TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Tietoturvan vuosi 2020

## Kyberturvallisuuskeskuksen vuosikatsaus

Traficomin julkaisuja
**13/2021**

# Sisältö

# Kyberturvallisuus nousi pysyvästi johdon agendalle

Matkaviestinverkkojen, etenkin 5G-verkkojen turvallisuus oli yksi vuoden puhututtaneimmista aiheista maailmalla. EU:ssa laadittiin pikavauhtia ohjeistus toimista 5G-verkkojen kyberturvallisuusriskien minimoimiseksi. Suomessa valmisteltiin uutta lainsäädäntöä viestintäverkkojen kriittisten osien suojaamiseksi. Uudessa lainsäädännössä kansallinen näkökulma on aiempaa korostetummassa asemassa, se myös antaa uusia työkaluja puuttua mahdollisiin kansallista turvallisuutta ja maanpuolustusta uhkaaviin kyberturvallisuusriskeihin.

Kuluneena vuonna kohtasimme Suomessa tähän asti merkittävimmän tietomurron, kun Psykoterapiakeskus Vastaamon potilastietoja päätyi rikollisten käsiin. Varastamillaan tiedoilla hyökkääjä kiristi niin Vastaamoa kuin kymmeniätuhansia sen palveluita käyttäneitä kansalaisia. Autoimme uhreja muun muassa tietovuotoapu.fi-sivustolle kootuilla ohjeilla yhdessä viranomaisten, järjestöjen ja yritysten kanssa. Vastaamon tapaus herätti yhteiskunnallista keskustelua yritysjohdon vastuusta kriittisten tietovarantojen ja -järjestelmien suojaamiseksi. Se muistutti myös siitä, että verkkopalveluissa henkilötunnus ei sovi tunnistusmenetelmäksi.

Vuotta väritti myös Emotet-haittaohjelma, josta julkaisimme varoituksen elokuussa. Haittaohjelman tarkoituksena on varastaa organisaation tietoja. Hyökkäyksellä on mahdollista tunkeutua syvälle kohteen verkkoon ja käynnistää esimerkiksi kiristyshaittaohjelmahyökkäys. Emotet on hyvä esimerkki ammattimaisesti toteutetusta tietomurrosta, jonka avulla pyritään saavuttamaan jalansija ja takaovi kohteena olevaan organisaatioon.

Alkuvuonna globaali pandemia siirsi meidät ennennäkemättömin joukoin etätöihin. Näin myös etätyöratkaisuista löydettyjen haavoittuvuuksien hyödyntäminen esimerkiksi tietomurroissa lisääntyi selvästi. Lisäksi kansainväliset kybertrendit tarttuivat Suomen televerkkoihin helmikuussa, kun huijauspuheluiden aalto pyyhkäisi maamme läpi. Pelkästään helmikuun aikana suomalaiset teleoperaattorit kertoivat miljoonista huijauspuheluista.

Raskaaseen vuoteen kuului myös hyvää. Jouko Katainen (Ilmarinen), Jussi Törhönen (Enfo), Tomi Vehkasalo (Aditro) ja Jani Räty (Aditro) saivat Tietoturvan suunnannäyttäjä -tunnustuksen aktiivisesta yhteistyöstä Kyberturvallisuuskeskuksen kanssa. Lisäksi olimme mukana rakentamassa Koronavilkku-sovellusta. Sen tietoturva- ja tietosuojaratkaisut vaikuttavat osuneen oikeaan. Nyt miljoonat suomalaiset käyttävät sovellusta ja tukevat maamme koronatilanteen hallintaa.

Poikkeusvuosi osoitti, että työt ja asiointi on mahdollista siirtää verkkoon turvallisesti. Näimme myös, että yhteistyössä viranomaisten ja kansalaisjärjestön kanssa voimme auttaa kyberrikollisuuden aiheuttamissa inhimillisissä kriiseissä. Tapahtumien vakavuus ja vaikutukset nostivat kyberturvallisuuden pysyvästi johdon agendalle.

Vuonna 2021 juhlistamme CERT-toimintamme 20-vuotispäivää. Näihin vuosikymmeniin on sisältynyt paljon yllätyksiä.

Seuraathan verkkosivujamme ja somekanaviamme! Jos kyberennustukset vuodelle 2021 kiinnostavat, löydät ne katsauksemme lopusta.

Helsingissä 11.2.2021,

**Sauli Pahlman**
Vt. ylijohtaja,
Kyberturvallisuuskeskus

# Kybersääilmiöt

# Verkkojen toimivuus

## Viestintäverkkojen häiriöt

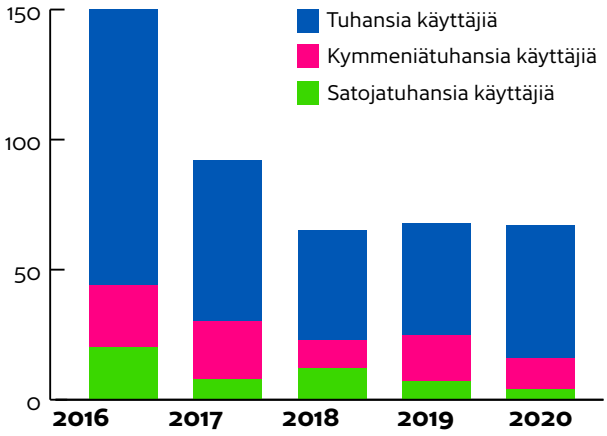
On tärkeää, että kotimaiset viestintäverkot toimivat mahdollisimman luotettavasti ja häiriöttömästi. Muutoin esimerkiksi yhteiskuntamme digitaaliset palvelut eivät voi toimia. Keräämiemme häiriötietojen perusteella voimme analysoida häiriöiden juurisyitä ja parantaa verkkojen toimintavarmuutta muun muassa sääntelyä kehittämällä.

Merkittävien häiriöiden määrä laski selvästi vuoteen 2018 asti ja on pysynyt siitä lähtien 65:n ja 68:n välillä. Vuonna 2020 merkittäviä häiriöitä oli 67. Kriittiset häiriöt, jotka koskevat vähintään 100 000 käyttäjää, kuitenkin vähenivät. Kokonaisuutena kehityssuuntaa voidaan pitää positiivisena, vaikka merkittävien häiriöiden määrän lasku on pysähtynyt.

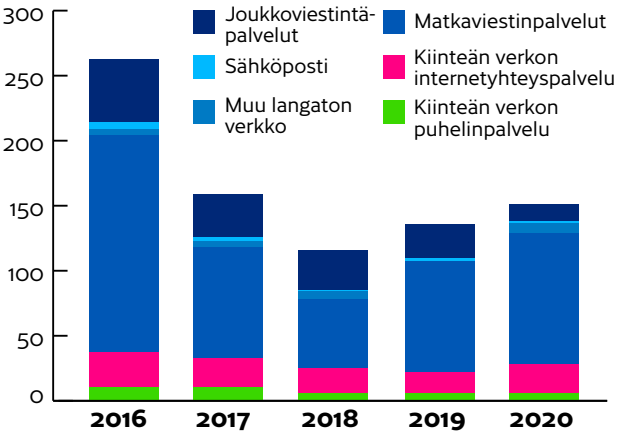
Valtaosa kotimaisten viestintäverkkojen merkittävistä häiriöistä koskee matkaviestinverkkojen palveluita eli puhelujen, internetyhteyksien ja tekstiviestien toimivuutta. Ne johtuvat esimerkiksi myrskyjen aiheuttamista sähkökatkoista, jotka vaikuttavat myös matkaviestinverkon tukiasemien sähkönsaantiin. Matkaviestinverkko on myös teknisesti monimutkaisempi kuin esimerkiksi kiinteä laajakaistaverkko, siksi muun muassa ohjelmistovioista aiheutuvat häiriöt ovat matkaviestinverkoissa yleisempiä.

Häiriöitä aiheuttavien voimalaitejärjestelmä- ja ohjelmistovikojen määrä lisääntyi vuodesta 2019. Järjestelmien huolellinen testaaminen voi vähentää häiriöitä. Silti myös laite- ja ohjelmistokomponenttien laatua kannattaa valvoa, koska epäluotettavasti toimivat komponentit voivat jäädä testauksessa piiloon.

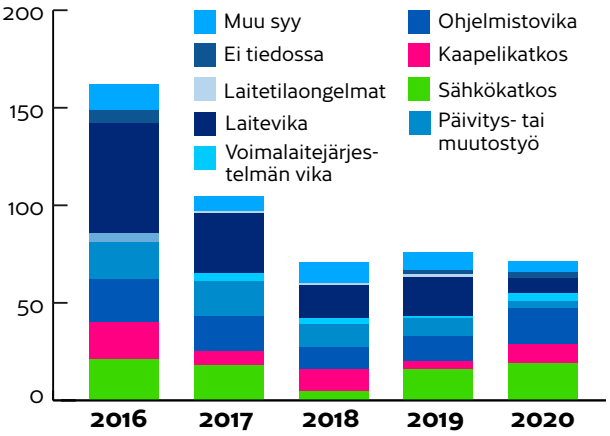
Päivitys- ja muutostyöt puolestaan aiheuttivat aiempaa vähemmän häiriöitä. Tämä on hyvä uutinen ja kertoo siitä, että teleyritykset ovat tehneet pitkäjänteisesti töitä palveluidensa ylläpidon kehittämiseksi.




Yleisten viestintäpalveluiden merkittävien toimivuushäiriöiden lukumäärät vuosina 2016–2020




Merkittävien toimivuushäiriöiden vaikutukset yleisiin viestintäpalveluihin vuosina 2016–2020. Yksi häiriötilanne voi vaikuttaa useaan palveluun.

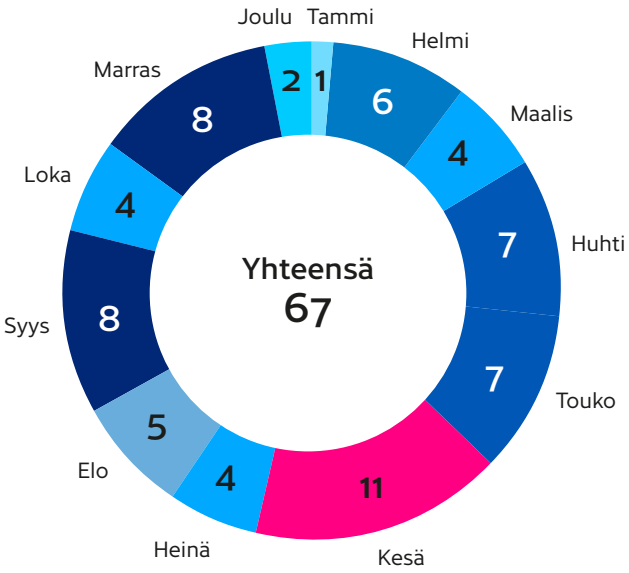



Merkittävien toimivuushäiriöiden juurisyyt vuosina 2016–2020. Yhdellä häiriötilanteella voi olla monta juurisyytä.

## Netti pätki pitkin Suomea ja myrskyt katkoivat sähköjä

Telian matkaviestinverkon internetyhteyspalvelun valtakunnallinen häiriö 25.4. herätti myös median huomion.

Myös myrskyt aiheuttivat merkittäviä toimivuushäiriöitä. Viestintäpalvelujamme katkoivat erityisesti Päivö 30.6. ja Aila 16.–17.9. Niiden aiheuttamien toimivuushäiriöiden hallinta sujui teleyrityksiltä, sähköverkkourakoitsijoilta ja pelastuslaitoksilta rutiinilla. Häiriöiden vaikutukset jäivät suhteellisen pieniksi muutaman vuoden takaisiin myrskyihin verrattuna.




Merkittävien toimivuushäiriöiden jakautuminen kalenterikuukausille.

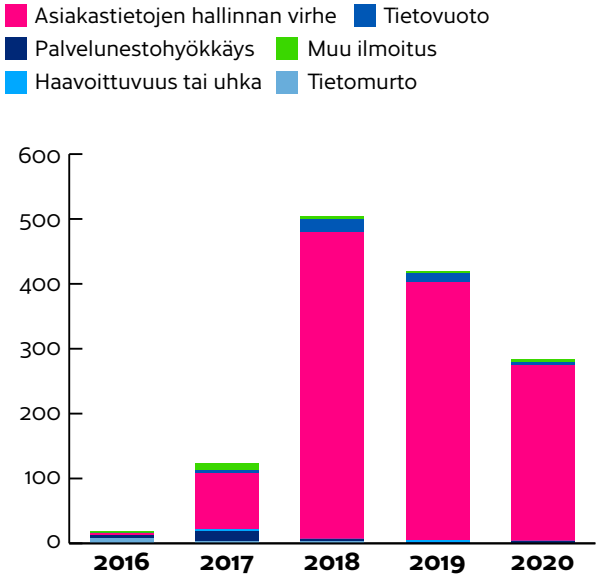
## Etätyökalut aiheuttivat huolta

Yleiset viestintäpalvelut kestivät Suomessa ja muualla Euroopassa hyvin, vaikka ihmiset siirtyivät joukoittain etätöihin koronapandemian levitessä.

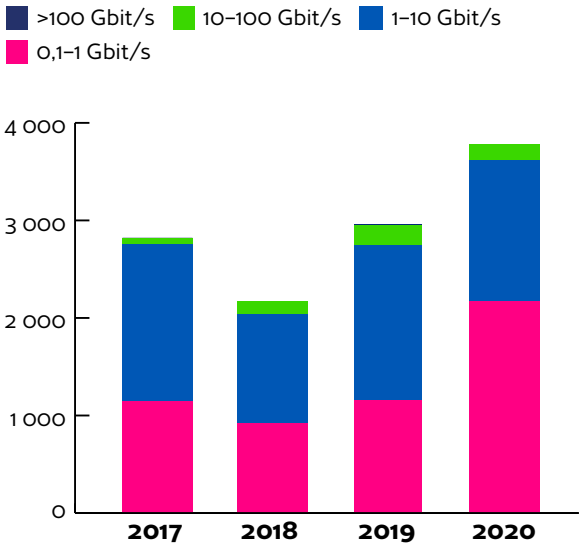
Pandemian alkuvaiheissa esimerkiksi organisaatioiden omissa VPN-palveluissa ja kansainvälisissä pilvipalveluissa oli kapasiteettiongelmia. Ne pääosin ratkaistiin muutamissa viikoissa. Maaliskuussa pilvipalveluiden käyttö moninkertaistui maailmanlaajuisesti. Useassa organisaatiossa etätyöskentelyvälineitä ja -palveluita otettiin käyttöön hallitsemattomasti, mistä saattoi koitua hallitsemattomia tietoturvariskejä.

Annoimme neuvoja muun muassa *split tunnel* -tekniikan käytöstä. Tekniikalla voidaan esimerkiksi ohjata ohjelmistojen päivitysliikenne VPN:n ohi ja näin vähentää organisaation VPN-palvelun kuormaa.

Verkkopalveluiden varmenteiden käsittelyn virheet ja unohdukset aiheuttivat laajoja häiriöitä lukuisten palveluiden käytettävyydelle. Microsoft

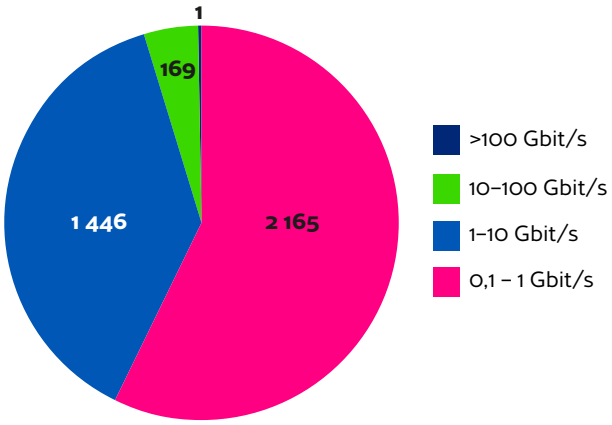



Teleyritysten ilmoitukset merkittävistä tietoturvaloukkauksista ja henkilötietojen tietoturvaloukkauksista vuosina 2016–2020.




Palvelunestohyökkäysten volyymien kehitys Suomessa. Lähde: Telia

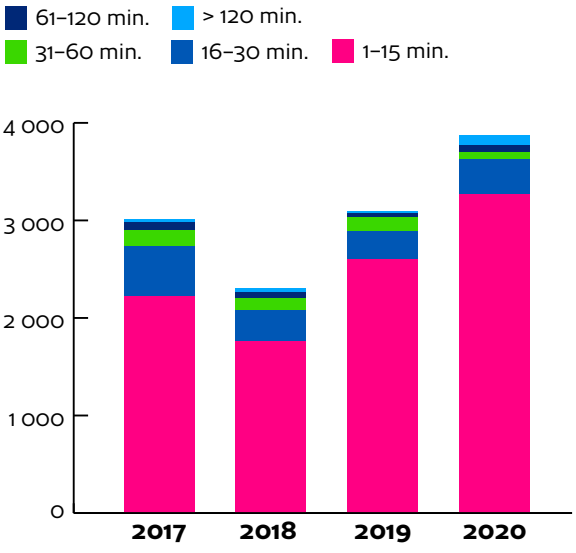
Teamsin varmenteita vanheni helmikuussa. Onneksi tilanne saatiin haltuun ennen pandemia-aikaa, sillä häiriö iski voimalla länsimaihin, joissa Teams-palvelun käyttö on yleistä. Let's Encrypt joutui mitätöimään myöntämiään varmenteita nopealla aikataululla maaliskuun alussa ja DigiCert heinäkuussa, koska niiden varmennepyyntöjen käsittelyprosesseissa oli tehty virheitä. On tärkeää, että organisaatioilla on selkeät ja nopeat prosessit verkkopalveluidensa varmenteiden uusimiselle.




Palvelunestohyökkäysten volyymien jakauma Suomessa 2020. Lähde: Telia

## Teleyritysten tietoturvaloukkausilmoitusten määrä vähenee yhä

Teleyritysten ilmoitusten määrät henkilötietoja koskeneista tietoturvaloukkauksista ovat pienentyneet tasaisesti vuoden 2018 huipusta lähtien. Tyypillinen henkilötietoja koskeva tietoturvaloukkaus on, että teleyritys on merkinnyt asiakkaalleen väärän osoitteen ja lähettää sinne kirjeen tai sähköpostia, joka sisältää asiakkaan henkilötietoja. Merkittäviä tietoturvaloukkauksia on tyypillisesti alle kymmenen kappaletta vuodessa. Vuonna 2020 niitä ilmoitettiin viisi.




Palvelunestohyökkäysten kestojen kehitys Suomessa. Lähde: Telia

# Palvelunestohyökkäykset

Kotimaisissa organisaatioissa palvelunestohyökkäyksiin on varauduttu vuosi vuodelta paremmin. Operaattoreiden tarjoamat suodatuspalvelut ja organisaatioiden osaaminen ovat yleistyneet ja kehittyneet niin, että yleisimmät palvelunestohyökkäykset eivät juuri pääse vaikuttamaan yritysten toimintaan. Myös palveluiden siirtyminen pilvipalveluihin on parantanut palvelunestohyökkäyksiin varautumista.

## Poikkeusoloissa verkkopalveluiden saatavuus korostuu

Kansainvälisistä uutisista saimme lukea kokoluokaltaan suurista palvelunestohyökkäyksistä, jotka ovat vaikuttaneet esimerkiksi internetin infrastruktuurin palveluihin. Hyökkäyksiin on varauduttu vuosi vuodelta paremmin, mutta pitkäkestoinen ja kooltaan suuri hyökkäys voi silti vaikuttaa laajasti yrityksen toimintaan.

Keväällä etätyön määrä kasvoi ennennäkemättömällä tavalla myös Suomessa. Palvelunestohyökkäykset ovat joissain tapauksissa vaikuttaneet sivullisesti esimerkiksi organisaation sisäisiin palveluihin kuten Skypeen ja VPN-ratkaisuihin. Etätyön kannalta kriittiset palvelut on hyvä suunnitella ja toteuttaa niin, että palvelunestohyökkäykset vaikuttaisivat niihin mahdollisimman vähän.

Myös vuonna 2020 havaittiin hyökkäyksiä koulujen järjestelmiä kohtaan. Hyökkäysten takana on voinut olla nuoria, jotka eivät ymmärrä palvelunestohyökkäyksen vakavuutta. Palvelunestohyökkäyksen tekeminen tai sen yrittäminen voidaan tulkita rikokseksi, josta voi seurata tekijälle sakkoa tai enintään kaksi vuotta vankeutta.

Tavallisesti saamme ilmoituksia palvelunestohyökkäyksistä, jotka ovat kooltaan alle 10 Gbit/s. Edellisvuonna suurin meille ilmoitettu hyökkäys oli 161 Gbit/s.

Syksyllä eurooppalaiset operaattorit olivat palvelunestohyökkäysten kohteina. Hyökkääjien maalina olivat erilaiset internetin infrastruktuurin palvelut ja erityisesti DNS-palvelimet. Hyökkäyksien raportoitiin yltäneen jopa 300 Gbit/s-kokoluokkaan ja kestäneen useita tunteja.

Edellisvuonna Euroopassa nähtiin myös digitaalisiin palveluihin kohdistuneita palvelunestohyökkäyksiä. Palveluntarjoajien mukaan heidän havaitsemansa palvelunestohyökkäykset olivat suurempia kuin koskaan aiemmin.

## Palvelunestohyökkäyksillä kiristettiin yrityksiä myös Suomessa

Palvelunestohyökkäyksiä käytetään myös tehostamaan kiristyshaittaohjelmahyökkäysten lunnasvaatimuksia.

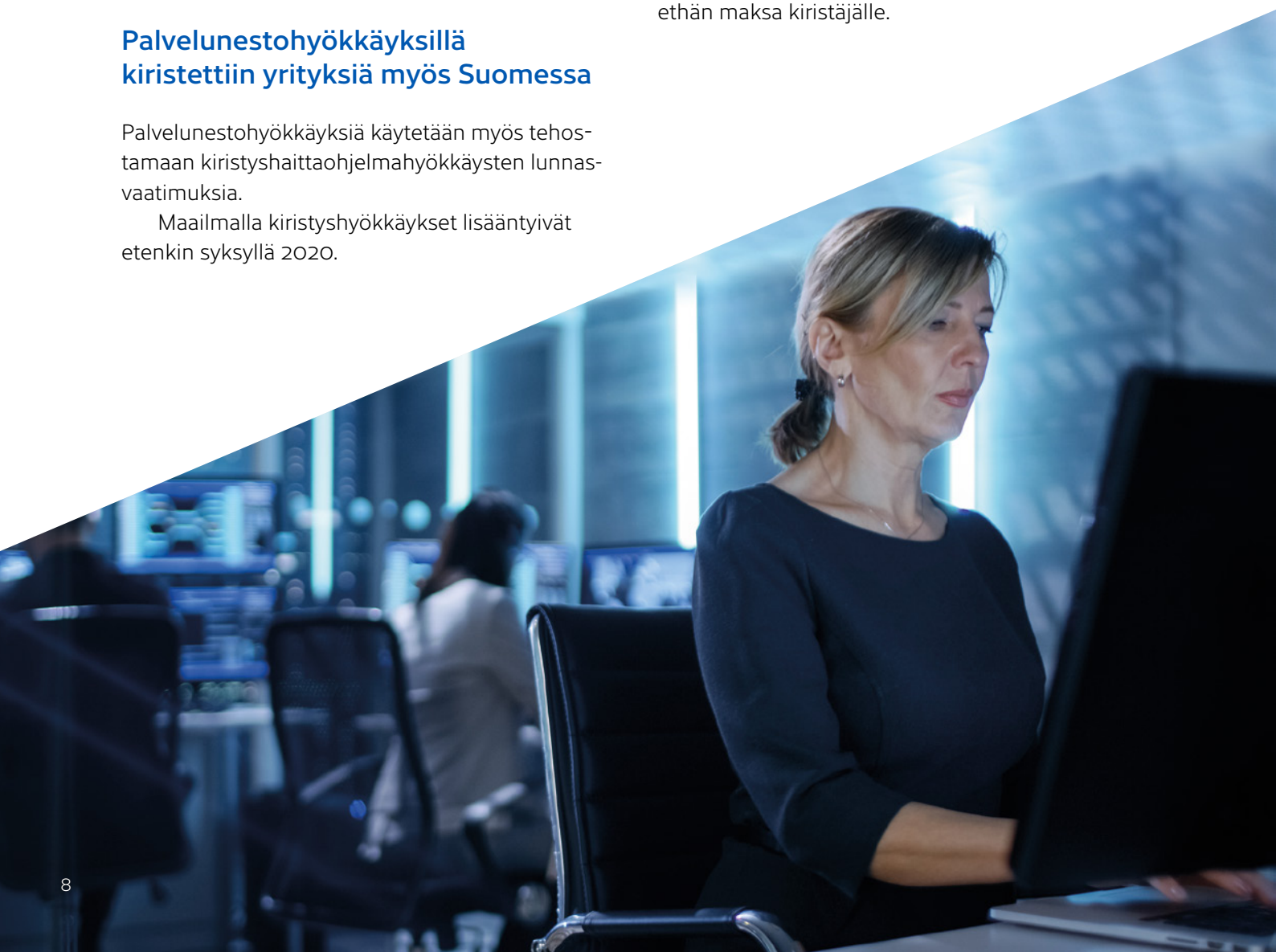
Maailmalla kiristyshyökkäykset lisääntyivät etenkin syksyllä 2020.

Hyökkäyksen ensivaiheessa yritys saa sähköpostin, jossa vastaanottajalta kiristetään yleensä BitCoineja, jotta hyökkäystä ei toteutettaisi. Yleensä kiristysviesti lähetetään alalla tunnetun rikollisryhmän tai yksittäisen toimijan nimissä. Usein rikollinen myös ryydittää uhkausviestiään lyhyillä mutta voimakkailla palvelunestohyökkäyksillä, joilla se yrittää pakottaa kohteensa maksamaan rahat, jotta se välttyisi isommalta hyökkäykseltä.

Tiedossamme on tapauksia, joissa kohdetta on uhkailtu hyökkäyksellä, jonka koko olisi ollut jopa 2Tb/s. Useimmiten kiristysviestit ovat olleet aiheettomia, mutta hyökkääjä on voinut tehdä pienempiä palvelunestohyökkäyksiä.

Myös suomalaiset organisaatiot ilmoittivat meille vastaanottamistaan kiristysviesteistä. Tietojemme mukaan hyökkäyksiä ei kuitenkaan toteutettu. Vaadittu rahasumma oli pienehkö ja kiristysviestien lähettäjät vaihtelivat. Kiristyksen kohteena olleilla organisaatioilla ei ollut yhdistäviä tekijöitä. Hyökkääjä vaikutti valinneen kohteensa satunnaisesti rahan toivossa.

Vanha ohjeistuksemme ei ole muuttunut: ethän maksa kiristäjälle.



# Vakoilu ja vaikuttaminen

Vuonna 2020 kybervakoilun painopiste vaikutti olevan muualla kuin Suomessa, mutta myös suomalaiset organisaatiot olivat säännöllisesti tunkeutumisyritysten kohteita. Isoimmat uutiset onnistuneista kybervakoilutapauksista ovat länsimaissa keskittyneet isoihin EU-maihin ja Yhdysvaltoihin sekä sen liittolaisiin.

Myös EU ja Norja ottivat päättyneen vuoden aikana aiempaa näkyvämmin kantaa kyberhyökkäysten taustavoimiin, ja esimerkiksi EU määräsi niihin liittyviä pakotteita.

**”Vaikka kybervakoilu keskittyi Suomen ulkopuolelle, myös kotimaiset organisaatiot olivat tunkeutumisyritysten kohteina.**

## Pandemia heijastui myös kybervakoiluun

Alkuvuonna paljastui haavoittuvuuksia tietoverkkojen turvaamiseen ja turvallisten yhteyksien muodostamiseen käytetyistä ratkaisuista. Näitä haavoittuvuuksia mahdollisesti hyödynnettiin myös valtiollisten toimijoiden tekemissä kyberhyökkäyksissä. Vuodenvaihteen huoli liittyi erityisesti tietyistä Citrix-tuotteista paljastuneisiin haavoittuvuuksiin. Vuoden aikana myös useiden muiden valmistajien erilaisista tietoverkkoihin ja verkon turvaamiseen liittyvistä tuotteista löydettiin vastaavia haavoittuvuuksia.

Kevään viruspandemian yhteydessä kiinnostaviksi näkökulmiksi nousivat erityisesti seuraavat teemat:

1. Koronavirukseen liittyneen tiedonjanon ja erilaisten pelkojen hyödyntäminen kohdistetuissa tietojenkalastteluviesteissä tai haittaohjelmien jakelussa.

2. Koronavirukseen, sen hoitoon ja rokotetutkimukseen kohdistuva kybervakoilu.

Tiedotimme mahdollisista uhkista organisaatioita suoraan omien kontaktiemme, yhteistyöverkostojemme ja kumppaniemme kautta.

## Loppuvuonna useita merkittäviä tietomurtotapauksia

Kybervakoilutapausten syksy oli kiireinen. Esimerkiksi Euroopan lääkevirasto (EMA) kertoi joutuneensa tietomurron kohteeksi juuri hieman ennen kuin yhden koronavirusrokotteen oli määrä saada hyväksyntä virastolta. Jo aiemmin syksyllä Norja nosti esiin parlamenttiinsa eli Suurkäräjiin kohdistuneen tietomurron, jonka taustalla se on julkisuudessa arvioinut olevan Venäjän sotilastiedusteluun (GU, aiemmin GRU) yhdistetty APT28.

Suomen eduskunta puolestaan kertoi joulukuun lopussa siihen kohdistuneesta kyberhyökkäyksestä, jota Keskusrikospoliisi tutkii epäiltyinä törkeänä tietomurtona ja vakoiluna. Eduskunta on kertonut, että muutamia sähköpostitilejä – joukossa myös kansanedustajien tilejä – vaarantui syksyllä tapahtuneessa hyökkäyksessä.

Loppuvuodesta alihankinta- ja toimitusketjuihin liittyvät uhkat konkretisoituivat jälleen, kun useisiin yhdysvaltalaisministeriöihin ja -organisaatioihin kohdistunut tietomurto paljastui. Tietomurto liittyi SolarWinds-etähallintatuotteisiin. Hyökkääjä oli onnistunut ujuttamaan omaa koodiaan mukaan asiakkaille jaeltuun päivitykseen. Näin hyökkääjällä oli halutessaan pääsy kaikkiin organisaatioihin, jotka olivat asentaneet haitallista koodia sisältäneen päivityksen. Näitä organisaatioita oli myös Suomessa. Vallitsevan käsityksen mukaan hyökkääjä kuitenkin hyödynsi pääsymahdollisuutta vain harvalukuiseen, itse valitsemaansa kohdejoukkoon muualla kuin Suomessa.

## Perinteiset menetelmät yhä käytössä

Myös perinteiset tunkeutumiskeinot, esimerkiksi salasanojen koneellinen arvaaminen ja kohdistettu tietojenkalastelu, ovat yhä osa kybervakoilun keinovalikoimaa. Esimerkiksi salasanojen murtoyrityksiä havaittiin vuoden aikana runsaasti.

Erityisesti Lähi-idässä kriittisen teollisuustuotannon, logistiikan ja energiahuollon toimivuuteen liittyvät valtiolliset kyberuhkat olivat myös läsnä.

## Kybervakoiluun varautumista tulee edelleen parantaa

Vaikka organisaatioiden havainnointikyky ja varautuminen paranivat edelleen, esimerkiksi lokien keräyksen kattavuudessa sekä niiden hallinnassa ja analysoinnissa on edelleen puutteita. Tämä heikentää suomalaisten organisaatioiden kykyä selvittää niihin kohdistuneita tietomurtoja tai tietomurron yrityksiä. Edelleenkin merkittävä osa tietomurroista saadaan selvitettyä vain osittain. Tavallista on, että selvityksessä ei päästä kaikkia osapuolia tyydyttävään varmuuteen tapahtumien kulusta ja seurauksista.

Kybervakoilu ei koske vain valtionhallintoa tai poliittisia organisaatioita, vaan se voi kohdistua myös yrityksiin esimerkiksi teollisuusvakoiluna. Varautumisessa on hyvä huomioida myös kohdistetut kyberhyökkäykset, jotka tilaaja ostaa kyvykkäältä toimijalta. Tilaustyöhyökkäykset myös vaikeuttavat hyökkäyksiin varautumista ja tekijöiden tunnistamista.

# Haittaohjelmat ja haavoittuvuudet

Kuluneena vuonna näimme haavoittuvuuksia ja haittaohjelmien levitysaaltoja, joihin oli reagoitava nopeasti. Etätyöratkaisuistakin löydettiin merkittäviä haavoittuvuuksia, jotka piti päivittää tai vähintäänkin huomioida eri toteutuksissa viipymättä.

## Arvioi etätyöratkaisut tietoturvan näkökulmasta

Huhtikuussa löysimme useita internetiin avoimena olevia RDP-palveluja. Ilmoitimme havainnoista ylläpitäjille ja suosittelimme sopivia jatkotoimia. Etäkäyttöratkaisuista löydettyjä haavoittuvuuksia hyödynnettiin tietomurtoihin, haittaohjelmien levittämiseen ja kiristyshaittaohjelmien käyttöön.

Ylipäänsä viime vuosi tarjosi hyökkääjille useita tunkeutumismahdollisuuksia organisaatioiden verkkoympäristöihin. Väyliä tarjosivat myös yleistyneiden etätyöratkaisujen ja tiedostonjakopalveluiden tietoturva-aukot.

Verkkohyökkäyksien niin kutsuttua hyökkäyspinta-alaa lisäävät merkittävästi julkiseen verkkoon näkyvät tai hyökkääjän saatavilla olevat palvelut ja niiden heikkoudet. Suojaamalla, rajaamalla palveluiden näkyvyyttä ja poistamalla käytöstä tarpeettomat palvelut vähennetään hyökkääjälle tarjolla olevia keinoja tunkeutua verkkoon.

> ”Suojaamalla, rajaamalla palveluiden näkyvyyttä ja poistamalla käytöstä tarpeettomat palvelut vähennetään hyökkääjälle tarjolla olevia keinoja tunkeutua verkkoon.

Sisäverkkoon päästyään hyökkääjä voi arvailla salasanoja ja hyödyntää muitakin haavoittuvuuksia, joita ei ole päivityksin paikattu. Etätyöjärjestelyt eivät saisi vaarantaa yhdenkään organisaation tietoturvaa. Poikkeusratkaisut, jos sellaisia on, pitäisi purkaa normaalioloihin palattaessa. Ilman ratkaisujen dokumentointia niiden purkaminen huolellisesti ei ole mahdollista.

## Päivittäminen voi pelastaa isoilta vahingoilta

Kun haavoittuvuus tulee julki, sitä skannataan aktiivisesti heti julkaisun jälkeen. Jos päivitysten asentaminen viivästyy, pitää varmistaa, ettei hyökkääjä ole jo ehtinyt hyödyntämään haavoittuvuutta.

Ennen uuden laitteen ostoa pitäisi aina tarkistaa, onko laitteen ohjelmistolle saatavilla päivityksiä tulevaisuudessakin. Jos päivitykset päättyvät, käyttöjärjestelmät ovat aiempaa alttiimpia tietomurroille. Suomessakin käytössä on useita vanhoja Windows-versioita, joihin ei enää saa päivityksiä, vaikka kyseessä olisi kriittinen haavoittuvuus.

## Emotet levisi ja kiristyshaittaohjelmat yleistyivät

Julkaisimme elokuussa varoituksen Suomessa aktiivisesti leviävästä Emotet-nimisestä haittaohjelmasta. Emotet levisi esimerkiksi liitetiedostojen makrojen ja haitallisten linkkien kautta. Sitä yritettiin levittää vanhan sähköpostiketjun jatkoksi lähetetyillä huijausviesteillä. Sähköpostien linkit ja tiedostot sekä väärennetyt lähettäjätiedot ovat haittaohjelmatartunnoissa merkittävässä roolissa. Organisaation pitäisikin kiinnittää huomiota oman sähköpostinsa väärennettyjen lähettäjätietojen käsittelyyn.

Kiristyshaittaohjelmien uhkaan tulee varautua myös Suomessa, sillä yleistyneet hyökkäykset voivat kohdistua kaiken kokoisiin organisaatioihin. Kiristyshaittaohjelmille on tyypillistä aktivoitua viikonloppuisin tai sellaisina ajankohtina, jolloin työntekijöitä on vähemmän paikalla. Yritysten maksuvalmius tai halukkuus on vähentynyt, minkä vuoksi rikolliset kehittävät uusia tapoja hyödyntää ja myydä saatua tietoa. Viime vuonna yleistyi trendi, jossa tietojen salaamisen lisäksi rikolliset varastivat tietoja uhrilta ja uhkasivat julkaista tiedot, jos lunnaita ei makseta.

> ”Kiristyshaittaohjelmien uhkaan tulee varautua myös Suomessa, sillä ne ovat yleistyneet ja voivat kohdistua kaiken kokoisiin organisaatioihin.

### Arviomme merkittävimmistä haavoittuvuuksista 2020

1. **VPN:** monta eri haavoittuvuutta ja useita valmistajia – kaikissa oli ongelmia.
2. **Zerologon**: aktiivisesti hyväksikäytetty protokolla-haavoittuvuus.
3. **SMBGhost/SMBleed**: kriittiset protokolla-haavoittuvuudet.
4. **Oracle WebLogic**: aktiivisesti hyväksikäytetty haavoittuvuus mahdollistaa pääsyn palvelimelle.
5. **TCP/IP Treck / Ripple**: vaikutus maailmanlaajuisesti satoihin miljooniin laitteisiin.

Kaikkia haavoittuvuuksia on hyödynnetty tietomurroissa, ja ne ovat olleet useissa palveluissa käytössä, etäyhteyksin hyödynnettävissä ja näkyvissä avoimeen verkkoon.

# Tietomurrot ja tietovuodot

Ilmoitukset tietomurroista ja tietovuodoista sekä niiden yrityksistä lisääntyivät. Vuoden 2019 kaltaisia kuntasektoriin kohdistuneita tietomurtoja ei tullut esille, mutta eduskuntaan kohdistunut tietomurto nousi julkisuuteen joulukuussa.

Lokakuussa uutisoitiin laajasti psykoterapiakeskus Vastaamosta, jota kiristettiin tietovuodon uhalla. Kyseessä oli Suomen ensimmäinen suuren luokan tietomurto. Hyökkääjä päätyi toteuttamaan uhkauksensa osittain ja vuoti erittäin arkaluontoista materiaalia julkisuuteen.

Office 365 -tietomurrot ja niiden yritykset jatkuivat myös vuonna 2020. Näyttää siltä, että tapausmäärät eivät ole merkittävästi vähenemässä.

Tammikuussa yleistyivät teknisen tuen huijauspuhelut. Niistä seurasi myös tietomurtoja, koska soittaja kehotti uhriaan asentamaan koneelleen etähallintaohjelman, jonka kautta rikollinen pääsi käsiksi koneen tietoihin. Maaliskuussa puhelut taukosivat hetkellisesti, kun kansainväliset pandemiasta johtuvat kokoontumisrajoitukset tulivat voimaan.

## Oma havainnointikyky suojaa rikollisilta

Rikolliset kartoittavat uusia hyökkäysmahdollisuuksia jatkuvasti, siksi organisaatioiden omalla havainnointikyvyllä on tärkeä rooli hyökkäyksiltä suojautumisessa. Avainasemassa on kyky havaita normaalista poikkeavat tapahtumat, esimerkiksi kirjautumiset outoon aikaan tai oudosta paikasta. Lokituksen laatuun, määrään ja riittävään säilytysaikaan tulee myös kiinnittää huomiota, koska ilman laadukkaita lokitietoja tapahtumia ei voi tutkia.

Raportoitujen haittaohjelma- ja kalasteluviestien kautta paljastuu usein myös tietomurtoja, siksi kaikki tietoturvailmoitukset ovat tärkeitä tilannekuvan koostamisen takia.

## TAPAUS VASTAAMO

Psykoterapiakeskus Vastaamon tietomurto oli kuluneen vuoden suurin tietoturvaloukkaustapaus Suomessa. Tietomurtoa seurasivat kiristysviestit, joissa sekä Vastaamoa että sen asiakkaita vaadittiin maksamaan lunnaita, jos he halusivat välttää potilastietojensa vuotamisen internetiin muiden saataville.

Poliisille on kirjattu tapauksesta yli 25 000 rikosilmoitusta. Myös monet muut organisaatiot ja viranomaiset ovat olleet mukana tukemassa ja auttamassa tietomurron uhreja.

Kyberturvallisuuskeskus tuki Vastaamoa tapauksen käsittelyn ensivaiheissa. Autoimme myös poliisia ja asiaa tutkivaa tietoturvayhtiötä teknisessä selvityksessä.

Opit olivat ilmeiset: omat palvelut tulee tuntea ja niitä tulee tarkkailla ja arvioida. Jos omat resurssit tai osaaminen eivät riitä, pitää pyytää apua alan ammattilaisilta. Verkkopalvelujen skannaus ja omien järjestelmien testaaminen kyberharjoitusmielessä ovat pieni satsaus vakavaan tietomurtoon verrattuna.

Tapaus muistutti myös siitä, että verkkopalveluissa ei pidä käyttää henkilötunnusta asiakkaan tunnistamiseen. Vahva sähköinen tunnistaminen on turvallisempi keino.

### Monipuolinen ja epäitsekäs yhteistyö tuo avun nopeasti

Vastaamon tietomurto sai uuden käänteen lauantai-iltana 24.10., kun rikollinen ryhtyi kiristämään Vastaamon asiakkaita uhkaamalla julkaista heidän luottamuksellisia tietojaan.

Aloitimme työn Kyberturvallisuuskeskuksessa lauantai-iltana. Sunnuntaina kerääntyimme yhteen useiden eri viranomaisten, järjestöjen ja vapaaehtoistoimijoiden kesken kokoamaan ohjeita kiristyksen uhreille. Työn tuloksena julkaisimme maanantaina 26.10. tietovuotoapu.fi-verkkosivuston apua tarvitseville. Toimme sivustolle eri toimijoiden tuottamaa monipuolista ohjeistusta ja yhteystietoja, joista uhrien oli mahdollista saada myös keskusteluapua.

Tietovuotoapu.fi-sivusto osoitti, kuinka toimivaa, helppoa ja tarvittaessa nopeaa eri organisaatioiden yhteistyö Suomessa on. Oli hienoa olla mukana todistamassa, kuinka kaikki halusivat tuottaa yhteistä hyvää omista toimiala- tai vastuurajoista huolimatta. Tällaisen luottamuksen ja yhteistyökyvyn varaan on helppo rakentaa yhä turvallisempaa tulevaisuuden yhteiskuntaa.

> ”Vastaamon tietomurto oli vuoden 2020 suurin tietoturvaloukkaustapaus Suomessa.

# Tietojenkalastelu ja huijaukset

## Puhelinhuijaukset synkensivät poikkeusvuotta

Helmikuussa huijarit totisesti löysivät Suomen televerkon. Aiemmin puhelimitse tehdyt huijaukset ovat olleet Suomessa vähäisiä.

Ainoastaan helmikuun aikana suomalaiset teleoperaattorit kertoivat miljoonasta teknisen tuen huijauspuhelusta. Niin kutsutuista häläri-huijauksista kertyi myös miljoona puhelua.

Teknisen tuen huijauksessa huijari soittaa ja kertoo, että kohteen tietokoneella on ongelma. Huijari voi väittää ongelman johtuvan esimerkiksi haittaohjelmasta, hakkerista tai ”verkkotukoksesta”. Hälärihuijauksessa kohteen puhelin soi kerran tai pari niin, että puheluun ei mitenkään ehdi vastata. Puhelu tulee ulkomaan suuntanumerosta – Samoalta, Papua-Uusi-Guineasta, Tunisiasta – tai satelliittipuhelinpalvelusta. Numeroon takaisin soittaminen voi maksaa jopa 10 euroa minuutilta.

Huijauspuhelut ovat aiheuttaneet paljon harmia ja merkittäviä menetyksiä suomalaisille. Tekemämme yhteistyö suomalaisten teleoperaat-toreiden kanssa on kuitenkin auttanut, ja Suomeen ulkomailta tulevat häläripuhelut on saatu kitkettyä minimiin. Heinäkuun jälkeen olemme saaneet puheluista enää kourallisen ilmoituksia.

Teknisen tuen huijauksista eroon pääsy on vai-keampaa, koska huijareiden käyttämät puhelinnu-merot ovat väärennettyjä. Puhelut näyttävät tulevan suomalaisista, isobritannialaisista tai ruotsalaisista puhelinnumeroista, mutta tosiasiassa ne tulevat puhelukeskuksesta, jossa kymmenet työntekijät tehtailevat huijauksia liukuhihnalta eri maihin.

## Laskutuspetoksista tuntuvia rahallisia menetyksiä

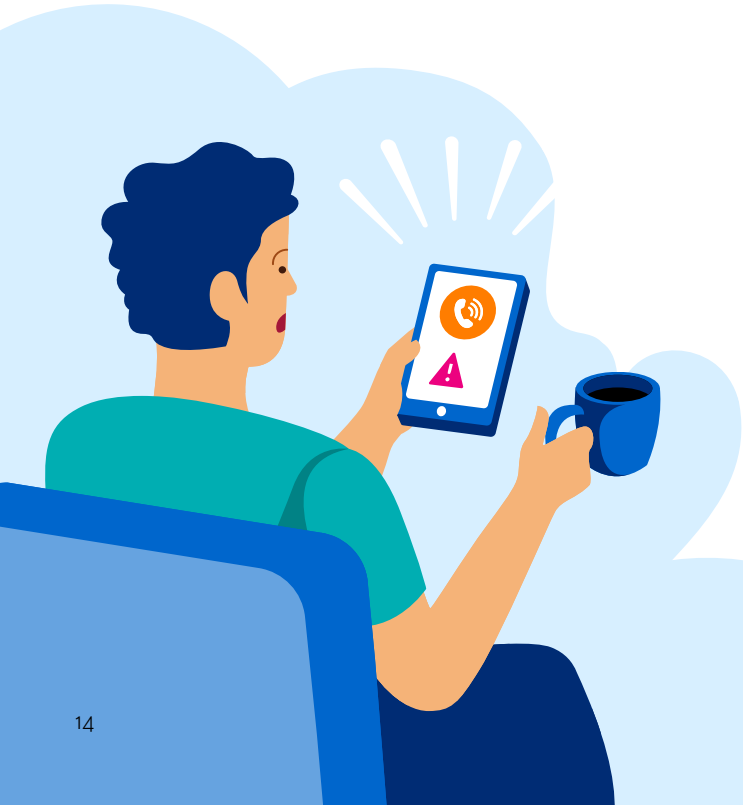
Laskutushuijaukset aiheuttivat taas tuntuvia talou-dellisia menetyksiä organisaatioille. Muun muassa kansainvälinen rikollisryhmä esiintyi Finanssivalvon-nan ja lakitoimistojen nimissä päästäkseen käsiksi suurten yrityskauppojen varansiirtoihin.

Tavallisin tapa toteuttaa laskutuspetos on tekeytyä organisaation johtajaksi ja lähettää hänen nimissään viestejä organisaation taloushenkilös-tölle. Rikoksella saatu kertahyöty voi olla satojakin tuhansia euroja. Laskutuspetokset huomataan usein vasta viikkoja vahingon jälkeen, jolloin raho-jen palauttaminen on merkittävästi vaikeampaa.

## Tekstiviestien huijauslinkit aiheuttivat taas harmia

Tekstiviestien linkit vievätkin usein tilausansoihin, haittaohjelmiin tai muihin petoksiin. Tätä keinoa huijarit käyttivät runsaasti. Älypuhelimen ruudulla huijauslinkin osoite ei välttämättä näy, siksi vastaan-ottaja ei osaa epäillä huijausta.

Erityisesti Postin ja eri kuriiripalveluiden nimissä lähetettiin huijausviestejä, joiden tarkoituksena oli tartuttaa Android-puhelimiin haittaohjelmia ja ohjata Apple-käyttäjiä tietojenkalastelusivuille. Itselle tuntemattomien ohjelmien asennusta omalle puhelimelle ei pidä sallia. Jos luvan antaa, tuhansia tekstiviestejä ulkomaille lähettävä haittaohjelma voi aiheuttaa liittymälle mittavia laskuja.



# Esineiden internet ja automaatiojärjestelmät

## Hyökkäys kriittisen infrastruktuurin automaatiojärjestelmään

Kulunut vuosi toi iskuja kriittisen infrastruktuurin automaatiojärjestelmiin, kun hyökkääjät ottivat kohteekseen Israelin vesijärjestelmän. Ensimmäinen isku tapahtui huhtikuussa, kesäkuussa havaittiin kaksi uutta yritystä. Israel onnistui estämään hyökkäyksen, joka olisi voinut vahingoittaa väestöä merkittävällä tavalla.

Tämä oli tiettävästi ensimmäinen kerta, kun IoT- ja automaatiojärjestelmien avulla yritettiin aiheuttaa fyysistä vahinkoa kansalaisille. Aiemmat iskut ovat kohdistuneet ensisijaisesti tietoihin ja tietojärjestelmiin. Hyökkääjäksi epäiltiin Irania. Hyökkäystä pidetään ensimmäisenä merkkinä kybersodankäynnin todellisesta kiihtymisestä.

**”Mitä enemmän tietoturvapuutteisia laitteita verkkoon tuodaan, sitä suuremmin verkon käytettävyys ja tietoturva kärsii.**

Edellisvuosien kartoituksiin verrattuna määrät eivät muuttuneet merkittävästi, siten laitteiden ja järjestelmien tietoturvallisuustyötä tulee jatkaa ja tehostaa edelleen. Mitä enemmän tietoturvapuutteisia laitteita verkkoon tuodaan, sitä suuremmin verkon käytettävyys ja tietoturva kärsii.

Internetissä suojaamattomana oleva laite on houkutteleva kohde murtautujille. Laitteen voi valjastaa esimerkiksi palvelunestohyökkäyksiin tai laite voi tarjota helpon pääsyn yrityksen verkkoon.

## Tuhansia laitteita ja järjestelmiä yhä suojaamatta

Syyskuussa julkaistu tutkimus tulostinten haavoittuvuuksista osoittaa, että verkkoon kytketyissä älylaitteissa on yhä paljon tietoturvapuutteita. Tutkimuksessa löydettiin verkosta noin 500 000 suojaamatonta tulostinta, joista 50 000 tutkittiin tarkemmin. Näistä noin puolet saatiin otettua haltuun niin, että tunkeutuja pystyi tulostamaan laitteella.

Vuosittaisessa suojaamattomien automaatiolaitteiden kartoituksessamme kävimme läpi noin 1280 verkkoa ja 12,8 miljoonaa IP-osoitetta suomalaisessa verkkoavaruudessa. Eniten havaitsimme erilaisia rakennusautomaatiolaitteita, joita oli noin 800 IP-osoitteessa. Teollisuusautomaatioon kuuluvia järjestelmiä havaittiin noin 120 ja kriittiseen teollisuusautomaatioon kuuluvia järjestelmiä noin 30. Löysimme suomalaisista verkoista noin 1000 suojaamatonta automaatiojärjestelmää.

## IoT-maailman merkittävä muutos häämöttää

Tietoturvaongelmat IoT-laitteissa ja automaatiojärjestelmissä ovat havahduttaneet monet erilaisten tietoturvallisuusvaatimusten ja -sertifiointien tarpeeseen.

EU:n kesäkuussa 2019 voimaan astuneessa kyberturvallisuusasetuksessa määriteltiin eurooppalaisen tietoturvallisuuden sertifiointijärjestelmä, jonka perusteella suunnitellaan tulevina vuosina myös IoT-laitteiden sertifiointia.

Kesäkuussa 2020 julkaistiin ensimmäinen viralinen kuluttajien älylaitteiden tietoturvastandardi ETSI 303645 Cyber Security for Consumer Internet of Things: Baseline Requirements.

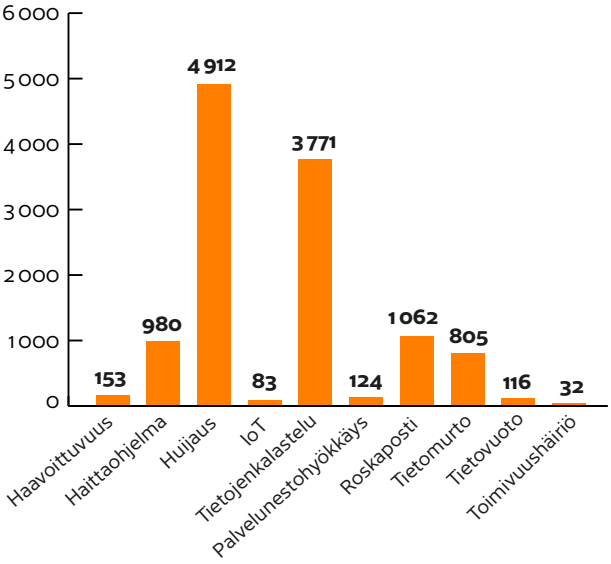
Komissiokin havaitsi, että verkkoon kytkettävien laitteiden tietoturvaa tulee parantaa myös lainsäädännön keinoin. Yhtenä keinona pidetään EU:n radiolaitedirektiiviä (Radio Equipment Directive, RED). Sen mukaan on alettu valmistella delegoitua säädöstä radiolaitteiden tietoturvasta. Säädöksellä tulee olemaan IoT-maailmaan merkittävä vaikutus.

# Palvelumme

# Tilannekeskus – Ensiapua tietoturvaloukkauksiin

Tilannekeskuksemme tietoturva-asiantuntijat antavat ensiapua ja neuvoja tietoturvaloukkausten uhreille. Keskuksessamme käsiteltyjen tapausten lukumäärä lisääntyi vuodesta 2019 yli 100 %. Tuolloin tapausmäärä oli 4500, mutta vuonna 2020 luku oli yli 10 900.

Tapausmäärät kasvoivat käytännössä jokaisessa eri kategoriassa, joihin tietoturvapoikkeamia luokittelemme. Eniten saimme ilmoituksia erilaisista huijauksista ja tietojenkalastelusta.




Tapausmäärät tapaustyypeittäin vuonna 2020.

## Emotet-haittaohjelmasta lukuisia yhteydenottoja

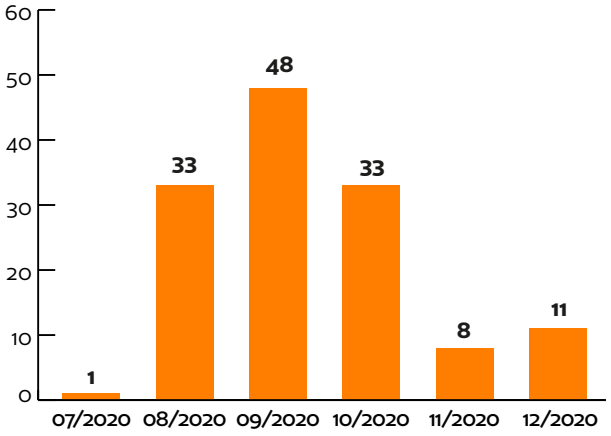
Emotet on hyvä esimerkki haittaohjelmasta, jonka avulla pyritään saavuttamaan jalansija ja takaovi kohteena olevaan organisaatioon. Sitä käyttävät ammattimaisesti tietomurtoja tekevät rikolliset. Saimme ensimmäiset ilmoitukset Emotet-haittaohjelman levittämisyrityksistä elokuussa 2020.

Merkittävä osa Emotet-tapauksista jäi organisaatioiden omien tietoturvakontrollien vuoksi vain levittämisyrityksiksi. Toisille kävi huonommin. Tartuntatapauksissa päivystäjämme neuvoivat useita uhriorganisaatioita, kuinka toipua tilanteesta.

Julkaisimme keltaisen varoituksen Emotet-haittaohjelmaa levitetään aktiivisesti Suomessa 18.8.2020. Poistimme varoituksen marraskuussa, vaikka haittaohjelman uhka ei ollut täysin väistynytkään. Hyviä uutisia saimme tammikuussa 2021, kun Emotet-bottiverkko nujerrettiin kansainvälisessä poliisioperaatiossa.

Kun haittaohjelmia levittävä kampanja osuu Suomeen, tilannekeskuksemme ryhtyy välittömästi toimeen. Kaivamme kampanjasta esiin oleelliset yksityiskohdat. Jakamalla niin kutsuttuja haittaohjelman tunnistetietoja eri kanaviimme tarjoamme apua uhalta suojautumisessa.

Haittaohjelmahyökkäysten torjumiseksi organisaatioiden kannattaa suojautua monipuolisesti, esimerkiksi kouluttamalla henkilöstöä ja rakentamalla teknisiä kontrolleja.




Emotet-haittaohjelmaan liittyvät ilmoitukset kuukausittain.

### Tunnistetieto – Indicator of Compromise, IOC

- Esimerkiksi IP-osoite, domain tai url, jota haittaohjelma käyttää komentokanavana.
- Onko organisaatiollasi kyky etsiä lokeista liikennettä tunnistetiedon perusteella esimerkiksi viimeisen vuoden ajalta?

# Haavoittuvuuskoordinaation tarve on kasvanut

Tilannekeskukseen ilmoitetaan viikoittain haavoittuvuustapauksista, jotka vaativat koordinointia tuotteen ja sen eri komponenttien valmistajien, tietoturvatutkijoiden sekä käyttäjäryhmien välillä. Suurin osa tapauksista on luonteeltaan melko yksinkertaisia, ja ne liittyvät nettipalveluihin ja IoT-laitteisiin.

Nettipalveluihin liittyvät ilmoitukset olivat pääosin toteutusvirheitä yksittäisissä palveluissa ja niiden taustajärjestelmissä. Tällaisissa tapauksissa palveluntarjoajat tai koodin tuottaneet alihankkijat voivat itse korjata haavoittuvuuden. Siksi näissäkin meille ilmoitetuissa tapauksissa ei tiettävästi päässyt aiheutumaan vahinkoja. Vuonna 2020 saimme myös edellisvuosia enemmän ilmoituksia palveluiden tietosuojapuutteista ja puutteisiin liittyvistä epäilyistä.

> **”Vastuulliset valmistajat korjaavat haavoittuvuudet ripeästi ja päivittävät avoimet järjestelmät parhaimmillaan viipymättä. Avointen ja riskialttiiden palvelujen kokonaismäärät eivät kuitenkaan näytä vähentyvän.**

Lähes kaikki IoT-laitteissa raportoidut haavoittuvuudet olivat luonteeltaan alkeellisia toteutustason virheitä tai turvattomia oletusasetuksia. Useimmissa tapauksissa hyökkääjä pystyisi haavoittuvuuden avulla saamaan laitteen haltuunsa. Haavoittuvuuksien korjaamisprosessit ovat paikoin hankalia ja hitaita.

Tietoomme tulee runsaasti internetiin avoimia palveluita, joita käytetään turvallisuuden varmistamiseen tai eri järjestelmien hallintaan. Avoimuuden tarpeellisuus vaikuttaa usein kyseenalaiselta. Avoimiin palveluihin kohdistuu paljon erilaista hyökkäysliikennettä ja yksikin heikkous tai väärä asetus voi asettaa ne alttiiksi tietomurrolle.

Edellisvuoden vakavimmat haavoittuvuudet liittyivät tapauksiin, joissa löydettiin uusi haavoittuvuus palvelusta, joita on verkossa useita. Syystä tai toisesta nämä palvelut olivat myös verkkoon avoinna. Vastuulliset valmistajat korjaavat haavoittuvuudet yleensä nopeasti, ja avoimia järjestelmiä päivitetään parhaimmillaan viipymättä, mutta avointen ja riskialttiiden palvelujen kokonaismäärät eivät näytä vähentyvän.

# Turvallisuussääntely

## Kansallinen turvallisuus menee syvemmälle viestintäverkkoihin

Matkaviestinverkkojen ja ennen kaikkea 5G-verkkojen turvallisuus oli läpi vuoden yksi kuumimmista puheenaiheista kaikkialla maailmassa.

EU:ssa laadittiin pikavauhtia poliittisesti neutraali ohjeistus toimenpiteistä 5G-verkkojen kyberturvallisuusriskien minimoimiseksi. Suomessa puolestaan valmisteltiin uutta lainsäädäntöä viestintäverkkojen kriittisten osien suojaamiseksi. Molemmat olivat näkyvästi läsnä tekemisessämme, kun laadimme EU-tason ohjeistuksia ja valmistelimme määräyksen viestintäverkkojen kriittisistä osista uutta lainsäädäntöä varten. Aikaisemmin viestintäverkon ja siellä kulkevan liikenteen hallintaan ja ohjaamiseen käytettäviä keskeisiä osia ei ollut määritelty.

Jo vuosikymmenet kansallinen turvallisuus ja maanpuolustus ovat olleet yksi näkökulma viestintäverkkojen ja -palvelujen turvallisuuden sääntelyssä. Uudessa lainsäädännössä kansallinen näkökulma on aiempaa korostetummassa asemassa ja antaa uusia työkaluja puuttua mahdollisiin kansallista turvallisuutta ja maanpuolustusta uhkaaviin kyberturvallisuusriskeihin.

## Sijaintitietopalvelu – verkkoinfrastruktuurien uusi koti

Lokakuussa 2022 meillä suomalaisilla on käytössä Sijaintitietopalvelu. Tuolloin maanrakennustöihin ryhtyvällä on mahdollisuus saada tiedot kaivuualueella olevien kaapeleiden ja putkien sekä tele-, sähkö-, vesihuoltoverkkojen infrastruktuureiden sijainneista. Palvelun tarkoituksena on helpottaa ja tehostaa suunnittelijoiden ja maanrakentajien työtä. Se myös vähentää kaivuuvahingoista syntyviä kustannuksia ja palvelukatkoksia tele-, sähkö- ja vesihuoltoyrityksille ja niiden palveluja käyttäville.

Keskitetty tietopiste parantaa verkkotoimijoiden tietoisuutta toistensa fyysisen verkkoinfrastruktuurin sijainnista ja helpottaa niiden välistä yhteistyötä. Määräyksemme (71/2020 M) mukaan Sijaintitietopalveluun toimitettavat tiedot tulee toimittaa tietyssä muodossa, mikä helpottaa ja parantaa tietojen käytettävyyttä. Määräys on myös helpottanut Sijaintitietopalvelun toiminnallisuuksien ja teknisten rajapintojen teknistä määrittelyä.

Sijaintitietopalvelun tuotantokäyttöön on vielä pitkä matka, mutta yhdessä eri toimialojen edustajien, maanrakennustoimijoita edustavien toimijoiden ja Suomen Infratieto Oy:n kanssa tehtävällä yhteistyöllä meillä on mahdollisuus saavuttaa tavoitteemme.

## Pandemia näytti, että EU:n eIDAS-asetuksen uudistamista tarvitaan

Poikkeusaikana etäasioinnin, etäneuvottelujen ja sähköisen sopimisen tarve kasvoi räjähdysmäisesti. Siksi myös EU:n eIDAS-asetuksen muutostarpeiden arviointi oli ajankohtaista.

Asetuksen perusteella palveluntarjoajat voivat hankkia EU-tasoisen hyväksynnän sähköisille luottamuspalveluilleen, joita tarvitaan hallinnossa ja liiketoiminnassa esimerkiksi sopimusten ja palvelujen sähköistämisessä. Tietoturvallisuuden lisäksi asetus koskee myös oikeudellista pätevyyttä.

Herättelimme kotimaista keskustelua muutostarpeista ja kokosimme kansainvälisessä ja kotimaisessa työssä kertyneet kokemukset kesäkuussa arviointimuistioksi.

Suomessa vahva sähköinen tunnistus on vakiintunut ja tuttu palvelu, mutta sähköistä allekirjoitusta ja muita sähköisiä luottamuspalveluja hyödynnetään huomattavasti vähemmän. Saimme havainnoistamme toimialalta varsin kiittävää palautetta.

eIDAS-asetuksen uudelleenarvioinnissa pitäisi tarkentaa vaatimuksia ja lisätä palveluvalikoimaa. Näin varmistettaisiin yhtenäinen sääntely eri jäsenvaltioissa ja parannettaisiin tarjonnan edellytyksiä. Lisääntynyt ja asiakkaiden tarpeita vastaava luottamuspalveluiden tarjonta helpottaisi vuorostaan niiden hankintaa. Esimerkiksi eri tasoisten sähköisten allekirjoituspalveluiden valintaan ja käyttöönottoon liittyy paljon epävarmuutta.

**EU Trust Mark kertoo sähköisen luottamuspalvelun EU-tasoisesta hyväksynnästä**

# Arvioinnit

## Koronavilkku arvioitiin ennätysajassa

Kansallisen ja kansainvälisen turvallisuuspolitiikan ilmiöt näkyivät edellisvuoden tapaan arviointikohteissamme. Myös koronavirustilanne toi arviointitoimintaamme omat lisämausteensa. Kansainväliseen turvallisuusluokiteltuun tietoon kohdistuvat velvoitteet ja suojausperiaatteet eivät oleellisesti eronneet normaaliolojen tilanteesta. Toisaalta pystyimme osaltamme tukemaan koronatilanteen hallintaa arvioimalla muun muassa THL:n tuottaman tartuntaketjujen katkaisua tukevan Koronavilkku-sovelluksen ja sen taustajärjestelmän tietoturvallisuuden. Arvioimme myös useita kotimaisia turvallisuusluokitellun tiedon suojaamiseen tarkoitettuja salaustuotteita.

## Neuvontaa turvallisista videoneuvotteluratkaisuista ja tukea pilvipalvelujen käyttöön

Neuvontapalvelumme kysyntä jatkoi kiihtyvää kasvuaan. Turvallisuusluokitellun tiedon perinteisten käsittely-ympäristöjen ja kriittisen infrastruktuurin suojaamisen lisäksi tukeamme toivottiin erityisesti turvallisten videoneuvotteluratkaisujen valintaan ja käyttöönottoon. Myös pilvipalveluihin liittyvät tukitarpeet jatkoivat kasvuaan. Maaliskuussa julkaisemamme Pilvipalvelujen turvallisuuden arviointikriteeristön (PiTuKri) päivitetty versio otettiin saadun palautteen perusteella innolla käyttöön.

# Satelliittijärjestelmät näkyvät jo ihmisten arjessa

Maailmanlaajuiset satelliittinavigointipalvelut levittäytyvät kiihtyvällä tahdilla ihmisten arkipäivään. Satelliittipaikannus on oleellinen osa arkisia palveluita eikä ole enää pelkkä paikasta toiseen suunnistamisen väline. Peliteollisuus, erilaiset palvelusovellukset, liikennesuoritteiden optimointi, liikuntasuoritukset: kaikissa näistä satelliittipaikannuksella on keskeinen rooli.

Euroopan unionin rahoittama Galileo-satelliittipaikannusjärjestelmä on noussut vahvasti GPS:n rinnalle vuoden 2020 aikana lähes kaikissa paikannusta hyödyntävissä päätelaitteissa. Oman lisänsä paikannustarkkuuden ja -varmuuden parantamiseen tuovat myös kiinalainen BeiDou – joka otettiin virallisesti käyttöön elokuussa 2020 – sekä venäläinen GLONASS.

Mitä useampia satelliitteja käyttäjälaite pystyy ottamaan vastaan, sitä parempi on paikannustarkkuus. Galileo on näistä globaaleista järjestelmistä kaikkein tarkin ja tarjoaa lisäksi ainoana järjestelmänä kaksitaajuisen vastaanottomahdollisuuden kuluttajatason vastaanottimiin.

## Galileo ja EGNOS kehitys-polulla

Galileo-järjestelmä saavutti helmikuussa uuden vaiheen: hätäviestipalvelu SAR (Search and Rescue) otettiin täysimittaisesti käyttöön. Galileon SAR-palvelu tarjoaa ensimmäisenä järjestelmänä maailmassa hätäviestin lähettäjälle automaattisen kuittauksen viestin perille menosta. Myös muiden Galileo-palveluiden kehitystyö eteni lähes suunnitellusti, vaikka koronavirus viivästytti-kin hieman aikatauluja.

## Kyberturvallisuuskeskuksen satelliittipalvelut

Satelliittipalvelumme on käynyt keskusteluja GNSS-käyttäjien kanssa ja nostanut esiin erityisesti Galileo- ja EGNOS-palveluista jatkossa saatavia hyötyjä. Kotimaisen elinkeinoelämän kanssa käymme jatkuvaa vuoropuhelua, jotta alan yritykset pystyvät varautumaan tuleviin markkinamuutoksiin. Keskusteluihin on otettu mukaan myös EU:n satelliittinavigointivirasto.

Galileon turvallisuuskriittisimmän osuuden eli julkisesti säännellyn PRS-palvelun käyttöönoton valmisteluohjelma laadittiin vuoden 2020 aikana. Lopputuloksena oli kaikkien hallinnonalojen hyväksymä PRS-toteutussuunnitelma, joka on perusta sekä hankkeen rahoitusratkaisuille että palvelun operatiiviselle suunnittelulle. Marraskuussa 2020 hallituksen talouspoliittinen ministerivaliokunta linjasi, että PRS-palvelu otetaan Suomessa käyttöön vuonna 2024 ja palvelun edellyttämää kansallista infrastruktuuria aletaan rakentaa vuodesta 2021 alkaen. Rakentaminen alkaa suunnittelutyöllä ja siihen liittyvällä teknisen arkkitehtuurin määrittelyllä vuoden 2021 aikana.

# Matkapuhelimesi ei ole yksin!

## Katso kaikki laitteet, joissa on Galileo-valmius.

**www.useGalileo.eu**




# Galileo pitää yhteiskunnan toimintakykyisenä!


**kyberturvallisuuskeskus.fi/fi/toimintamme/satelliittipaikannus**

# Yhteistyö ja tiedonjako

## Tiedonvaihtoryhmien tilannetietoisuus ja tiedonvaihto on yhä parempaa

Tiedonvaihtoryhmiemme jäsenistä muodostuu lähes 300 toimijan kansallinen verkosto, jonka ydintehtävänä on jakaa kyberturvallisuuteen ja -uhkiin liittyvää toimialakohtaista tietoa ja kokemuksia.

Luottamusverkostojen toiminta on vakiintunut ja laajentunut vuosittain, niin myös 2020. Etenkin Liikenne ja logistiikka-alan tiedonvaihtoryhmän toiminta asettui uomiinsa, ja verkostoon liittyi uusia jäsenorganisaatioita.

Tiedonvaihtoryhmien edellisvuosista kehittynyt kyberturvallisuuden tilannetietoisuus ja tiedonvaihto antoivat myös meille paremmat mahdollisuudet havaita ja huomioida alakohtaisia kyberturvallisuuden erityispiirteitä.

Ryhmiltä saatu tieto on merkittävässä roolissa kansallisen kyberturvallisuuden tilannekuvan koostamisessa. Lisäksi ryhmillä on tärkeä tehtävä häiriötilanteiden hallinnassa ja toimialojen kyberturvallisuuden edistämisessä.

## Etätyöratkaisut, pilvipalvelut ja tiedonhallintalaki pöydällä

Myös tiedonvaihtoryhmissä etätyöratkaisujen toimivuus ja turvallisuus sekä etäympäristön valvontaratkaisut olivat paljon esillä. Lisäksi keskusteltiin videoneuvotteluratkaisujen tietoturvasta, pilvipalveluiden tietoturvallisesta käytöstä ja organisaation toiminnan ja tietojärjestelmien saattamisesta tiedonhallintalain mukaisiksi.

Kehitämme yhteistyössä ryhmien kanssa muun muassa häiriötilanteiden hallintaan liittyvää harjoitustoimintaa. Viime vuonna toteutettiin telealan toimijoiden tiedonvaihtoryhmän (ISP-ISAC) pilottiharjoitus. Vuonna 2021 tukemaamme luottamusverkostojen harjoitustoimintaa tullaan laajentamaan. Lisää harjoitustoiminnasta voit lukea sivulta 28.

**Tiedonvaihtoryhmä**, englanniksi Information Sharing and Analysis Center eli ISAC. Ryhmät ovat eri toimialoille perustettuja ja luottamukseen perustuvia kyberturvallisuuden yhteistyöelimiä.

**Kyberturvallisuuskeskuksen tiedonvaihtoryhmiä:**

- Valtionhallinto
- Finanssi
- Vesihuolto
- Teleyritykset (ISP)
- Sote
- Energia
- Kemia ja metsäteollisuus
- Elintarvike, kauppa ja jakelu
- Media
- Logistiikka ja liikenne

## Vuoden onnistumisia

Moni kotimainen ja kansainvälisen tietoturvayhteisö siirsi useita perinteisiä tietoturvakonferenssejaan virtuaalisiksi. Edulliset virtuaalitapahtumat tarjosivat etenkin pienten suomalaisyritysten tietoturvavastaaville ainutlaatuisen mahdollisuuden päästä seuraamaan ajankohtaisen ja korkeatasoisen tietoturvatutkimuksen tuloksia. Toivottavasti tapa jatkuu tavalla tai toisella tulevinakin vuosina.

## Verkko- ja tietoturva-direktiivin vaikutukset ja yhteistyö

Verkko- ja tietoturvadirektiivi, NIS, täytti neljä vuotta. Direktiivillä säännellään yhteiskuntamme kriittisiä toimialoja ylläpitävien palveluntarjoajien verkkojen ja tietojärjestelmien tietoturvallisuutta, riskienhallintaa ja varautumista sekä velvoitetaan keskeisiä palveluntarjoajia raportoimaan tietoturvahäiriöistä. Kyseessä on ensimmäinen kriittisten toimialojen kyberturvallisuutta yhteisesti sääntelevä direktiivi, jota parhaillaan uudistetaan. Meillä NIS-direktiivin vaikutukset ovat näkyneet parhaiten kriittisillä toimialoilla, joissa tietoturvatietoisuus on lisääntynyt. Silti osaamisessa ja valvonnassa on edelleen puutteita.

Direktiivi toi useille toimialoille vaatimuksen raportoida merkittävistä tietoturvahäiriöistä.

Merkittävin tapaus vuonna 2020 oli terveydenhuoltosektorin Vastaamo-tietomurto. Tapaus johti muutoksiin tietoturvallisuuden sääntelyssä ja toimiin tietoturvallisuuden ja tietosuojan parantamiseksi. Liikenne-ja viestintäministeriö asetti marraskuussa poikkihallinnollisen työryhmän, jonka tehtävänä on kartoittaa yhteiskunnan toiminnan kannalta keskeisten toimialojen tietoturvaa ja tietosuojaa koskevan lainsäädännön muutostarpeita.

## Yksin lakiteksteillä ei nosteta tietoturvan tasoa

Mikään lainsäädäntö ei yksin lisää verkkojen tai tietojärjestelmien tietoturvaa. Yritysten on otettava riskienhallintaa ja tietoturvaa parantavat prosessit ja toimet osaksi päivittäistä liiketoimintaansa. Valvovien viranomaisten on taas pidettävä huolta, että yritysten toiminta sekä järjestelmien laatu ovat lainmukaisia. Tarkentavat ohjeet, suositukset ja viranomaismääräykset auttavat toimijoita oikeaan suuntaan, niitä kaivattaisiin lisää Suomessakin.

NIS-direktiivi on ensimmäinen EU-tason säädös, jonka tavoitteena on nostaa tietoturvan tasoa kriittisillä toimialoilla kaikkialla Euroopassa. Kyse on pitkäjänteisestä työstä, joka vaatii ensisijaisesti johdon sitoutumista, mutta myös aktiivista vuoropuhelua yksityisen ja julkisen sektorin välillä sekä viranomaisten tiivistä yhteistyötä.

**Häiriöilmoituslomake merkittävistä verkko- ja tietojärjestelmähäiriöistä yhteiskunnan kriittisten sektoreiden toimijoille:**

www.kyberturvallisuuskeskus.fi/fi/ilmoita

# Koronakriisi sähköisti kansainvälistä kyberturvallisuusyhteistyötä

Toimimme Euroopan unionin CSIRT-verkoston puheenjohtajana kauden 1.1.2019–31.6.2020. Verkosto toimi tehostetusti ja seurasi koronatilanteen kyberturvallisuusvaikutuksia 18.3.–6.5.

Merkittävimmät havainnot liittyivät etätyöjärjestelyjen tietoturvaan, etäyhteyskapasiteetin riittävyyteen ja koronateeman käyttöön tietojenkalastelu- ja haittaohjelmakampanjoissa. Sairaalat ja tutkimuskeskukset olivat selvästi erityishuomion kohteina. Tehostetun toiminta-ajan jälkeen pandemian kyberturvallisuusvaikutusten kansainvälistä tilannetta on seurattu normaalissa yhteistyössä.

Korona on näkynyt kaikessa kansainvälisten yhteistyöverkostojemme yhteistyössä. Toiminta on yleisesti jäntevöitynyt ja tiivistynyt.

Useissa kansainvälisissä yhteisöissä turvallisuusluokitellun tiedon vähimmäissuojauksista ei ole haluttu joustaa, vaikka toimintatapa on osin hidastanut yhteistyötä. Tosin poikkeusaika on myös nopeuttanut turvallisuusluokitellun tiedon tietojenkäsittely-ympäristöjen suunnittelu-, toteutus- ja hyväksyntäprosesseja.

# Harjoittelulla lisää toimintavarmuutta

Harjoitustoiminta on yksi keskuksemme peruspalveluista. Tuemme huoltovarmuuskriittisten organisaatioiden kyberharjoittelua, osallistumme kansallisiin kyberharjoituksiin ja yhteistoimintaharjoituksiin sekä kehitämme harjoittelua tukevia työkaluja.

Eduskunnan käyttöönottama valmiuslaki ja etätyökehotukset muuttivat kyberharjoitustoimintaa. Aiemmin valtaosa jatkuvuuden hallinnan kyberharjoituksista järjestettiin lähityöskentelytapahtumina. Koronan vuoksi harjoitusten järjestäjien ja palvelun-tuottajien piti kehittää lyhyessä ajassa uudet harjoitustoiminnan mallit, joissa huomioidaan muun muassa etätyöskentely ja organisaatioiden epävarmat tulevaisuudennäkymät.

Myös lähitulevaisuudessa vastaamme huoltovarmuuskriittisten organisaatioiden harjoitustarpeisiin, mutta panostamme myös palveluidemme skaalautuvuuteen, jotta mahdollisimman moni kyberharjoittelusta kiinnostunut hyötyisi niistä. Saamamme palautteen perusteella teimme palveluidemme tarpeista esiselvityksen, jonka tulokset valmistuvat keväällä 2021.

**Martti Setälä, Insta Digital Oy:**

”Heittäydy rohkeasti etäharjoittelun maailmaan, se palkitsee.

**Antti Nyqvist, Huoltovarmuusorganisaation Digipooli:**

”Etäharjoitukseen on helpompi saada enemmän pelaajia.

**Anu Laitila, Nixu Oyj:**

”Osallista kaikkia harjoituksen aikana mahdollisimman tasapuolisesti ja testaa tekniikka ennen harjoitusta.

# Tietoturvamerkki

Kuluttajien älylaitteille tarkoitettu Tietoturvamerkki julkaistiin marraskuussa 2019 kolmen pilottituotteen voimin. Merkki on ensimmäinen viranomaisen myöntämä laatuaan maailmassa ja herätti heti alusta pitäen kansainvälistä kiinnostusta.

Uusia merkkejä myönsimme kuusi. Joukkoon sisältyi myös kaksi sovellusta. Näistä toinen on 2,5 miljoonaa latauskertaa kerännyt Koronavilkku, mikä myös kasvatti tietoisuutta Tietoturvamerkistä. Kansainvälistä näkyvyyttä toi myös Signifyn Philips Hue -älyvalaisinjärjestelmälle myönnetty Tietoturvamerkki.

## Tietoturva-merkin kehitys

Tutkimuksemme osoittavat, että Tietoturvamerkin uskottavuus perustuu siihen, että sen myöntää luotettava viranomainen. Näin tulee tapahtumaan myös jatkossa, ja Traficom myös omistaa merkin. Kysynnän lisääntyessä on tärkeää varmistaa saatavuus, siksi teknisiä tarkastuksia ollaan ulkoistamassa kaupallisille toimijoille. Niistä ensimmäiset aloitettiin loppuvuodesta 2020. Sekä kotimaiset että kansainväliset tietoturvayritykset ovat olleet kiinnostuneita tarkastusten tekemisestä.

Kun Tietoturvamerkki julkaistiin, sen vaatimukset perustuivat ETSIn tekniseen spesifikaatioon. Siihen perustuen julkaistiin maailman ensimmäinen virallinen IoT-standardi kesäkuussa 2020. Myös Tietoturvamerkin vaatimukset päivitettiin vastaamaan uunituoretta standardia. Ennen standardin julkaisemista myönnetyt Tietoturvamerkit päivitetään vuosikatselmoinnin yhteydessä.

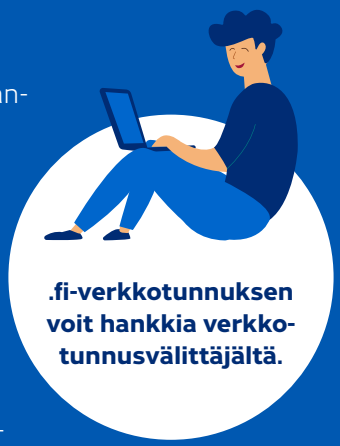
# Maksuton Traficom Anycast -palvelu parantaa .fi-tunnusten toimintavarmuutta

Vuonna 2020 otimme käyttöön Traficom Anycast -nimipalvelun .fi-verkkotunnusten toimintavarmuuden parantamiseksi. Tarjoamme sitä toissijaisena nimipalveluna .fi-verkkotunnusten välittäjille – maksutta – nyt ja tulevaisuudessa. Lokakuisessa Traficom Anycast -webinaarissamme kerroimme palvelusta ja sen hyödyistä verkkotunnusvälittäjille.

Traficom Anycast -palvelu perustuu Canadian Internet Authorityn (CIRA) ylläpitämään anycast-verkkoon, jota pidetään yhtenä maailman laadukkaimmista palveluista.

Palvelu tuo lisäturvaa ja tarjoaa laite-, ohjelmisto- ja reitityskokoonpanon, jonka avulla nimipalvelut sietävät muun muassa hajautettuja palvelunestohyökkäyksiä aiempaa paremmin.

Anycast-tekniikka on laajasti käytössä internetin juurinimipalvelussa sekä .fi-juurinimipalvelussa, mutta .fi-verkkotunnuksille määritellyissä nimipalvelimissa anycast-tekniikan lisäturvaa ei pääsääntöisesti hyödynnetä.



**.fi-verkkotunnuksen voit hankkia verkkotunnusvälittäjältä.**

Nimipalvelun vikaantuminen ei lamauta pelkästään digitaalisia palveluita, vaan pahimmillaan myös kaiken tavaraliikenteen ja palvelutuotannon. Tästä syystä nimipalvelun toimintavarmuuteen ja tietoturvaan on syytä kiinnittää huomiota.

Lisätietoja Traficom Anycast -palvelun käyttöönotosta saa omalta verkkotunnusvälittäjältä tai meiltä osoitteesta **fi-domain-tech@traficom.fi**.

**Nimipalvelu eli domain name system, DNS, on internetin järjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi. Nimipalvelun ansiosta numeeristen osoitteiden sijaan voidaan käyttää helpommin muistettavia nimiä.**

**Maailmankartalla anycast-verkon solmukohdat sijoittuvat Pohjois-Amerikkaan, Eurooppaan ja Aasiaan.**

# Oppien avulla turvallisempaa 5G:tä

Vuonna 2019 olimme mukana järjestämässä maailman ensimmäistä 5G:n tietoturvaan keskittynyttä hakkeritapahtumaa 5G Cyber Security Hackathonia. Helmikuussa 2020 5G Leading Edge Forumissa hackathonin haasteen asettajat jakoivat kokemuksiaan hakkeritapahtumasta. Kävi selväksi, että ilman hackathonia olisimme jääneet paitsi tiedosta, jonka avulla 5G-tuotteiden turvallisuutta on mahdollista yhä parantaa.

Loppuvuodesta 2020 – hackathonin oppien perusteella – lähdimme laatimaan 5G Standalone -verkkojen referenssiarkkitehtuuria. Tarkoituksemme on kuvata parhaat arkkitehtuurilliset ja ylläpitoprosesseihin liittyvät menetelmät, joilla voidaan operoida 5G-verkkoa tietoturvallisesti. Referenssiarkkitehtuurilla haluamme vastata yleisiin teknisiin uhkiin, joita 5G-verkkoihin tulee kohdistumaan.

Referenssiarkkitehtuurityön tuloksia tullaan testaamaan vuoden 2021 5G Cyber Security Hackathonissa, jossa hakkerit pääsevät testaamaan laadittuja menetelmiä todellisessa verkkoympäristössä. Referenssiarkkitehtuuri tullaan julkaisemaan dokumenttina, joka on kaikkien operaattoreiden ja valmistajien vapaasti käytettävissä.

# KYBER 2020 ja uudistettu HAVARO-palvelu

Vuonna 2020 Huoltovarmuuskeskuksen KYBER 2020 -ohjelma vietiin onnistuneesti päätökseen. Ohjelmaan liittyvät hankkeet, muun muassa harjoitustoiminta, Kybermittari ja KYBER-terveys, saatiin maaliin. Myös uudistunutta HAVARO-palvelua veimme eteenpäin.

Palvelun uudessa mallissa kaupalliset palvelukeskukset (SOC) tuottavat HAVARO-palvelua asiakkailleen yhteistyössä kanssamme.

Pilotoimme uutta palvelumallia koko vuoden usean palvelukeskuksen ja heidän asiakkaidensa kanssa. HAVARO-palvelun kaupallinen käyttöönotto tapahtuu vuoden 2021 aikana.

Vuonna 2021 käynnistämme Kyberilmasto-hankkeen, jonka tavoitteena on kehittää kykyämme hyödyntää dataa ja informaatiota kansallisen kyberturvallisuuden tilannekuvan muodostamiseksi, uusien palveluiden ja toimintamallien synnyttämiseksi ja kyberturvallisuusuhkiin ja -poikkeamiin vastaamiseksi.


HAVARO

# Kybermittari – Uusi työkalu johdolle kyberuhkien hallintaan

Lokakuussa julkaisemamme Kybermittarin tavoitteena on parantaa organisaatioiden ja lopulta koko yhteiskunnan kyberuhkien torjuntakykyä.

Kybermittarin avulla organisaatio saa näkymän, jossa erottuvat tärkeät kyberturvallisuuden eri osa-alueet tavoitteineen ja niiden kypsyystasot. Kybermittari näyttää, millä tasolla on organisaation kyberriskien tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen. Mittari antaa myös tietoa mahdollisista kehityskohteista, vertailutietoa sekä yhteisen kielen, jolla keskustella kyberturvallisuudesta ja sen kehittämisestä.

Lokakuussa Huoltovarmuuskeskus julkaisi myös Kyberturvallisuus eri toimialoilla -kartoituksen tuloksia. Sen pohjana käytettiin Kybermittarin suomenkielistä kehitysversiota. Keskeisin havainto oli: Jos johto sitoutuu ja ohjaa kyberstrategiaa osana yrityksen kokonaisstrategiaa ja riskienhallintaa, yritys on paremmin varautunut kyberhyökkäyksiin ja selviää niistä.

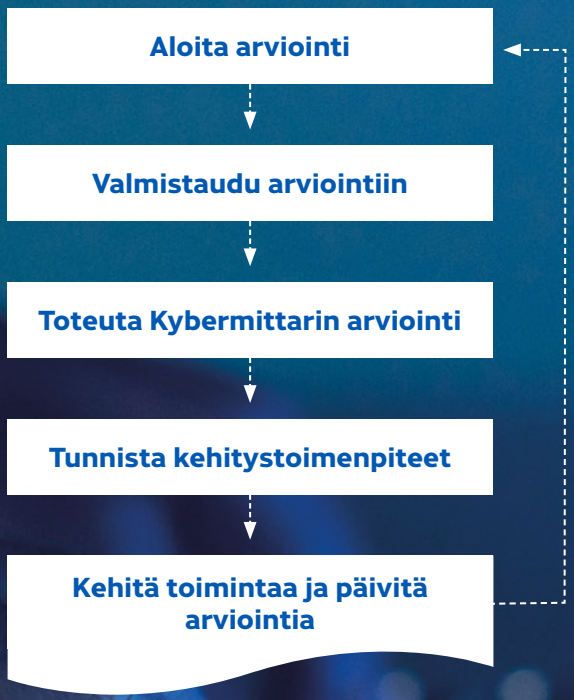
Tarvittaessa yritysjohto voi saada Kybermittarin avulla arvokasta tietoa siitä, miten oma kyberriskeihin varautuminen vertautuu oman toimialan keskiarvoon tai muihin mittauksen tehneisiin kumppaneihin. Kybermittarin avulla voi saada näkyväksi myös oman toimitusketjun kypsyystason.

# Mittarin mahdollisuudet ovat monet: Luottamuksellisesta tiedonjaosta kansalliseen kyberturvallisuuteen

Halutessaan organisaatiot voivat jakaa Kybermittarin avulla tuottamansa arviointitulokset luottamuksellisesti keskuksemme kanssa. Näiden tulosten perusteella voimme laatia anonymisoituja referenssi- ja suositustasoja, joita voimme tarjota organisaatioille tukemaan Kybermittarin käyttöä ja kyberturvallisuuden kehitystä. Tätä tilannekuvaa voimme myös käyttää kansallisten toimenpiteiden suunnittelussa ja ohjauksessa. Lisäksi voimme hyödyntää tuloksia luottamuksellisesti lakisääteisiin tehtäviimme ja siten parantaa tilannekuvaa. Kybermittarista saat lisätietoja verkkosivuiltamme.

**www.kybermittari.fi**

**KYBERMITTARIN ARVIOINTIPROSESSI:**






”Jos johto sitoutuu ja ohjaa kyberstrategiaa osana yrityksen kokonaisstrategiaa ja riskienhallintaa, yritys on paremmin varautunut kyberhyökkäyksiin ja selviää niistä.

# Toimintamme tunnuslukuja

Lukujen perusteella poikkeusvuotemme oli hektinen. Haitallisten sivujen alasajot ja käsittelemiemme tapausten määrät kaksinkertaistuivat edellisvuoteen verrattuna. Someseuraajiemme joukko kasvoi ja tilannekuva-tuotteisiimme oltiin tyytyväisiä.

**1**
Varoitukset

**24/7/365**
Katkeamaton päivystys

**115 000**
Autoreporter

**13 353**
Twitter-seuraajat

**24**
Haavoittuvuus-koordinaation käsitte-lemät tapaukset

**8 500**
Haitallisten sivustojen alasajot

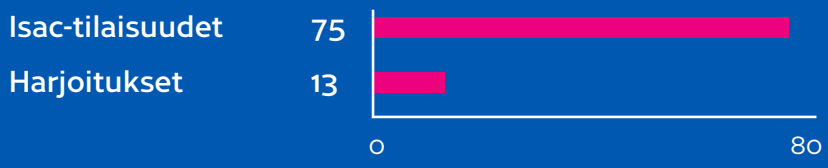
**10 892**
Käsitellyt tapaukset

**6 066**
Facebook-seuraajat

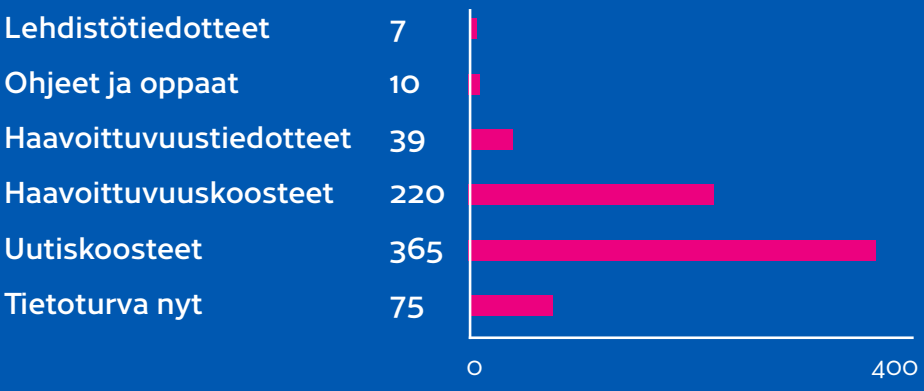
## Häiriömäärät

| 4 | 12 | 51 | 67 |
|---|---|---|---|
| Kriittiset häiriöt | Vakavat häiriöt | Merkittävät häiriöt | Kaikki häiriöt yhteensä |

## Tilaisuudet ja harjoitukset




## Viestintä ja tiedotteet




Toteutimme vuoden aikana asiakastyytyväisyyskyselyt tilannekuvatuotteisiimme ja tiedonvaihtoryhmiimme liittyen. Kyselyidemme arviointiskaala oli huonosta (1) kiitettävään (5).

4,4

Hyödyllisyys

### Tilannekuvatuotteisiimme ollaan tyytyväisiä

4,2

Keskiarvo

### Kysely toimialojen tiedonvaihtoryhmille

4,5

Arvosana

# Kybersää 2020 ja katse vuoteen 2021

## 10 tietoturvanäkymää vuodelle 2021

### 1. Myös vuonna 2021 tapahtuu jotakin ikävää

Monen organisaation riskienhallinta ei pysy digitalisaation vauhdissa. Ratkaisuja otetaan käyttöön sokkona ilman, että niiden aiheuttamia riskejä arvioidaan, saati ymmärretään. Lopputulos saattaa olla surkea niin kansalaisen, organisaation itsensä kuin koko yhteiskunnan kannalta. Kybervuosi 2020 oli ikävä, mutta ennustamme synkkiä pilviä myös tulevalle vuodelle.

### 2. Lisää sääntelyä, lisää vakautta

Sateiseen kybersäähän halutaan jo poutaa. Kyberturvallisuusriskejä pyritään hallitsemaan yhä enemmän kansallisella ja ylikansallisella sääntelyllä. Vaatimukset lisääntyvät erityisesti yhteiskunnan toiminnan kannalta keskeisillä aloilla. Myös datalla, muun muassa ihmisten terveystiedoilla, tehtävää kauppaa halutaan rajoittaa sääntelyn keinoin. Tämä saattaa johtaa jopa suurten teknoyritysjättien pilkkomiseen pienemmiksi palasiksi.

### 3. Aidon ja väärennetyn erottaminen vaikeutuu entisestään

Deepfake ja muut tekoälyyn nojautuvat ratkaisut tarjoavat mahdollisuuden hämärtää informaatioympäristöämme entisestään. Populistit ja kansainvälisen politiikan kiistapukarit käyttävät mahdollisuutta armotta hyväkseen.

### 4. Osaamisen saaminen riittävälle tasolle kestää vielä pitkään

Digitaalisen yhteiskunnan tarvitsemien ammattilaisten kysyntä kasvaa. Tämä pätee myös tietoturva- ja tietosuojaosaajiin. Tarve on tunnistettu ja suunta koulutuksen kehittämisessä on oikea, mutta muutos tapahtuu hitaasti.

### 5. Rikolliset tahkovat virtuaalivaluuttaa kyberhyökkäyksillä

Suomessa nähdään yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet ovat pikkuvaluuttaa. Erityisen merkittävä uhka on kiristyshaittaohjelmahyökkäykset, joiden kohteeksi voi joutua kuka tahansa pienestä konepajasta kansainväliseen high tech -jättiin.

## 6. Etätyö tuli jäädäkseen – niin myös riskit

Vuonna 2020 siirryttiin kiireen vilkkaa etätyö-moodiin. Osa toimijoista rakensi etätyöjärjeste-lynsä kiireessä kirjavien viritysten varaan. Tämän massan kuntoon laittamisessa kestää vielä pitkään.

## 7. Kilpailu kvantinkestävästä salauksesta kiihtyy

Kvanttitietokoneet ovat vuonna 2021 taas askeleen kehittyneempiä. Tietoturvateollisuus varautuukin kiivaasti kvanttitietokoneiden aikaan. Kvantinkestävät salaustuoteratkaisut lisääntyvät tasaisesti.

## 8. Teknologinen suurvalta-kilpailu kiihtyy

Teknologisen suurvaltakilpailun vaikutukset yltävät myös puhelin- ja sovelluskauppojen hyllyille. Kiinalaisvalmisteinen Huawei vs. amerikkalainen iPhone – millaisia tekniikoita ja sovelluksia näissä laitteissa voi jatkossa käyttää?

## 9. Kybervaikuttaminen valtioiden välillä jatkaa kasvuaan

Kyberhyökkäykset, disinformaation levittäminen ja hybridivaikuttaminen lisääntyvät. Kyberympäristössä vaikuttaminen ja hyökkääminen on verkossa usein halvempaa ja huomaamattomampaa kuin fyysisessä maailmassa.

## 10. Kyberturvallisuus on vihdoin johdon agendalla

Vastaamon tapaus nosti kyberturvallisuuden ja tieto-suojan johdon agendalle. Kehittäminen edellyttää kuitenkin pitkäjänteisyyttä, sillä kyberturvallisuus-uhat muuttuvat jatkuvasti. Kybermittarimme on erinomainen työkalu, jonka avulla saa nopeasti johdolle yleiskuvan organisaation kyberkyvyk-kyyksien tasosta.

# Vuoden 2020 kybersää

## Tammi

Määräys 66 teletoiminnan häiriötilanteista astui voimaan.

Valtioiden lisäksi myös yrityksiä vakoillaan.

## Helmi

**Office 365:** Käyttäjätunnusten kalastelu jatkuvaa, tietomurrot lisääntyvät.

**Teknisen tuen huijauspuhelut:** Suomalaiset saaneet satoja tuhansia soittoja. Tapausten määrä lisääntyi räjähdysmäisesti.

**Varmennehäiriöt:** Microsoft unohti uusia varmenteensa, mikä aiheutti häiriöitä Teams-palveluissa.

EKANS – 1. automaatiojärjestelmiin kohdistettu kiristyshaittaohjelma havaittu maailmalla.

## Maalis

**Korona:** Olemattomia korona-suojaimia ja -testipaketteja kaupan. Ihmisten hätää hyödynnetään haittaohjelmien levityksessä, huijauksissa ja vakoilussa.

**Teknisen tuen huijauspuhelut:** Soitot loppuivat 24.3.

Tietovuotoja eri kanta-asiakas-järjestelmissä. Myös suomalaisten tietoja päätyi vääriin käsiin.

## Huhti

**Korona:** Rokotetutkimus mahdollisena vakoilukohteena.

Telian internetyhteyshäiriö 25.4.

## Touko

**Posti-huijaukset:** Postin nimissä lähetetty tuhansia tilausansaan, kalasteluun tai haittaohjelmaan johtavia tekstiviestejä.

**Kiristyshyökkäykset:** Kiristäjät huutokauppasivat varastamiaan tietoja.

Sandworm-ryhmä pyrki tunkeutumaan haavoittuviin Exim-sähköpostipalvelimiin jo 2019/08.

Kiristyshaittaohjelmahyökkäys kotimaiseen kriittisen infrastruktuurin järjestelmään.

## Kesä

**Teknisen tuen huijauspuhelut:** Soitot alkoivat taas.

EKANS-haittaohjelmahyökkäykset kohdistettiin Hondaan ja ENEL Groupiin.

Useita kriittisiä haavoittuvuuksia, jotka vaikuttivat muun muassa VPN-palveluiden tietoturvallisuuteen.

Huippulukemat: 12 merkittävää viestintäverkkohäiriötä, joista 3 aiheutti Päivö-myrsky.

= Kansainvälinen uutisnosto

**Teknisen tuen huijauspuhelut:** Soitot jatkuvat yhä. Suomeen satoja tuhansia puheluja.

**Varmennehäiriöt:** DigiCert mitätöi useita varmenteita 11.7. Vaikutti useiden suomalaisten palveluiden toimintaan.

Havaintoja suomalaisista murretuista ja haavoittuvista VPN-ohjelmistoihin liittyvistä palvelimista.

Runsaasti kriittisiä haavajulkaisuja. Verkkolaitteiden turva-aukkoja hyödynnettiin roimasti.

EU asetti 1. kertaa pakotteita valtiollisia kyberhyökkääjiä vastaan.

Uusi kiristyshaittaohjelmien aalto. Maailmalla useita havaintoja terveysalaan kohdistuneista kiristyshyökkäyksistä.

Zerologon-haavoittuvuutta hyödynnetään aktiivisesti.

Aila-myrsky: 9 merkittävää toimivuushäiriötä, jotka saatiin hallintaan pian.

Havainnot palvelunestohyökkäyksillä uhkailusta lisääntyivät.

**Office 365:** Lisää tietomurtoja, murretuista sähköpostilaatikoista lähetetään kalasteluviestejä.

Emotet-tapausten määrä on vähentynyt, siitä tehty varoitus poistettiin.

Tietovuoto Virossa, kohteena useita ministeriöitä.

Tietoturvayritys FireEye ja Euroopan lääkevirasto vakoilun kohteina.

## Heinä

## Elo

**VAROITUS 1/2020:** Emotet-haittaohjelmaa levitetään Suomessa aktiivisesti.

Norjan parlamentti tietomurron kohteena. Norja syytti kyberhyökkäyksestä Venäjää.

1. virallinen standardi IoT-kuluttajalaitteiden tietoturvallisuudesta julkaistiin.

Maailmanlaajuinen CenturyLinkin häiriö 30.8. Koko internet-liikenteen volyymi laski 2 %.

## Syys

## Loka

**Office 365:** Tunnuksia kalasteltu uskottavilla Zoom-kokouskutsuilla.

**Psykoterapiakeskus Vastaamo:** Yritystä ja asiakkaita kiristettiin uhkaamalla julkaista potilas- ja henkilötietoja.

Ilmoituksia laajavaikutteisista palvelunestohyökkäyksistä, jotka näkyivät myös palveluiden toimivuudessa.

## Marras

## Joulu

SolarWinds-hallintatyökalusta löytyi takaovi – mahdollisuus tietomurtoon ja vakoiluun.

Kotiturvalistit – tietoturvan kansalaiskampanja alkoi.

Eduskunnan tietomurto uutisissa.

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 978-952-311-744-0
ISSN 2669-8757

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus