni tietokone ohjelmistoineen.
- Laitteen valmistaja saattaa lopettaa laitteen tukemisen esimerkiksi konkurssin takia. Jos laitteen tuki loppuu, potilaille tulee ennemmin tai myöhemmin ongelmia.(14)

Analyysi

- Valmistajan tuen loputtua voi ilmetä useita ongelmia:
  - Implantin säätämisestä saattaa tulla mahdotonta.
  - Implantin ja sitä tukevien ohjelmistojen vikoja ei korjata, mikä voi altistaa potilaan kyberhyökkäyksille.
  - Hyvällä onnella potilaalle on tarjolla vaihtoehtoinen hoitomenetelmä. Implantin vaihtaminen on monesti vaativa kirurginen operaatio ja sinällään riski potilaan terveydelle.
- Potilaita voisi hyödyttää, jos valmistajat julkaisisivat sellaisten implanttien lähdekoodit, joiden tukemisen ne lopettavat. Tällöin jokin muu taho voisi ottaa päivitysten tuottamisen tehtäväkseen.
- Lähdekoodin avaamiseen velvoittavaa sääntelyä on esitetty mm. Euroopassa. Toisaalta terveydenhuoltoalan vaativa sääntely laskee kiinnostusta kehittää lääkinnällisten laitteiden ohjelmistoja, sillä sääntely edellyttää huolellista ja usein kallista potilasturvallisuuden varmistamista ennen päivitysten käyttöönottoa.

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

- Joulukuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä, joka on keskiarvoa vähemmän.
  - Vakavuusluokat: A: 0, B: 0, C: 2
- Verkot toimivat vakaasti vuonna 2022 - häiriöitä oli noin 25% vähemmän kuin aiempina vuosina.
- Gmailissa oli maailmanlaajuinen häiriö joulukuussa, joka näkyi myös Suomessa.(15)
  - Häiriö vaikutti sähköpostien toimittamiseen, ja suurin osa raportoiduista ongelmista liittyi sähköpostin vastaanottamiseen.

Analyysi

- Sähkön kantaverkkoyhtiö Fingrid Oyj on kertonut, että tämänhetkisessä maailmantilanteessa on järkevää varautua sähkön niukkuuteen ja siihen, että talvella sähköpula voi aiheuttaa sähkökatkoksia.(16)
- Yleisesti voidaan todeta, että erilaiset viestintäverkot ja -palvelut ja toimivat kiertävissä sähkökatkoissa vaihtelevasti, peruspalvelut pääosin vähintään muutamia tunteja.
- Niissäkin kohteissa, joissa ei ole kiinteää varavoimalaitosta, on useimmiten siirrettävän varavoiman eli vaikkapa kuljetettavan dieselgeneraattorin kytkentämahdollisuus.
- On kuitenkin hyvä huomata, että koska viestintäverkkokomponentteja ja -laitetiloja on Suomessa kymmeniä tuhansia, siirrettävää varavoimaa ei riitä niihin kaikkiin.

Palvelunestohyökkäykset

- Joulukuussa ilmoitettiin aiempaakin aktiivisemmin palvelunestohyökkäyksistä.
  - Joulukuun ilmoitusmäärä oli noin 25% koko vuoden ilmoituksista.
  - Useilla hyökkäyksillä oli vaikutuksia palveluiden saatavuuteen tai organisaation toimintaan.
- Hyökkäykset olivat myös eri tavoin toteutettuja:
  - Useat ilmoitetut hyökkäykset olivat kooltaan yli 50Gbit/s.
  - Osa hyökkäyksistä kohdistui useisiin eri organisaation osoitteisiin ”carpet bombing” eli mattopommitustekniikalla, eli yksittäisen kohteen sijaan hyökkäys on kohdistunut useampiin eri kohteisiin uhriorganisaation verkkoalueella.
  - Jotkin hyökkäykset olivat pitkäkestoisia - jopa päivien mitassa.
  - Haktivismitoiminta näkyi hyökkäyksissä - osa verkossa uhatuista hyökkäyksistä toteutui.
- Julkaisimme aktivoituneesta palvelunestohyökkäysten tilanteesta artikkelin joulukuussa.[(17)]

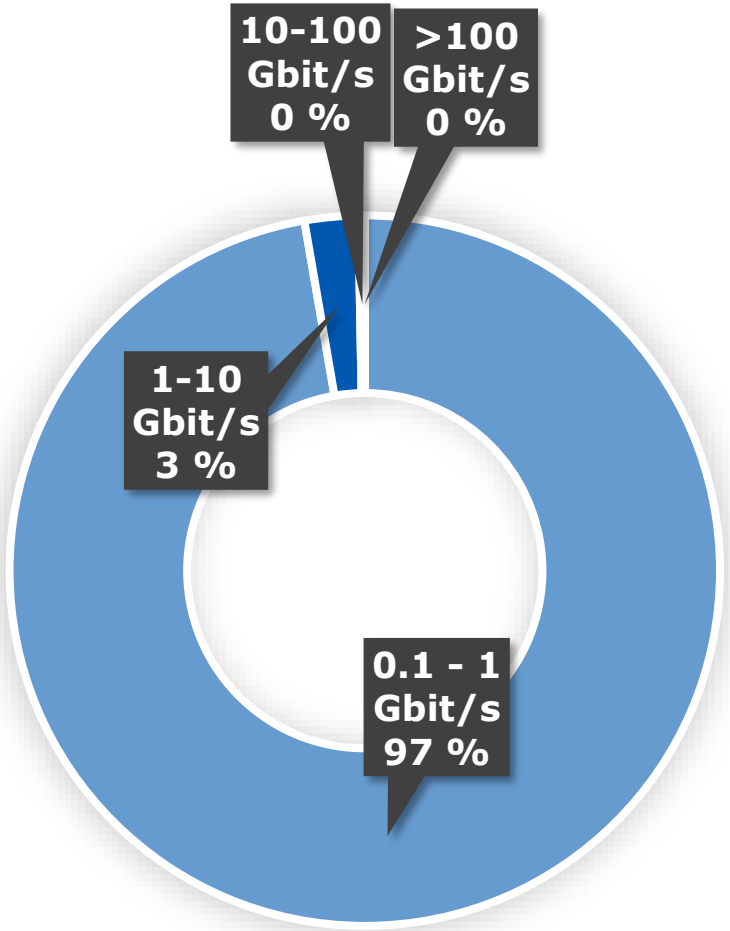
Analyysi

- Vuoden 2022 lokakuussa alkanut nouseva trendi palvelunestohyökkäyksien määrässä tulee näkymään myös vuonna 2023.
- Kyberturvallisuuskeskukselle ilmoittaminen parantaa kansallista tilannekuvaa palvelunestohyökkäysten suhteen.
  - Ilmoitattehan meille teihin kohdistuneista hyökkäyksistä - luottamuksellisesti. Kyberturvallisuuskeskus muodostaa tilannekuvaa ja analysoi tilannetta ilmoitustenkin perusteella.
- Organisaatioiden tulee arvioida, mitkä verkossa olevat palvelut on suojattava hyökkäyksiltä.
  - On myös tärkeää valmistautua siihen, että suojautumisenkin jälkeen osa hyökkäyksistä voi vaikuttaa palveluihin. Miten toimitaan, kun suojaus ei toimikaan ja palvelut ovatkin hetkellisesti alhaalla?

Palvelunestohyökkäysten tunnuslukuja

3kk

- 52 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q4/2022.
- Noin 58% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q4/2022 - tilasto päivitetään kvartaaleittain.)
Tilasto tarkentuu helmikuun 2023 Kybersäähän.

Vakoilu

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

Vakoilu

- Julkisuudessa Kiinaan yhdistetyn APT5-ryhmän (Manganese, UNC2630) on raportoitu hyödyntäneen joulukuussa korjattua, tietyissä Citrix-tuotteissa ollutta haavoittuvuutta kohdistetuissa hyökkäyksissä.(22)
  - Yhdysvaltojen NSA on listannut organisaatioille keinoja tunnistaa ja havaita haavoittuvuuden mahdollinen hyödyntäminen omista järjestelmistä.(18)
- Hyökkääjät kiertävät Microsoftin Mark-of-the-Web-suojausmekanismia (MOTW) eri tavoin. MOTW:n tarkoituksena on ilmaista tiedoston avaajalle tiedoston olevan alkuperältään internetistä.(23)
  - Joulukuussa kerrottiin pohjoiskorealaiseksi epäillyn APT-ryhmän välttäneen MOTW-tunnistusta välittämällä haitalliset tiedostot uhrilleen piilotettuna esimerkiksi levykuviin.
  - Ryhmän on arvioitu linkittyvän Lazarus-ryhmään, jonka on myös kerrottu jatkaneen esimerkiksi virtuaalivaluuttoihin liittyviin toimijoihin kohdistuvia kybervakoilukampanjoitaan.
- Myös Iraniin julkisuudessa yhdistetty MuddyWater-ryhmä on jatkanut aktiivisesti vakoilukampanjoitaan. Toiminnan painopiste on raportoinnin mukaan keskittynyt Lähi-itään, mutta toimintatapoja on päivitetty.

Analyysi

- Verkkolaitteiden ja VPN-ratkaisujen haavoittuvuudet ovat säilyneet houkuttelevina murtautumiskohteina APT-toimijoille.
- Uhkatoimijat myös reagoivat suojaustoimiin tehtyihin muutoksiin ja erilaisiin teknisiin rajoituksiin, joilla pyritään estämään pahantahtoista toimintaa.

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

- Televiestintäneuvosto hyväksyi 6.12.2022 EU:n neuvoston yleisnäkemyksen eIDAS-asetuksen muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamiseksi.(19) (20)
  - Vuonna 2014 annettu eIDAS-asetus koskee jäsenvaltioiden ilmoittamia eli notifioituja sähköisen tunnistamisen järjestelmiä, joilla voi tunnistautua toisen jäsenvaltion julkishallinnon palveluihin.
  - Tunnistusvälineen avulla henkilö voi luotettavalla tavalla todentaa identiteettinsä sähköisessä asioinnissa. Lisäksi asetuksessa säädetään sähköisistä luottamuspalveluista, joiden tarkoitus on mahdollistaa luottamus sähköisiin asiakirjoihin ja sähköisiin prosesseihin.
- Yksi muutoksen tärkeimmistä tavoitteista on tarjota yhdenmukaistettu eurooppalainen digitaalisen identiteetin väline eli digitaalisen identiteetin lompakko. Ehdotuksessa edellytetään, että jäsenmaat ottavat käyttöön digitaalisen lompakon, joka perustuu yhteisiin teknisiin normeihin ja edellyttää pakollista sertifiointia.
- Henkilökohtaisen, digitaalisen lompakon tarkoituksena on varmistaa jäsenmaiden kansalaisille, asukkaille ja yrityksille yleisesti saatavilla oleva turvallinen ja luotettava sähköinen tunnistautuminen ja todentaminen matkapuhelinsovelluksen avulla.

Oikeudelliset asiat

- CER-direktiivi on annettu 14.12.2022 ja julkaistu EU:n virallisessa lehdessä 27.12.2022 (21)
- CER = Critical Entities Resilience, kriittisten toimijoiden häiriönsietokyvystä annetun Euroopan parlamentin ja neuvoston direktiiviehdotus. Sen tarkoituksena on parantaa yhteiskunnan kriisinkestävyyttä ja vahvistaa kriittisen infrastruktuurin häiriönsietokykyä esimerkiksi hybridivaikuttamistilanteissa.
  - Tavoitteena on ylläpitää yhteiskunnan elintärkeitä ja taloudellisia toimintoja määrittäen tietyt kriittiset sektorit, jotka tarjoavat tällaisia palveluja. Suomessa ei ole aiemmin määritelty kansallista kriittistä infrastruktuuria, kriittisiä sektoreita tai toimijoita lainsäädännön tasolla.
  - Soveltamisalaan kuuluu yksitoista sektoria, jotka ovat liikenne, energia, pankit, finanssimarkkinat, terveys, ruoka, vesi- ja jätevesihuolto, digitaalinen infrastruktuuri, julkishallinto ja avaruus.
- Toimijoiden suoritettava oma riskinarviointi, toteutettava kriisinsietokykyä parantavat toimenpiteet ja raportoitava häiriötilanteista viranomaiselle.
- Jäsenvaltioiden on myös säädettävä seuraamukset kansallisten säännösten rikkomisesta.
- Direktiivin edellyttämille säädösmuutoksille on annettu 21 kuukautta valmisteluaikaa.

Arjen kyberturvallisuus

Pornokiristyksiä runsaasti liikkeellä – älä usko huijarien väitteitä

- Huijarit ovat jälleen aktivoituneet aikuisviihdeteemaisten eli "pornokiristys" -huijausviestien lähettelyssä. Viestejä on lähetetty viime päivinä runsaasti myös hyvin suomeksi käännettyinä.
- Lue lisää: www.kyberturvallisuuskeskus.fi

Pankkitunnusten kalastelua edelleen runsaasti liikkeellä. Tutustu ohjeisiimme huijausten tunnistamiseksi

- Verkossa on runsaasti huijareita, jotka haluavat rahasi tai tietosi. Huijausviestejä satelee sähköpostitse, tekstiviestitse ja puhelimitse.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta

Tunnista turvallinen verkkosivu osoitteen perusteella

- Nettisivuja ja sähköpostia käyttäessä tärkeintä on säilyttää arkijärki ja pitää pää kylmänä. Hätiköityjä päätöksiä ei pidä tehdä, vaikka sinulle luvattaisiin satumaisia voittoja tai uhattaisiin "pankkitilin jäädyttämisellä" tai syytteellä laittomuudesta.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnista-turvallinen-verkkosivu-osoitteen-perusteella

Uutisia Kyberturvallisuuskeskuksesta

Tekoäly tulee muuttamaan myös kyberhyökkäyksiä

- Traficomin Kyberturvallisuuskeskuksen ja Huoltovarmuuskeskuksen teettämä selvitys käsittelee tekoälyn roolia kyberhyökkäyksissä.
- Nyt julkistettu selvitys on toinen osa Traficomin ja Huoltovarmuuskeskuksen tekoälyn kyberturvallisuutta koskevaa kokonaisuutta, joka rahoitetaan Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -ohjelmasta.
- https://www.traficom.fi/fi/ajankohtaista/tekoaly-tulee-muuttamaan-myos-kyberhyokkayksia

Tietoturvaseteli saavutti suuren suosion

- Tietoturvan kehittämisen tukea eli tietoturvaseteliä on voinut hakea Liikenne- ja viestintävirasto Traficomista 1.12. alkaen.
- Haettu rahoitus on ylittänyt myönnettävänä olevan rahoituksen.
- Tuen tavoitteena on nostaa yritysten tietoturvallisuuden tasoa ja sitä kautta parantaa koko yhteiskunnan kykyä suojautua kyberturvallisuusuhkia vastaan.
- https://www.traficom.fi/fi/ajankohtaista/tietoturvasetelin-valtava-suosio-oli-iloinen-yllatys

Kyberturvallisuusdirektiivi vahvistaa koko EU:n kyberturvallisuustasoa – kansallinen toimeenpanohanke käynnistyi

- Liikenne- ja viestintäministeriö käynnisti 2.1.2023 kansallisen toimeenpanohankkeen uuden NIS2 -direktiivin velvoitteiden saattamiseksi osaksi kansallista lainsäädäntöä.
- Kansallinen toimeenpano tehdään laajassa poikkihallinnollisessa yhteistyössä.
- https://www.lvm.fi/-/kyberturvallisuusdirektiivi-vahvistaa-koko-eu-n-kyberturvallisuustasoa-kansallinen-toimeenpanohanke-kaynnistyi-1903681

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) Tiedote kohonneesta uhkatasosta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

2) Ohjeet ja oppaat organisaatioille ja yrityksille https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

3) Ilmoittaminen Kyberturvallisuuskeskukselle https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

4) Kyberturvallisuuskeskuksen viikkokatsaus 47/2022
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-472022

5) Näin suojaudut tietomurroilta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta

6) Toimintaohje tietomurron tapahtuessa https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/toimintaohje-tietomurto

7) Pwndefend, Lastpass breach https://www.pwndefend.com/2022/12/24/lastpass-breach-the-danger-of-metadata/

8) Nakedsecurity: Lastpass breach https://nakedsecurity.sophos.com/2022/12/23/lastpass-finally-admits-they-did-steal-your-password-vaults-after-all/

9) Neuvoja salasanan hallintasovelluksen käyttöönottoon https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon

Lähdeluettelo

10) Toimintaohje kiristyshaittaohjelmatilanteissa https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/KiristyshaittaohjelmaToimintaohje.pdf

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

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

13) The Nature: Abandoned, the human cost of neurotechnology failure https://www.nature.com/immersive/d41586-022-03810-5/index.html

14) Patients Are Being Left High And Dry When Medical Implant Makers Implode https://www.techdirt.com/2022/12/15/patients-are-being-left-high-and-dry-when-medical-implant-makers-implode/

15) Yle: Googlen sähköpostipalvelu Gmail palautumassa ennalleen https://yle.fi/a/74-20008146

16) Teleyritysten verkkojen ja palvelujen toimivuus kiertävissä sähkökatkoissa https://www.kyberturvallisuuskeskus.fi/fi/teleyritysten-verkkojen-ja-palvelujen-toimivuus-kiertavissa-sahkokatkoissa

Lähdeluettelo

17) Palvelunestohyökkäyksissä selvää kasvua joulukuussa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkayksissa-selvaa-kasvua-joulukuussa

18) NSA, APT5: Citrix ADC Threat Hunting Guidance https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF

19) Eurooppalainen digitaalinen identiteetti (eID) https://www.consilium.europa.eu/fi/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/

20) Ehdotus Euroopan parlamentin ja neuvoston asetukseksi asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/fi/pdf

21) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 https://eur-lex.europa.eu/eli/dir/2022/2555/oj

22) Citrix ADC and Gateway zero day under active exploitation https://www.techtarget.com/searchsecurity/news/252528327/Citrix-ADC-and-Gateway-zero-day-under-active-exploitation

23) The Hacker News: APT hackers turn to malicious excel add-ins as initial intrusion vector https://thehackernews.com/2022/12/apt-hackers-turn-to-malicious-excel-add.html