TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Lokakuu 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

10.11.2022

Kybersää lokakuu 2022

Tietomurrot ja -vuodot

- Zalando-verkkokaupan tilejä murrettiin suuria määriä. Murrossa on mahdollisesti käytetty aiemmin vuodettuja käyttäjätunnus- ja salasanalistoja.
- Tietomurtojen ja -yritysten kohteina oli korostetusti energia-, teollisuus-, media- ja koulutussektorit.

Huijaukset ja kalastelut

- Poliisiteemaiset kiristyshuijaukset ovat jatkuneet entistäkin runsaampina. Juhlallisilla syytösväärennöksillä yritetään huijata uhreilta rahaa sekä Suomessa että muualla Euroopassa.

Haittaohjelmat ja haavoittuvuudet

- Emotet-haittaohjelmasta havaintoja maailmalta.
- Muutamia ilmoituksia kiristyshaittaohjelmahavainnoista. Syyskuussa kerroimme kiristyshaittaohjelmien määrän kasvusta Suomessa.

Automaatio ja IoT

- Lääkinnällisten laitteiden haavoittuvuuksien hallintaa täytyy yhä parantaa.

Verkkojen toimivuus

- Yleisissä viestintäpalveluissa kaksi merkittävää toimivuushäiriötä.
- Palvelunestohyökkäysten määrä on kasvussa.
- Lokakuussa ilmoitettu 25% koko vuoden 2022 palvelunestohyökkäyksistä.

Vakoilu

- Valtiolliset toimijat hyödyntävät sekä aiemmin tuntemattomia mutta myös jo tunnettuja haavoittuvuuksia.
- Microsoft Exchangen ProxyNotShell-haavoittuvuutta on Microsoftin mukaan hyödynnetty tiettävästi elokuusta lähtien valtiollisen toimijan operaatiossa.

TRAFICOM

10.11.202

Kuukauden tunnuslukuja

25%

Lokakuussa Kyberturvallisuuskeskukselle tietoon tullut palvelunestohyökkäysten määrä vastasi 25 prosenttia koko vuoden ilmoitusmäärästä.

10-30

FBI:n raportin mukaan lääkinnälliset laitteet pysyvät käytössä jopa 10-30 vuotta, ja niiden elinkaaren hallinta korostuu. Suomessa asiaan on kiinnitetty huomiota esimerkiksi sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimusten mallilla.

2

Lokakuussa yleisissä viestintäpalveluissa oli vain kaksi merkittävää toimivuushäiriötä, joka on selvästi keskiarvoa vähemmän.

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

10.11.2022

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.(1)
- Vaikka tavanomaisten kyberhyökkäysten määrä on kokonaisuudessaan kasvanut, myös mm. kohdennetut tietojenkalasteluviestit ja murtautumisyritykset ovat lisääntyneet.
- Tutustu Kyberturvallisuuskeskuksen tiedotteeseen kohonneesta kyberuhkatasosta.(2)

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.(3)

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.(4)

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)

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.

TRAFICOM

10.11.2022

Tietomurrot ja –vuodot

- Lokakuu oli tavanomainen tietomurtojen osalta.
  - Zalando-verkkokauppaan kohdistui alkukuusta medianäkyvyyttä saanut tilienmurtokampanja. Murtojen seurauksena pyrittiin tunnistamaan tilit, joihin oli tallennettu maksutietoja. Tämän jälkeen murtautuja pyrki tekemään luvattomia hankintoja tilejä hyväksi käyttäjien.
  - Suomessa, Euroopassa, sekä Pohjois-Amerikassa tietomurtojen ja –yritysten kohteina on korostunut terveydenhuollon-, teollisuuden-, energia-, media- ja koulutusalan toimijat. Osassa tapauksista on ollut havaittavissa aiempiin kalastelukampanjoihin liittyviä jatkohyökkäyksiä.
  - Vaikka viime kuukausien aikana ei kiristyshaittaohjelmahyökkäysten määrässä olekaan ollut suurta vaihtelua, raportoidaan tapauksia viikoittain Kyberturvallisuuskeskukselle.

Analyysi

- Kyberhyökkäysten monivaiheisuus korostuu varsinkin tietomurtojen kohdalla.
- Mahdollisia ensimmäisiä vaiheita murroissa:
  - Kalastelu tai muuten haitallinen sähköposti / verkkosivu.
  - Kohteen suojausta pystytään selvittämään myös pienillä palvelunestohyökkäyksillä tai erilaisilla verkko- ja palveluskannauksilla.
- Suojautumiseen auttaa usein:
  - Älä avaa tuntemattomia liitteitä / linkkejä.
  - Pidä järjestelmäsi päivitettyinä.
  - Pohdi, pitääkö laitteesi olla saavutettavissa internetistä.
  - Varmuuskopio, ja tarvittaessa varmista ns. offline varmuuskopioidenkin saatavuus, palautettavuus ja eheys.

Tietomurrot ja –vuodot

- Viestintä osana tietomurrosta toipumista on tärkeää.
  - Uponor Oyj ilmoitti julkisesti yritykseensä kohdistuneesta kiristyshaittaohjelman aiheuttamasta tietomurrosta. Tiedotteessa kerrottiin julkisesti sekä murron vaikutuksesta, aloitetuista toimenpiteistä sekä tehdyistä viranomaisilmoituksista.
  - Muuramen kunta tiedotti sekä kotisivuillaan että sosiaalisessa mediassa kuntaan kohdistuneesta tietomurrosta ja sen aiheuttamasta laajasta häiriötilasta. Muuramen kunta tiedotti avoimesti tietomurron vaikutuksista mm. kunnan lakisääteisiin tehtäviin. Muuramen kunta oli jo ennen tietomurtoa uutisoinut yhdessä ulkoisen tietoturvatoimijan kanssa tehdystä laaja-alaisesta yhteistyöstä toimintojen turvaamiseksi.
  - Posti-konserni tiedotti konserniin kuuluvaan Itella Estonia OÜ:n kohdistuneesta tietomurrosta. Tiedotteessa avattiin murron laajuutta ja aloitettuja palautumistoimenpiteitä. Lisäksi Posti kertoi tapaukseen liittyvästä asiakas- ja viranomaisviestinnästä.
  - Tiedon jakaminen tukee yhteiskunnan eri sektorien kyberuhkiin varautumista ja vastaamista. Tämä varmistaa osaltaan sen, että Suomi on jatkossakin hyvin varautunut kyberuhkia vastaan.

Analyysi

- Kriisiviestintä:
  - Oikea-aikaisuus
  - Sisäinen ja ulkoinen viestintä
  - Viestintäkanavat (sisäiset ja ulkoiset)
  - Avoimuus
- Mitä viestiä:
  - Mitä on tapahtunut
  - Koska on tapahtunut
  - Miten tapahtunut vaikuttaa
    - Yritykseen
    - Kumppaneihin
    - Asiakkaisiin
  - Mitä on tehty tapatuman hallintaan saamiseksi
  - Kenelle ja mitä on viestitty
  - Koska viestitään seuraavaksi
- Mahdollisesti toimijaa velvoittava viestintä:
  - NIS-direktiivi
  - Muu velvoittava viranomaisviestintä

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.

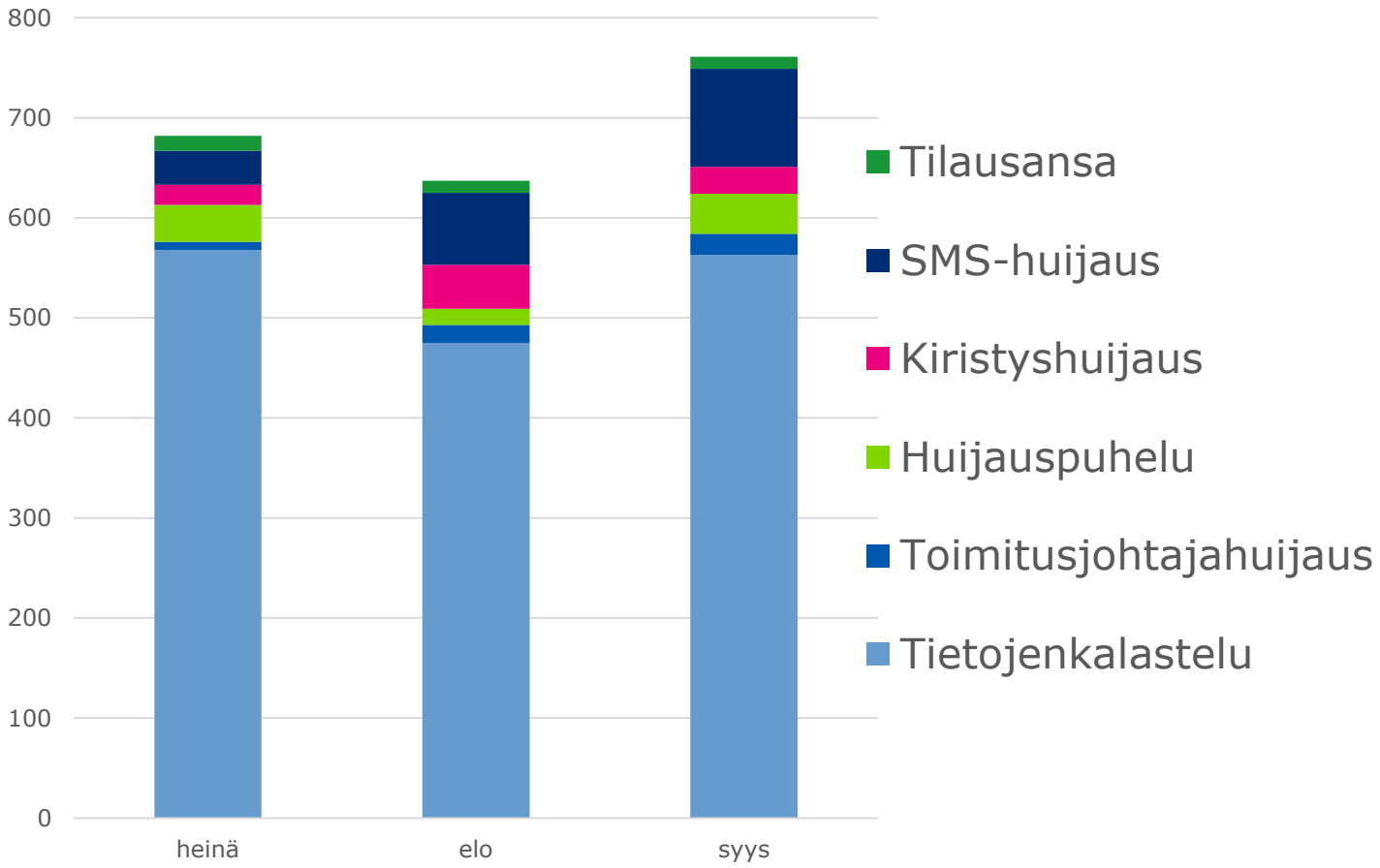
Huijaukset ja kalastelut

- Poliisiaiheella kiristäminen jatkuu.
  - Poliisiteemaiset kiristyshuijaukset ovat jatkuneet edelleen entistäkin runsaampina. Juhlallisen näköisillä tekaistuilla syytösdokumenteilla yritetään huijata uhreilta rahaa sekä Suomessa että muualla Euroopassa.
  - Runsain leimoin ja tittelein koristelluissa syyteväärennöksissä esiinnytään sekä kansallisten että kansainvälisten poliisiviranomaisten nimissä ja vaaditaan tuhansien eurojen summaa vastineeksi syytteistä selviytymiselle.
  - Myös muita sekalaisia kiristyshuijauksia on liikkeellä. Huijarit ovat lähettäneet viestejä, joissa väitetään että "olemme varastaneet datasi palvelimeltasi" tai että sivusto on hakkeroitu ja vaaditaan lunnaita.

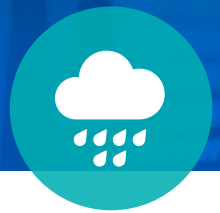
Analyysi

- Useat organisaatiot ovat ilmoittaneet sinnikkäistä laskutuspetosten yrityksistä, joissa organisaation johtajan nimissä on lähetetty kymmenille työntekijöille huijausviestejä.
- Huijauksissa yritetään saada henkilökuntaa hyväksymään tuhansien eurojen valelaskuja.
- Toimitusjohtajahuijausten ja laskutuspetosten kohteiksi on valikoitunut kaikenlaisia organisaatioita valtion virastoista pörssiyrityksiin ja urheiluseuroista tilitoimistoon.

Käsiteltyjä huijaustapauksia Q3/2022



- Vuoden 2022 kolmannen neljänneksen ilmiöitä olivat:
  - Tekstiviestien määrä on edelleen kasvanut. Tekstiviestihuijauksia käytetään suurissa määrin pankkitunnusten kalasteluun.
  - Poliisiaiheiset kiristyshuijaukset ovat rantautuneet Suomeen Euroopasta.
  - Huijauspuheluita soitetaan ulkomaisista numeroista sen jälkeen, kun määräys 28 on vähentänyt kotimaisten numeroiden käyttöä huijauksiin.



Haittaohjelmat ja haavoittuvuudet

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

Haittaohjelmat

- Emotet-haittaohjelmasta on tehty havaintoja maailmalla.
  - Noin viisi kuukautta sitten maailmalla hiljentynyt Emotet-haittaohjelma näyttää aktivoituneen jälleen. Emotet-haittaohjelma leviää sähköpostin liitetiedostojen kautta.
  - Tällä hetkellä maailmalta raportoidut tapaukset ovat pitäneet sisällään joko Excel- tai Word -tiedostoja, jotka ovat voineet saapua myös salasanasuojatuissa pakatuissa ZIP-tiedostoissa.
  - Viestien ja tiedostojen aiheet ovat liittyneet mm. laskutukseen, skannauksiin ja erilaisiin lomakkeisiin.

Analyysi

- Varsinkin Microsoft Office -tuotteissa nykyään käytöstä oletuksena poistettu makrojen suorituksen estäminen vaikeuttaa myös Emotetin leviämistä.
- Tämän hetken tietojen mukaan haittaohjelma pyrkii saamaan käyttäjän siirtämään saastuneen tiedoston tietokoneen Templates-kansioon, jolla edellä kuvattua suojaustoimintoa pystytään kiertämään.

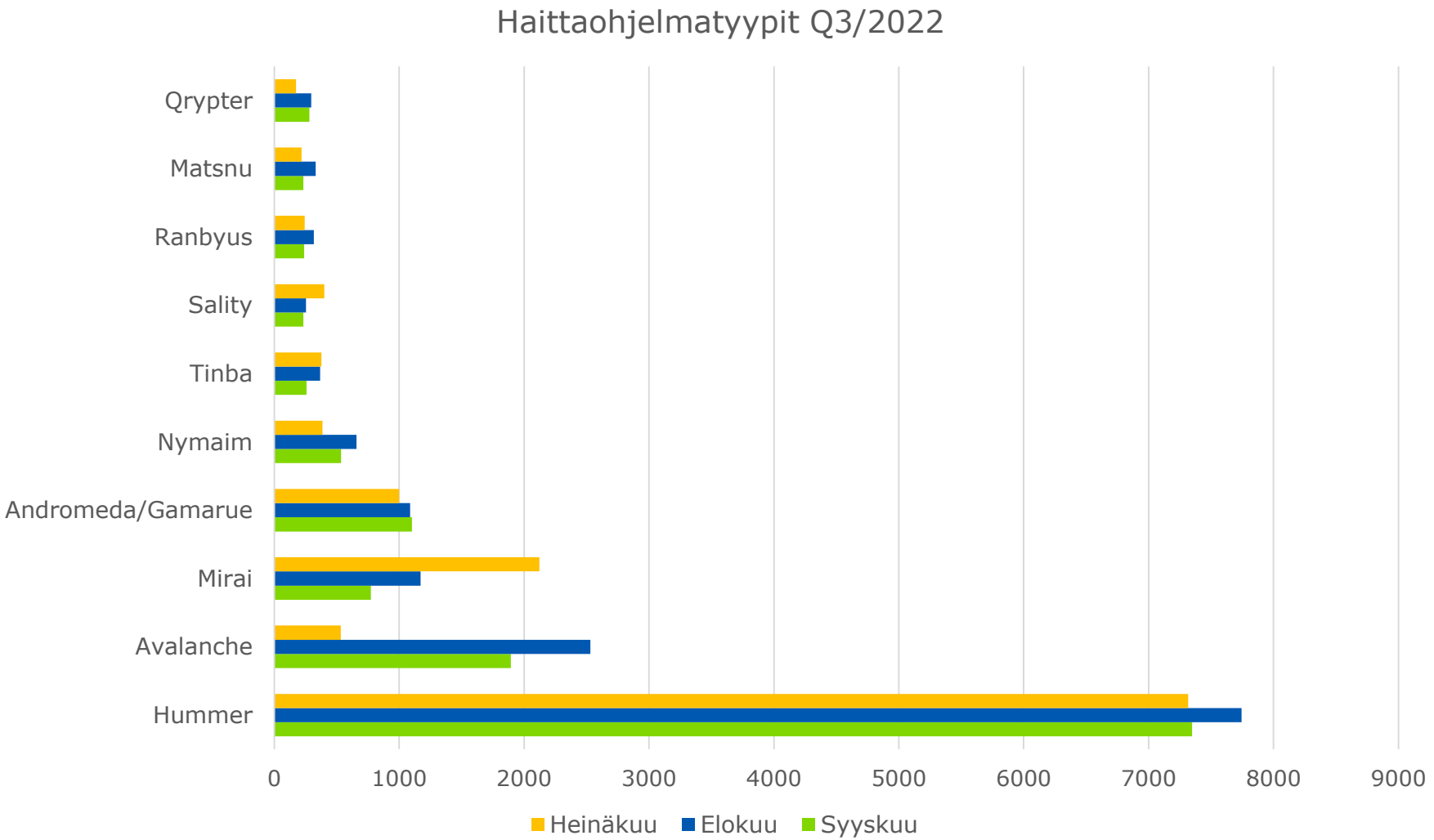
Haittaohjelmat

- Olemme vastaanottaneet muutamia ilmoituksia kiristyshaittaohjelmista lokakuun aikana.
  - Kiristyshaittaohjelmia ilmoitetaan tasaisesti, viimeaikoina olemme saaneet useita ilmoituksia eri varianteista.
  - Syyskuussa kerroimme kiristyshaittaohjelmien määrän kasvusta Suomessa. Ne ovat havaintojemme mukaan lisääntyneet noin 30 prosenttia vuoden 2021 jälkeen.
  - Kiristyshaittaohjelmahyökkäyksestä kannattaa aina ilmoittaa Kyberturvallisuuskeskukselle(4), sekä tehdä rikosilmoitus poliisille.
  - Kyberturvallisuuskeskus keräsi kysymyksiä kiristyshaittaohjelmista artikkelin kautta, ja vastaamme kysymyksiin kootusti.(6)

Analyysi

- Kiristyshaittaohjelmia (engl. Ransomware) käytetään kyberhyökkäyksissä, joissa verkkorikolliset pyrkivät salaamaan organisaation datan salausalgoritmilla ja vaativat lunnaita tietojen palauttamista vastaan.
- Rikolliset usein myös varastavat luottamuksellisia tietoja ja voivat kiristää organisaatiota tietovuodoilla.

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.(7)

Haavoittuvuus

- OpenSSL-kirjaston versiossa 3.0 on kriittinen haavoittuvuus.
  - Tietojen salaamiseen ja salattuun välittämiseen käytetyn OpenSSL-kirjaston versiosta 3.0 on löydetty kaksi vakavaa haavoittuvuutta.
  - Uusin versio 3.0.7 on syytä päivittää mahdollisimman pian. Haavoittuvuudet eivät koske vanhempia 1.1.1 tai sitä edeltäneitä versioita.
  - Aluksi kriittiseksi arvioidut haavoittuvuudet CVE-2022-3602 ja CVE-2022-3678 muuttuivat OpenSSL:n ja yhteistyötahojen tarkastelun jälkeen luokitukseltaan vakaviksi.
  - Sähköpostiosoitteiden käsittelyyn liittyvät haavoittuvuudet voivat pahimmillaan mahdollistaa etänä suoritettavat komennot - mutta todennäköisin tilanne on palvelunestotila.
  - Lisätietoa haavoittuvuustiedotteessa verkkosivuillamme.(8)

Kuukauden haavoittuvuusjulkaisut

- Kriittinen haavoittuvuus Adobe Commerce- ja Magento-verkkokauppa-alustoissa (17/2022).
  - Adobe on julkaissut korjauksen kriittiseksi luokiteltuun haavoittuvuuteen, joka antaa hyökkääjälle mahdollisuuden suorittaa komentoja etänä verkkokauppapalvelimella.
- Kriittinen haavoittuvuus Adobe Acrobat ja Reader tuotteissa (18/2022).
  - Onnistunut hyväksikäyttö voi johtaa mielivaltaisen koodin suoritukseen.
- Kriittinen haavoittuvuus Apache Commons Text –komponentissa (19/2022).
  - Apache Commons Text -komponentissa oleva haavoittuvuus mahdollistaa mielivaltaisen koodin suorittamisen etänä.
- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

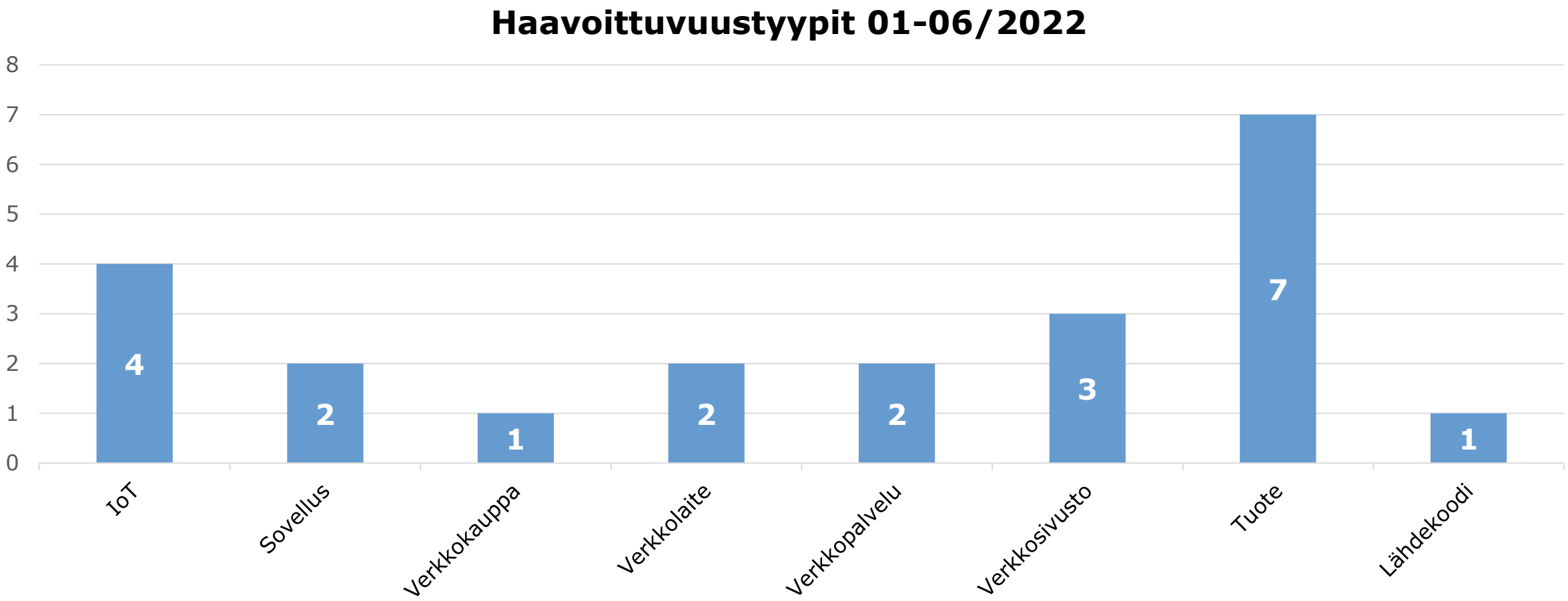
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- **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 19 kpl (tilanne 1.11.2022)**
  - 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

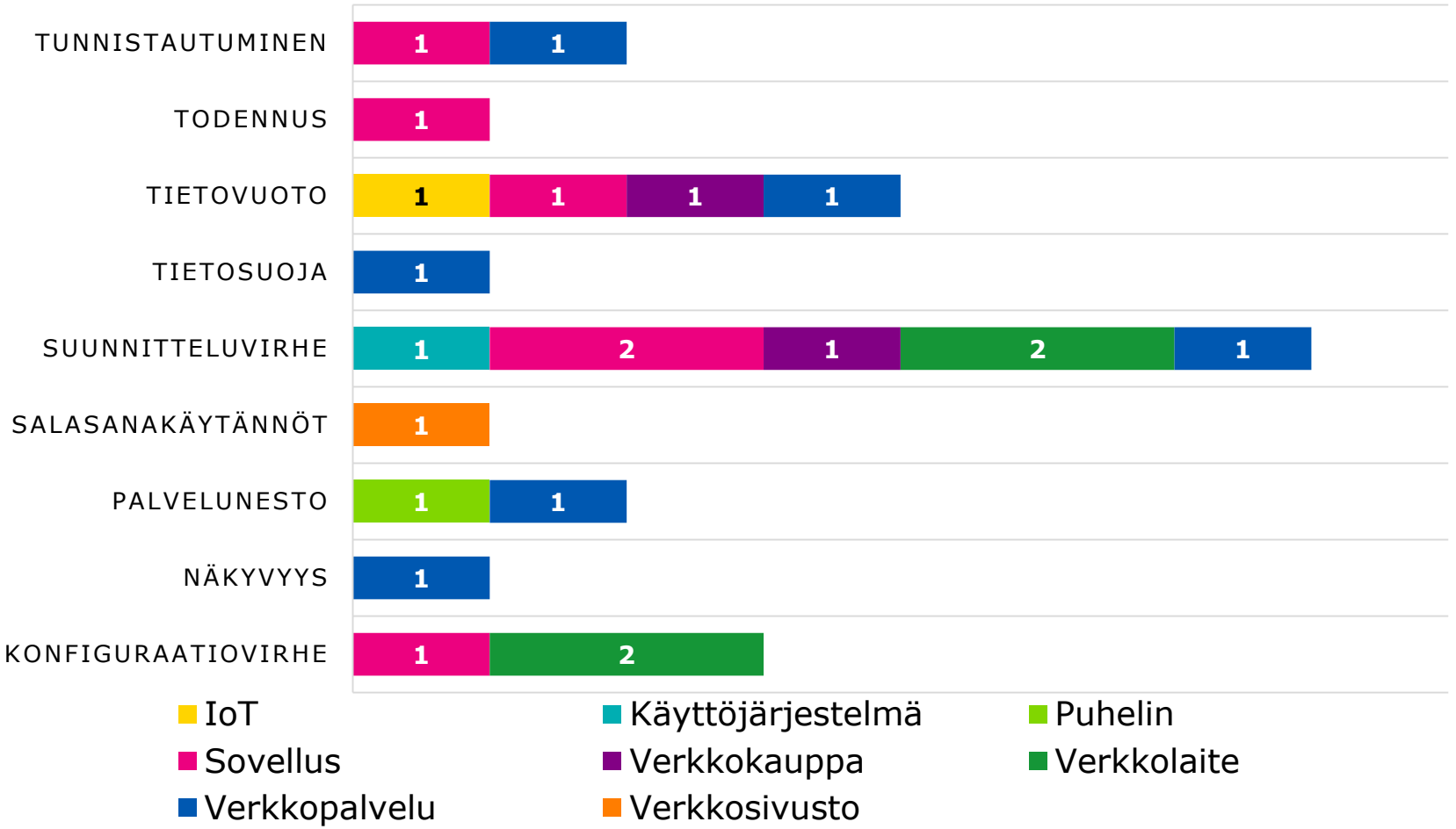
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- 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



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 – standardit ja lainsäädäntö

- Vuotuinen Singapore Cybersecurity Week järjestettiin 18.–20.10. 2022. Tapahtuman yhteydessä julkistettiin Singaporen ja Saksan tietoturvallisuusviranomaisen BSI:n välinen sopimus kansallisten IoT-tietoturvamerkkien vastavuoroisesta tunnustamisesta.(10)
  - Traficom ja Singapore julkaisivat vuosi sitten vastaavan vastavuoroisen tunnustamisen sopimuksen samaisessa tapahtumassa.(11)
  - Kaikkien merkkien vaatimukset perustuvat standardiin ETSI EN 303645 Cyber Security for Consumer Internet of Things: Baseline Requirements.
  - ETSIn standardin odotetaan olevan merkittävässä roolissa myös helmikuussa voimaan astuneen radiolaitedirektiivin (RED) delegoidun tietoturvasäädöksen harmonisoitujen standardien luomisessa.
- Singapore on tehnyt myös työkohde-ehdotuksen kansainvälisestä standardista ISO/IEC PWI 27404 Universal cybersecurity labelling framework for consumer IoT. Ehdotus on parhaillaan lausuttavana.
- Myös Yhdysvaltain Valkoinen talo on ilmaissut aikovansa julkaista tietoturvamerkin IoT-kuluttajalaitteille.(12)

Analyysi

- Laitteiden määrän kasvaessa myös niihin liittyvät riskit kasvavat ja yleistyvät.
- Kehitys heijastuu sääntelyn standardien ja suositusten lisääntymisenä.
- Internetiin kytkettävien laitteiden tietoturvallisuus vaikuttaa yli rajojen. Sirpaleiset vaatimukset vaikeuttavat myös kansainvälisillä markkinoilla toimivien yritysten asemaa. Tämän vuoksi vaatimuksia pyritään kehittämään ja harmonisoimaan kansainvälisessä yhteistyössä.

IoT – lääkinnällisten laitteiden haavoittuvuudet

- Yhdysvaltain liittovaltion poliisi FBI varoitti päivittämättömien lääkinnällisten laitteiden mahdollistavan kyberhyökkäyksiä.(13)
- FBI perustaa varoituksensa muiden aikaisemmin julkaisemiin raportteihin, joiden mukaan korjaavat päivitykset lääkinnällisten laitteiden ohjelmistoihin tulevat saataville hitaasti ja osaan haavoittuvuuksia ei julkaista korjauksia lainkaan. Laitteiden omistajat asentavat päivityksiä hitaasti tai eivät ollenkaan. Lisäksi laitteet ovat käytössä selvästi pidempään kuin esimerkiksi toimistotietotekniikka, jopa 10-30 vuotta.
- FBI suosittelee hallitsemaan riskejä ainakin laitteita suojaavilla tietoturvaohjelmistoilla, käyttäjien ja pääsyoikeuksien hallinnalla, ajantasaisella laiteinventaariolla, aktiivisella haavoittuvuuksien hallintaprosessilla sekä käyttäjien kouluttamisella.

Analyysi

- Lääkinnällisiin laitteisiin vaikuttavat kyberhyökkäykset voivat uhata suoraan ihmisten terveyttä ja jopa elämän edellytyksiä.
- FBI ei ilmaissut, että se olisi havainnut lääkinnällisten laitteiden haavoittuvuuksien hyväksikäyttöä. Hyväksikäytön mahdollisten seurausten vakavuuden vuoksi riskejä tulisi silti hallita aktiivisesti.
- EU:ssa lääkinnällisistä laitteista annettuun asetukseen sisältyy myös tietoturvallisuutta koskevia vaatimuksia. Suomessa asetuksen valvonnasta vastaa Fimea.(14)
- Huoltovarmuuskeskuksen Kyber-Terveys-hankkeessa kehitettiin sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimusten malli, jota kannattaa käyttää jo ennen laitteiden hankintaa.(15)

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

- Lokakuussa yleisissä viestintäpalveluissa oli 2 merkittävää toimivuushäiriötä.
  - Vakavuusluokat: A: 0, B: 1, C: 1
- Häiriöt aiheuttivat muutaman tunnin katkoksen yritysliittymien puheluihin ja paikallisesti kaupunginosan mobiiliverkon toimintaan.
  - Yleisesti verkot ovat toimineet lokakuussa hyvin, ja poikkeamia oli keskitasoa vähemmän.
- Merikaapelit ovat puhuttaneet syksyllä myös Suomessa. Valtaosa internetin infrastruktuurista sijaitsee maailman valtamerten pohjissa.
  - Aiheesta on uutisoitu aktiivisesti ja seuraavassa artikkelissa eri tahot kertovat tilanteesta ja varautumisesta.(16)
- WhatsAppin toiminnassa oli käyttökatko lokakuussa. Sovelluksen käyttäjät eivät pystyneet lähettämään tai vastaanottamaan viestejä.(17)
  - Varautuminen pikaviestimienkin katkoksiin on suositeltavaa.

Analyysi

- Yleisten viestintäpalveluiden toimivuus Suomessa oli vuonna 2022 keskimäärin hyvä.
- Kuukaudessa on keskimäärin noin kuusi merkittävää toimivuushäiriötä.
- Toimivuushäiriöt kotimaan verkossa ja globaaleissa palveluissa osoittavat meille, että 2020-luvulla merkittävän palvelukatkoksen aiheuttajana voi olla edelleen hajonnut laite, kaivinkoneen kauha tai työntekijä näppäimistöineen.

Palvelunestohyökkäykset

- Palvelunestohyökkäysilmoituksia aiempaa enemmän.
  - Lokakuussa Kyberturvallisuuskeskukselle ilmoitettujen palvelunestohyökkäysten määrä on noin 25% koko vuoden ilmoituksista. Julkaisimme artikkelin aiheesta verkkosivuillamme.(18)
- Lokakuu on ollut palvelunestohyökkäysten osalta kuluvan vuoden aktiivisin, ja kesän jälkeen ilmoitusmäärät Kyberturvallisuuskeskukselle ovat kasvaneet kuukausi kuukaudelta
  - Kyberturvallisuuskeskus on vastaanottanut tänä vuonna enemmän ilmoituksia palvelunestohyökkäyksistä, kuin viime vuonna.
- YLE kertoo artikkelissaan esimerkiksi Yle Areenaan kohdistuneista palvelunestohyökkäyksistä.(19)

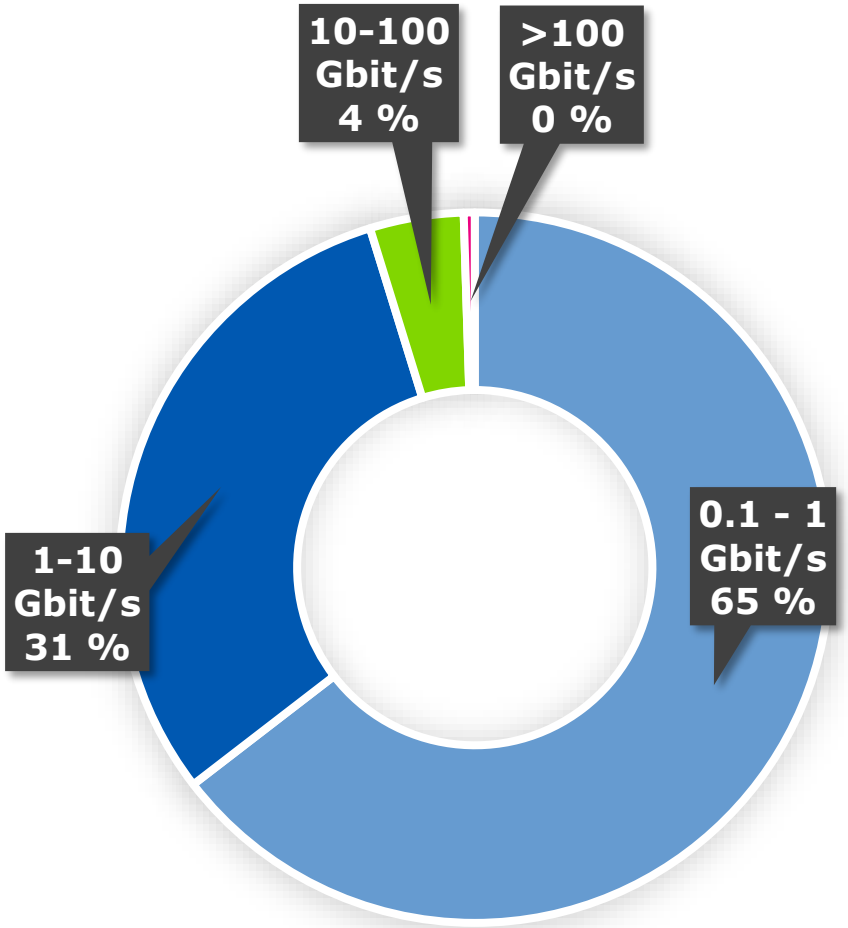
Analyysi

- Syksyllä "carpet bombing"-, eli ns. mattopommitustekniikka, on näkynyt ilmiönä joissain ilmoituksissa.
  - Tämä tarkoittaa, että hyökkäyksen kohteena on yhden tai muutaman palvelimen sijasta suurempi osa kohdeorganisaation verkko-osoitteista.
  - Hyökkäystapa saattaa osoittaa organisaation verkosta suojaamatta jääneet osat, jotka voivat aiheuttaa vaikutuksia palvelimille tai palveluihin.
  - Kokonaisen verkko-osoiteavaruuden hyökkäysten torjuminen on usein haastavampaa kuin yksittäisiin osoitteisiin kohdistuva hyökkäys.
- Yleisesti sovellustason hyökkäykset ovat aiheuttaneet organisaatioille suurinta päänvaivaa.
  - Näissä tapauksissa sivustolle voi saapua miljoonia tavallisia pyyntöjä hyvin lyhyessä ajassa aiheuttaen ongelmia palveluihin.

Palvelunestohyökkäysten tunnuslukuja

3kk

- 207 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q3/2022.
- Noin 78% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q3/2022 - 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

- Haavoittuvuuksien hyödyntäminen on säilynyt edelleen kybervakoilun yhtenä keskeisenä keinona tunkeutua organisaatioiden järjestelmiin.
- Valtiolliset kybertoimijat voivat hyödyntää joko aiemmin tiedossa olleita mutta syystä tai toisesta paikkaamatta jätettyjä tai niin sanottuja nollapäivähaavoittuvuuksia.
  - Esimerkiksi Microsoft Exchangessa ollutta, ProxyNotShell-nimellä kutsuttua haavoittuvuuskokonaisuutta on raportoidusti hyödynnetty ainakin elokuusta lähtien. Microsoftin analyysiryhmä MSTIC:n mukaan tekijänä on todennäköisesti ollut yksi APT-ryhmä.
  - APT-toimijoiden on varoitettu hyödyntäneen myös Zimbran haavoittuvuutta, joka nousi esiin syyskuussa.
  - Fortinet puolestaan varoitti tuotteissaan olleen haavoittuvuuden aktiivisesta hyödyntämisestä tunkeutumisissa ja kehotti pikaiseen korjaavan päivityksen asentamiseen. Fortinet ei täsmentänyt toimijoiden motiiveja.[(25)]

Analyysi

- Internetistä saavutettavissa olevien järjestelmien ja laitteiden päivitysten ajantasaisuus on ensiarvoisen tärkeä osa suojautumista myös APT-hyökkäyksiltä.
- APT-hyökkäyksissä hyödynnetään usein jo tiedossa olevia haavoittuvuuksia, mutta ryhmät voivat ottaa ketterästi työkalupakkiinsa myös uusia haavoittuvuuksia hyödyntäviä menetelmiä, mikä asettaa paineita organisaatioiden päivitystahdille.

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

- Uusi ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta.
  - Liikenne- ja viestintävirasto on antanut ohjeen välitystietojen käsittelyyn liittyvien tapahtuma- eli lokitietojen tallentamisesta ja säilyttämisestä.
  - Ohje korvaa Viestintäviraston suosituksen 308/2004 S tunnistamistietojen käsittelyä koskevien tietojen tallentamisesta ja se koskee kaikkia viestinnän välittäjiä.
  - Sähköisen viestinnän palveluista annetun lain 145 § säätämisen myötä tapahtumatietojen tallennusvelvollisuus laajennettiin teleyrityksistä kaikkiin viestinnän välittäjiin, kuten yhteisötilaajiin.
  - Ohje ei koske lokitietoja yleisellä tasolla, vaan keskeisenä sisältönä niiden välitystietojen käsittely, joka tapahtuu luottamuksellisuuden ja yksityisyyden suojan kannalta keskeisiä välitystietoja sisältävissä tietojärjestelmissä. Ohje tuli voimaan 27.10.2022.(20)

Oikeudelliset asiat

- Hallituksen esitys eduskunnalle laeiksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä Puolustusvoimissa annetun lain 29 §:n ja henkilötietojen käsittelystä poliisitoimessa annetun lain 22 §:n muuttamisesta (HE 243/2022).
  - Tavoitteena viranomaisten välisen tiedonvaihdon tehostaminen yhteiskunnan elintärkeiden toimintojen kannalta merkittävissä tietoturvaloukkaustilanteissa ja niiden uhkissa.
  - Ehdotuksessa Puolustusvoimien ja poliisin Liikenne- ja viestintävirastolle antamaa virka-apua ehdotetaan laajennettavaksi koskemaan merkittäviä tietoturvaloukkauksia ja -uhkia. Lisäksi ehdotetaan säädettäväksi viestinnän välittäjän oikeudesta oma-aloitteisesti luovuttaa Liikenne- ja viestintävirastolle tietoja viesteistä ja välitystiedoista tietoturvaloukkausten selvittämiseksi tai ennaltaehkäisemiseksi. Lait on tarkoitettu tulemaan voimaan 1.2.2023.(21)
- Hallituksen esitys eduskunnalle laeiksi sähköisen viestinnän palveluista annetun lain sekä Liikenne- ja viestintävirastosta annetun lain 3 §:n muuttamisesta (HE 170/2022).
  - Tavoitteena lainsäädäntömuutokset, jotta Galileo-satelliittipaikannusjärjestelmän julkisesti säännelty satelliittipalvelu on mahdollista ottaa Suomessa kansallisesti käyttöön vuoden 2025 aikana.
  - Liikenne- ja viestintävirastolle säädettäisiin nykyistä laajempi toimivaltuus tehdä tarkastuksia satelliittipalvelun tarjoajaan, käyttäjään ja teknologian valmistajaan sekä Puolustusvoimiin, silloin kun se tarjoaa palvelua maanpuolustuksen tarpeisiin. Lisäksi ehdotetaan tietoyhteiskuntamaksun korottamista Liikenne- ja viestintävirastolle sijaintitietopalvelusta aiheutuvien vuosittaisten toiminta- ja ylläpitokustannusten kattamiseksi.
  - Liikenne- ja viestintävirastosta annettua lakia muutettaisiin siten, että jatkossa viraston Kyberturvallisuuskeskus vastaisi osaltaan julkisesti säännellyn palvelun järjestämisestä. Lait on tarkoitettu tulemaan voimaan 1.1.2023.(22)

Oikeudelliset asiat

- Hallituksen esitys eduskunnalle laeiksi maa-asemista ja eräistä tutkista sekä avaruustoiminnasta annetun lain muuttamisesta ja sakon täytäntöönpanosta annetun lain 1 §:n muuttamisesta (HE 113/2022).
  - Suomessa ei nykyisellään ole lainsäädäntöä, jonka nojalla satelliittikaukokartoitusinstrumenteilla, vastaanottavilla maa-asemilla tai tutkilla harjoitettava toiminta taikka siinä taltioidun datan ja tiedon jakelu ja käyttö olisivat sellaisenaan luvanvaraista toimintaa.
  - Laissa säädettäisiin maa-aseman tai tutkan perustamisen sekä maa-asema- ja tutkatoiminnan luvanvaraisuudesta. Lupaviranomaisena toimisi Liikenne- ja viestintävirasto. Luvan edellytyksenä olisi erityisesti toiminnan riskittömyys kansallisen turvallisuuden kannalta ja tiettyjen teknisten turvallisuusvaatimusten täyttyminen. Luvan käsittelyä varten pyydettäisiin lausuntoa turvallisuusviranomaisilta. Toiminnanharjoittaja olisi velvollinen raportoimaan toiminnastaan ja asiakkaistaan, lupaviranomaiselle.
  - Myös satelliittikaukokartoituksen harjoittaminen olisi jatkossa samoin edellytyksin luvanvaraista. Lupaviranomaisena toimisi työ- ja elinkeinoministeriö, joka toimii myös avaruustoiminnan lupaviranomaisena. Laki on tarkoitus saada voimaan mahdollisimman pian.(23)
- Hallituksen esitys eduskunnalle julkisen hallinnon automaattista päätöksentekoa koskevaksi lainsäädännöksi (HE 145/2022).
  - Tavoitteena mahdollistaa automaattinen päätöksenteko julkisessa hallinnossa sekä säätää EU:n yleisen tietosuoja-asetuksen edellyttämä kansallinen oikeusperusta automatisoitujen yksittäispäätösten tekemiseksi.
  - Esityksessä ehdotetaan lisättäväksi hallintolakiin uusi asioiden automaattista ratkaisemista koskeva luku. Ehdotuksen mukaan viranomainen voisi ratkaista automaattisesti asian, johon ei sisälly seikkoja, jotka viranomaisen etukäteisen harkinnan mukaan edellyttäisivät tapauskohtaista harkintaa, tai johon sisältyvät tapauskohtaista harkintaa edellyttävät seikat virkamies tai muu asian käsittelijä on arvioinut. Ehdotetut lait on tarkoitettu tulemaan voimaan 1.1.2023.(24)

Arjen kyberturvallisuus

Tunnista turvallinen verkkosivu

- Sähköpostiviestin tai verkkosivun aidon näköinen ulkoasu ei takaa verkkosivun sisällön aitoutta. Rikolliset voivat kopioida verkkosivujen sisällön ja ulkoasun aidoilta sivuilta toisille sivuille ja muuttaa tuottamiaan kopioita haitallisella tavalla.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tunnista-turvallinen-verkkosivu-osoitteen-perusteella

Kiertävät sähkökatkot vaikuttavat myös teleyritysten verkkojen ja palvelujen toimivuuteen

- Artikkelissa kerromme, miten mahdolliset kiertävät sähkökatkot vaikuttavat mobiiliyhteyksien, kiinteiden laajakaistojen sekä televisio- ja radiopalvelujen toimintaan.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kiertavat-sahkokatkot-vaikuttavat-myos-teleyritysten-verkkojen-ja-palvelujen

Traficomin Älyä ostoksiin –kampanja tulee taas

- Loppuvuodesta kauppa käy kiivaimmillaan, kun ostoskampanjat ovat vauhdissa. Keräsimme siksi muistilistan vastuullisista valinnoista, joita tehdä ostoksilla ja ostosten jälkeen.
- Kampanjan sivuilta löydät tärkeää tietoa kodin älylaitteiden tietoturvasta, käytetyn elektroniikan kierrätyksestä ympäristöä säästäen ja ohjeita langattomien laitteiden ostamisesta ja käytöstä sekä dronen turvallisesta lennättämisestä.
- Lue lisää: https://www.traficom.fi/fi/s/alyaostoksiin

Uutisia Kyberturvallisuuskeskuksesta

Tietoturvan suunnannäyttäjä -tunnustus STT:lle - avoin tiedon jakaminen tukee kyberuhkiin varautumista

- Liikenne- ja viestintävirasto Traficomin jakaman Tietoturvan suunnannäyttäjä -tunnustuksen sai tänä vuonna Suomen tietotoimisto STT.
- Tunnustuksen perusteluissa STT:tä kiitettiin avoimesta viestinnästä, sen jouduttua kyberhyökkäyksen kohteeksi kesällä 2022.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-suunnannayttaja-tunnustus-sttlle-avoin-tiedon-jakaminen-tukee-kyberuhkiin

Ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta astui voimaan 27.10.2022

- Liikenne- ja viestintävirasto Traficom on antanut uuden ohjeen välitystietojen käsittelyyn liittyvien tapahtuma- eli lokitietojen tallentamisesta ja säilyttämisestä, josta säädetään sähköisen viestinnän palveluista annetun lain (917/2014) 145 §:ssä.
- Ohje koskee kaikkia viestinnän välittäjiä.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohje-valitystietojen-kasittelya-koskevien-tietojen-tallentamisesta-astuu-voimaan

Digiturvabarometrin tulokset herättävät huolen suomalaisten digiturvaosaamisen tasosta

- Digi- ja väestötietoviraston tuoreen Digiturvabarometrin mukaan 75 prosenttia suomalaisista ei ole osallistunut digiturvakoulutukseen ainakaan vuoteen tai kenties koskaan.
- Tilanne huolestuttaa ajassa, jossa sekä digitaalisten palveluiden käyttö että verkkorikollisuus ovat jatkuvassa kasvussa.
- https://dvv.fi/-/digiturvabarometrin-tulokset-herattavat-huolen-suomalaisten-digiturvaosaamisen-tasosta-nyt-tarvitaan-koulutusta

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) Suojelupoliisin kansallisen turvallisuuden katsaus https://supo.fi/kansallisen-turvallisuuden-katsaus

2) Kyberturvallisuuskeskuksen tiedote kyberympäristön uhkatason noususta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

3) Kyberturvallisuuskeskuksen ohjeet ja oppaat organisaatioille ja yrityksille https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

4) Kyberturvallisuuskeskukselle ilmoittaminen https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

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

6) Kyberturvallisuuskeskuksen artikkeli, Kysy kiristyshaittaohjelmista – me vastaamme https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kysy-kiristyshaittaohjelmista-me-vastaamme

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

8) OpenSSL haavoittuvuustiedote https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_20/2022

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

Lähdeluettelo

10) Singapore and Germany Sign Mutual Recognition Arrangement on Cybersecurity Labels for Consumer Smart Products https://www.csa.gov.sg/News/Press-Releases/singapore-and-germany-sign-mutual-recognition-arrangement-on-cybersecurity-labels-for-consumer-smart-products

11) Traficom: International cooperation helps Finnish businesses enter the market of secure smart devices https://www.traficom.fi/en/news/international-cooperation-helps-finnish-businesses-enter-market-secure-smart-devices

12) Statement by NSC Spokesperson Adrienne Watson on the Biden-Harris Administration's Effort to Secure Household Internet-Enabled Devices https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/20/statement-by-nsc-spokesperson-adrienne-watson-on-the-biden-harris-administrations-effort-to-secure-household-internet-enabled-devices/

13) FBI private industry notification https://www.ic3.gov/Media/News/2022/220912.pdf

14) Fimean tiedote asetuksesta https://www.fimea.fi/web/guest/-/laakinnallisia-laitteita-koskeva-uusi-eu-asetus-voimaan-26.5.2021

15) Traficomin tiedote Kyber-Terveys –hankkeesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja

16) Yle: Merenalainen internet sisältää haavoittuvuuksia myös Suomen osalta – näin Venäjä voisi halutessaan eristää Yhdysvallat https://yle.fi/uutiset/74-20000693

Lähdeluettelo

17) Yle: Whatsapp toimii taas – viestisovellus ehti olla kaatuneena pari tuntia https://yle.fi/uutiset/3-12666457

18) Kyberturvallisuuskeskus: Palvelunestohyökkäysten määrä on kasvussa - vaikutukset vähäisiä
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaysten-maara-kasvussa-vaikutukset-vahaisia

19) Yle: Palvelunestohyökkäykset ryöpsähtivät – kohteena muun muassa suosittu Yle Areena https://yle.fi/uutiset/3-12665063

20) Kyberturvallisuuskeskus: Ohje välitystietojen käsittelyä koskevien tietojen tallentamisesta
https://www.kyberturvallisuuskeskus.fi/fi/saadokset/ohje-valitystietojen-kasittelya-koskevien-tietojen-tallentamisesta

21) Hallituksen esitys HE 243/2022 vp https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_243+2022.aspx

22) Hallituksen esitys HE 170/2022 vp https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_170+2022.aspx

23) Hallituksen esitys HE 113/2022 vp https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_113+2022.aspx

24) Hallituksen esitys HE 145/2022 vp https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_145+2022.aspx

25) Bleepingcomputer: Fortinet urges admins to patch bug with public exploit immediately
https://www.bleepingcomputer.com/news/security/fortinet-urges-admins-to-patch-bug-with-public-exploit-immediately/