Tietoturvan vuosi 2021

Kyberturvallisuus elää kasvun aikaa – torjumme häiriöitä ennakolta

Kyberturvallisuuskeskuksen
vuosikatsaus

Traficomin julkaisuja
3/2022

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Sisältö

Kyberturvallisuus ohitti teini-iän

Vuonna 2021 arkeamme sävyttivät useat tietoturva- ja kyberhäiriöt. Muun muassa verkkopankkitunnuksia kalastelevat huijaukset tulivat mahdollisesti jäädäkseen. Viime vuonna suomalaiset menettivät huijausten takia rikollisille kymmeniä miljoonia euroja.

Lähes jokaiselle tulivat tutuiksi tekstiviestit, jotka levittivät FluBot-haittaohjelmaa eri teemoja hyödyntäen. Haittaohjelma ei ollut vain kiusallinen, vaan uhrit menettivät tietojaan ja rahojaan. Saastuneet laitteet myös levittivät haittaohjelmaa eteenpäin.

Huijauksen uhriksi voi joutua kuka tahansa. Jokainen meistä voi auttaa läheisiään jakamalla tietoa huijauksista.

Arjen sujuvuuteen vaikuttaneita kyberhäiriöitä nähtiin ympäri maailmaa. On hyvä muistaa, että kyberhäiriöt eivät kunnioita valtioiden rajoja ja vaikutukset voivat ulottua myös Suomeen. Esimerkiksi naapurissamme Ruotsissa Coop-päivittäistavaraketju joutui sulkemaan myymälänsä kyberhyökkäyksen vuoksi.

Koska tietoturva ja kyberturvallisuus koskevat yhä useamman ihmisen arkea, myös me Kyberturvallisuuskeskuksessa etsimme tiedotuskanavia, jotka tavoittaisivat mahdollisimman monia. Loppuvuodesta aloimme tiedottaa laajoista suomalaisia koskevista tietoturvahäiriöistä 112 Suomi -sovelluksessa.

Toimintamme painottuu yhä enemmän vakavien kyberhäiriöiden ennaltaehkäisyyn. Tässä työssä auttaa se, että Kyberturvallisuuskeskus ja meidän loistavat asiantuntijamme tunnetaan entistä paremmin. Käsittelemiemme tietoturvatapausten määrä kasvaa vuosi vuodelta. Vuonna 2021 käsittelimme kymmeniä tuhansia tietoturvatapahtumia. Niiden avulla kyettiin välttämättään valtava määrä ongelmia ennen kuin ne saivat vakavamman muodon. Verkkojen vakavien vikatilanteiden määrä Suomessa jatkoi laskusuunnassa pitkällä aikavälillä. Suomalaisista verkoista vastaavat toimijat ja heitä tukeva sääntely ovat siis selkeästi oikealla polulla. Tapausmäärissämme tietojenkalastelu on edelleen kärkisijoilla. Myös palvelunestohyökkäysten voimakkuudet kasvoivat.

Ennakoivaa työtä tehtiin myös päivittämällä määräyksiä ja valmistelemalla suosituksia yhteistyössä teleoperaattoreiden kanssa. Työ jatkuu muun muassa vuonna 2021 julkaistun Kyberturvallisuuden kehittämisohjelman puitteissa. Tietoturvan suunnannäyttäjä -tunnustus jaettiin LähiTapiolalle sen ennaltaehkäisevään toimintaan tekemien panostuksien johdosta.

”Vuonna 2021 kyberhäiriöt arkipäiväistyivät uudeksi normaalitilaksi.

Lisäksi sääntelyrintamalla tapahtui paljon. Valtioneuvosto antoi periaatepäätöksen tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (Titukri). Kaikille kriittisille toimialoille halutaan säätää lakisääteiset tietoturvavaatimukset, ja kriittisiä tietojärjestelmiä tulee arvioida nykyistä kattavammin. Vuoden aikana valmisteltiin uutta kyberturvallisuutta koskevaa sääntelyä liittyen EU:n verkko- ja tietoturvadirektiiviin (NIS 2). Myös tulevassa EU:n tekoälysäädöksessä kyberturvallisuusasiat tulevat saamaan huomiota.

Vuoteen 2021 kuului myös juhlaa, kun CERT-toimintomme 20-vuotissyntymäpäivät lähestyivät. Virallisesti CERT-FI perustettiin tammikuussa 2002. Suomi on ollut tietoturvan ja kyberturvallisuuden suunnannäyttäjä jo pitkään, ja tämän haasteen otamme vastaan myös vuonna 2022.

Vuosi piti sisällään myös monia resurssihaasteita, eivätkä kyberturvallisuuden kasvukivut ole ohi. Vuosi voidaan kuitenkin summata todeten, että kyberturvallisuus on ohittanut teini-iän. Kohtaamme uusia, entistä suurempia haasteita entistä vahvempina.

Sauli Pahlman
ylijohtaja
Kyberturvallisuuskeskus

Toimintamme tunnuslukuja

2021 2020

Katkeamaton päivystys

Käsitellyt tapaukset

Varoitukset

Haitallisten sivustojen alasajot

Haavoittuvuus-koordinaation käsittelemät tapaukset

Autoreporter

media-yhteydenotot

Facebook-seuraajat

Twitter-seuraajat

Häiriömäärät

Kriittiset häiriöt

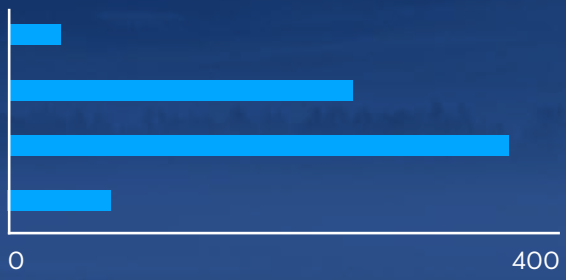
Vakavat häiriöt

Merkittävät häiriöt

Kaikki häiriöt yhteensä

Viestintä ja tiedotteet

Haavoittuvuustiedotteet	38
Haavoittuvuuskoosteet	249
Uutiskoosteet	364
Tietoturva nyt	75



Asiakastyytyväisyyskyselyt

Toteutimme vuoden aikana asiakastyytyväisyyskyselyt tilannekuvatuotteisiimme ja tiedonvaihtoryhmiimme liittyen. Kyselyidemme arviointiskaala oli huonosta (1) kiitettävään (5). Molempien kyselyiden tyytyväisyyttä osoittava keskiarvo oli 4,3.

Tilannekuvakyselyn mukaan tilannekuvatuotteitamme käytetään organisaation tietoturvan ylläpitämiseen, niistä saadaan tietoa uusista haavoittuvuuksista ja ajankohtaisista tapahtumista. Kyberturvallisuuskeskus koostaa tilannekuvaa useasta eri lähteestä saatujen tietojen avulla ja jakaa sitä edelleen eri tuotteiden välityksellä.

Tilannekuvatuotteista luetuimpia ovat:

- Kybersää
- varoitukset
- haavoittuvuustiedotteet
- viikkoraportit

Kyberturvallisuuskeskukselle ISAC-yhteistyö tuottaa tietoa tilannekuvan rakentamiseen ja rikastamiseen. Yhteistyöllä on myös pystytty estämään tietoturvapoikkeamia.

Tiedonvaihtoryhmät (ISAC) arvostivat erityisesti, että

- ryhmissä käydään avointa tiedonvaihtoa luottamusverkostossa
- ryhmissä saa julkisen tiedonvälityksen ulkopuolista tietoa
- ISAC-ryhmät ovat tehokas ja neutraali viranomaisen ja toimialan yhteydenpito- ja tiedonvaihtokeino.

Tilannekuvatuotteet

4,2 (2020) → 4,3 (2021)

Keskiarvo

Toimialakohtaiset tiedonvaihtoryhmät

4,4 (2020) → 4,3 (2021)

Keskiarvo

Kuinka vaikutimme?

Digitaalinen kehitys tuo jatkuvasti saatavillemme uusia palveluita, parantaa ja helpottaa meidän arkeamme ja elämää sekä tuo uusia ratkaisuja globaalien haasteiden ratkaisemiseen. Vaikka tämä kehitys tuo pääasiassa hyvää, on digitaalisen kehityksen varjopuolena alati kasvava kyberrikollisuus sekä erilaiset häiriöt.

Kuten kaikille digitaalisille ilmiölle, myös kyberuhkille on luonteenomaista nopea kehitys. Kyberturvallisuuteen liittyvät ilmiöt ovat usein myös monimutkaisia eivätkä noudata ennalta määritettyjä viranomaisvastuita. Tämä edellyttää uudenlaista toiminta- ja reagointikykyä myös viranomaisilta.

Kyberturvallisuuskeskuksen etuna on laaja toimintakenttä sekä tätä tukeva monipuolinen teknologinen, juridinen ja yhteiskunnallinen osaaminen. Näiden avulla pystymme järjestäytymään tarvittaessa nopeastikin yhteistyössä kansallisten ja kansainvälisten yhteistyökumppaniemme kanssa vastaamaan erilaisiin tilanteisiin ja tarpeisiin.

Kehittämisohjelma ja Titukri kehityksen vetureina

Kyberturvallisuuden parantamiseksi tehtiin aloitteita. Näistä keskeisimmät olivat kansallinen kyberturvallisuuden kehittämisohjelma ja valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (Titukri). Kehittämisohjelmassa parannetaan kyberturvallisuutta pitkällä aikavälillä, yli toimialarajojen. Titukri vauhdittaa yhteiskunnan kriittisten tietojärjestelmien tietoturvan ja tietosuojan tason parantamista.

Vuonna 2021 laaditussa Kyberturvallisuuden kehittämisohjelmassa määritetään keskeiset toimenpiteet kyberturvallisuuden parantamiseksi koko yhteiskunnassa. Laajassa yhteistyössä laaditun kehittämisohjelman aikajänne ulottuu aina vuoteen 2030 asti. Kehittämisohjelman ensisijaisena tavoitteena on luoda Suomeen kyberturvallisuuden ekosysteemi, joka tuottaa elinvoimaa ja kasvua, lisää alan työpaikkoja, luo tarvittavaa osaamista ja parantaa koko digitaalisen yhteiskuntamme kestävyyttä sekä sietokykyä kybertoimintaympäristön eri ilmiöitä vastaan. Kehittämisohjelma rakentuu neljän pääteeman ympärille: **huippuluokan osaaminen**, **kiinteä yhteistyö**, **vahva kotimainen kyberturvateollisuus** ja **tehokkaat kansalliset kyberturvallisuuskyvykkyydet.** On selvää, että vahva kansallinen kyberturvallisuus edellyttää tarvittavaa osaamista yhteiskunnan kaikilla eri tasoilla. Viranomaisten puolelta Kyberturvallisuuskeskuksella on keskeinen rooli osaamisen kehittämiseksi niin viranomaisten, yritysten kuin tavallisten kansalaisten parissa.

Kyberturvallisuuden ekosysteemin vahvistaminen edellyttää yhteistyön pitkäjänteistä vahvistamista. Kyberturvallisuuskeskuksella on merkittävä rooli yhteistyön kehittämiseen niin kansallisella kuin kansainvälisellä tasolla. Yksi keskeisempiä tunnistettuja yhteistyön kehittämisen työkaluja on kyberturvallisuutta koskeva harjoitustoiminta.

Vahvan kotimaisen kyberturvateollisuuden osalta tulee kiinnittää erityistä huomiota perustettavaan EU:n kyberturvallisuuden kompetenssikeskukseen ja kansallisten koordinointikeskusten verkostoon. Liikenne- ja viestintäviraston Kyberturvallisuuskeskus on nimetty kansalliseksi koordinointikeskukseksi ja Kyberturvallisuuskeskus pyrkii tämän roolin kautta tukemaan kansallisia kyberturvallisuusmarkkinoita ja -teollisuutta kiihtyvässä kansainvälisessä kilpailussa. Viimeinen kehittämisohjelman pääteemoista koskee kansallisten kyberturvakyvykkyyksien tehostamista. Nämä kyvykkyydet luovat pohjaa koko yhteiskunnan toiminnalle ja turvallisuudelle sekä edistävät suvereniteettiamme kybertoimintaympäristössä.

”Kehittämisohjelman ensisijaisena tavoitteena on luoda Suomeen kyberturvallisuuden ekosysteemi.

Titukri auttaa torjumaan tulevaisuuden vastaamoja

Vuoden 2021 aikana laadittiin Vastaamon tietomurtotapauksen seurauksena valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. Jotta periaatepäätöksen tavoitteet voivat täyttyä, roolimme tässä työssä on tärkeä. Periaatepäätöksessä on kiinnitetty huomiota erityisesti viranomaisten entistä tehokkaampaan ja järjestäytyneempään yhteistyöhön, velvoittaviin tietoturvavaatimuksiin, vaatimusten säännölliseen valvontaan, kriittisten prosessien ja toimintojen tunnistamiseen sekä tietojärjestelmien arviointiin ja auditointiin. Kyberturvallisuuskeskuksen rooli on avainasemassa periaatepäätöksen tavoitteiden edistämisessä, kyberturvallisuutta koskevan yhteistyön kehittämisessä ja muiden viranomaisten toiminnan tukemisessa. On selvää, että Kyberturvallisuuskeskuksen resursseja tulee vahvistaa, jotta se pystyy tukemaan ja antamaan vielä aikaisempaa enemmän periaatepäätöstyössä tunnistettua toimialakohtaista neuvontaa ja tukea muille toimialoille.

Vaikka Kyberturvallisuuskeskuksen tukitoimenpiteiden ja tuottamien palveluiden käyttöä pyritään edistämään eri toimialoilla, jokaisen toimialan tulee jatkaa oman toimintansa kehittämistä entistä tietoturvallisempaan suuntaan. Tietoturvan tulisi olla lähtökohtaisesti sisäänrakennettua kriittisten toimialojen toimintakulttuuriin ja toimijoiden on itse kannettava siitä vastuu.

”Tietoturvan tulisi olla sisäänrakennettuna kriittisten toimialojen toimintakulttuuriin.

Verkkohuijarit nitistetään yhteisvoimin

Nettihuijauksien uhriksi voi joutua kuka tahansa, rikollisten haltuun on valunut kymmeniä miljoonia euroja. Huijauksia vastaan tehdään laajaa yhteistyötä viranomaisten, yritysten ja järjestöjen kesken. Vuonna 2021 tiedot kyberhäiriöistä saatiin suoraan kännykkään Suomi 112- sovelluksen kautta ensimmäistä kertaa.

Suomalaiset menettävät erilaisiin nettihuijauksiin vuosittain kymmeniä miljoonia euroja. Kyberturvallisuuskeskus toimii aktiivisesti yhteistyössä teleoperaattoreiden, poliisin, muiden viranomaisten ja järjestöjen kanssa torjuakseen nettihuijauksia. Kyberturvallisuuskeskuksen laatimat tiedotteet ja varoitukset kertovat ajankohtaisesti ja täsmällisesti, millaisia huijauksia ja tietojenkalastelukampanjoita on liikkeellä. Rikollisten huijauskampanjat eivät ole mitään näpertelyä tai hakkereiden harrastelua, vaan sitä tekevät kansainväliset ammattirikollisliigat. Pelkkä viranomaisten tiedotus ei ongelmaa ratkaise, vaan valistamiseen tarvitaan mukaan koko mediakenttä iltapäivälehdistöstä aamu-uutisiin. Lehdistöä on kiittäminen siitä, että huijausilmiöt saatetaan yleisön tietoon. Kyberturvallisuuskeskus on mukana myös Kuluttajaliiton Huijarit kuriin -hankkeessa, joka tekee aktiivista valistustyötä huijausten torjumiseksi.

Uudeksi tiedotuskanavaksi Kyberturvallisuuskeskus on saanut Hätäkeskuksen lanseeraaman 112 Suomi -sovelluksen, jota käyttää lähes kaksi miljoonaa suomalaista. Vuoden 2021 aikana mittavista yksityishenkilöihin suunnatuista huijauskampanjoista on varoitettu 112 Suomi -sovelluksen kautta kaksi kertaa. Vaarallisista huijaus- ja haittaohjelmahyökkäyksistä on varoitettu miljoonia suomalaisia, mutta uusia uhreja silti tulee jatkuvasti. Tavoitteena on saada sekä uhrien että rikoshyödyn määrä laskuun tulevina vuosina.

”Pelkkä viranomaisten tiedotus ei ongelmaa ratkaise, vaan valistamiseen tarvitaan mukaan koko mediakenttä iltapäivälehdistöstä aamu-uutisiin.

Traficom ja teleoperaattorit kampittavat yhdessä huijaussoittoja ja tekstiviestitse leviäviä haittaohjelmia

Joidenkin huijausten taltuttamiseksi tarvitaan teleoperaattoreiden toimia. Vuonna 2021 teleoperaattorit ja Traficom etsivät yhdessä keinoja puhelinnumeron väärentämisen estämiseksi. FluBot-haittaohjelman taltuttamisessa operaattoreiden viestisuodattimiin jäi yli miljoona haittaviestiä.

Soittajan puhelinnumeron väärentäminen suomalaiseksi puhelinnumeroksi on kansainvälisten rikollisten laajasti hyödyntämä tekniikka, jonka avulla suomalaiset uhrit saadaan paljon suuremmalla todennäköisyydellä luottamaan ja vastaamaan ulkomailta tuleviin huijauspuheluihin ja esimerkiksi luovuttamaan verkkopankkitunnuksensa tai tietokoneensa rikollisten etäohjattavaksi. Ulkomailta soitettujen puheluiden soittajan numeron väärentäminen huijauspuheluissa on ollut viime vuodesta alkaen merkittävä ongelma myös Suomessa. Tilanteen korjaamiseksi Traficom ryhtyi valmistelemaan yhdessä teleoperaattorien kanssa keinoja, joilla soittajan numeron väärentäminen suomalaiseksi puhelinnumeroksi estetään. Tavoitteena on kansainvälisten rikollisten toiminnan vaikeuttaminen ja estäminen. Ratkaisun ansiosta teleoperaattori voi huolehtia siitä, että numero kuuluu liittymäasiakkaalle, jolla on käyttöoikeus kyseiseen numeroon. Puhelun vastaanottaja voi puolestaan luottaa siihen, että suomalaisesta numerosta tulevaa puhelu on soitettu suomalaisesta puhelinliittymästä. Lisäksi suomalaisen puhelinliittymän ja numeron haltija voi luottaa siihen, ettei hänen puhelinnumeroaan käytetä rikoksiin.

Ripeät toimenpiteet teleoperaattoreiden kanssa FluBot-haittaohjelman leviämisen estämiseksi

Torjuimme kesällä alkanutta FluBot-mobiilihaittaohjelman aaltoa yhteistyössä teleyritysten kanssa. Välitimme teleyrityksille ajantasaista tietoa haittaohjelman käyttämistä komentokanavista, jotta teleyritykset pystyivät suodattamaan niihin suuntautuvan verkkoliikenteen. Tämä teki haittaohjelman toimintakyvyttömäksi ja esti sen tartunnan leviämisen saastuneelta laitteelta eteenpäin.

Marraskuussa FluBot-haittaohjelmasta alkoi levitä uusi kehittyneempi versio, joka käytti komentokanavana DNS Over HTTPS (DoH) -protokollaa. Tätä ei pysty torjumaan verkkoliikenteen suodattamisella häiritsemättä useiden muiden palveluiden toimintaa. Taistelimme uutta FluBot-aaltoa vastaan muun muassa suosittelemalla teleyrityksiä suodattamaan FluBot-haittaohjelmaa levittäviä SMS-viestejä. Viestejä suodatettiin yli miljoona, joten toimilla oli merkittävä vaikutus jatkoleviämisen hillitsemisessä.

Sähköisten tunnistus- ja luottamuspalvelumääräyksen päivitys yhteistyössä toimialan kanssa.

Päivitimme määräystämme sähköisistä tunnistus- ja luottamuspalveluista. Uudistetussa määräyksessä säädetään muun muassa

1. Loppukäyttäjän turvallisuutta parantavia pakollisia kontrolleja kuten istuntotunnisteet, varmistetut kohdepalvelutiedot.
2. Käyttäjää informoidaan yhteneväisesti ja paremmin koko tunnistustapahtuman ajan
3. Uusia vaihtoehtoja varmentaa ja turvata tietoliikenneyhteydet eri toimijoiden välillä
4. Päivitetyt ja joustavammat vaatimukset salauskäytännöistä mahdollistaen esimerkiksi uusien salausratkaisujen helpomman käyttöönoton
5. Tunnistusmenetelmästä on tehtävä erillinen riskiarvio, jossa arvioidaan tunnistusmenetelmään ja -tekijöihin kohdistuvia uhkia ja suojaavia toimenpiteitä.

Palvelumme elinkeinoelämälle

Kyberturvallisuuskeskus kehittää ja tuottaa elinkeinoelämällä ja huoltovarmuuskriittisille toimijoille kyberturvallisuuspalveluita, jotka auttavat ylläpitämään ja kehittämään tietoturvaa nopeasti muuttuvassa maailmassa. Kyberturvallisuuskeskuksen palveluiden käyttäjät muodostavat tietoturvayhteisön, jossa tietoa jaetaan luottamuksellisesti.

Kybermittari

Kybermittarin ensimmäinen vuosi on takana, ja saadun palautteen perusteella kyberturvallisuuden kyvykkyyksien systemaattiselle arviointimallille on kysyntää. Vuoden aikana Kybermittaria on esitelty sidosryhmille, kerätty palautetta, pidetty koulutuksia ja testattu uusia ideoita. Kybermittarista julkistetaan alkuvuodesta 2022 uusi versio, jossa on huomioitu asiakaspalaute ja johon on toteutettu myös Cybersecurity Capability Maturity Model (C2M2) versioon 2 kesällä julkaistut muutokset.

ISAC-harjoittelusta toimialoja hyödyntäviä oppeja

Kuluneen vuoden 2021 aikana olemme yhteistyössä ISAC-toimijoiden* kanssa kehittäneet Kyberturvallisuuskeskuksen tiedonvaihtoryhmien kyberharjoittelua. Olemme järjestäneet harjoitukset Elintarvike- , Energia-, Vesi- sekä Logistiikka- ja liikenne ISAC -ryhmille yhteistyössä Instan ja Fraktalin kanssa. Harjoitusten teemana on ollut tiedonvaihto, tilannekuva ja viranomaisten rooli laajamittaisissa toimialaa koskettavissa kyberhäiriötilanteissa. ISAC-toimijoiden yhteisharjoituksista on tehty hyviä havaintoja ja saatu oppeja, joiden avulla kyseisten toimialojen valmius ja kyky kohdata kyberuhkatilanteita paranee.

HAVARO

Vakavien tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä HAVARO uudistui vuonna 2021. Palvelua tarjotaan nyt laajemmin suomalaisille organisaatioille yhteistyössä kaupallisten tietoturvatoimijoiden kanssa. Tietoturva ry palkitsi HAVAROn vuoden tietoturvatuotteena.

* ISAC-tiedonvaihtoryhmät (ISAC=Information Sharing and Analysis Centre) ovat eri toimialoille perustettuja kyberturvallisuuden yhteistyöelimiä.

Luotettava aika- ja paikkatieto on yhteiskunnan tukipilari

Yhteiskunta on yhä riippuvaisempi satelliittipaikannusjärjestelmien tuottamasta sijainti- ja aikatiedosta. Eurooppalaisen Galileo-paikannusjärjestelmän julkisesti säännellyn satelliittipalvelun (Public Regulated Service, PRS) tarkoitus on tuottaa viranomaisille ja huoltovarmuuskriittisille yrityksille varmistettua ja jatkuvaa sijainti- ja aikatietoa kaikissa olosuhteissa.

PRS-palvelun tulevia käyttäjiä Suomessa ovat esimerkiksi poliisi, Tulli, Puolustusvoimat, pelastustoimi sekä huoltovarmuuden kannalta kriittiset yritykset, kuten teleyritykset ja pankit sekä energiasektori ja liikenne- ja logistiikka-ala.

Yhteiskunnan tukipilari – luotettava aika- ja paikkatieto – sai tukevan maaperän marraskuussa 2020, kun hallituksen talouspoliittinen ministerivaliokunta linjasi, että PRS-palvelu otetaan Suomessa käyttöön vuonna 2024. Käynnistimme palvelun suunnittelutyön yhdessä tulevien palveluoperaattorien, Suomen Erillisverkot Oy:n ja Puolustusvoimien kanssa.

> **”Harjoitusten teemana on ollut tiedonvaihto, tilannekuva ja viranomaisten rooli laajamittaisissa toimialaa koskettavissa kyberhäiriötilanteissa.**

Viestintäverkkojen turvallisuus

Yhteiskuntamme on yhä riippuvaisempi viestintäverkoista ja verkkoteknologiat kehittyvät. Vuonna 2021 pohdittiin erityisesti 5G-verkkojen tietoturvaa ja verkon kriittisimpien osien suojausta.

Viestintäverkkojen turvallisuus on säilynyt korkeana prioriteettina niin EU:n kuin kansainvälisen tason keskusteluissa. EU:ssa jäsenvaltiot ovat käsitelleet tuoreimman 5G-verkkosukupolven käyttöönottoa ja turvallisuutta ennennäkemättömän aktiivisesti. Nämä keskustelut tulevat myös jatkumaan ja niiden painoarvo tulee kasvamaan entisestään viestintäverkkoteknologian kehittyessä ja yhteiskunnan viestintäverkkoja koskevan riippuvuuden kasvaessa.

Vuoden 2021 alussa Suomessa tuli voimaan viestintäverkkojen turvallisuutta koskevia uusia säännöksiä. Kansallisen sääntelyn taustalla vaikutti erityisesti EU:n yhteinen lähestymistapa 5G-verkkoihin liittyviin turvallisuushuoliin vastaamiseksi. EU:n yhteinen 5G-verkkojen turvallisuutta koskeva työ huipentui komission ja jäsenvaltioiden laatimaan yhteiseen keinovalikoimaan (toolbox), jossa nostetaan esille lukuisia toimenpiteitä 5G-verkkojen ja niiden varassa toimivien palveluiden turvallisuuden varmistamiseksi. Yksi keskeisimmistä keinovalikoiman toimenpiteistä on verkon kaikkein kriittisimpien osien riittävä suojaaminen.

Vuoden alusta voimaan tulleessa kansallisessa sääntelyssä mahdollistetaan viestintäverkkojen kriittisten osien arviointi kansallisen turvallisuuden ja maanpuolustuksen näkökulmasta. Lähtökohtana on, että viestintäverkon kriittisissä osissa ei saisi käyttää laitteita, jotka voivat vaarantaa kansallisen turvallisuuden. Jos tällainen laite löytyy, se voidaan määrätä poistettavaksi.

Yllä mainittua sääntelyä viestintäverkon kriittisten osien turvallisuudesta täydennettiin keväällä 2021 Liikenne- ja viestintäviraston teknisellä määräyksellä. Määräyksellä on selvennetty kriittisten osien teknistä määrittelyä ja tunnistamista. Niin kansallinen sääntely kuin Liikenne- ja viestintäviraston määräys laadittiin laajassa poikkihallinnollisessa yhteistyössä. Myös toimialan edustajat osallistuivat aktiivisesti valmistelutyöhön.

Laaditun sääntelyn ja erityisesti tuoreen määräyksen osalta tulee muistaa, että teknologiakehityksen seurauksena laadittuja työkaluja pitää pystyä päivittämään nopeallakin aikataululla. Tämän johdosta teknologista kehitystä ja sen asettamia muutostarpeita muun muassa sääntelyn osalta arvioidaan säännöllisesti alkuvuonna 2021 perustetussa Verkkoturvallisuuden neuvottelukunnassa.

”Yksi keskeisimmistä keinovalikoiman toimenpiteistä on verkon kaikkein kriittisimpien osien riittävä suojaaminen.

Kybersääilmiöt

Kybersääkartoilla näkyi voimakkaita palvelunestohyökkäyksiä, ärhäköitä haittaohjelmia ja ennätysmäärä tietojenkalastelua.

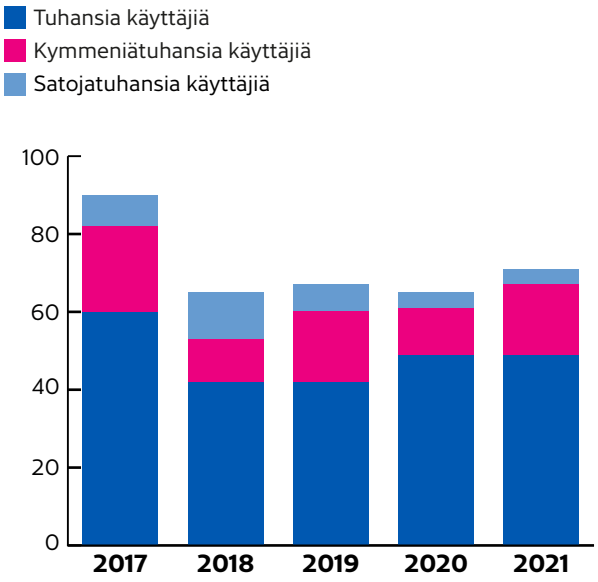
Verkkojen toimivuus

Verkkojen vakavien vikatilanteiden määrä Suomessa jatkoi laskusuunnassa pitkällä aikavälillä. Globaalien palveluiden katkokset tuntuivat myös meillä.

Viestintäverkkojen häiriöt

Vuonna 2021 erilaiset katkokset yleisessä viestintäverkossa ja kansainvälisissä palveluissa osoittivat meille jälleen, kuinka riippuvaisia olemme toimivista yhteyksistä ja erilaisista digitaalisista palveluista. Laaja palvelukatko voi aiheuttaa vaikutuksia yhteiskunnan kriittisissä toiminnoissa – samanaikaisesti sama katko voi myös estää kansalaisen sosiaalisen median käytön, kunnes vika on korjattu.

Olemme tottuneet siihen, että palvelut ovat saatavilla verkossa jatkuvasti. Erilaiset katkokset kotimaisessa verkossa, pankkipalveluissa tai sosiaalisessa mediassa osoittavat konkreettisesti, että riskienhallinta ja varautuminen on tärkeää myös palveluiden käyttäjille. Katkoksen takia ostokset saattavat jäädä maksamatta, pienyrityksen sometili päivittämättä ja suoratoistopalvelun elokuvahetki välistä.



Yleisten viestintäpalveluiden merkittävien toimivuushäiriöiden lukumäärät vuosina 2017–2021

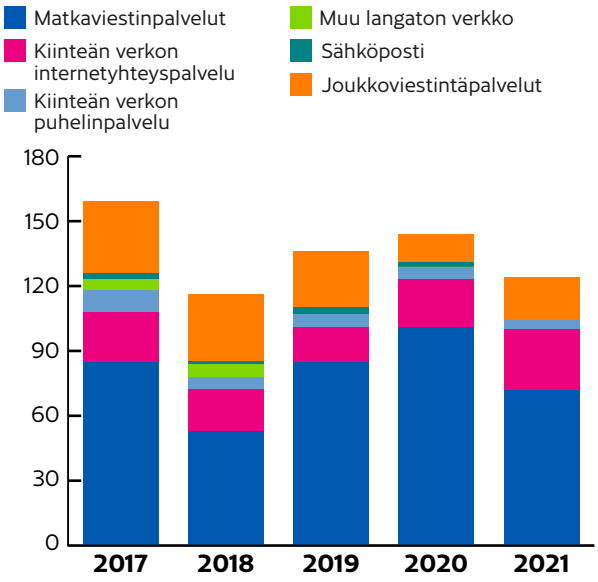
”Kehityssuuntaa voidaan pitää positiivisena, vaikka merkittävien häiriöiden määrä ei ole enää pienentynyt.

Suomessa viestintäverkkojen tila on yhä vakaa

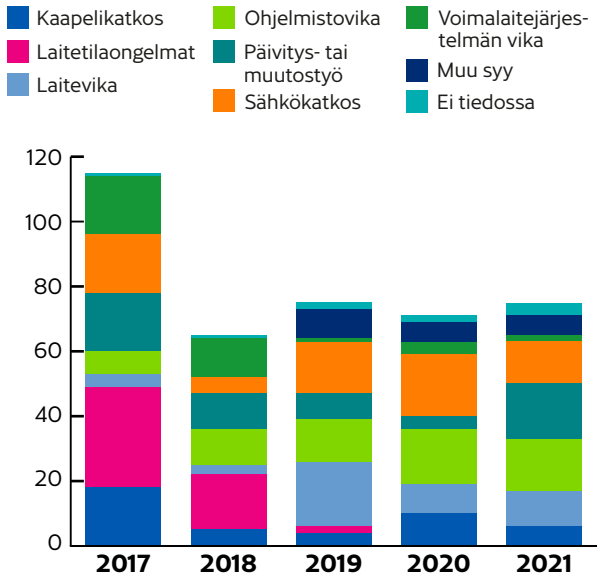
Keräämme tietoa kotimaisten viestintäverkkojen häiriöistä. Näin pääsemme käsiksi häiriöiden juurisyihin ja voimme parantaa verkkojen turvallisuutta ja toimintavarmuutta yhteistyössä toimialan kanssa.

Merkittävien häiriöiden määrä pieneni selvästi vuoteen 2018 asti. Siitä lähtien häiriöitä on vuosittain raportoitu 65–73. Vuonna 2021 merkittäviä häiriöitä oli 73. Verkkojemme kapasiteetti on riittänyt mainiosti läpi pandemia-ajan ja kasvaneen kuormituksen.

Kriittiset häiriöt, jotka koskevat vähintään 100 000 käyttäjää, ovat vähentyneet viime vuosina. Kokonaisuutena kehityssuuntaa voidaan pitää positiivisena, vaikka merkittävien häiriöiden määrä ei ole enää pienentynyt.



Merkittävien toimivuushäiriöiden vaikutukset yleisiin viestintäpalveluihin vuosina 2017–2021. Yksi häiriötilanne voi vaikuttaa useaan palveluun.



Merkittävien toimivuushäiriöiden juurisyyt vuosina 2017–2021. Yhdellä häiriötilanteella voi olla monta juurisyytä.

”Katkokset muistuttavat meitä siitä, että mikä tahansa palvelu voi keskeytyä millä tahansa hetkellä.

Valtaosa kotimaisten viestintäverkkojen merkittävistä häiriöistä koskee matkaviestinverkkojen palveluita eli puhelujen, internetyhteyksien ja tekstiviestien toimivuutta. Esimerkiksi sähkökatkot, erilaiset konfiguraatiovirheet, laiteviat ja kaapelikatkot aiheuttavat vikoja verkossa. Vian syynä voi olla myös inhimillinen näppäilyvirhe tai kaapeliin uponnut kaivurin kauha. Teleyritykset saivat osakseen myös palvelunestohyökkäyksiä ja esimerkiksi nimipalvelimet olivat hyökkääjien kohteina vuonna 2021. Hyökkäykset eivät kuitenkaan aiheuttaneet merkittäviä vaikutuksia.

Vuonna 2021 merkittävät myrskyt saivat nimekseen Aatu ja Paula, jotka osuivat Suomeen kesäkuun loppupuolella. Kesäkuussa Kyberturvallisuuskeskukseen raportoitiinkin 14 merkittävää häiriötä yleisissä viestintäverkon palveluissa. Heinäkuussa kaivinkone aiheutti kuitukatkon, joka vaikutti Valtorin eri palveluihin tuntien ajan. Toimiva yhteistyö viranomaisten, teleoperaattoreiden ja sähköyhtiöiden kesken edesauttaa varautumista myrskyihin ja erilaisiin poikkeamatilanteisiin.

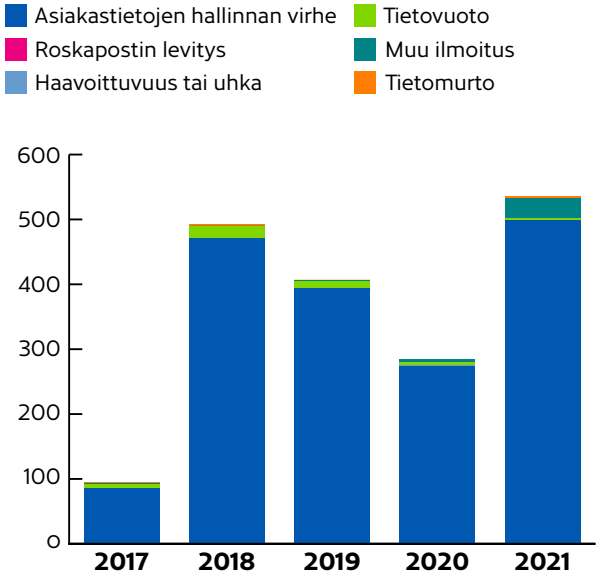
Suosittujen ja globaalien palveluiden hikat tuntuivat myös meillä

Sähköpostipalvelut katkeilivat etenkin maaliskuussa Microsoftin Exchange -sähköpostipalvelimien haavoittuvuuden vuoksi. Haavoittuvuuden päivitykset ja palvelinten tietoturvatutkinnat pitivät sähköpostiliikenteen hetkellisesti paikoittain hiljaisena. Merkittävä haavoittuvuus aiheutti ainakin hetkellisesti katkoksia sähköpostiliikenteeseen, kun palvelimet tuli kriittisyyden vuoksi päivittää mahdollisimman pian – jopa keskellä työpäivää.

Syyskuussa maailmanlaajuiset palvelukatkokset Facebookissa, WhatsAppissa ja Instagramissa keskeyttivät palveluiden käytön arki-iltana tunneiksi. Myös esimerkiksi Microsoftin, Slackin, Salesforcen ja Fastlyn palvelut pätkivät vuoden aikana. Katkokset näkyivät eri palveluiden saatavuudessa ja esimerkiksi erilaisten verkkosivujen toimimattomuutena. Kansainvälisten palveluntarjoajien mukaan ongelmia aiheuttivat muun muassa erilaiset konfigurointivirheet tai sovellusten suunnitteluvirheet. Katkokset muistuttavat meitä siitä, että mikä tahansa palvelu voi keskeytyä millä tahansa hetkellä. Kansalaisten ja organisaatioiden tuleekin tiedostaa se, että sosiaalisen median palvelut voivat joskus olla pitkällisestikin pois saatavilta. Olemme tottuneet palveluiden hyvään saatavuuteen, mutta esimerkit osoittavat, että katkoksilla voi olla harmillisia vaikutuksia vaikkapa pk-yrityksen mainossivun päivityksiin tai kansalaisen yhteydenpitoon läheisten kanssa.

Henkilötietoja koskevat tietoturva-ilmoitukset ovat vähentyneet

Teleyritysten ilmoitusten määrät henkilötietoja koskeneista tietoturvaloukkauksista ovat pienentyneet tasaisesti vuoden 2018 huipusta lähtien. Tyypillinen tapaus on, että teleyritys lähettää asiakkaan henkilötietoja sisältävän kirjeen tai sähköpostin väärään osoitteeseen. Merkittäviä tietoturvaloukkauksia on tavallisesti alle kymmenen vuodessa. Vuonna 2021 niitä ilmoitettiin 17.



Teleyritysten ilmoitukset merkittävistä tietoturvaloukkauksista ja henkilötietojen tietoturvaloukkauksista vuosina 2017–2021. Vuonna 2021 useampi teleyritys alkoi ilmoittaa loukkauksista, jonka vuoksi määrä vaikuttaa suuremmalta kuin aiemmin.

Palvelunestohyökkäykset

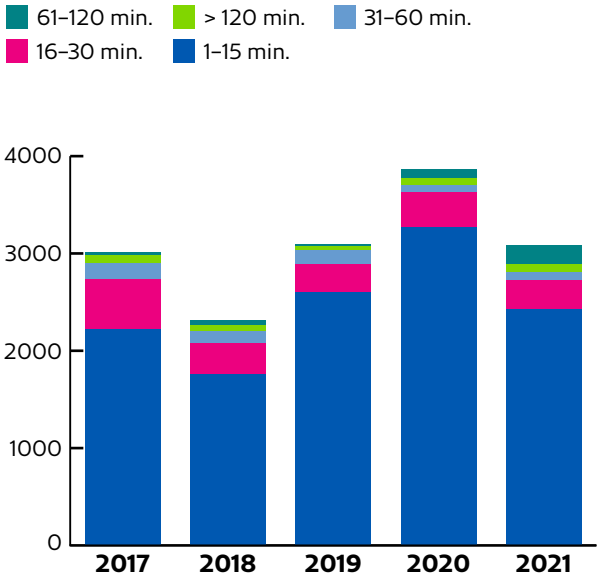
Kyberturvallisuuskeskus vastaanotti kymmeniä ilmoituksia palvelunestohyökkäyksistä, jotka vaikuttivat organisaatioiden toimintakykyyn. Hyökkäykset aiheuttivat joko lyhyitä katkoksia esimerkiksi työntekijöiden etäyhteyksissä tai olivat tunteja kestäviä hyökkäyksiä esimerkiksi verkkopalveluun.

Toistuessaan lyhyetkin palvelunestohyökkäykset voivat olla riesa organisaatiolle, jos ne välillisesti aiheuttavat ongelmia sisäisten palveluiden toimintaan. Olemme saaneet useita ilmoituksia, missä hyökkäyksellä on ollut vaikutuksia organisaation VPN-yhteyksiin. Tällöin työn tekeminen saattaa pysähtyä hetkellisesti ja etäpalaveritkin jäävät odottamaan yhteyksien palautumista. Usein organisaatiot siirtävät palvelujaan pilvipalveluihin, jotka on toteutettu kestämään suuriakin palvelunestohyökkäyksiä niin, että ne eivät vaikuta palveluiden käytettävyyteen.

Kunnissa koulujen sähköiset palvelut saivat iskuja

Kunnilta saimme ilmoituksia hyökkäyksistä, joiden kohteena ovat olleet erilaiset koulujen opiskelupalvelut tai koulun ulkoverkon osoitteet. Palvelut kannattaakin suunnitella niin, että lyhytkestoinenkaan palvelunestohyökkäys ei pääsisi vaikuttamaan niiden toimivuuteen.

Palvelunestohyökkäyksistä kirjataan myös poliisille vuosittain rikosilmoituksia. Lyhyt hyökkäys voi aiheuttaa katkoksia palveluissa ja käynnistää esimerkiksi poliisin tutkintaprosessin. On hyvä muistaa, että alle 15-vuotiaskin voi joutua niistä vastuuseen. Kannustamme organisaatioita tekemään palvelunestohyökkäyksistä rikosilmoituksen.



Palvelunestohyökkäysten kestojen kehitys Suomessa. Lähde: Telia

Palvelunestohyökkäysten volyymit rikkoivat ennätyksiä

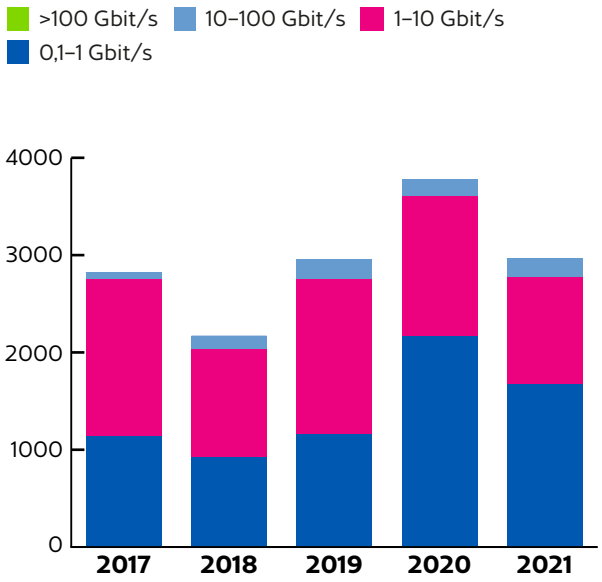
Kuluneena vuonna tuimme useita organisaatioita palvelunestohyökkäyksen sattuessa kohdalle ja täydensimme hyökkäysten tilannekuvaa yhteistyössä kansainvälisten yhteistyökumppaniemme kanssa.

Suomessa Kyberturvallisuuskeskukselle ilmoitettujen palveluestohyökkäysten koko on tavallisesti noin 1–10 Gbit/s. Kotimaiset organisaatiot ovat varautuneita tämän kokoisiin hyökkäyksiin esimerkiksi operaattoreiden mitigaatiopalveluiden avulla.

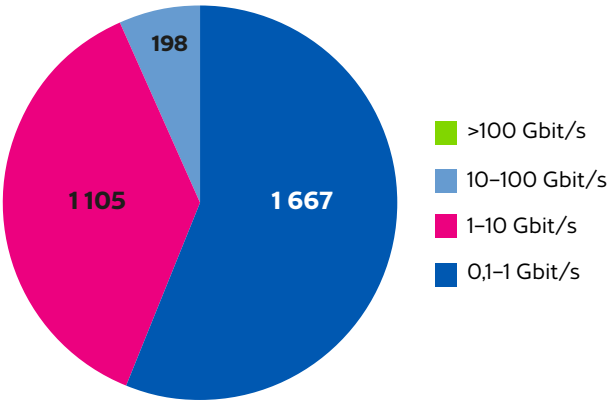
Vuonna 2021 Suomessa havaittiin kourallinen massiivisia noin 100 Gbit/s -kokoisia hyökkäyksiä, jotka aiheuttivat muun muassa palvelukatkoksia organisaatioille. Saimme myös ilmoituksen tähän asti suurimmasta palvelunestohyökkäyksestä Suomessa. 260 Gbit/s:n hyökkäys oli ennätysluokkaa, mutta mitigaatiopalvelut onnistuivat estämään sen.

Myös vuonna 2021 kotimaisiin organisaatioihin osui palvelunestohyökkäyksiä, joihin liittyi kiristysviesti. Muutamissa tapauksissa kiristysviesti oli löytynyt sähköpostin roskakorista, kun taas toiset olivat saaneet kiristysviestin näytehyökkäyksen kera. Suurempia hyökkäyksiä, joilla uhkailtiin, ei kuitenkaan koskaan toteutettu.

Näytehyökkäykset voivat hyvinkin olla voimakkuudeltaan yli 10 Gbit/s. Maailmalla kiristysviestejä on lähetetty esimerkiksi teleoperaattoreille. Lisäksi suuret kansainväliset palvelutarjoajat kertoivat jälleen ennätyksellisen suurista palvelunestohyökkäyksistä esimerkiksi pilvipalveluja kohtaan. Pilvipalvelut ovat kuitenkin suunniteltu kestämään erilaisia hyökkäyksiä ja usein vaikutukset eivät näy palveluiden toimivuudessa.



Palvelunestohyökkäysten volyymien kehitys Suomessa.
Lähde: Telia



Palvelunestohyökkäysten volyymien jakauma Suomessa 2021.
Lähde: Telia

”260 Gbit/s:n hyökkäys oli ennätysluokkaa, mutta mitigaatiopalvelut onnistuivat estämään sen.

Kybervakoilu

Haavoittuvat verkkolaitteet ja -palvelut ovat kybervakoilussa kiinnostuksen kohteena, koska niitä hyödyntämällä voidaan päästä käsiksi luottamukselliseen tietoon, viestintään tai järjestelmiin.

Kybervakoilu on jatkunut aktiivisena myös vuonna 2021, mutta Suomessa pahimmilta myrskyiltä on säästytty. Pyrkimys erilaisten haavoittuvuuksien hyödyntämiseen kybervakoiluoperaatioissa on näkynyt huomattavan paljon niin julkisessa keskustelussa kuin kybervakoiluun liittyvissä havainnoissa. Kasvaneen etätyön lisäämä etäyhteyksien käyttö on myös pysynyt kybervakoilulle otollisena kohteena.

Haavoittuvat verkkolaitteet kohteena

Suomalaisiin organisaatioihin kohdistuu jatkuvasti erilaisia haavoittuvien palveluiden tai heikkojen salasanojen löytämiseen tähtäävää toimintaa, ja tämä on jatkunut myös vuonna 2021. Osa toiminnasta viittaa julkisten, kaupallisten tai muiden lähteiden pohjalta valtiollisten toimijoiden pahantahtoiseen toimintaan. Salasanojen arvaamisen kohteena ovat tyypillisesti organisaatioiden pilvipalvelut tai muutoin verkon yli saavutettavissa olevat palvelut.

Haavoittuvat verkkolaitteet ja -palvelut ovat kybervakoilussa kiinnostuksen kohteena luottamukselliseen tietoon ja viestintään tai muihin järjestelmiin pääsyn vuoksi. Tällaisia laitteita ja palveluita ovat esimerkiksi sähköpostipalvelimet, kuten Microsoft Exchange, ja toisaalta VPN-ratkaisut, kuten Pulse Connect Secure. Molempiin tuli vuonna 2021 julki haavoittuvuuksia, joiden hyödyntäminen on kuulunut myös valtiollisten kybertoimijoiden keinovalikoimaan.

Suomessa sijaitsevia haavoittuvia pien- ja kotireitittimiä puolestaan voidaan hyödyntää osana kybervakoojien hyökkäysinfrastruktuuria.

Verkkolaitteisiin, haavoittuviin palveluihin sekä näiden etsimiseen ja hyödyntämiseen liittyvien toimien arvioidaan jatkuvan myös ensi vuonna.

”Osa toiminnasta viittaa julkisten, kaupallisten tai muiden lähteiden pohjalta valtiollisten toimijoiden pahantahtoiseen toimintaan.

Useat ryhmät näkyneet myös Suomessa

Eri APT-ryhmät kohdistavat mielenkiintoaan sekä suomalaisiin yrityksiin että julkishallintoon.

Esimerkiksi keväällä otsikoissa ollut NOBELIUM-ryhmään julkisuudessa liitetty kampanja näkyi myös Suomessa. Lukuisissa Euroopan maissa näkyneessä kampanjassa ryhmä, joka tunnetaan myös nimillä APT29 ja Cozy Bear, lähetti kohdeorganisaatioihin kohdistettuja kalasteluviestejä tai haitallisen liitteen sisältäneitä viestejä. Sama ryhmittymä oli väitetysti myös vuoden 2020 lopulla paljastuneen SolarWinds Orion -hallintatyökaluun tehdyn haitallisen muutoksen taustalla. Sitä myös syytetään tietomurroista lukuisiin IT-palvelutaloihin eri puolilla maailmaa vuonna 2021.

Odotettavissa on, että toimitusketjuhyökkäykset aiheuttavat myös vuonna 2022 laajoja selvityksiä, kun organisaatiot joutuvat tutkimaan, onko jonkin murretun yrityksen, palvelun tai järjestelmän kautta yritetty päästä niiden omiin järjestelmiin.

Keväällä Suojelupoliisi myös attribuoi eduskuntaan vuoden 2020 lopulla kohdistuneen kybervakoilutapauksen APT31-operaatioon liittyväksi. Eduskunta kertoi vuosien 2020 ja 2021 vaihteessa siihen kohdistuneesta kyberhyökkäyksestä, joka vaikutti joihinkin sen sähköpostitileihin. Ulkoministeriön henkilöstöä puolestaan oli pyritty vakoilemaan mobiililaitteiden vakoiluun tarkoitetulla Pegasus-työkalulla. Sen käyttö kybervakoilussa nousi laajaan keskusteluun kesällä 2021.

Kyberturvallisuuskeskus neuvoo, tiedottaa ja selvittää

Kyberturvallisuuskeskus seuraa aktiivisesti kybervakoiluoperaatioihin liittyviä kehityskulkuja, havainnoi uhkia ja tiedottaa suomalaisia organisaatioita niistä sekä laajemmin että kohdennetusti. Kyberturvallisuuskeskus tarjoaa apua tahoille, jotka epäilevät heihin kohdistuneen kybervakoiluyrityksen tai muun vakavan tietomurron tai sen yrityksen. Tuki voi sisältää esimerkiksi neuvontaa, teknistä analyysiä tai tietomurron selvittämisen koordinointia.

Lisäksi Kyberturvallisuuskeskus tekee kansallista ja kansainvälistä yhteistyötä useilla eri suunnilla tavoitteenaan ajantasaisen tilannekuvan ylläpitäminen ja sen varmistaminen, että Suomessa pystytään varautumaan ennalta erilaisiin kehityskulkuihin ja uhkiin.

Haittaohjelmat ja haavoittuvuudet

Microsoftin Exchange-sähköpostipalvelimen kriittinen haavoittuvuus ja Log4j-komponentin haavoittuvuus sekä tekstiviestitse levinnyt FluBot-haittaohjelma hallitsivat haavoittuvuuksien ja haittaohjelmien vuotta.

Exchange-haavoittuvuus sai kyberrikolliset liikkeelle ja vaati varoituksen

Keväällä Suomessa ja maailmalla uutisoitiin Exchange-sähköpostipalvelimen kriittisen haavoittuvuuden aktiivisesta hyödyntämisestä. Haavoittuvuuden julkitulon jälkeen sen hyödyntäminen yleistyi nopeasti etenkin kyberrikollisen ja valtiollisten kybertoimijoiden keskuudessa. Kehotimme ja opastimme organisaatioita tietomurtotutkinnan aloittamisessa. Korostimme ohjeissamme erityisesti, että pelkkä ohjelmistopäivityksen asentaminen ei riittänyt pitämään hyökkääjää loitolla. Julkaisimme haavoittuvuudesta myös varoituksen 1/2021.

Havaitsimme Suomessa aluksi noin 300 haavoittuvaa Exchange-palvelinta, joista osaan oli jo murtauduttu. Tällainen haavoittuvuuskokonaisuus on tärkeää saada nopeasti suuren yleisön tietoon, jotta haavoittuvuuden hyväksikäyttö voidaan estää tai ainakin huomata nopeasti. Otimme yhteyttä yli 250 organisaatioon ja maaliskuun loppuun mennessä meille oli kerrottu 74:stä murrosta. Suomalaisten organisaatioiden haavoittuvat Exchange-palvelimet oli päivitetty huhtikuun alkuun mennessä.

Paljon ilmoituksia Android-haittaohjelmista – FluBot kärjessä

Saamiemme tietoturvailmoitusten perusteella vuoden 2021 teemana olivat erilaiset Android-haittaohjelmat. Saimme vuoden aikana yli 15 400 ilmoitusta, joista yli 5400 koski Android-haittaohjelmia. Erityisen paljon tietoturvailmoituksia tehtiin FakeCop/FakeSpy ja FluBot-haittaohjelmista.

Vuoden toisen sekä neljännen varoituksen julkaisimme FluBot-haittaohjelmasta. Tätä Android-haittaohjelmaa yritettiin levittää pitkin vuotta esimerkiksi kuljetuspalveluiden nimissä lähetettyjen tekstiviestien avulla. Kesäkuussa yleistyivät viestit, joissa kerrottiin vastaajaan saapuneesta viestistä. Marraskuussa viestien teemat olivat ääniviestit ja pakettitoimitukset. Tietojemme mukaan suomenkielisiä huijausviestejä lähetettiin tuhansille suomalaisille.

FluBot voi varastaa tietoja esimerkiksi älypuhelimesta ja lähettää siitä haittaohjelmaa levittäviä huijaustekstiviestejä ja myös muita tekstiviestejä ulkomaille. Haittaohjelman levitysyritys voi kohdistua mihin tahansa laitteeseen, ennaltaehkäisy on siis tärkeää. Etenkin yritysten on hyvä tietää, mitä tietoja työntekijöiden puhelimissa on ja tehdä riskiarvio siitä, minkälaiset vaikutukset haittaohjelman aiheuttamalla tietovuodolla voisi olla.

Log4shell-haavoittuvuus synkensi loppuvuotta

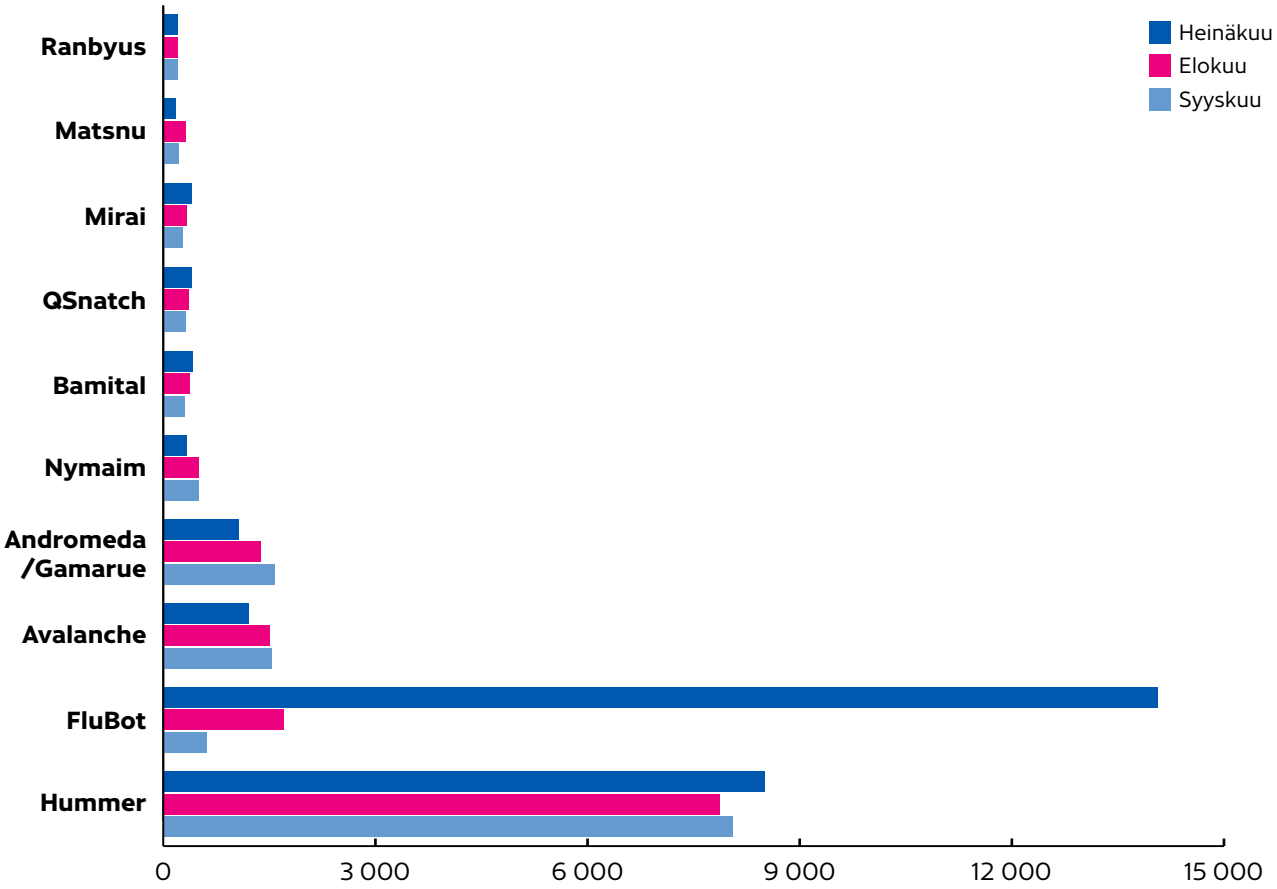
Joulukuun 2021 alussa löytynyttä Log4j-kirjaston haavoittuvuutta käytettiin aktiivisesti hyväksi ja siihen liitettyjä tietomurtoja on tapahtunut myös Suomessa. Julkaisimme haavoittuvuudesta vuoden 2021 viimeisen kriittiseksi luokitellun varoituksen 5/2021.

Haavoittuvuuden tekee poikkeukselliseksi se, että se koskee hyvin eri tyyppisiä ympäristöjä. Haavoittuvuudella voi olla vaikutuksia niin organisaatioiden omissa ICT-ympäristöissä kuin myös sen käyttämissä pilvipalveluissa. Haavoittuvuuden vaikutukset eivät myöskään rajoitu millekään tietylle toimialalle. Haavoittuvuus voi koskea sekä toimistojärjestelmiä, organisaatioiden taustajärjestelmiä, että teollisuuden automaatiojärjestelmiä. Haavoittuvuus on kriittinen, koska se toimii käytännössä haavoittuneen palvelun yleisavaimena.

"Log4j-haavoittuvuus altistaa valtavan määrän järjestelmiä hyökkäyksille. Se on tämän vuosikymmenen toistaiseksi vakavin haavoittuvuus. Log4j voi johtaa suurempiin vaikutuksiin kuin vuoden 2017 WannaCry-tapaus, joka aiheutti maailmanlaajuisesti jopa miljardiluokan vahingot", Kyberturvallisuuskeskuksen johtava asiantuntija Juhani Eronen toteaa.

Kyberturvallisuuskeskus tiedotti haavoittuvuudesta mediassa ja muistutimme myös yritysten johtoa siitä, että haavoittuvuutta tulisi lähestyä organisaation oman liiketoiminnan jatkuvuusriskinä. Kiristyshaittaohjelma saattaa esimerkiksi estää kokonaan organisaatiota toteuttamasta ydinliiketoimintaansa. Haavoittuvuuden todelliset vaikutukset selviävät vasta lähikuukausien aikana, ja haavoittuvuuden hyväksikäyttömenetelmät tulevat jäämään hyökkääjien työkalupakkiin vuosien ajaksi.

Haittaohjelmatyypit Q3/2021



Vuonna 2021 Kyberturvallisuuskeskuksen Autoreporter-järjestelmän keräämistä haittaohjelmahavainnoista erottuvat selvästi Hummer ja FluBot. Hummer-havaintoja on ollut joka kuukausi noin 8 500. Eniten havaintoja yksittäisestä haittaohjelmasta oli heinäkuussa 2021, jolloin FluBot-havaintoja oli 14 067.

Tietomurrot ja tietovuodot

Vuoden 2021 aikana maailmalla tapahtui useita tietomurtoja, joiden yhteydessä rikolliset käyttivät kiristyshaittaohjelmia organisaatioita vastaan. Tietovuodon tapahduttua tietoja on käytännössä mahdotonta saada pois internetistä.

Kevään Microsoft Exchange -tietomurroille oli tyypillistä, että uhrin sähköpostipalvelimelle asennettiin niin kutsuttu webshell-takaportti. Näissä tietomurtotapauksissa toimintamalli on tunnistettu jo vuodesta 2020 lähtien. Tutkinta vaatii paljon teknistä osaamista ja resursseja, siksi apua on hyvä hankkia esimerkiksi tietoturvapalveluja tarjoavilta yrityksiltä. Julkaisimme keväällä oppaan tietomurtojen tutkinnan avuksi.

Tietomurtojen yhteydessä käytetään yhä useammin kiristyshaittaohjelmia

Kuluneena vuonna Suomessa ja maailmalla raportoitiin useita tapauksia, joissa tietomurron jälkimainingeissa muun muassa uhrin omien järjestelmien ja tietojen käyttö oli estetty kiristyshaittaohjelmalla.

Eniten maailmaa kohautti tapaus Colonial Pipeline Yhdysvalloissa, mikä päättyi lunnaiden maksamiseen. Organisaation johdon mukaan päätös ei ollut helppo. Lunnaiden maksamista ei suositella, sillä rahavirrat ylläpitävät rikollisten liiketoimintaa eikä lunnaiden maksaminen tarkoita, että hyökkääjä luovuttaisi uhrilleen kiristyshaittaohjelman purkuavainta.

Vuoden 2020 syksyllä julkisuuteen tullut Psykoterapiakeskus Vastaamon tapauksen käsittely jatkui myös vuonna 2021. Saimme muutamia ilmoituksia sivustoista, joilla tietomurron uhrien henkilötietoja oli julkaistu uudelleen. Kun saimme sivut tietoomme, teimme niitä poistopyyntöjä. Silti ikävä tosiasia on, että kerran julkisuuteen päätynyttä materiaalia on lähes mahdoton saada lopullisesti verkosta pois.

Tietomurroilta suojautuminen vaatii paljon

Organisaatiossa voi tapahtua tietomurto tai -vuoto, vaikka omien tietojen suojaamiseksi olisi tehty kaikki mahdollinen. Palvelussa tai verkkosivustossa voi olla aiemmin tuntematon haavoittuvuus, konfiguraatiossa voi olla virhe tai työntekijän kirjautumistunnukset voivat päätyä rikollisten käsiin.

Tietomurroilta suojautuminen on vaativa laji. On kuitenkin mahdollista tehdä tunkeutumisesta hyökkääjälle hankalaa ja puolustautujalle helpommin havaittavaa. Haluamme kannustaa kaikkia toimijoita suojautumisen kehittämiseen ja resursointiin myös tulevaisuudessa. Asiaan osoitetut resurssit voivat monissa tapauksissa olla melko vähäisiä siihen nähden, millaisia vahinkoja kyberhyökkäyksestä voi aiheutua.

”Tietomurroilta suojautuminen on vaativa laji.

Tietojenkalastelu ja huijaukset

Tekstiviestihuijauksia tehtailtiin ennätystahtiin ja ennennäkemättömän kekseliäästi. Myös huijareiden saama rikoshyöty rikkoi aiemmat ennätykset.

Suomalaisilta huijattiin kymmeniä miljoonia

Tänäkin vuonna huijarit ovat saaneet rikoshyötyä yli 30 miljoonan euron edestä. Summa on noussut yli 60 prosenttia edellisestä vuodesta. Erityyppisiä tietoverkossa tehtyjä huijauksia raportoidaan poliisille vuosittain tuhansia ja niistä koituvat rahalliset tappiot kasvavat kymmeniin miljooniin. Pelkästään pankkitunnusten kalastelusta aiheutui vuonna 2021 yli kahdeksan miljoonan euron menetykset, kun rikolliset saivat tietojenkalastelulla haltuunsa kuluttajien pankkitunnuksia ja niiden avulla tyhjensivät pankkitilejä. Poliisille pankkikalastelusta tehtiin rikosilmoituksia yli 800 ja Kyberturvallisuuskeskukselle tietoturvailmoituksia yli 1 800.

Pankkitunnusten kalastelu on muuttunut yhä huolellisemmaksi ja ammattimaisemmaksi rikollisuudeksi. Tunnuksia kalastellaan tyypillisimmin lähettämällä pankin nimiin väärennettyjä huijausviestejä. Rikolliset ovat nyt huomanneet, että pankkitunnuksia käytetään muuhunkin kuin pankkiasiointiin ja sitä voi hyödyntää huijauksiin: myös viranomaispalveluihin kirjaudutaan tunnistautumalla pankkitunnuksilla. Vuonna 2021 pankkitunnuksia huijattiin viesteillä, jotka oli väärennetty näyttämään viranomaisen palveluilta kuten OmaKanta tai suomi.fi.

Kyberturvallisuuskeskus julkaisi lokakuussa varoituksen, jossa varoitettiin pankkitunnusten kalastelusta viranomaispalveluiden nimissä. Varoitus noteerattiin hyvin mediassa ja siitä kirjoitettiin useita uutisjuttuja. Varoituksesta tiedotettiin vielä älypuhelimien 112 Suomi -sovelluksessa, jonka kattavuus on liki kaksi miljoonaa suomalaista. Uusi varoituskanava otettiin hienosti vastaan ja toivomme voineemme estää sillä tuhansien asiakkaiden pankkitietojen joutumisen rikollisten käsiin.

Myös räjähdysmäisesti alkuvuonna Android-puhelimiin levinnyt FluBot-haittaohjelma varastaa pankkitietoja. Lisäksi se saa aikaan uhrin puhelinliittymälle mittavan laskun lähettelemällä tuhansia tekstiviestejä ympäri maailmaa. FluBot-haittaohjelmasta kesäkuussa julkaistu keltainen varoitus poistettiin ilmiön laannuttua. Epidemia kuitenkin uusiutui pian varoituksen poistamisen jälkeen, jolloin varoitus aktivoitiin uudelleen heinäkuussa. Sama ilmiö palasi vielä uudistuneena, ja marraskuussa FluBotista julkaistiin uusi varoitus. Haittaohjelma lähettää huijausviestejä, jotka johtavat haitakkeen lataussivulle tiheästi muuttuvin verukkein. Traficomin varoitukset ovat saaneet runsaasti näkyvyyttä mediassa.

Tekstiviesti sai muutenkin paljon jalansijaa keskeisenä huijausten välineenä. Puhelimiin lähetetyn tekstiviestin lähettäjä on miltei yhtä helppo väärentää kuin sähköpostin lähettäjätieto. Tekstiviestejä on tähän saakka käytetty huijauksiin vähemmän kuin sähköpostia, joten sen uskottavuutta pidetään vielä parempana. Siksi se on rikollisille houkutteleva huijausväline. Puhelimen ruudulta tekstarilla saatu linkki vie silti yhtä usein tietojenkalastelusivulle kuin sähköpostillakin. Klikkailusta pidättäytymisen opettelussa on vielä paljon tekemistä.

> **”Pankkitunnusten kalastelu on muuttunut yhä huolellisemmaksi ja ammattimaisemmaksi rikollisuudeksi**

Esineiden internet ja automaatiojärjestelmät

Kaikki julkisessa verkossa avoimesti näkyvät laitteet ovat kyberturvallisuusriski. Teollisuuden ja kotitalouksien IoT-laitteiden käyttö on helppoa, mutta kokemuksemme perusteella valitettavan usein turvatonta. Kyberturvallisuuskeskus kannustaa laitevalmistajia kehittämään tietoturvallisempia laitteita ja pyrkii edistämään niiden näkyvyyttä. Kuluttajien laitteissa Tietoturvamerkki kertoo, että laitevalmistaja on asiamukaisesti huolehtinut laitteensa tietoturvasta. Organisaatiolle Kyberturvallisuuskeskus suosittelee Kybermittaria.

Riskit kasvavat, kun toimisto- ja automaatiojärjestelmät yhdentyvät

Perinteiset toimistojärjestelmät (IT) ja automaatiojärjestelmät (OT) kietoutuvat toisiinsa yhä tiiviimmin. Tästä hyvä esimerkki on Colonial Pipeline, joka joutui toukokuussa kiristyshaittaohjelman uhriksi. Koko Yhdysvaltain länsirannikon polttoaineen jakelu häiriintyi useiden päivien ajaksi. Tapaus on merkittävä, koska hyökkäys ei kohdistunut polttoaineen jakeluautomaatioon vaan sitä tukeviin liiketoimintajärjestelmiin. Kriittistä tuotantoa ei voitukaan pitää käynnissä, koska siihen liittyvä rahaliikenne estyi.

Esimerkiksi tuotantoon liittyviin materiaalivirtoihin ja kunnossapidon järjestelmiin liittyy samankaltaisia riippuvuuksia. Kehotamme suomalaisia yrityksiä tarkastelemaan niiden tuotannon turvaamiseen liittyviä riskejä myös tästä keskinäisriippuvuuksien näkökulmasta.

Suojaamattomia laitteita on verkossa edelleen

Kyberturvallisuuskeskuksen vuosittaisessa suojaamattomien automaatiolaitteiden kartoituksessa käytiin läpi noin 12,2 miljoona IP-osoitetta suomalaisessa verkkoavaruudessa. Valitettavasti löysimme jälleen verkosta runsaasti huonosti suojattuja yritysten automaatiolaitteita ja haavoittuvia kuluttajien IoT-laitteita.

Yritysten käyttämiä automaatiolaitteita ei ole perinteisesti suunniteltu suoraan julkiseen verkkoon kytkettäviksi, siksi niiden tietoturvakontrollitkaan eivät ole siihen riittäviä. Jos näitä laitteita on tarve tavoittaa julkisesta verkosta, on otettava käyttöön riittävän turvallinen etäyhteysratkaisu.

Yksittäinen julkiseen verkkoon näkyvä tuotantoautomaation laite altistaa koko tuotantoverkon suureen varaan, koska se antaa hyökkääjälle mahdollisuuden ja väylän edetä tuotantoverkon muihin osiin.

Useat kuluttajalaitteiden valmistajat suhtautuvat tietoturvallisuuteen leväperäisesti. Laitteiden alkuperäinen toteutustapa saattaa olla täysin tietoturvaton, tai valmistaja ei korjaa olleenkaan löydettyjä haavoittuvuuksia. Esimerkiksi rikollisten hallinnoiman bottiverkon osana kodin laitteet ovat jatkuva uhka kaikille internetin palveluille ja käyttäjille. Kuluttajalaitteiden bottiarmeija voi saada aikaan järisyttäviä palvelunestohyökkäyksiä.

Saastunut kodin IoT-laite avaa myös kotimme verkkorikollisille. Kuluttaja voi omilla valinnoillaan pienentää tätä riskiä merkittävästi. Halvin on harvoin tietoturvaominaisuuksiltaan paras valinta. Jos laitteeseen ei saa päivityksiä, sen oikea paikka on sähkö- ja elektroniikkaromukierrätys.

Tietoturvamerkin vuosi

Traficomin Tietoturvamerkki auttaa kuluttajaa tunnistamaan turvallisen tuotteen. Merkin vaikutusalue kasvoi lokakuussa 2021, kun Traficom aloitti vastavuoroisen tunnustamisen Singaporen kyberturvallisuusviranomaisen Cybersecurity Labelin kanssa. Nyt Tietoturvamerkin saaneet tuotteet ovat siis myös Singaporen hyväksymiä.

Lisäksi kehitimme yhteistyötä antamalla kaupallisille toimijoille mahdollisuus suorittaa Tietoturvamerkin myöntämiseen liittyvä tekninen tarkastus. Ensimmäisenä mahdollisuutta hyödynsi norjalainen NEMKO, jonka tarkastamalle Datekin Smart Hubille myönnettiin Tietoturvamerkki kesäkuussa. Toivomme yhteistyön kaupallisten toimijoiden jatkuvan hedelmällisenä myös jatkossa.

Kybersää 2021 ja katse vuoteen 2022

Kyberturvallisuuden suunta on kohti ennalta-ehkäisyä. Sääntelyllä haetaan haetaan toimintavarmuutta ja turvallisuutta, mutta arjen tietoturvaan voivat vaikuttaa kaikki. Kentällä tehdään arvokasta vapaaehtoista työtä kyberturvallisuustietoisuuden parantamiseksi. Olemme kampanjoineet muun muassa ikäihmisille tietoturvan puolesta.

10 tietoturvanäkymää vuodelle 2022

1.

Sääntely ulottuu uusiin teknologioihin ja uusille toimialoille
Euroopan unionissa on parhaillaan käynnissä useita lainsäädäntöhankkeita, joiden tarkoituksena on muun muassa selkeyttää digitaalisten palveluiden pelisääntöjä, luoda tekoälystä, älylaitteista ja datan hallinnasta turvallisempaa ja tarkentaa eri toimijoiden tietoturvavelvollisuuksia. Lisäksi uudella sääntelyllä luodaan ja suunnitellaan aktiivisesti uusia digitaalisen turvallisuuden toimijoita EU:n pelikentälle.

2.

Teknologiasta suurvaltakilpailun näyttämö
Maiden välinen suurvaltakamppailu on entistä vahvemmin myös kilpailua maailman teknologiaherruudesta. Tämä näkyy esimerkiksi teknologian standardoinnissa, jossa erityisesti Kiina on vahvistaa rooliaan China Standards 2035 -suunnitelman mukaisesti. Siten myös suomalaiset teknologiset innovaatiot kiinnostavat kybervakoilun kohteina.

3.

Kaikki eivät pysy digitalisaatiossa mukana
Koronapandemia vauhditti palveluiden digitalisaatiota, ja yhä useampi palvelu on saatavilla verkosta ympäri vuorokauden. Digitalisaatio helpottaa asiointia ja nopeuttaa arkea – mutta ei kaikille. Digitaitojen, verkkoyhteyden tai kielitaidon puute saattaa heikentää osallisuuden tunnetta digitaalisessa ympäristössä. Palveluita kehitettäessä tulee entistä enemmän kiinnittää huomiota saavutettavuuteen ja osallisuuteen.

4.

Pula puolijohteista jatkuu
Pula puolijohteista ei näytä helpottamisen merkkejä. Organisaatiot saattavat joutua odottamaan uusia laitteita kuukausikaupalla ja siten joutua käyttämään elinkaaren päässä olevia laitteita pidempään ja uusien suojausratkaisujen rakentamisessa kestää suunniteltua pidempään. Laitekaupoilla kannattaakin olla tarkkana, sillä saatavuushäiriöt ja hintojen nousu houkuttelevat markkinoille myös halpoja kopioita. Vaikka Eurooppa ja Yhdysvallat pyrkivät vähentämään riippuvuuttaan Aasian puolijohdetehtaista, pulan odotetaan jatkuvan vielä pitkälle vuoteen 2022.

5.

Älylaitteetkin kuuluvat kierrätykseen
Uusilla teknologioilla voidaan auttaa löytämään ratkaisuja ilmastonmuutoksen torjuntaan, mutta kääntöpuolena lisääntyvä älylaitteiden määrä synnyttää kasvavaa ympäristökuormaa. Huolehdi siis käyttöikänsä päässä olevat elektroniikka- ja älylaitteet kierrätykseen, korjaa laitteita, mikäli mahdollista ja kysy myyjältä älylaitteiden päivityksistä. Traficomin Tietoturvamerkki auttaa älylaiteostoksilla.

6.

Tarve kyberturvallisuuden osaajille monipuolistuu

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

7.

Kybervakoilun ja -rikollisuuden rajat hämärtyvät entisestään

Kyberrikollisten ja -vakoojien käyttämät menetelmät ja työkalut muistuttavat entistä enemmän toisiaan, ja kyberrikollisuuden ammattimaistuminen johtaa entistä kehittyneempiin taloudellisesti motivoituneisiin kyberhyökkäyksiin. Toisaalta autoritääriset valtiot hyödyntävät erilaisia toimijoita välikappaleina päästäkseen tarkoitusperiinsä, mikä hämärtää tekijän ja hyökkäysten motiivien tunnistamista.

8.

Autotkaan eivät ole suojassa kyberhyökkäyksiltä

Uudet autot ovat edeltäjiään yhä älykkäämpiä ja yhdessä autossa saattaa olla useita kymmeniä erilaisia ohjelmistoja. Autojen ohjelmistojen ajantasaisuudesta tulee huolehtia kuten muidenkin ohjelmistojen. Tullaanko siis vuonna 2022 näkemään ensimmäinen autoihin kohdistettu haittaohjelmahyökkäys?

9.

Tekoäly avustaa tietomurroissa

Tekoälyä otetaan yrityksissä käyttöön kiihtyvällä tahdilla eivätkä rikollisetkaan tipu kehityksen kelkasta. Tekoälyn ja koneoppimisen avulla voidaan tehdä entistä uskottavampia deep fake -videoita tai hyödyntää bottia kohdennettuun kalasteluun. Vuonna 2022 tekoäly voikin toimia esimerkiksi toimitusjohtaja-huijauksen takana auttamassa organisaation sisälle pääsemisessä.

10.

Kiristyshaittaohjelmien käyttö murroksessa

Vaikka moni organisaatio on ymmärtänyt varmuus-kopioiden tärkeyden ja myös viranomaiset jahtaavat haittaohjelmien taustalla olevia rikollisia, eivät kiristyshaittaohjelmat ole suinkaan menneen talven lumia. Tulevaisuudessa haittaa aiheutetaan tietojen salaamisen sijaan yhä useammin tietovuodolla tai operatiivisen toiminnan häiritsemisellä erityisesti OT-verkoissa. Myös globaalisti yleistyvät kybervakuutukset saattavat avata kyberikollisille uudet rahahanat ja kannustimet, kun lunnaat maksetaan vakuutusyhtiön pussista. Kyberturvallisuuskeskuksen ohje pysyy samana: älä maksa rikollisille.

Vuoden 2021 kybersää

Varoitus | Haavoittuvuus

Tammi
Vastaamon **potilastietoja jaetaan** jälleen verkossa

Helmi
OmaPosti-teemaiset **huijaustekstiviestit** piinaavat suomalaisia päivittäin

Maalis
Exchange-sähköpostipalvelimen **kriittinen haavoittuvuus** on aktiivisen hyväksikäytön kohteena

Huhti
Pulse Connect Secure -etäkäyttöhaavoittuvuutta hyödynnetään kansainvälisesti vakoilutapauksissa

Touko
Tietoturvamerkki herättää kiinnostusta kansainvälisessä älylaitteiden tietoturvawebinaarissa

Kesä
Kyberturvallisuuden **kehittämisohjelmassa** määritetään toimenpiteet kyberturvallisuuden parantamiseksi yhteiskunnassa

Heinä
Windowsin taustatulostuspalvelun haavoittuvuus aiheutti pitkäaikaista vaivaa organisaatioille

Elo
Instagramissa leviää **tietojenkalastelukampanja**, joka onnistui kaappaamaan monen käyttäjätilin omakseen

Syys
Azure-pilvipalvelun OMI-komponentista löytyi OMIn luvin komentojen suorittamisen mahdollistava haavoittuvuus

Loka
Tiedotamme ensimmäistä kertaa tietoturvahäiriöistä **112 Suomi** -sovelluksessa.

Marras
Julkaisemme Suomen ensimmäisen **tekoälyselvityksen**

Joulu
Kriittinen **Log4j-komponentin haavoittuvuus** vaatii välittömän huomion toiminnan turvaamiseksi

Tarvitsetko sinä tai organisaatiosi apua tietoturvaloukkausten torjunnassa tai onko sinulla kysyttävää kyberturvallisuuteen liittyvästä säädännöstä? Arvioimme ja hyväksymme myös tietojärjestelmiä.

Kehitämme ja valvomme viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Tavoitat meidät näin:

sähköpostitse: kyberturvallisuuskeskus@traficom.fi
asiakaspalvelu: 0295 345 630

Seuraa meitä ja uutisiamme
kyberturvallisuuskeskus.fi
@CERTFI
facebook.com/NCSC.FI

Ilmoita meille tietoturvaloukkauksesta
kyberturvallisuuskeskus.fi/fi/ilmoita

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus

PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978-952-311-777-8
ISSN 2669-8757

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus