TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Syyskuu 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

13.10.2022

Kybersää Syyskuu 2022

Tietomurrot ja -vuodot

- Kuukauden aikana havaittiin muutamasta M365 murrosta lähtenyt laajalle levinnyt M365/Turvaposti teemainen kalastelukampanja.
- Monivaiheisen tunnistautumisen väsytyshyökkäyksistä havaintoja myös Suomessa.

Huijaukset ja kalastelut

- Syyskuussa nähtiin tuhansittain poliisiaiheisia kiristysviestejä.
- Huijauspuheluita on taas soitettu suomalaisille kuluttajille ulkomaisista numeroista.

Haittaohjelmat ja haavoittuvuudet

- Haittaohjelmien levitystä sähköpostitse syyskuun aikana.
- Tunnistautumista vaativa etäkäytön mahdollistava haavoittuvuus Microsoft Exchangessa.

Automaatio ja IoT

- EU julkaisi 15.9.2022 älytuotteiden tietoturvaa käsittelevän kyberkestävyyssäädöksen luonnostekstin. Säädös asettaa vaatimuksia valmistajille, jälleenmyyjille ja maahantuojille.

Verkkojen toimivuus

- Neljä merkittävää toimivuushäiriötä.
- Häiriöt olivat yleisesti ottaen lyhyitä ja vaikuttivat paikallisesti yleisten viestintäpalveluiden saatavuuteen.
- Palvelunestohyökkääjät ovat aktivoituneet kesän jäljiltä ja vaikutuksiakin on koettu.

Vakoilu

- Venäjän arvioidaan lisäävän kybervakoilua tulevana talvena. Vakoilu voi kohdistua myös tuotekehitystietoon pakotteiden aiheuttaman teknologiavajeen paikkaamiseksi.
- Iranin valtionhallintoon liitetty ryhmä hyökkäsi uudelleen Albaniaa vastaan.

TRAFICOM

13.10.2022

Kuukauden tunnuslukuja

1000+

Yksittäisestä murretusta sähköpostitilistä lähetettiin yli tuhat kalasteluviestiä kuntasektorilla.

405 milj.

Irlannin tietosuojaviranomainen määräsi Metalle 405 miljoonan euron seuraamusmaksun tietosuojarikkomuksista lasten henkilötietojen käsittelyssä Instagramissa.

78%

Heinä-elo-syyskuun aikana 78% palvelunestohyökkäyksistä oli kestoltaan alle 15 minuuttia.

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 kohdistuneen kyberuhkatason katsotaan nousseen. 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

13.10.2022

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. Energiamarkkinoihin vaikuttamista kybertoimintaympäristössä ei voi sulkea pois.
  - 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 kohdistuneen kyberuhkatason katsotaan nousseen.

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.

- Kyberturvallisuuskeskus on tämän johdosta arvioinut kyberturvallisuuden uhkatason nousseen Suomessa.
- 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.
- Vaikka tavanomaisten kyberhyökkäysten määrä on kokonaisuudessaan kasvanut, myös mm. kohdennetut tietojenkalasteluviestit ja murtautumisyritykset ovat lisääntyneet.
- Tutustu Kyberturvallisuuskeskuksen tiedotteeseen kohonneesta kyberuhkatasosta.(1)

OHJE

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

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

3. Puutteet tavanomaisissa torjuntatoimissa aiheuttavat edelleen valtaosan tietoturvapoikkeamista.

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

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

CASE

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

4. Puutteellinen tiedonvaihto heikentää kyberturvallisuuden kokonaistilannekuvaa.

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

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

CASE

ISAC-tiedonvaihtoryhmät (ISAC=Information Sharing and Analysis Centre) ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä. ISAC-ryhmissä käsitellään luottamuksellisesti kyberturvallisuuteen liittyviä asioita, kuten uhkia, ilmiöitä ja hyviä käytäntöjä.

Ryhmät kehittävät myös edustamansa toimialan ja yhteiskunnan kyberturvallisuutta esimerkiksi toteuttamalla toimialaansa liittyviä riskianalyysejä, tutkimuksia ja ohjeistusta.[3]

5. Kyberturvallisuus on riippuvainen osaajista ja kyberturvallisuustaidot kuuluvat kaikille!

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

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

CASE

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

Tietomurrot ja -vuodot

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

Tietomurrot ja –vuodot

- Syyskuu oli Suomessa tavanomainen tietomurtojen osalta.
  - Loppukuusta Suomessa levisi laajalle M365 pohjainen kalastelu – ja tietomurtokampanja, jossa yksittäisistä murretuista tunnuksista lähetettiin suurimmillaan yli 1000 uutta kalasteluviestiä.
  - Ilmoitukset muista tietomurroista ja niiden yrityksistä painottuivat syyskuun aikana yksityisiin henkilöihin, sekä yrityskenttään.
  - Yksityishenkilöihin kohdistuneissa tietomurroissa pääosaa ilmoituksista edustaa erilaisten sosiaalisen median tilien murrot. Lisäksi saimme joitain ilmoituksia myös sähköposti- ja muiden verkkopalveluiden tunnuksien murroista ja kaappauksista.

Analyysi

- Erilaisiin huijauksiin kannattaa edelleen varautua. Kalasteluiden ja huijauksien seurauksena voi tapahtua myös tietomurto.
  - Murrettuja sähköpostiosoitteita voidaan käyttää useisiin erilaisiin jatko huijauksiin ja tietomurtoihin.
  - Ohjeita huijausten varalle löytyy Kyberturvallisuuskeskuksen verkkosivuilta.(3)

Tietomurrot ja -vuodot

- Maailmalla raportoitiin muutamista suuriin toimijoihin kohdistuneista tietomurroista.
  - Lentoyhtiöistä sekä American Airlines, että TAP Air Portugal ilmoittivat kumpikin heihin kohdistuneista tietomurroista, joiden seurauksena hyökkääjät olivat saaneet haltuunsa mm. henkilötietoja.
  - Liikennepalveluita tarjoava Über ilmoitti niin ikään järjestelmiinsä kohdistuneesta tietomurrosta. Saatujen tietojen mukaan järjestelmiin olisi päästy sisälle murretun käyttäjätunnuksen ja salasanan avulla ja monivaiheiseen tunnistautumiseen kohdennetulla väsytyshyökkäyksellä.
  - Yli 25 maassa toimiva EasyPark ilmoitti syyskuun alussa heihin kohdistuneesta tietoturvapoikkeamasta. Yrityksen tietojen mukaan tapauksen seurauksena hyökkääjä sai haltuunsa osan asiakkaiden perustietoja, kuten nimen, sähköpostiosoitteen ja puhelinnumeron.
  - Myös suuri hotelliketju IHG kertoi joutuneensa tietomurron kohteeksi. Mediassa olleiden tietojen mukaan hyökkääjän tavoitteena oli kiristyshaittaohjelman asentaminen kohteeseen. Vastatoimien takia hyökkääjä päätyi kiristysoperaation sijaan toteuttamaan tiedon tuhoamisoperaation.

Analyysi

- Tietomurron yhteydessä oikea-aikainen ja laadukas viestintä nousee suureen arvoon. Nostoista varsinkin TAP Air Portugalin viestintä oli laadukasta ja informatiivista.
- Edelliskuukauden tietomurroissa korostui myös negatiivisessa valossa heikko tunnistautumisen hygienia.
  - Yhdessä suuressa murrossa salasana oli nykymittakaavalla lyhyt ja heikko ”Asdfgh2345”.
- Hyvä ja huono monivaiheinen tunnistautuminen (Multi Factor Authentication, MFA).
  - Edelleen merkittävä määrä palveluista ei ole ottanut käyttöön monivaiheista tunnistautumista, jolla olisi estettävissä tietomurtoja.
  - Ilmiönä on havaittavissa MFA pyyntöihin liittyviä väsytyshyökkäyksiä. Muistisääntönä, älä hyväksy MFA pyyntöä, ellet ole varma, että olet juuri kirjautumassa kyseiseen palveluun.

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

- Huijauksia poliisin nimissä liikkeellä jälleen.
  - Syyskuussa nähtiin tuhansittain poliisiaiheisia kiristysviestejä.
  - Sähköpostien liitteeksi on liitetty virallisen oloinen PDF-dokumentti, jolla koetetaan uskotella kiristyksen uhri maksamaan huijarille.
  - Konvokaatio.pdf -nimisessä tiedostossa vaaditaan maksamaan 5777 euroa, jotta huijaripoliisi jättäisi uhrin rauhaan.

Analyysi

- Huijauspuheluita on taas soitettu suomalaisille kuluttajille ulkomaisista numeroista.
- Syyskuussa raportoitiin useita saksalaisesta puhelinnumerosta soitettuja teknisen tuen huijauspuheluita ja brittiläisestä numerosta soitettuja huijauspuheluita.
- Puhelinhuijauksia täytyy edelleen varoa, sillä niiden uhrit ovat tässäkin kuussa menettäneet rahaa huijareille.

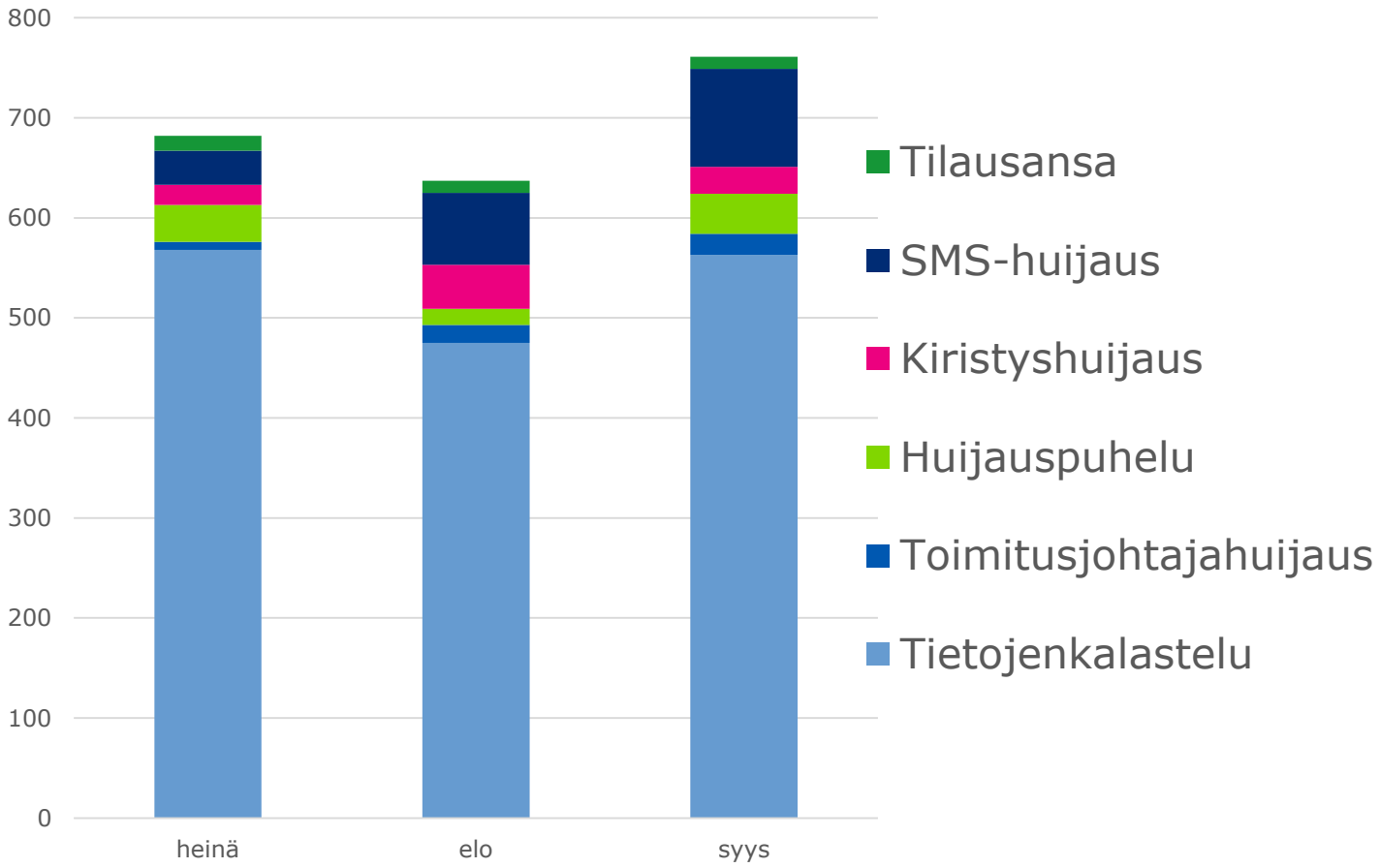
Huijaukset ja kalastelut

- Toimitusjohtajahuijauksilla tehty laskutuspetoksia.
  - Toimitusjohtajahuijauksilla on yritetty viedä rahaa kaikenlaisilta organisaatioilta kouluista kiinteistönvälitysyritykseen ja liikuntajärjestöstä pörssikonserniin.
  - Yhteistä huijauksille on, että johtajan nimissä yritetään saada työntekijöitä maksamaan tekaistuja huijauslaskuja.
- Tuhansittain huijausviestejä liikkeellä.
  - Pankkitunnuksia on kalasteltu jälleen kaikkien pankkien ja lisäksi veroviranomaisen nimissä.
  - Oli huijauksen veruke mikä tahansa, verkkopankkiin ei koskaan pidä kirjautua tekstiviestissä tulleen linkin kautta.

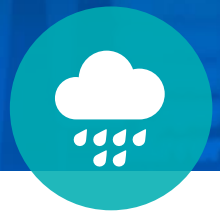
Analyysi

- Microsoftin Office 365 -sähköpostipalvelun tunnuksia kalastellaan edelleen ahkerasti.
- Kaapattuja sähköpostitilejä rikolliset käyttävät uusiin huijauksiin ja monenlaisiin muihin rikoksiin.
- Monivaiheisen tunnistautumisen käyttöönotto estää tehokkaasti kaapattujen tunnusten hyväksikäytön.

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.

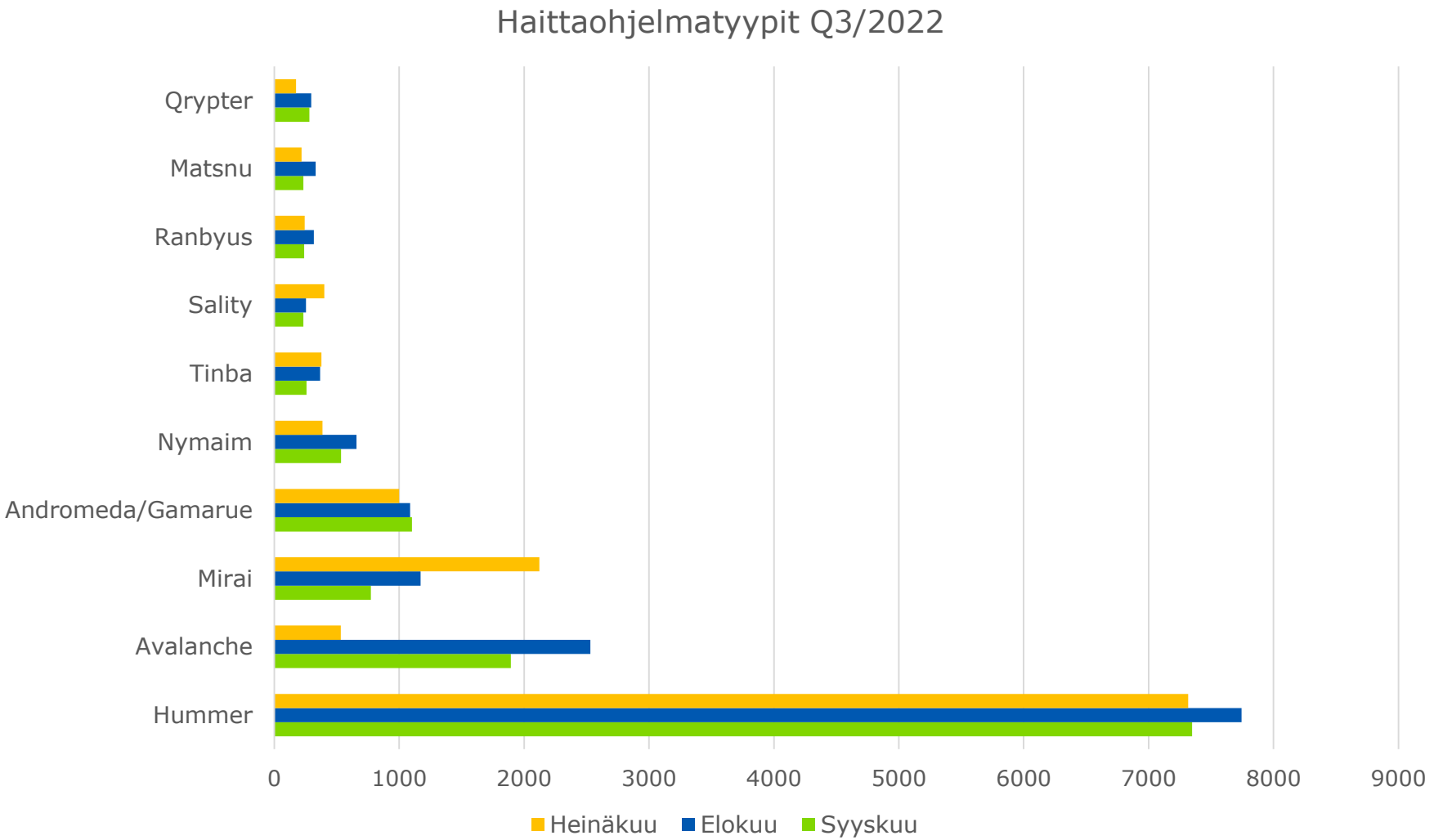
Haittaohjelmat

- Haittaohjelmien levitystä sähköpostitse
  - Sähköpostin liitteenä levitettäviä haittaohjelmia on raportoitu aktiivisesti.
  - Joissain tapauksissa haitallinen liitetiedosto pääsee suojausmekanismien läpi sähköpostiin, jossa se odottaa käyttäjää avaamaan tiedoston.
  - Haittaohjelmajakelua tapahtui syyskuussa myös Sharepoint-linkkien avulla.
  - Käyttäjää saatetaan huijata avaamaan liitetiedostoa esimerkiksi luomalla kiireen tunne vastaanottajalle.
  - Viestit saattavat viitata vaikkapa allekirjoitettavaan asiakirjaan tai maksettavaan laskuun.
  - Lisää tietoa Kyberturvallisuuskeskuksen viimeisimmästä viikkokatsauksesta.(4)

Analyysi

- Haittaohjelmat tavoittelevat pääsyä sähköpostilaatikkoon eri tiedostomuodoin, esim. .zip, .html, .pdf ja eri Office-tuotteiden tiedostopäättein.
  - Käyttäjien tulee olla tarkkana mistä osoitteesta liitetiedoston sisältävät sähköpostit saapuvat.
- Olemme vastaanottaneet ilmoituksia, joissa haittaohjelmaa on levitetty myös luotetun sähköpostiosoitteen avulla.
  - Tällöin tunnetun lähettäjän sähköpostitili on murrettu ja sitä käytetään haittaohjelman levityksessä.

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.(5)

Haavoittuvuus

- Microsoft Exchange -sähköpostipalvelimien haavoittuvuudet.
  - Mielivaltaisen koodin suorittamisen mahdollistava haavoittuvuus vaatii käyttäjän tunnistautumisen palvelimelle. Tällöin hyökkääjän hallussa tulee olla käyttäjätunnus ja salasana päästäkseen palvelimelle hyödyntämään haavoittuvuutta.
  - Tämän hetkisten tietojen mukaan haavoittuvuus koskee Exchange-palvelimia, joita ylläpidetään käyttäjien omissa ympäristöissä (OnPrem) ja niiden selainpohjainen käyttäjäympäristö (OWA) on avoinna internet-rajapintaan.
  - Korjaavia päivityksiä ei toistaiseksi ole saatavilla, eli kyse on niin sanotusta nollapäivähaavoittuvuudesta.
  - Tämän hetken tietojen mukaan Suomessa ei ole havaittu tietomurtoja tämän Exchange-haavoittuvuuden osalta.
  - Microsoft kuitenkin kertoo tiedotteessaan, että heillä on tiedossa joitain kohdistettuja hyökkäyksiä, joissa on hyödynnetty näitä tuoreita haavoittuvuuksia.

Analyysi

- Tämä "ProxyNotShell" -nimen saanut haavoittuvuus ei ole yhtä kriittinen, kuin viime vuoden maaliskuussa kyberkenttää järisyttänyt "ProxyShell"-haavoittuvuus, josta julkaisimme punaisen varoituksen.
  - Kyseistä haavoittuvuutta hyväksikäytettiin internetissä automatisoidusti ilman tunnistautumista.
- Haavoittuvat palvelimet ovat hetkessä hyökkääjien kohteena ja ongelman mitigoiminen tai päivitysten asentaminen tuleekin suorittaa heti.

Kuukauden haavoittuvuusjulkaisut

- Tunnistautumista vaativa etäkäytön mahdollistava haavoittuvuus Microsoft Exchangessa (14/2022).
  - Microsoft Exchange -sähköpostipalvelimesta on löydetty haavoittuvuus, joka mahdollistaa tunnistautuneelle käyttäjälle mielivaltaisen koodin suorittamisen.
  - Microsoft on kertonut kahdesta nollapäivähaavoittuvuudesta, joiden CVE-tunnisteet ovat CVE-2022-41040 ja CVE-2022-41082.
- Kriittinen haavoittuvuus Zimbra Collaboration (ZCS) –ohjelmistossa (15/2022).
  - Haavoittuvuutta käytetään aktiivisesti hyväksi, mutta sen väliaikaiseen korjaamiseen on jo keinoja.
- Kriittinen haavoittuvuus Fortinetin FortiOS ja FortiProxy –ohjelmistoissa (16/2022).
  - Fortinet julkaisi päivityspaketit FortiOS ja FortiProxy-ohjelmistoihin, jotka korjaavat kriittiseksi luokitellun haavoittuvuuden.
- Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

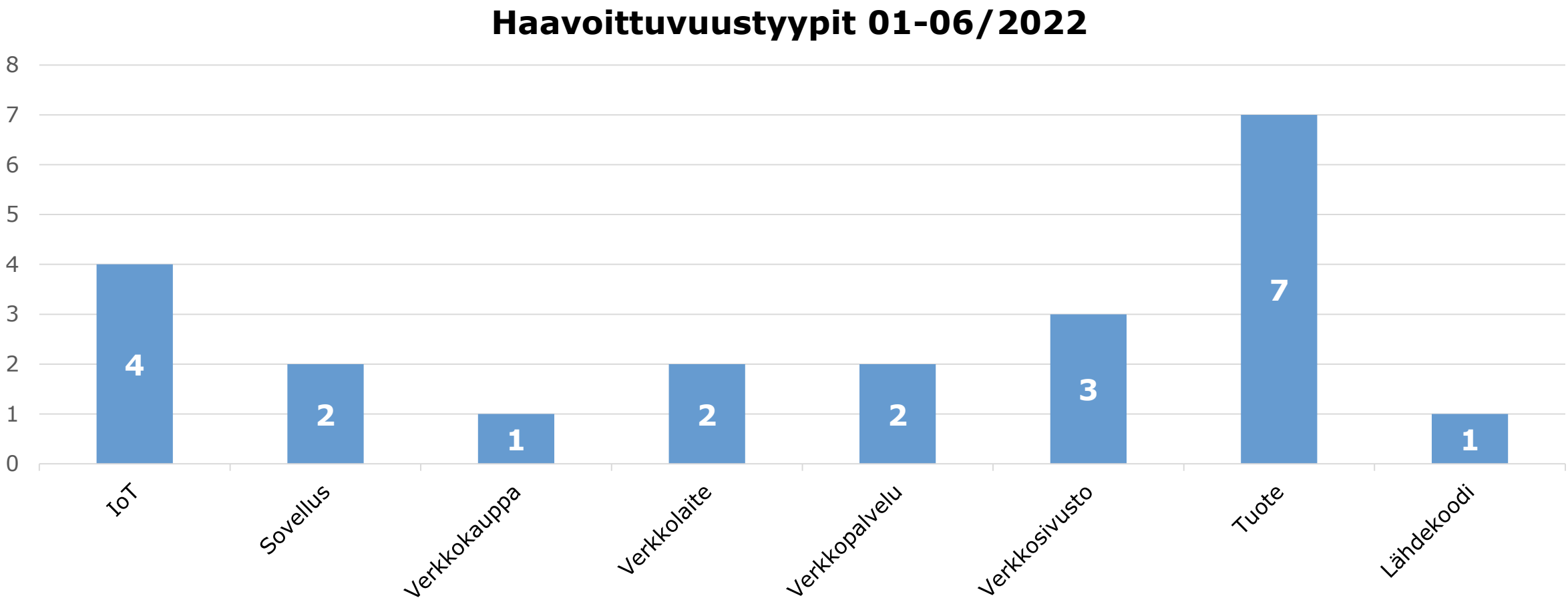
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- **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 16 kpl (tilanne 10.10.2022).**
  - 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

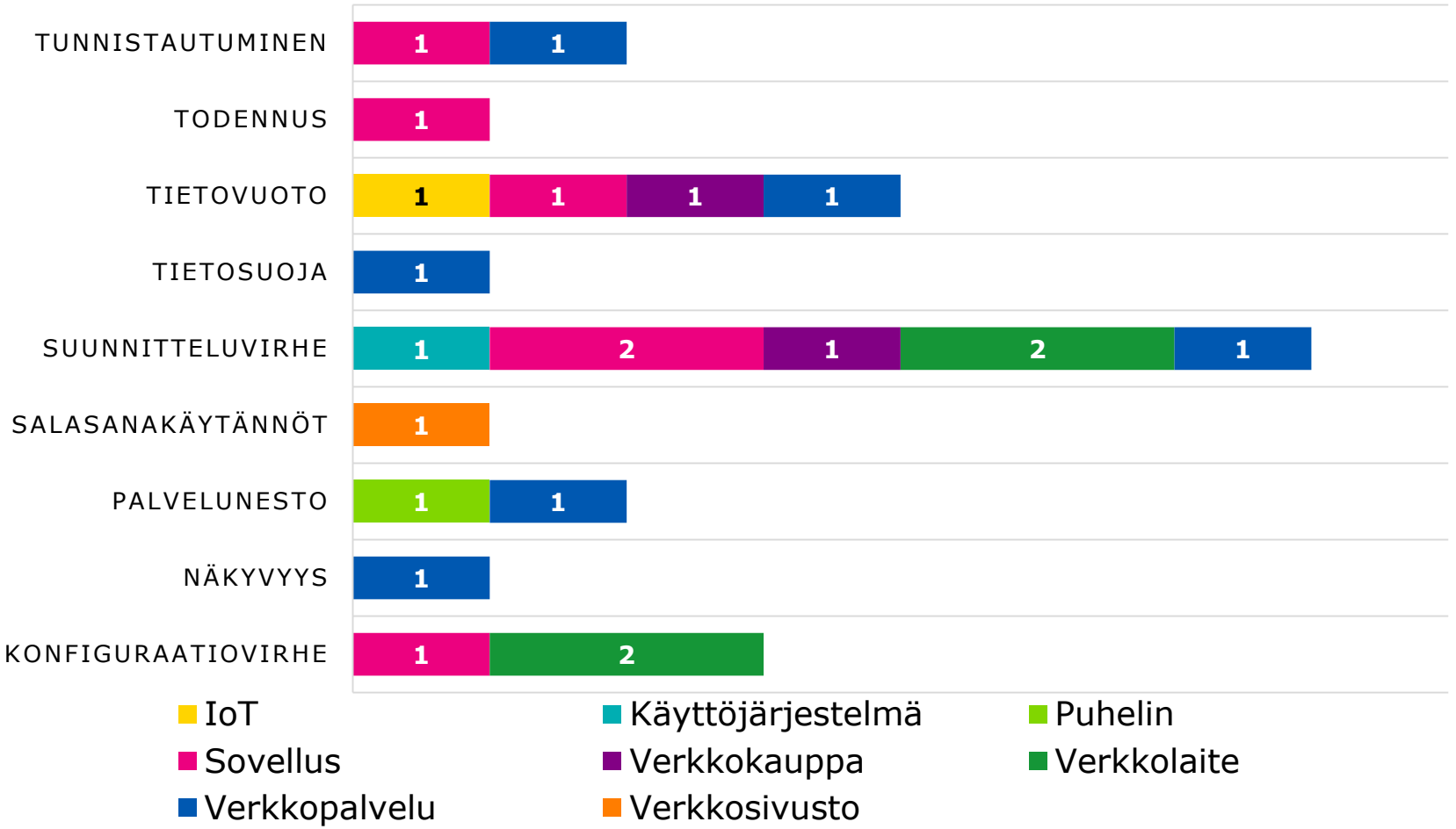
Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- 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.

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 - uudet standardit ja asetusehdotukset

- Teknologiajättien tukema allianssi julkaisee IoT-standardin yhteentoimivuuden ja tietoturvallisuden parantamiseksi.(6)
  - Standardista vastaa Connectivity Standards Alliance (CSA), ja standardia tukevat mm. Amazon, Apple ja Google.
  - Tavoitteena on parantaa IoT-tuotteiden yhteentoimivuutta ja turvallisuutta.
  - Erityisenä fokuksena standardissa on käytettävyys, jota pyritään tukemaan mm. helpottamalla laitteen käyttöönottoa.
  - Standardi on IP-pohjainen avoimen lähdekoodin ratkaisu.
- EU Komissio on julkaissut ehdotuksen kyberkestävyyssäädökseksi (Cyber Resiliance Act).
  - Kyseessä on ensimmäinen EU:n laajuinen lainsäädäntö, joka asettaa pakollisia kyberturvavaatimuksia digitaalisia toimintoja sisältäville tuotteille niiden koko elinkaaren ajaksi.
  - Kyberkestävyyssäännöksestä on kerrottu lisää oikeudellisten asioiden osiossa.

Analyysi

- IoT-tuotteiden määrän ja käyttäjien lisääntyessä niiden tietoturvaan ja yhteentoimivuuteen kiinnitetään yhä enemmän huomiota.
- Teollisuuden standardit voidaan nähdä pyrkimyksenä itsesääntelyyn, jolla pyritään välttämään tarvetta pakottavaan viranomaislähtöiseen sääntelyyn.
- Suurten kaupallisten toimijoiden muodostamien liittoumien standardit voivat helposti saavuttaa de facto -aseman markkinoilla, jos viranomaiset katsovat niiden täyttävän keskeiset vaatimukset.

IoT – älylelujen tietoturva

- Tietoturvayhtiö ESET kirjoittaa, kuinka älylelujen avulla voi kannustaa lapsien oppimista sekä luovuutta esimerkiksi tarjoamalla vuorovaikutteisia ja viihdyttäviä kokemuksia. Kauppojen joululahjahyllyt ovat täyttyneet jo![7]
- Haavoittuvien älylelujen tai niiden hyödyntämien pilvipalveluiden kautta voidaan vakoilla tai häiritä lapsia sekä leikkimisympäristöä.
- Älylelut voivat sisältää mm. mikrofoneja, kameroita, kaiuttimia, näyttöjä, langattomia verkkorajapintoja sekä yhteyksiä pilvipalveluihin ja sovelluksiin. Valitettavasti valmistajat saattavat jättää näiden suojaamisen liian vähälle huomiolle.
- Jo löydettyjä haasteita ovat olleet esimerkiksi:
  - Ilman todentamista tehty langaton pariliitos lelun ja muiden laiteiden välillä, joka mahdollistaa vakoilun
  - Mahdollisuus kommunikoida suoraan samanlaisten lelujen kesken, joka mahdollistaa häirinnän

Analyysi

- Lelut mahdollistavat teoriassa muitakin hyökkäyksiä kuin ympäristön vakoilun ja häirinnän. On mahdollista esim. murtautua älykodin järjestelmiin lähettämällä niihin lelujen kautta äänikomentoja.
- Älä tee harkitsemattomia ostoksia! Leluihin sekä niiden ominaisuuksiin on hyvä tutustua ennen ostopäätöstä. Tarkasta, millaisia uutisia tai tutkimuksia on julkaistu mallien tietoturvaan –tai yksityisyydensuojaan liittyen. Tutustu ostamaasi leluun hyvin. Ymmärrä, minne tiedot tallennetaan.
- Minimoi antamasi tiedot. Harkitse, tarvitseeko palveluihin syöttää oikeita tietoja. Voit keksiä esimerkiksi nimen ja osoitteen. Tämä helpottaa tilannetta mahdollisessa tietovuototapauksessa.
- Mikäli lelu on yhteydessä langattomasti kodin reitittimeen, pidä erityistä huolta reitittimen suojaamisesta, salatuista yhteyksistä, oletussalasanojen vaihtamisesta sekä laitteiden pitämisestä päivitettyinä.
- Sammuta lelu, kun sillä ei leikitä.

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

- Syyskuussa yleisissä viestintäpalveluissa oli neljä merkittävää toimivuushäiriötä.
  - Vakavuusluokat: A: 1, B: 1, C: 2
- Syyskuussakin verkot toimivat normaalisti.
  - Katkokset olivat yleisesti 1-2 tunnin pituisia ja vaikuttivat vain paikallisesti yleisiin viestintäpalveluihin.
  - Yksi vika vaikutti hetkellisesti tekstiviestien vastaanottamiseen muiden operaattoreiden liittymistä.
- ICT-palvelut toimivat syyskuussa normaalisti.
  - Youtuben reaalitoistopalvelut olivat hetkellisesti saavuttamattomissa.(8)

Analyysi

- Yleisten viestintäpalveluiden toimivuus Suomessa on ollut 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.

Merikaapelit ovat internetin selkäranka

- Nord Stream -kaasuputkien vuodot ovat ymmärrettävästi aiheuttaneet huolta myös kansainvälisten tietoliikenneyhteyksien toimivuudesta.(9)
  - Suomesta on useita yhteyksiä maailmalle ja vaikka häiriöt ovat mahdollisia, internet on varsin vikasietoinen.
  - Teemme jatkuvaa yhteistyötä viestintäverkkoinfrastruktuurin suojaamiseksi sekä mahdollisten ongelmien ennaltaehkäisemiseksi, havaitsemiseksi ja korjaamiseksi.
  - Sataprosenttista tietoturvallisuutta tai toimintavarmuutta ei ole olemassa vaan esimerkiksi rikkoutumiset ovat mahdollisia.
  - Kaapeleita katkeaakin aika-ajoin ja merikaapelit ovat esimerkiksi alttiina sään ja merenkäynnin aiheuttamille vahingoille.
  - Oleellista onkin, että ongelmat havaitaan ja korjaaviin toimenpiteisiin ryhdytään. Merikaapeleita huolletaan ja korjataan säännöllisesti eli siihen on varauduttu.

Analyysi

- Verkottunut merikaapelijärjestelmä on erittäin tärkeä osa Suomen viestintäverkkojen infrastruktuuria.
  - Yleiseen teletoimintaan käytettävien merikaapelien suojaamista koskevat vaatimukset asetetaan laissa sähköisen viestinnän palveluista.(10)
  - Lain mukaan yleiset viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä mm. siten, että ne kestävät normaalit odotettavissa olevat ilmastolliset, mekaaniset, sähkömagneettiset ja muut ulkoiset häiriöt, sekä että niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt voidaan havaita.

Palvelunestohyökkäykset

- Syyskuussa palvelunestohyökkäyksiä tapahtui määrällisesti yhtä paljon kuin elokuussakin.
  - Kesän jälkeen hyökkääjät ovat aktivoituneet ja aiheuttaneet myös vaikutuksia palveluiden tai verkkosivustojen hetkelliseen saatavuuteen.
  - Suosittelemme tekemään ilmoituksia palvelunestohyökkäyksistä Kyberturvallisuuskeskukselle sekä poliisille, vaikka niillä ei olisi merkittäviä vaikutuksia.
- Hyökkääjät ovat aiempaa kyvykkäämpiä.
  - Kuluvan vuoden aikana olemme havainneet, että hyökkääjät saattavat vaihtaa aiempaa useammin toimintatapaa kesken hyökkäyksen.
  - Hyökkääjä seuraa sivuston tai palvelun toimintaa ja tarkkailee, miten valittu hyökkäystapa toimii.
  - Kuukauden sisällä olemme vastaanottaneet neljä ilmoitusta, joissa hyökkäyskohteena ovat olleet organisaation yksittäisen osoitteen sijaan suurempi määrä osoitteita, esimerkiksi verkon tietyn osan kaikki osoitteet.

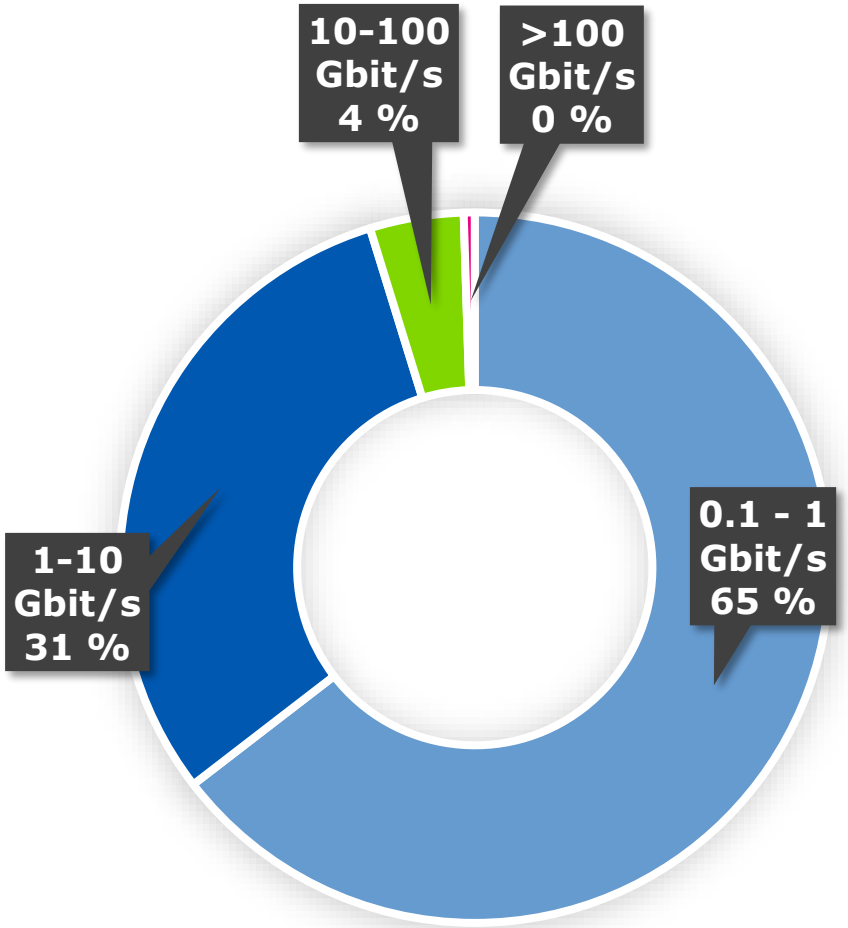
Analyysi

- Hyökkääjien erilaiset toimintamallit saattavat aiheuttaa hetkellistä vahinkoa, vaikka organisaatio olisi varautunut eri keinoin palvelunestohyökkäyksiin
- Esiin nousseena ilmiönä organisaation verkon useisiin osoitteisiin tehdyt hyökkäykset kuormittavat monia - mahdollisesti jopa satoja kohdeosoitteita samaan aikaan-
  - Netscout kertoo ajankohtaisessa artikkelissa, kuinka tämän kaltaisilla hyökkäyksillä pyritään ehkä jopa huomaamatta kuormittamaan kohdeverkkoa.(11)

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

- Suomalaisiin tietoverkkoihin ja -järjestelmiin kohdistuva kybervakoilu korostuu Suojelupoliisin arvion mukaan Venäjän tiedonhankintakeinona tulevana talvena.
  - Suojelupoliisi on kuvannut ajankohtaista turvallisuustilannetta Kansallisen turvallisuuden katsauksessaan.(16)
  - Esimerkiksi päätöksentekoon liittyvän tiedonhankinnan lisäksi on mahdollista, että Venäjä pyrkii hankkimaan tuotekehitykseen liittyviä tietoja paikatakseen pakotteiden synnyttämiä aukkoja.
  - Myös Kiinan todetaan jatkavan aktiivisesti kybervakoilua.
- Sekä Suojelupoliisi että Kyberturvallisuuskeskus myös varoittivat jo aiemmin syyskuussa kyberuhkiin liittyvän uhkatason noususta Suomessa.(17) (18)
- Venäjä hyödyntää myös informaatiovaikuttamista keinovalikoimassaan.

Analyysi

- Vaikka kriittiseen infrastruktuuriin kohdistuva vaikuttamisen uhka on kohonnut, ei yhteiskunnan toimintaa lamauttavia kyberoperaatioita pidetä tällä hetkellä todennäköisinä.
- Kybervakoilun keinoin voidaan hankkia tietoa esimerkiksi päätöksenteosta tai tuotekehityksestä.
- Yritysten on entistä enemmän syytä varautua mahdolliseen tuotekehitystietoon kohdistuvaan vakoiluun.

Vakoilu

- Iranin valtionhallintoon julkisuudessa liitetty ryhmä on toteuttanut kyberhyökkäykset Albaniaa vastaan heinäkuussa ja syyskuussa.(19)
- FBI:n tutkimusten mukaan iranilaisryhmä ehti olla murtautuneena Albanian tietojärjestelmiin neljäntoista kuukauden ajan.
- ”HomeLand Justice” -nimellä itseään kutsuva ryhmä oli pitkäkestoisen tunkeutumisen aikana muun muassa säännöllisesti kopioinut itselleen sähköposteja, levittäytynyt verkossa laajemmalle ja lopulta käynnistänyt kohdejärjestelmän tietojen salauksen ja tietojen tuhoamisen.
- Albania myös katkaisi diplomaattisuhteet Iranin kanssa syyskuun alussa, mikä saattoi toimia kimmokkeena jälkimmäisen kyberhyökkäyksen toteuttamiselle.(20)
- Albania nosti jälkimmäisen hyökkäyksen jälkeen esille myös mahdollisuuden hyödyntää NATO:n artikla 5:tä, joka tarkoittaisi muiden NATO-maiden kutsumista puolustamaan Albaniaa.(21)

Analyysi

- Viimeaikaiset suorat kyberhyökkäykset Albanian valtionhallintoa ja tietoverkkoja vastaan ovat poikkeuksellinen toimi NATO-maata kohtaan.
- Syyskuun hyökkäyksen taustalla on arvioitu olevan hyökkäyksen julkinen attribuointi Iraniin sekä Albanian päätös katkaista diplomaattiset suhteet Iraniin.

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

Komissio on julkaissut ehdotuksen kyberkestävyyssäädökseksi (Cyber Resiliance Act).

- Kyseessä on ensimmäinen EU:n laajuinen lainsäädäntö, joka asettaa pakollisia kyberturvavaatimuksia digitaalisia toimintoja sisältäville tuotteille niiden koko elinkaaren ajaksi. EU pyrkii yhdenmukaistamaan direktiivien ja lakien avulla tuotteiden markkinoille tuontia sekä pakottamaan valmistajat tekemään turvallisempia tuotteita kuluttajille.
- Yritysten on syytä huomioida jo nyt, miten CRA-säädökset tulevat vaikuttamaan omiin tuotanto- ja hankintaprosesseihin sekä vaatimuksiin.
- Uusilla säännöillä siirretään vastuuta valmistajille, joiden on varmistettava että EU:n markkinoille saatettavien digitaalisia elementtejä sisältävien tuotteiden tietoturvavaatimukset täyttyvät. Säädöksen tavoitteena on:
  - Velvoittaa valmistajat tarjoamaan tietoturvatukea ja ohjelmistopäivityksiä havaittujen haavoittuvuuksien korjaamiseksi; ja
  - Varmistaa, että digitaaliset tuotteet ovat kuluttajien kannalta tietoturvallisempia kaikkialla EU:ssa ja että kuluttajat saavat riittävästi tietoa käyttämiensä tuotteiden kyberturvallisuudesta.
- Ehdotettua säädöstä sovellettaisiin kaikkiin tuotteisiin, jotka on liitetty joko suoraan tai välillisesti toiseen laitteeseen tai verkkoon. Säännöt eivät koskisi tiettyjä tuotteita, joiden kyberturvavaatimukset sisältyvät jo voimassa oleviin EU-sääntöihin (esim. lääkinnälliset laitteet, lentokoneet ja autot).
- Ehdotus etenee seuraavaksi Euroopan parlamentin ja neuvoston käsittelyyn. Lisätietoja Komission tiedotteessa.(12)

Oikeudelliset asiat

Traficom antoi päätöksen koskien Telian yritysliittymästä lähtevän sähköpostiliikenteen rajoittamista

- Traficom on 13.9.2022 antanut päätöksen Telialle internetyhteyspalvelun portin 25 estosta, joka rajoitti sähköpostipalvelimen käyttöä liittymässä. Estolle ei ollut riittäviä perusteita, kun kyse oli yritysasiakkaille tiedonsiirtoon matkaviestinverkossa tarkoitetusta liittymästä, jolla oli kiinteä IP-osoite.
- Kyseessä on Suomen ensimmäinen verkkoneutraliteettia koskeva valvontapäätös.
- Ratkaisu ei vaikuta Viestintäviraston määräyksen 67A/2015 M mukaiseen velvollisuuteen estää *kuluttajaliittymistä* lähtevä rajoittamaton SMTP-liikenne muuten kuin sovittujen lähtevälle SMTP-liikenteelle tarkoitettujen palvelimien kautta.

Oikeudelliset asiat

EU tuomioistuimelta uudet ennakkoratkaisut liikenne- ja paikkatietojen säilyttämisestä viranomaistarpeita varten

- EU tuomioistuin on 20.9.2022 antamassaan kahdessa päätöksessä (yhdistetyt asiat C-793/19 SpaceNet ja C-794/19 Telekom Deutschland sekä yhdistetyt asiat C-339/20 VD ja C-397/20 SR) katsonut, että unionin oikeus on esteenä liikenne- ja paikkatietojen yleiselle ja erotuksetta tapahtuvalle säilyttämiselle paitsi, jos kyse on kansalliseen turvallisuuteen kohdistuvasta vakavasta uhasta.
- Jäsenvaltiot voivat vakavan rikollisuuden torjumiseksi suhteellisuusperiaatetta tarkasti noudattaen säätää muun muassa tällaisten tietojen kohdennetusta säilyttämisestä ja/tai säilyttämisen nopeasta varmistamisesta sekä IP–osoitteiden yleisestä ja erotuksetta tapahtuvasta säilyttämisestä.
- Ratkaisut vahvistavat EUT:n aiempaa säilytysvelvollisuutta koskevaa oikeuskäytäntöä.(13) (14)

Oikeudelliset asiat

Irlannin tietosuojaviranomainen määräsi Metalle EU:n toiseksi suurimman seuraamusmaksun tietosuojarikkomuksista lasten henkilötietojen käsittelyssä Instagramissa(15)

- Irlanti antoi päätöksen Euroopan tietosuojaneuvoston kiistanratkaisumenettelyssä tehdyn päätöksen perusteella.
- Kiistanratkaisupäätöksessä Euroopan tietosuojaneuvosto katsoi, että Meta käsitteli lasten henkilötietoja ilman soveltuvaa käsittelyperustetta. Lasten sähköpostiosoitteiden tai puhelinnumeroiden julkaiseminen ei täyttänyt oikeutettua etua koskevia vaatimuksia, eikä tällainen tietojen käsittely ollut tarpeen sopimuksen täytäntöön panemiseksi.
- Metalle määrättiin 405 miljoonan euron seuraamusmaksu. Meta on sittemmin muuttanut käytäntöjään Instagramiin liittyvässä henkilötietojen käsittelyssä.
- Kyseessä on EU:n kaikkien aikojen toiseksi suurin seuraamusmaksu ja samalla ensimmäinen EU:n laajuinen päätös lasten tietosuojaoikeuksista.

Arjen kyberturvallisuus

Vahvan sähköisen tunnistuksen luotettavuudesta ja turvallisuudesta huolehditaan Suomessa monin tavoin

- Suomalaiset vahvan sähköisen tunnistuksen järjestelmät ovat turvallisuudeltaan kansainvälisestikin vertailtuna korkeatasoisia.
- Lue lisää: https://www.traficom.fi/fi/ajankohtaista/vahvan-sahkoisen-tunnistuksen-luotettavuudesta-ja-turvallisuudesta-huolehditaan

Näin suojaudut nettihuijauksilta

- Erilaisia huijauskampanjoita on liikkeellä tällä hetkellä etenkin tekstiviestitse. Tutustu ohjeisiin ja muista suojautua huijauksilta.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta

Euroopan kyberturvallisuuskuukausi alkaa

- Euroopan kyberturvallisuuskuukautta vietetään vuosittain lokakuussa. Kampanjan tarkoituksena on edistää EU:n kansalaisten ja organisaatioiden kyberturvallisuutta.
- Kampanjaa koordinoivat Euroopan unionin kyberturvallisuusvirasto (ENISA) ja Euroopan komissio, ja sitä tukevat EU:n jäsenvaltiot ja sadat yhteistyökumppanit kansalaisjärjestöistä yliopistoihin ja yrityksiin.
- Lue lisää: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/euroopan-kyberturvallisuuskuukausi-alkaa-ota-kayttoon-parhaat-tietoturvavinkit

Uutisia Kyberturvallisuuskeskuksesta

Viranomaiset harjoittelivat syyskuussa yhteistoimintaa kansallisessa kyberpuolustusharjoituksessa

- Turvallisuusviranomaiset ovat vuosittaisella kyberharjoittelulla kehittäneet toimintavalmiuksiaan ja reagointikykyään vakavien kyberpoikkeamatilanteiden varalle.
- Turvallisuusviranomaisten kyberharjoituksen (KYHA) järjestää vuosittain Jyväskylän ammattikorkeakoulun IT-instituutin kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus JYVSECTEC yhdessä liikenne- ja viestintäministeriön kanssa.
- https://www.jamk.fi/fi/uutiset/2022/kymmenen-vuotta-pitkajanteista-kyberharjoitustoimintaa-tuottaa-tulosta

Toimintaohjeita kyberhyökkäystilanteista toipumiseen

- Miten kyberhyökkäyksistä selvitään? Miten kartoitetaan hyökkäyksen laajuus ja miten hyökkäys pysäytetään?
- Muun muassa näihin kysymyksiin löytyy vastaus Kyberturvallisuuskeskuksen julkaisemista käytännönläheisistä oppaista, jotka ovat maksutta saatavilla Kyberturvallisuuskeskuksen verkkosivuilta.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toimintaohjeita-kyberhyokkaystilanteista-toipumiseen

Merikaapelit ovat internetin selkäranka

- Nord Stream -kaasuputkien vuodot ovat ymmärrettävästi aiheuttaneet huolta myös kansainvälisten tietoliikenneyhteyksien toimivuudesta.
- Suomesta on useita yhteyksiä maailmalle ja vaikka häiriöt ovat mahdollisia, internet on varsin vikasietoinen.
- Teemme jatkuvaa yhteistyötä viestintäverkkoinfrastruktuurin suojaamiseksi sekä mahdollisten ongelmien ennaltaehkäisemiseksi, havaitsemiseksi ja korjaamiseksi.
- https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/merikaapelit-ovat-internetin-selkaranka

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

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

3) Näin suojaudut verkkohuijauksilta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta

4) Kyberturvallisuuskeskuksen viikkokatsaus 40/2022
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-402022

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

6) Matter IoT standard https://www.thesslstore.com/blog/matter-iot-standard/

7) Welive security, Toys behaving badly: How parents can protect their family from IoT threats
https://www.welivesecurity.com/2022/09/08/toys-behaving-badly-how-parents-protect-family-iot-threats/

8) YouTube down: Live streams hit by worldwide outage https://www.bleepingcomputer.com/news/technology/youtube-down-live-streams-hit-by-worldwide-outage/

Lähdeluettelo

9) Merikaapelit ovat internetin selkäranka https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/merikaapelit-ovat-internetin-selkaranka

10) Laki sähköisen viestinnän palveluista https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

11) Adversaries Continue Cyberattack Onslaught with Greater Precision and Innovative Attack Methods https://www.netscout.com/press-releases/adversaries-continue-cyberattack-onslaught-greater

12) Unionin tila: Uusien EU-sääntöjen myötä laitteisto- ja ohjelmistotuotteista tietoturvallisempiahttps://ec.europa.eu/commission/presscorner/detail/fi/IP_22_5374

13) Infocuria https://curia.europa.eu/juris/documents.jsf?num=C-793/19

14) Infocuria https://curia.europa.eu/juris/documents.jsf?num=C-339/20

15) Irlannin tietosuojaviranomaiselta ennätyksellinen seuraamusmaksu Metalle – Euroopan tietosuojaneuvosto otti kantaa lasten henkilötietojen käsittelyn lainmukaisuuteen Instagramissa https://tietosuoja.fi/-/irlannin-tietosuojaviranomaiselta-ennatyksellinen-seuraamusmaksu-metalle-euroopan-tietosuojaneuvosto-otti-kantaa-lasten-henkilotietojen-kasittelyn-lainmukaisuuteen-instagramissa

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

17) Suojelupoliisin päällikön kolumni https://supo.fi/-/paallikon-kolumni-kyberympariston-nousseen-uhkatason-taustalla-on-myos-venaja

Lähdeluettelo

18) Kyberturvallisuuskeskus: kyberympäristön uhkataso noussut https://www.traficom.fi/fi/ajankohtaista/kyberymparistön-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt

19) CISA: Iranian State Actors Conduct Cyber Operations Against the Government of Albania https://www.cisa.gov/uscert/ncas/alerts/aa22-264a

20) DW: Albania cuts ties with Iran amid cyberattack allegations https://www.dw.com/en/albania-cuts-ties-with-iran-amid-cyberattack-allegations/a-63043309

21) Politico: Albania weighed invoking NATO's Article 5 over Iranian cyberattack https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347