TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Marraskuu 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

15.12.2022

Kybersää marraskuu 2022

Tietomurrot ja -vuodot

- Tietomurroista tehtyjen ilmoitusten määrä kasvaa tasaisesti. Loka-marraskuun välillä kasvu oli 12%.
- Kiristyshaittaohjelmien sekä sellaiseksi naamioituneiden tuhoavien haittaohjelmien määrät ovat kasvaneet maailmalla.

Huijaukset ja kalastelut

- Poliisihuijaukset ja muut kiristykset aiheuttavat edelleen kiusaa.
- Palkanmaksuhuijausten yritykset ovat lisääntyneet.
- Marraskuun ajankohtaisteema Black Friday sai myös huijarit liikkeelle.

Haittaohjelmat ja haavoittuvuudet

- Yhdysvaltain tietoturvaviranomainen CISA ylläpitää Shields Up –sivustoa, jolla on mm. hyväksikäytettyjen haavoittuvuuksien lista ja haavoittuvuuksien hallintaan liittyviä ohjeita.

Automaatio ja IoT

- Teollisuusympäristöjen kyberuhat ovat nousussa. Kiristyshaittaohjelma-tapausten määrä on lisääntynyt syksyn aikana.
- Asentamattomien päivitysten takia vanhoja haavoittuvuuksia lymyää IoT-laitteissa.

Verkkojen toimivuus

- Marraskuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä.
- Marraskuu oli ilmoitusten perusteella lokakuun jälkeen toiseksi vilkkain palvelunestohyökkäyskuukausi.
- Osalla hyökkäyksistä oli hetkellisiä vaikutuksia palveluiden toimintaan.

Vakoilu

- Ukrainan sotaan liittyvät kybervakoilu- ja sabotaasikampanjat jatkuvat edelleen.
- Tietoturvatutkijat kertovat Mustang Pandan aktiivisesta toiminnasta kuluneen vuoden aikana.

TRAFICOM

15.12.2022

Kuukauden tunnuslukuja

+12%

Tietomurroista tehtyjen ilmoitusten määrä jatkaa tasaista kasvuaan. Loka-marraskuun välillä kasvu oli 12%, ja syys-marraskuun välillä kasvu oli 27%.

487 MILJ.

487 miljoonan Whatsapp-käyttäjän puhelinnumeroa kaupitellaan verkossa. Tiedot eivät ole peräisin tietomurrosta, vaan ne on kerätty haravointitekniikalla, jossa tietoja kerätään verkkosivuilta.

NIS2

EU:n neuvosto hyväksyi uutta lainsäädäntöä EU:n korkean kyberturvallisuustason varmistamiseksi. Uusi kyberturvallisuusdirektiivi NIS2 korvaa nykyisen kyberturvallisuusdirektiivin NIS.

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

15.12.2022

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. 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

15.12.2022

Tietomurrot ja –vuodot

- Kyberturvallisuuskeskuksen saamat ilmoitukset tietomurroista ovat kasvaneet tasaisesti syksyn aikana. Loka-marraskuun välillä kasvu oli 12% ja syys-marraskuun välillä kasvu oli 27%.
  - Osiltaan kasvua loka-marraskuun välillä selittää sosiaalisen median sekä muiden vastaavien verkkopalveluiden tilien murrot. Näiden lukumäärä kasvoi loka-marraskuun välillä noin 47%.
- Tietomurtojen lisäksi marraskuussa saimme useita ilmoituksia korkean tason kiristyshaittaohjelmista. Ilmoituksista osassa uhkatoimija oli onnistunut tietomurrossa, ja osassa tapaukset olevat jääneet yrityksiksi.
  - Conti-ryhmittymän hajoaminen on tuonut uhkatoimijakentälle useita uusia Conti-johdannaisia kiristyshaittaohjelmatoimijoita.(5)

Analyysi

- Indikaatiot maailmalla ovat korostaneet tietomurtojen, sekä kirityshaittaohjelmien kasvutrendiä.
  - Havaintoja tukevat myös kansainvälisten tiedonvaihtoverkostojen kautta saadut tarkennukset.
- Kyberturvallisuus tarjoaa useita ohjeita tietomurtojen ja kiristyshaittaohjelmien varalta.(6)(7)(8)

Tietomurrot ja –vuodot

- Ranskalainen sairaala ilmoitti heihin kohdistuneesta kiristyshaittaohjelmasta joulukuun alussa. Hyökkäys aiheutti joidenkin toimenpiteiden perumisia, sekä potilaiden siirtoja toisiin sairaaloihin.(9)
  - Euroopassa terveydenhuoltosektoriin on muutenkin kohdistunut useita kiristyshaittaohjelmatapauksia kuluneen syksyn aikana.
- Ukrainasta ja sen naapurimaista on tullut tietoturvatutkijoiden myötä tietoa kiristyshaittaohjelmiksi naamioiduista tietoja tuhoavista haittaohjelmista (wiper).(10)
- Toimintamekanismi on hyvin usein samanlainen kuin kiristyshaittaohjelmissa, mutta näissä tapauksissa tietoja ei ole mahdollista palauttaa, eikä ”kiristäjään” saa kunnolla yhteyttä.
  - Tuhoavista haittaohjelmista on ollut havaintoja kasvavissa määrin Venäjän laittoman hyökkäyssodan alettua Ukrainassa tämän vuoden helmikuussa.

Analyysi

- Vaikka nyt terveydenhuoltosektori on ollut julkisuudessa tapausten takia, kansainväliset tapaukset ovat kohdistuneet laajasti maiden huoltovarmuuskriittisiin toimijoihin
- Ohjeita organisaatioille on tarjolla verkkosivuillamme.(3)

Tietomurrot ja –vuodot

- WhatsApp käyttäjien tietoja kaupitellaan verkossa. Tietojen mukaan aineisto käsittäisi noin 487 miljoonaa puhelinnumeroa, joista 1,3 miljoona olisi suomalaisia numeroita.(11)
- Tiedot on todennäköisesti kerätty automaattisesti haravointitekniikalla.
  - On mahdollista että vuotaneita puhelinnumeroita tullaan tulevaisuudessa käyttämään erilaisiin puhelimitse tapahtuviin huijauksiin.
- Salasanojen hallintaohjelmistoa valmistava LastPass ilmoitti heidän käyttämäänsä palveluun kohdistuneesta poikkeamasta. Ilmoituksen mukaan, käyttäjien tiedot eivät olisi vaarantuneet yrityksen ”Zero Knowledge” käytänteen takia.
  - Ilmoituksen mukaan, vain käyttäjillä itsellään on mahdollisuus purkaa palveluun tallennettujen tietojen salaus.

Analyysi

- Käytettäessä varsinkin sosiaalisen median palveluita, tulisi käyttäjien pohtia kriittisesti palveluihin kerrottavien tietojen tarpeellisuuden.
- Niin kutsutussa haravointitekniikassa ei ole kyse varsinaisesta tietomurrosta, vaan ohjelmistollisesti toteutetusta tiedon keruusta internetissä.
- Salasanan hallintaohjelmistot ovat edelleen turvallisia ja suositeltavia. Tässäkin tapauksessa käyttäjien tiedot pysyivät salattuina ja täten käyttökelvottomina rikollisille.(12)

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

- Kiristyshuijauksia liikkeellä uusilla teemoilla.
  - Sitkeästi riivaava poliisihuijaus aiheuttaa edelleen yhteydenottoja. Poliisin nimissä esiintyvä huijari koettaa kiristää uhrilta rahaa lunnaiksi siitä, että luopuu kiusallisista syytteistä.
  - Toisenlaisissa kiristyshuijauksissa huijari väittää hakkeroineensa yrityksen järjestelmät ja vaatii lunnaita, ettei aiheuta tuhoa. Nämäkin ovat huijauksia, mutta järjestelmien tietoturva kannattaa silti ottaa vakavasti.
  - Kolmas huijaustapa "pornokiristys" on saanut uuden käänteen: huijari väittää tietävänsä, että uhri on pettänyt puolisoaan ja uhkaa paljastaa pettämisen, ellei lunnaita makseta. Tässäkin tapauksessa on kyseessä vain sattumanvaraisesti vastaanottajajoukolle lähetetty huijausviesti.

Analyysi

- Toimitusjohtajahuijauksina tunnetaan erilaiset organisaation johtajan nimiin väärennetyt viestit, joilla pyritään maksattamaan huijarille valelaskuja, lahjakorttikoodeja tai muita etuuksia.
- Marraskuussa on saatu useita ilmoituksia huijauksista, joissa organisaation jäsenenä esiintyvä huijari yrittää vaihtaa palkansaajan palkkatiliksi huijarin tilin.
- Palkanmaksuhuijaukset ja muut laskutuspetokset eivät onnistu, kun organisaation omista tili- ja laskutusprosesseista pidetään kiinni eikä tehdä poikkeuksia, vaikka "johtaja" niin vaatisikin.

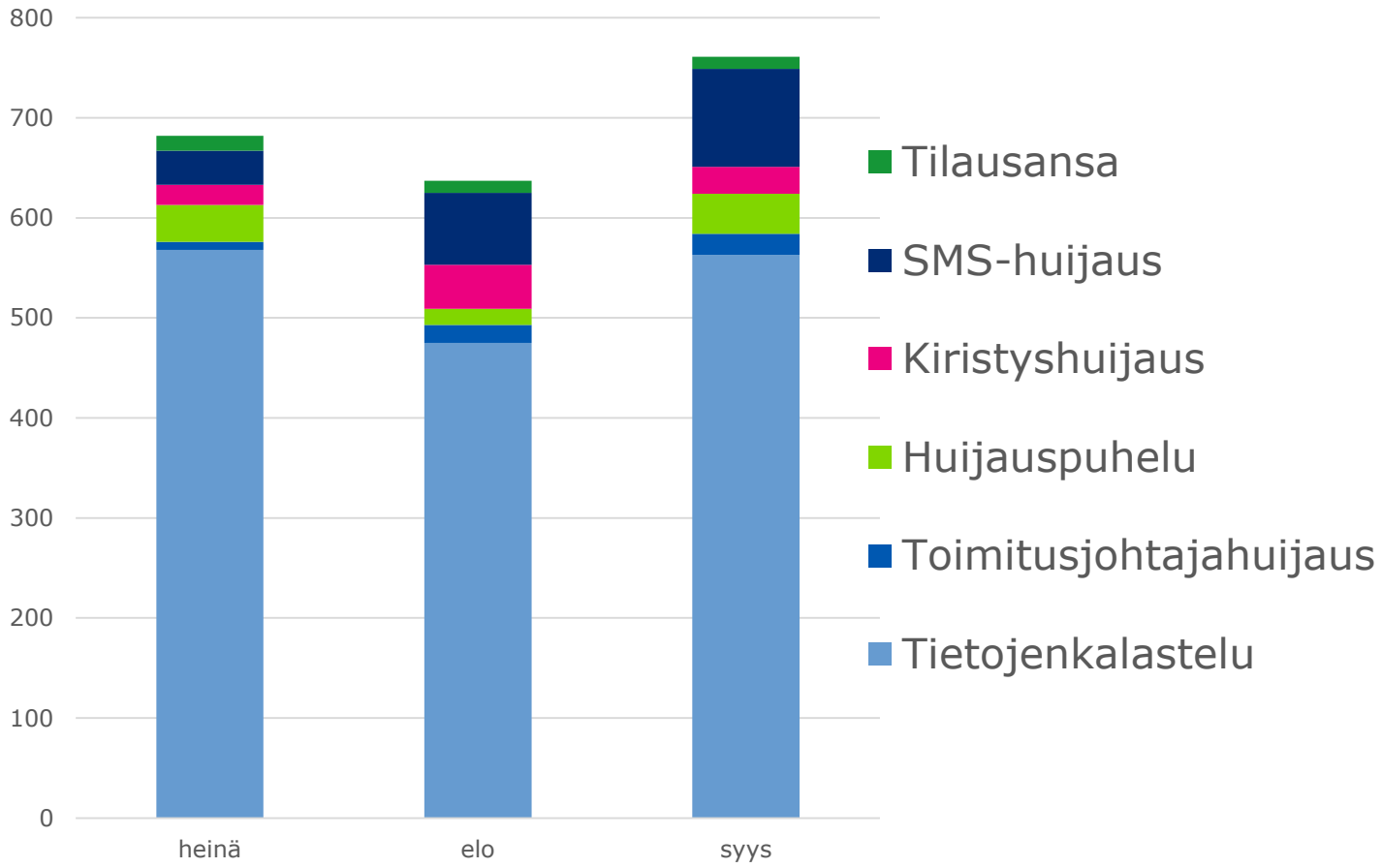
Huijaukset ja kalastelut

- Tilausansoja liikkeellä vaihtelevilla teemoilla.
  - Huijausten määrä pysyy korkeana kuukaudesta toiseen, mutta marraskuun erikoisuutena nähtiin paljon ajankohtaisia huijausviestejä Black Friday -teemalla.
  - Kaikki teemat ja uutisaiheet löytävät tiensä myös huijauksiin, niin myös Black Friday. Houkuttelevat mainostarjoukset johtivatkin tilausansoihin.
  - Muita tilausansoja tehtailtiin mm. Yle Areenan, Prisman, Tokmannin, lentoyhtiöiden ja hampurilaisravintolan nimissä lahjakorteilla houkutellen.

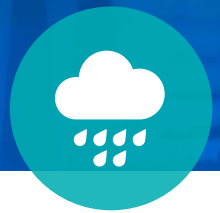
Analyysi

- Kyberturvallisuuskeskukselle on tehty useita ilmoituksia huijausviesteistä matkapuhelinoperaattorin nimissä.
- Väärennetyllä kirjautumissivulla pyydetään tunnistautumaan vahvasti pankkitunnuksilla.
- Huijari ei saamillaan pankkitunnuksilla kuitenkaan aio kirjautua operaattorin palveluun, vaan käyttää tunnuksia tyhjentääkseen uhrin pankkitilin.
- Samanlaisia kalasteluviestejä tehtaillaan edelleen pankkien, verottajan ja viranomaisten nimissä erityisestä tekstiviesteillä.

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 38 on vähentänyt kotimaisten numeroiden käyttöä huijauksiin.



Haittaohjelmat ja haavoittuvuudet

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

TRAFICOM

15.12.2022

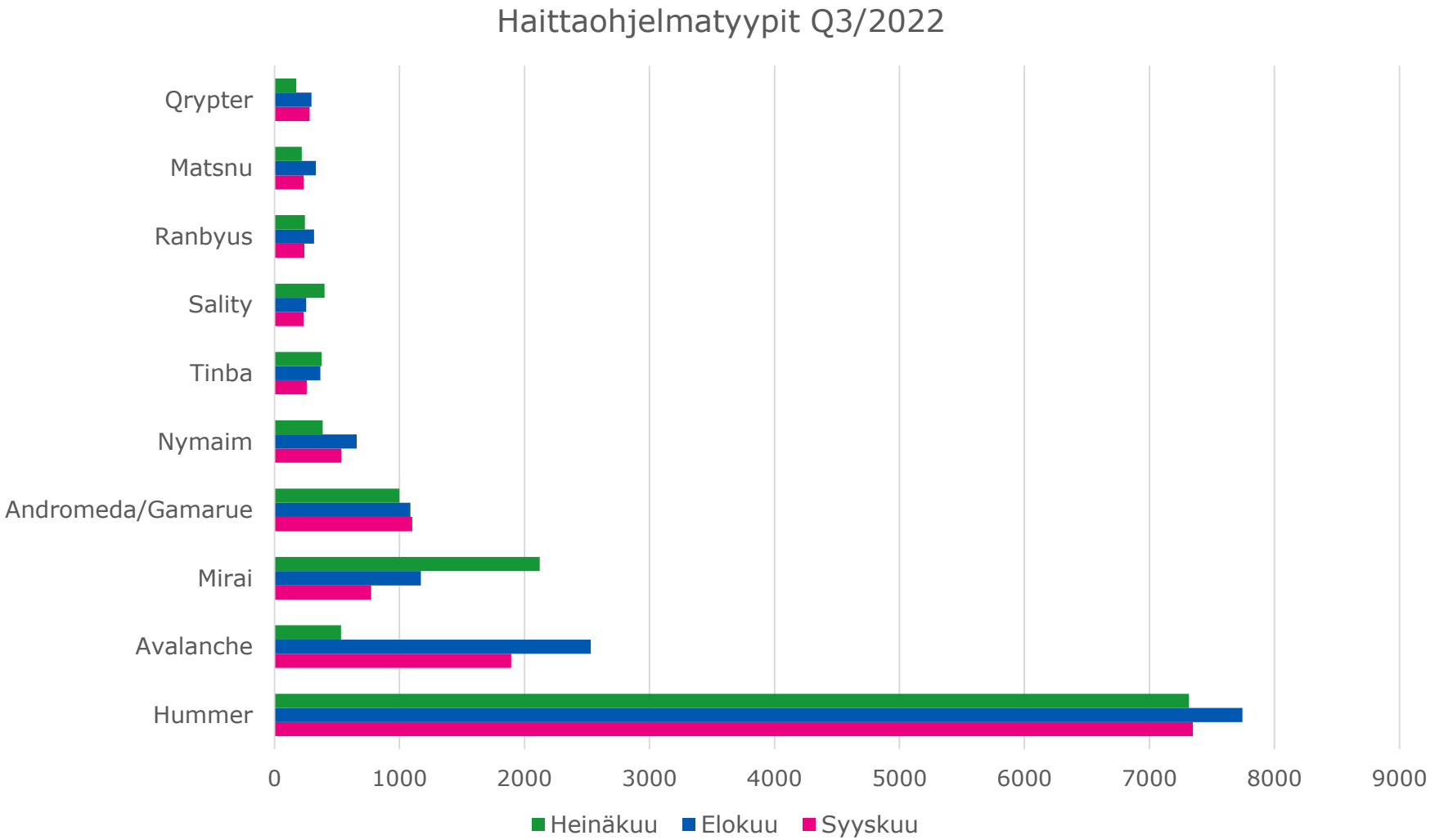
Haittaohjelmat

- Yhdysvaltain tietoturvaviranomainen CISA ylläpitää Shields Up –sivustoa, jolla on mm. hyväksikäytettyjen haavoittuvuuksien lista ja haavoittuvuuksien hallintaan liittyviä ohjeita.(13)
  - Listalla on yli 600 haavoittuvuutta.
  - Listalla olevat haavoittuvuudet ovat sellaisia, joiden hyväksikäyttötapauksia on havaittu.
  - Listaa päivitetään usein ja vanhin haavoittuvuus listalla on vuodelta 2008.

Analyysi

- CISA on todennut, että organisaatioiden tulisi olla nyt erityisen valppaina kyberympäristössä toimiessaan.
- Sivustolla on paljon ohjeita ja työkaluja, joilla organisaatioita pyritään avustamaan oman turvallisuuden ja varautumisen parantamisessa.
- Pahimmillaan paikkaamatta jäänyt haavoittuvuus voi johtaa jopa kiristyshaittaohjelmaan joten on hyvä katsoa läpi, mitä omasta ympäristöstä näkyy ulkoverkkoon.

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.(14)

Kuukauden haavoittuvuusjulkaisut

- Kaksi vakavaa haavoittuvuutta OpenSSL 3.0 –versiossa (20/2022).
- Kriittinen haavoittuvuus Citrix Gateway ja Citrix ADC –tuotteissa (21/2022).
- Kriittisiä haavoittuvuuksia VMware Workspace ONE Assist –ohjelmistossa (22/2022).

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

Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

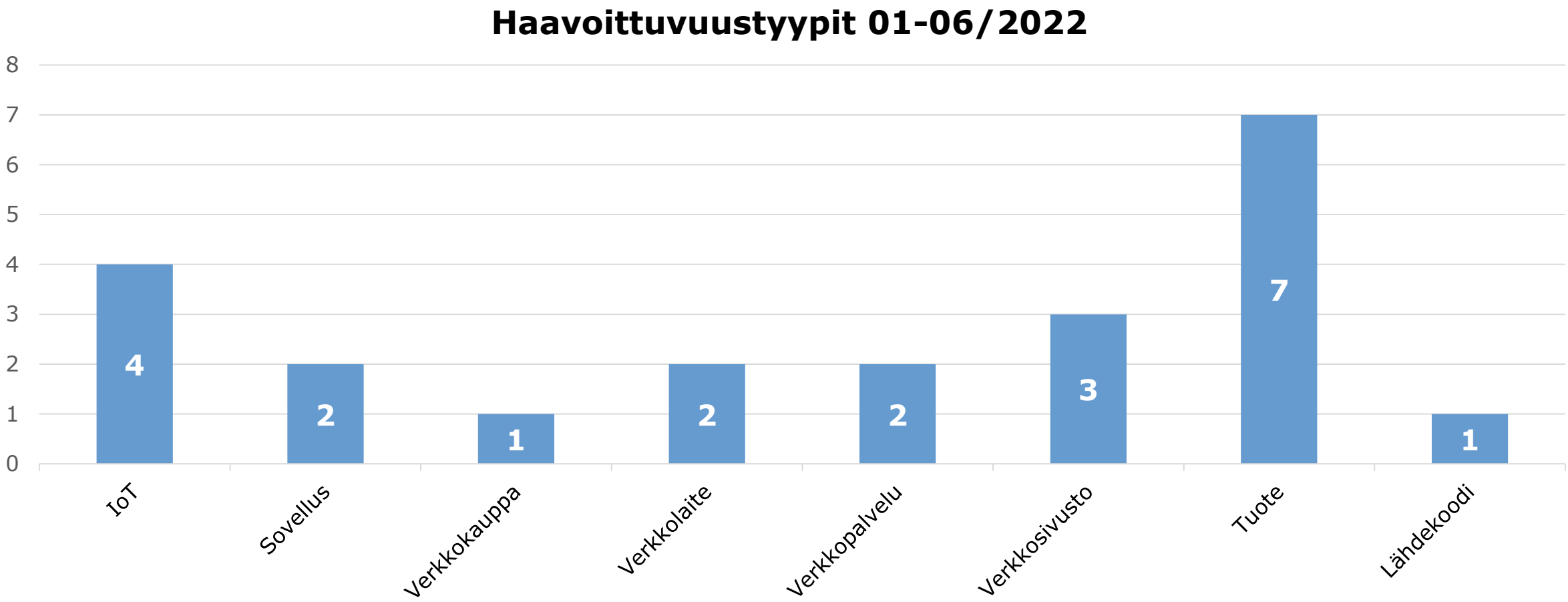
- **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta.**
  - Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
  - Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitteko haavoittuvuuden käsittelyn.
- **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta.**
  - Vastaanotamme ilmoituksia myös anonyymeiltä ilmoittajilta.
- **Haavoittuvuustiedotteita tänä vuonna 22 kpl (tilanne 9.12.2022).**
  - 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

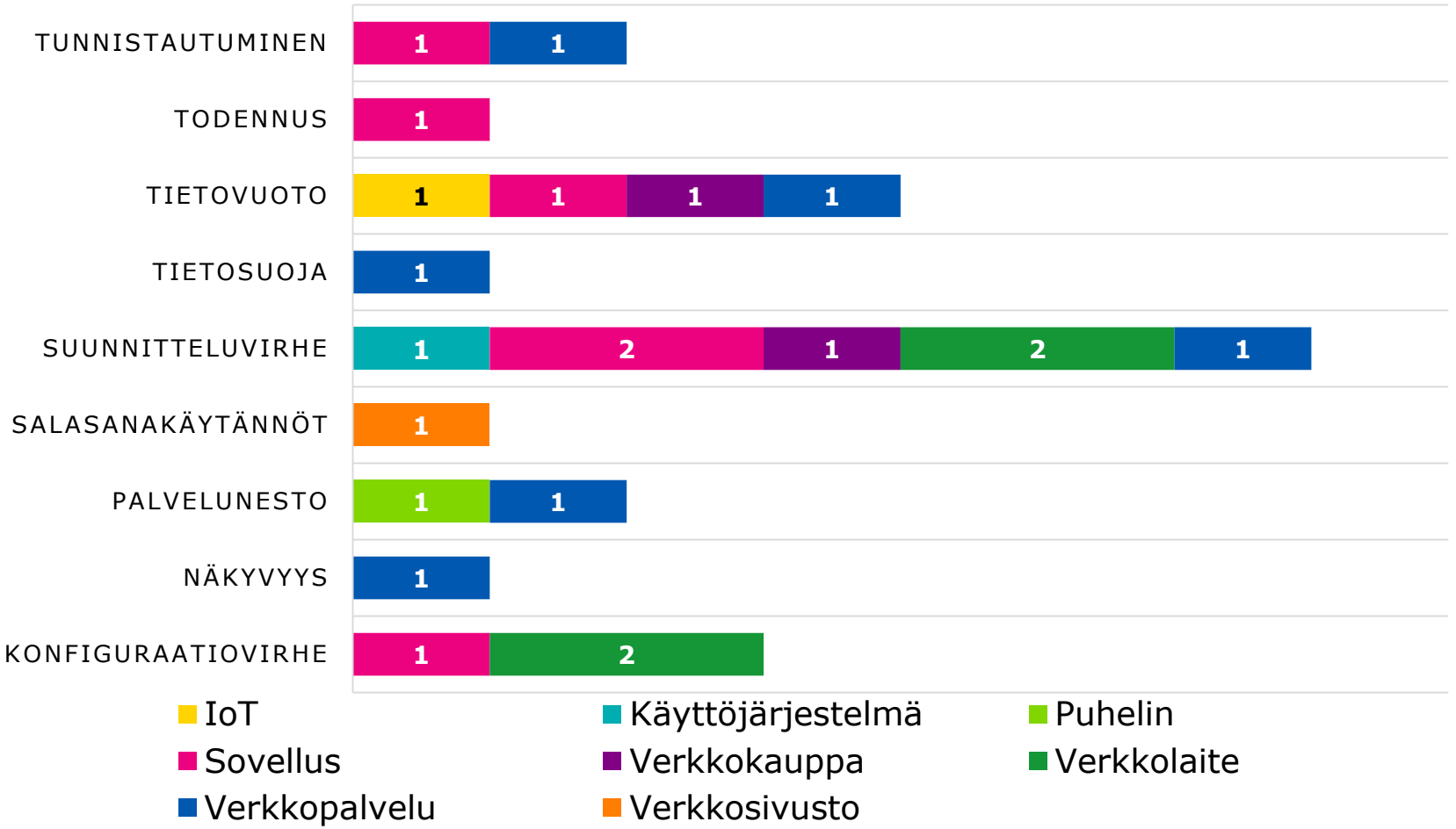
- Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- Vanhentuneet tai heikot salasanakäytännöt ovat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

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.

Automaatio

- Myös teollisuusympäristöjen kyberuhat ovat nousussa.
  - Kiristyshaittaohjelmatapausten määrä on lisääntynyt syksyn aikana niin Suomessa kuin muuallakin. Meilläkin uhreiksi on joutunut myös teollista tuotantoa harjoittavia yrityksiä. Toistaiseksi näiden tapausten ei kuitenkaan tiedetä päätyneen varsinaisiin tuotantoympäristöihin.
    - Tuotantoympäristöjä on näissäkin tapauksissa jouduttu varmuustoimena ajamaan alas haittaohjelman leviämisen estämiseksi.
  - Monissa kyberturvallisuutta käsittelevissä julkaisuissa on nostettu viime aikoina tarkasteluun kriittisessä infrastruktuurissa sekä teollisuuden tuotantolaitoksissa käytetyt teollisuusautomaatiojärjestelmät (ICS/OT).
    - Teollisuuden tuotantoympäristöihin erikoistunut tietoturvayhtiö Dragos esitti arviossaan, että loppuvuoden aikana tullaan näkemään kiristyshaittaohjelmatartuntoja myös näissä järjestelmissä.(15)
    - Samoilla linjoilla on myös Microsoft, joka nostaa raportissaan esiin usein tietoturvavalvonnan ulkopuolella olevat automaatiojärjestelmäspesifit tietoliikenneprotokollat.

Analyysi

- Kiristyshaittaohjelma saattaa päätyä myös erilaisten tiedonsiirtoyhteyksien johdosta eristetyksi kuviteltuun teollisuusympäristöön. Toipuminen voi silloin olla paljon monimutkaisempaa kuin toimistoympäristöissä.
- Kyberhyökkäyksen johdosta menetetty tuotanto saattaa muodostaa nopeasti suuret taloudelliset tappiot.
  - Pörssiyhtiö Uponor antoi 21.11.2022 tulosvaroituksen kyberhyökkäyksen seurauksena menetetyn tuotannon johdosta.(17)
- Teollisuusyritysten tulisi vahvistaa myös tuotantoympäristöjensä suojausta, havainnointikykyä sekä varmistaa tuotannon jatkuvuus.
  - Tässä työssä kannattaa hyödyntää Kyberturvallisuuskeskuksen organisaatioille ja yrityksille suunnattuja ohjeita.(3)

IoT

- Vanhoja haavoittuvuuksia lymyää IoT-laitteissa.
  - IoT-laitteiden yhteydessä valmistajat suhtautuvat välinpitämättömästi tietoturvapäivityksiin. Kriittisiä haavoittuvuuksia sisältävä laite muodostaa aina riskin esimerkiksi yrityksen verkkoympäristölle.
  - Tästä ongelmasta saatiin ennätyksiä hipova esimerkki, kun Microsoft nosti raportissaan esille monissa IoT-laitteissa sisäisesti hyödynnetyn ”Boa” web-palvelimen. Sen kehitys on lopetettu vuonna 2005 eikä siihen ole julkaistu tietoturvapäivityksiä sen jälkeen.(18)
    - Raportin mukaan esimerkiksi siruvalmistaja Realtek on paketoinut tämän vanhan ja erittäin haavoittuvan sovelluksen IoT-laitteita valmistaville asiakkailleen suunnatun sovelluskehitysalustan sisään.
    - Laaja haavoittuvien laitteiden määrä tekee niistä houkuttelevan kohteen esimerkiksi bottiverkkoja operoiville kyberrikollisille.
    - Intialaiseen Tata Power energiayhtiöön tehtiin lokakuussa tietomurto näitä haavoittuvuuksia hyödyntäen.

Analyysi

- Mikä tahansa haavoittuva sekä tavalla tai toisella julkisesta verkosta tavoitettavissa oleva IoT-laite nostaa tietomurron riskiä.
  - IoT-laitteet ovat nykyään täysiverisiä tietokoneita, joihin päässyt rikollinen voi hyödyntää niitä monella tavalla. Rikollinen voi esimerkiksi valjastaa laitteen palvelunestohyökkäyksiä tekevän bottiverkon osaksi. Toisen rikollisen tavoitteena saattaakin olla IoT-laitteen hyödyntäminen lopulta kiristyshaittaohjelmaan päätyvässä tietomurrossa.
- Kaikkien IoT-laitteita hankkivien tahojen tulisi aina arvioida myös niiden tietoturvaa ennen ostopäätöstä. Suhtautuuko valmistaja vakavasti tietoturvaan? Onko tietoturvapäivityksiä saatavilla?
- Kyberturvallisuuskeskuksen Tietoturvamerkki kertoo siitä, että valmistaja on sitoutunut varmistamaan tuotteen tietoturvallisuuden ja tarjoamaan siihen tietoturvapäivityksiä merkin voimassaoloajan.(19)

IoT

- Kyberturvallisuuskeskus osallistuu yhdessä Kilpailu- ja kuluttajaviraston (KKV) kanssa Turvallisuus- ja kemikaaliviraston (Tukes) joululelukampanjaan.
  - Tukes testautti 22 joulun suosikkilelua Tullilaboratoriossa. Testissä tutkittiin mm. mekaanisia ja fysikaalisia ominaisuuksia.
  - Kyberturvallisuuskeskus tutustui Tukesin pyynnöstä kolmeen myynnissä olevan älylelun tietoturvaominaisuuksiin.
  - Tukesin järjestämä joululelujen turvallisuusvalvonnan tiedotustilaisuus pidettiin 14.12. Museo Leikissä.

Analyysi

- Älyleluille, ei toistaiseksi ole pakollisia tietoturvavaatimuksia, mutta niitä on tulossa: CE-merkintä kertoo EU-alueella 1.8.2024 lähtien myös lelujen tietoturvasta.
- Tulevat vaatimukset parantavat käyttäjien yksityisyyttä ja suojaavat viestintäverkkoja. Lisäksi ne estävät taloudelliseen hyötyyn tähtääviä petoksia, joissa hyödynnetään verkkoon liitettyjä laitteita.
- Erityisesti lastenhoitoon liittyville laitteille ja leluille asetetaan pakollisia henkilötietojen ja yksityisyyden suojaamista koskevia vaatimuksia.
- Regulaatio on viranomaisten ja valmistajien yhteinen ponnistus. Valmistajien on mahdollista ottaa kantaa säädöstekstiin ja osallistua standardisointiin.

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

- Marraskuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä.
  - Vakavuusluokat: A: 0, B: 0, C: 2
  - Kesän jälkeen verkot ovat toimineet normaaliakin vakaammin ja kesäkuun jälkeen joka kuussa on ollut alle kuusi merkittävää häiriötä, joka on ollut aiemmin keskiarvo kuukausitasolla vuosittain.
- Liikenne- ja viestintävirasto Traficom on julkistanut pilottitutkimuksen viestintäverkkojen energiankulutuksesta Suomessa.
  - Tutkimuksen mukaan vuonna 2021 viestintäverkkojen energiankulutus kokonaisuudessaan oli noin 650 gigawattituntia.
  - Matkaviestinverkossa tiedonsiirto kuluttaa enemmän energiaa kuin kiinteässä verkossa. Suurin osa teleyritysten kuluttamasta energiasta perustuu kuitenkin uusiutuviin energialähteisiin.
  - Viestintäverkkojen energiankulutus kattaa arviolta noin neljänneksen koko ICT-sektorin hiilijalanjäljestä.(20)

- Sähkön kantaverkkoyhtiö Fingrid Oyj on kertonut, että tämänhetkisessä maailmantilanteessa on järkevää varautua sähkön niukkuuteen ja siihen, että talvella sähköpula voi aiheuttaa sähkökatkoksia.
- 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.(21)
- On kuitenkin hyvä huomata, että koska viestintäverkkokomponentteja ja -laitetiloja on Suomessa kymmeniä tuhansia, siirrettävää varavoimaa ei riitä niihin kaikkiin.

Palvelunestohyökkäykset

- Palvelunestohyökkäystilanne edelleen aktiivinen.
  - Marraskuun tilastot ovat hieman määrällisesti pienemmät kuin lokakuussa, mutta kyseessä oli kuitenkin vuoden toiseksi aktiivisin kuukausi vastaanottamiemme ilmoitusten perusteella.
  - Erityisesti sovellustason hyökkäykset ovat olleet jälleen yleisiä ja erityisesti ne onnistuvat aiheuttamaan vaikutuksia palveluiden toimintaan.
- OP kertoi perjantaina 25.11. joutuneensa palvelunestohyökkäyksen kohteeksi.(22)
  - Vaikka käyttäjille katko oli lyhyt tai ei aiheuttanut vaikutuksia, nousi se OP:n aktiivisen tiedottamisen myötä mediaan.
  - Mikäli palvelulla on runsaasti käyttäjiä ja vaikutus havaitaan nopeasti käyttäjäkunnassa, on syytä tiedottaa teknisestä ongelmasta tai palvelunestohyökkäyksestä mahdollisimman pian.

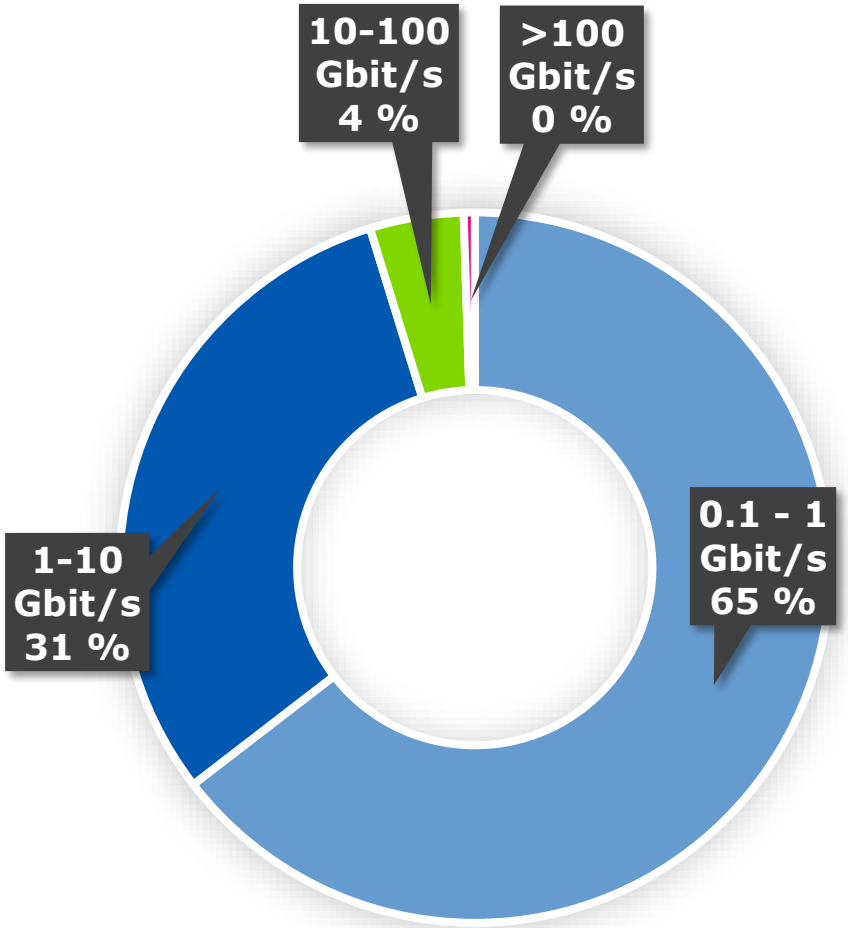
Analyysi

- Ilmoitetut hyökkäykset ovat olleet pääasiassa sovellustason hyökkäyksiä, jotka pyrkivät erilaisin pyynnöin kuormittamaan kohteen palveluita.
  - Yleisesti Kyberturvallisuuskeskukselle tulleiden ilmoitusten perusteella voidaan puhua miljoonista pyynnöistä muutamienkin minuuttien aikana.
- Tämän kaltaiset hyökkäykset ovat usein vaikuttaneet hetkellisesti palveluiden tai sivustojen saatavuuteen.
- Tällöin voidaan vaikkapa hetkellisesti estää ulkomailta tulevaa liikennettä tilanteen helpottamiseksi.

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

- Uhkatoimijat ovat jatkaneet aktiivisesti erilaisia kybervakoilukampanjoita ja -sabotaasiyrityksiä Venäjän ja Ukrainan väliseen sodankäyntiin liittyen.
- Esimerkiksi Callisto-ryhmän (Seaborgium, Coldriver) uutisoitiin kohdistaneen tietojenhankintaa sekä Ukrainan sodankäyntiä tukeviin toimijoihin että valtionhallintoihin Euroopassa ja Yhdysvalloissa.(23) (24)
  - Kohteiden joukossa on ollut maanpuolustustarvikkeisiin, logistiikkaan ja satelliittipalveluihin liittyviä organisaatioita sekä konfliktinratkaisuun ja sotarikosten tutkintaan liittyviä järjestöjä sekä ajatushautomoita.
- Tietoturvayhtiö Mandiantin mukaan Venäjän sotilastiedustelu on muuttanut toimintatapaansa Ukrainassa ja kiihdyttänyt kyberhyökkäysten tahtia.(25)
  - Kohdistetusta tietojenkalastelusta on Mandiantin analyysin mukaan siirrytty murtamaan yhä enemmän verkon reunalla sijaitsevia laitteita, kuten reitittimiä, palomuureja ja sähköpostipalvelimia.
  - Lisäksi Ukrainaan kohdistetut tietoja tuhoavat haittaohjelmat ovat aiempaa yksinkertaisempia ja samalla nopeammin muunneltavia.

Analyysi

- Mandiantin mukaan kiihtynyt operaatiotahti Ukrainassa näkyy myös tehtyjen virheiden laadussa.
- Ukrainan sotaan liittyvää kybervakoilua nähdään myös länsimaissa, kun esimerkiksi Ukrainaan kalustoa tai palveluita toimittaviin tahoihin tai sotaa tutkiviin toimijoihin kohdistetaan tiedonhankintaa.

Vakoilu

- Mustang Panda (Earth Preta, Bronze President) on ollut tietoturvatutkijoiden mukaan aktiivinen toimija kuluneen vuoden aikana. Ryhmän tavoitteena on tietojen anastaminen kohdeorganisaatiosta. Kohteita on havaittu niin Euroopassa kuin sen ulkopuolella.(26)
- Ryhmän hyödyntämiä haittaohjelmia on levitetty kohdistettujen sähköpostiviestien avulla.(27)
  - Viestit sisältävät tyypillisesti linkin tiedostonjakopalveluun, esimerkiksi Google Driveen. Palvelusta latautuu haitallinen .rar tai .zip -paketti. Paketin sisältävän .lnk-tiedoston ajaminen johtaa haittaohjelman aktivoitumiseen.
- Toimijan tyypillisesti käyttämiä haittaohjelmia ovat PlugX ja Cobalt Strike Beacon.

Analyysi

- Tietoturvatutkijoiden mukaan toimijan sähköposteissa käyttäminä houkuttimina on hyödynnetty kohteille ajankohtaisia poliittisia aiheita.
- Haittaohjelman aktivoitumiseksi vaaditaan useita askeleita. Näitä ovat esimerkiksi sähköpostiin saapuneen haitallisen linkin avaaminen, tiedoston lataaminen, tiedoston purkaminen ja LNK-tiedoston ajaminen.

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

EU:n neuvosto hyväksyi uutta lainsäädäntöä EU:n korkean kyberturvallisuustason varmistamiseksi(28)

- Uusi tarkistettu kyberturvallisuusdirektiivi (NIS2) korvaa nykyisen kyberturvallisuusdirektiivin (NIS).
- Keskeisimpinä muutoksina direktiivillä;
  - määritetään kyberturvallisuusriskien hallintatoimien ja raportointivelvoitteiden vähimmäistaso kaikille direktiivin soveltamisalaan kuuluville aloille, joita ovat esimerkiksi energia, liikenne, terveys ja digitaalinen infrastruktuuri.
  - perustetaan virallisesti Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe), joka tukee laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien koordinoitua hallinnointia.
- Direktiivi on yhdenmukaistettu alakohtaisen lainsäädännön kanssa, joihin kuuluu erityisesti rahoitusalan digitaalista häiriönsietokykyä koskeva asetus (DORA) sekä kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi (CER).
- Jäsenmailla on direktiivin voimaantulosta 21 kuukautta aikaa saattaa säännökset osaksi kansallista lainsäädäntöään.

Oikeudelliset asiat

Hallitus kannattaa EU:n kyberkestävyyssäädöksen tavoitteita.(29)

- Valtioneuvosto on 10.11.2022 antanut U-kirjelmän komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi horisontaalisista kyberturvallisuusvaatimuksista tuotteille, joissa on digitaalinen elementti (ns. kyberkestävyyssäädös).
- Kirjelmässä valtioneuvosto toteaa muun muassa pitävänsä verkkoon kytkettyjen laitteiden ja ohjelmistojen turvallisuuden parantamista merkittävänä kehityskohteena kyberturvallisuussektorilla.
- Valtioneuvosto toteaa lisäksi kannattavansa sitä, että vastuuta tuotteiden turvallisuudesta kyberympäristössä kohdistetaan nykyistä enemmän käyttäjältä valmistajalle riippumatta siitä, missä sisämarkkinoille asetettavat tuotteet valmistetaan.

Arjen kyberturvallisuus

Palvelunestohyökkäykset ja niiden torjunta ovat arkipäivää

- Esimerkiksi Osuuspankki kertoi joutuneensa palvelunestohyökkäyksen kohteeksi, vaikka vaikutukset jäivät lyhytaikaiseksi.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-ovat-arkipaivaa-suomessa

Älyä ostoksiin –kampanja edelleen ajankohtainen joulun kiivaana ostoskautena

- 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/alya-ostoksiin

Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi

- Monivaiheisella tunnistautumisella tarkoitetaan sitä, että henkilöllisyytesi varmistetaan kahta tai useampaa eri tunnistautumistapaa käyttämällä.
- Lähes kaikki käyttäjätilien kaappausyritykset voidaan estää monivaiheista tunnistautumista käyttämällä.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Uutisia Kyberturvallisuuskeskuksesta

Tietoturvasetelin haku avautui joulukuussa

- Valtioneuvosto teki lokakuussa päätöksen määräaikaisesta yrityksille myönnettävästä tietoturvan kehittämisen tuesta eli niin sanotusta tietoturvasetelistä.
- Tietoturvaseteliä voivat hakea huoltovarmuuskriittiset yritykset.
- Tietoturvasetelin tavoitteena on nostaa näiden yritysten tietoturvallisuuden tasoa ja sitä kautta parantaa koko yhteiskunnan kykyä suojautua kyberturvallisuusuhkia vastaan.
- https://www.traficom.fi/fi/ajankohtaista/tietoturvasetelin-haku-aukeaa-pian-tutustu-tietoturvan-kehittamisen-tuen-ehtoihin-ja

Digi- ja väestötietoviraston digitaalisen turvallisuuden tulevaisuus –seminaari pidettiin 1.12.2022

- Digitaalisen turvallisuuden tulevaisuus -webinaari summasi kuluvan vuoden tapahtumat ja tarkasteli tulevaisuuden uhkia ja mahdollisuuksia digiturvallisuuden näkökulmasta.
- Seminaarin tallenne julkaistaan myöhemmin.
- https://dvv.fi/-/digitaalisen-turvallisuuden-tulevaisuus-2022

Viestintäverkkojen energiankulutuksesta ensimmäinen tutkimus

- Liikenne- ja viestintävirasto Traficom on julkistanut pilottitutkimuksen viestintäverkkojen energiankulutuksesta Suomessa.
- Tutkimuksen mukaan vuonna 2021 viestintäverkkojen energiankulutus kokonaisuudessaan oli noin 650 gigawattituntia.
- Matkaviestinverkossa tiedonsiirto kuluttaa enemmän energiaa kuin kiinteässä verkossa. Suurin osa teleyritysten kuluttamasta energiasta perustuu kuitenkin uusiutuviin energialähteisiin.
- https://www.traficom.fi/fi/ajankohtaista/viestintaverkkojen-energiankulutuksesta-ensimmainen-tutkimus

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) Kyberympäristön uhkatason nousu https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

3) 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) The continuity of Conti https://blog.bushidotoken.net/2022/11/the-continuity-of-conti.html

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

7) Toimintaohje – kiristyshaittaohjelma https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/toimintaohje-kiristyshaittaohjelma

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

9) French hospital suspends operations after cyber attacks https://www.france24.com/en/france/20221205-french-hospital-suspends-operations-after-cyber-attacks

10) New “Prestige” ransomware impacts organizations in Ukraine and Poland https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

Lähdeluettelo

11) WhatsApp data leaked - 500 million user records for sale online https://cybernews.com/news/whatsapp-data-leak/

12) Nasevia neuvoja tiliesi turvaamiseksi https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nasevia-neuvoja-tiliesi-turvaamiseksi

13) CISA Shields up –sivusto https://www.cisa.gov/shields-up

14) Autoreporter https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporter-kategoriat

15) Dragos Industrial Ransomware Analysis: Q3 2022 https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q3-2022/

16) Microsoft Digital Defense Report 2022 https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

17) Uponor tulosvaroitus https://www.uponorgroup.com/fi-fi/sijoittajauutiset/2022/tulosvaroitus-uponor-poistaa-ohjeistuksensa-vuodelle-2022-kyberhyokkayksen-seurauksena

18) Vulnerable SDK components lead to supply chain risks in IoT and OT environments https://www.microsoft.com/en-us/security/blog/2022/11/22/vulnerable-sdk-components-lead-to-supply-chain-risks-in-iot-and-ot-environments/

19) Tietoturvamerkki https://www.tietoturvamerkki.fi/fi

20) Viestintäverkkojen energiankulutuksesta ensimmäinen tutkimus https://www.traficom.fi/fi/ajankohtaista/viestintaverkkojen-energiankulutuksesta-ensimmainen-tutkimus

Lähdeluettelo

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

22) OP:n tiedote palvelunestohyökkäyksestä https://twitter.com/OP_Ryhma/status/1596120992224804864

23) Russian Espionage APT Callisto Focuses on Ukraine War Support Organizations https://www.securityweek.com/russian-espionage-apt-callisto-focuses-ukraine-war-support-organizations

24) Calisto show interests into entities involved in Ukraine war support https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-war-support/

25) Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/

26) Mustang Panda Uses the Russian-Ukrainian War to Attack Europe and Asia Pacific Targets https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets

27) Earth Preta Spear-Phishing Governments Worldwide https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html

28) Vahvempi kyberturvallisuus ja häiriönsietokyky koko EU:hun: neuvosto hyväksyi uutta lainsäädäntöä https://www.consilium.europa.eu/fi/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

Lähdeluettelo

29) U 83/2022 vp https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/U_83+2022.aspx

30) TUKES kampanja https://tukes.fi/-/tukes-varoittaa-vaarallisista-joululeluista