



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Syyskuu 2021

#kybersää

Kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tämä tuote on ensisijaisesti suunnattu tietoturvasta vastaaville henkilöille. Lukija saa nopean kokonaiskuvan siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:



rauhallinen



huolestuttava



vakava

Kybersää syyskuu 2021



Tietomurrot ja -vuodot

- ▶ Suomalainen pörssiyhtiö Adapteo kertoi syyskuun alkupuolella tietomurrosta.
- ▶ Hakkeriforumilla oli myynnissä suomalaisten organisaatioiden palomuurien ylläpitotunnuksia.



Huijaukset ja kalastelut

- ▶ Pankkitunnuksia ja maksutietoja kalastellaan aktiivisesti kaikkien pankkien nimissä sekä sähköpostitse että tekstiviesteillä.
- ▶ Verkkopankkien lisäksi Omakannan hakutuloksia on väärennetty hakukoneisiin osoittamaan kalastelusivuille.



Haaitaohjelmat ja haavoittuvuudet

- ▶ Julkaisimme uuden sivun, josta voi lukea lisätietoja Autoreporter-järjestelmän yleisimmistä haaitaohjelmahavainnoista.
- ▶ Microsoftin autodiscovery-toiminnon haavoittuvuutta käytettiin hyväksi.



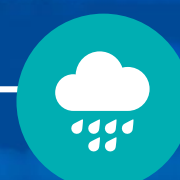
IoT ja automaatio

- ▶ Traficomien Kyberturvallisuuskeskus ja Singaporen kyberturvallisuusvirasto julkaisivat yhteistyön IoT-tietoturvamerkkien vastavuoroisesta hyväksynnästä.
- ▶ Uusia IoT-haavoittuvuuksia löytyi, myös teollisuusautomaation haavoittuvuuksien määrä on kasvussa.



Verkkojen toimivuus

- ▶ Kotimaassa oli kaksi merkittävää verkkojen toimivuushäiriötä.
- ▶ Facebookin ongelmat vaikuttivat myös Instagramin ja WhatsAppin käyttöön useamman tunnin ajan.
- ▶ Palvelunestohyökkäykset vaikuttivat syyskuussa jonkin verran palveluiden saatavuuteen.



Vakoilu

- ▶ ProxyShell-hyökkäys uhkaa paikallisesti ylläpidettyjä Microsoft Exchange -palvelimia.
- ▶ Saksa ja EU syyttävät Venäjää nk. Ghostwriter-toiminnasta.
- ▶ Suojelupoliisin mukaan Suomeen kohdistuu jatkuvia kybervakoilu-yrityksiä.

Kuukauden tunnuslukuja



6

Syyskuun aikana julkaistiin kuusi haavoittuvuustiedotetta.



8

Pankkikalastelussa rikoshyötynä menetetty määrä on vuonna 2021 jo yli kahdeksan miljoonaa euroa.



1

Traficomin Kyberturvallisuuskeskuksen ja Singaporen kyberturvallisuusviranomaisen (CSA) yhteistyö IoT-tietoturvamerkkien vastavuoroisesta hyväksymisestä.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon.

Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

2

Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta. Suomessa tullaan näkemään yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet eurot ovat pikkuvaluutta.

3



Pilvi on organisaatioille uutta ja pilven tietoturvan ymmärtävät parhaiten hyökkääjät.

Organisaatiot ovat siirtyneet vauhdilla pilvipalveluihin ja omaa ympäristöä ja sen kyvykkyyksiä ei ymmärretä tarpeeksi.

4



Toimitus- ja palveluketjujen tietoturva on yhä kriittisempää.

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä.

5



Etätyö tuli jäädäkseen – niin myös riskit.

Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.

Symbolit

Uusi



Päivitetty



1. Päivittämättömät haavoittuvuudet avaavat rikollisille reitin organisaatioon

Haavoittuvuuksien hyväksikäyttö on nopeaa. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja joiden suojaustoimet ja ylläpito ovat puutteellisia.

- ▶ Haavoittuvuus tarkoittaa mitä tahansa heikkoutta, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamiseksi. Haavoittuvuuksia voi olla esimerkiksi tietojärjestelmissä, sovelluksissa, laitteissa, prosesseissa, kotiautomaatiossa tai niitä voi aiheutua ihmisten toiminnan seurauksena.
- ▶ Vuonna 2020 siirryttiin kiireen vilkkaa etätyö-moodiin. Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.
- ▶ Rikolliset kehittävät hyväksikäyttömenetelmiä nopeasti heti ohjelmistopäivitysten ilmestyttyä ja tunnistavat kohteet, joita ei ole päivitetty. Erityisesti tietoturvaluotteissa olevat haavoittuvuudet ovat vakavia, sillä ne on yleensä sijoitettu muutenkin hyökkäyksille alttiisiin tietojärjestelmien kohtiin.
- ▶ Valtiolliset toimijat ovat tyypillisesti ensimmäisten joukossa hyödyntämässä uusia haavoittuvuuksia kybervakoiluun ja vaikuttamiseen. Valtiollisilla toimijoilla on myös riittävät resurssit päivitysten takaisinmallintamista varten uusien hyökkäysten mahdollistamiseksi kriittisissä ohjelmistoissa.

CASE

Microsoft tiedotti 2.3. Exchange-sähköpostipalvelimien kriittisistä haavoittuvuuksista ja niiden aktiivisesta hyväksikäytöstä. Kyberturvallisuuskeskus havaitsi suomessa aluksi lähes 300 haavoittuvaa Exchange-palvelinta. Mukana oli myös palvelimia, joihin oli jo murtauduttu haavoittuvuutta hyväksi käyttäen. Suomalaisten organisaatioiden haavoittuvat Exchange-palvelimet oli päivitetty huhtikuun alkuun mennessä. Organisaatioiden kyky reagoida kriittisiin haavoittuvuuksiin, päivityksiin sekä tietomurtojen tutkintaan nousi tärkeäksi osaksi Exchange-haavoittuvuuksien hoidossa.

2. Eri kyberhyökkäysmenetelmien käyttö kiristämiseen yleistyy ja uhkaavat liiketoiminnan jatkuvuutta

Suomessa tullaan näkemään yhä enemmän verkkohyökkäyksiä, joissa kymmenet tuhannet eurot ovat pikkuvaluuttaa.

- ▶ Erityisen merkittävä uhka on kiristyshaittaohjelmahyökkäykset, joiden kohteeksi voi joutua kuka tahansa pienestä konepajasta kansainväliseen high tech -jättiin.
- ▶ Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan takia.
- ▶ Kiristyshyökkäysten uutena ilmiönä kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.
- ▶ Toiminta on aktiivista ja kehittyy jatkuvasti.

CASE

Palvelunestohyökkäyksillä kiristäminen nousi maailmalla ilmiönä loppu-vuodesta 2020 ja ilmiö rantautui myös Suomeen. Kyberturvallisuuskeskus on saanut ilmoituksia myös vuonna 2021 aiheeseen liittyen.

Yleisesti organisaatio vastaanottaa kiristysviestin sähköpostitse, joka on allekirjoitettu näennäisesti tunnettujen haitallisten toimijoiden nimissä. Kiristysviestin lähettämisen aikoihin on joissain tapauksissa tehty myös palvelunestohyökkäys viestin tehostamiseksi. Viestissä kerrotaan organisaation kohtaavan suuren palvelunestohyökkäyksen, mikäli lunnaita ei makseta. Ohjeemme on ja pysyy: älä maksa kiristäjille.

3. Pilvi on organisaatioille uutta ja pilven tietoturvan ymmärtävät parhaiten hyökkääjät

Organisaatiot ovat siirtyneet vauhdilla pilvipalveluihin ja omaa ympäristöä ja sen kyvykkyyksiä ei ymmärretä tarpeeksi.

- ▶ Pilvipalveluratkaisuiden hahmottaminen on vaikeaa, koska ympäristö on laaja. Siirtyminen pilveen on jäänyt puolitiehen ja tietojärjestelmien migraatio on jäänyt viimeistelemättä. Vanhoja palveluita voidaan edelleen hyväksikäyttää.
- ▶ Aivan kuten perinteisessä tietoverkossa, mikäli hyökkääjä onnistuu pääsemään pilven reunalle, voi sen kautta levittäytyä myös organisaation muihin verkon segmentteihin pilven ulkopuolellakin.
- ▶ Tarve kehittää yleisesti hyväksytyt tietoturvavaatimukset pilvipalveluille.
- ▶ Suomessa pilven tietoturvavaatimuksia on lähestytty esim. PITUKRI <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/verkkosivuiltamme-neuvoja-pilvipalveluiden-turvalliseen-kayttoon>

CASE

Alkuvuonna 2021 laajamittainen Microsoft Exchange -sähköpostipalvelimien tietomurtoaalto pyyhkäisi myös Suomen yli. Tietomurtoaaltoa tutkittaessa paljastui, että kaikilla pilvipalveluiden käyttöön siirtyneillä organisaatioilla oli edelleen käytössään myös murrettavissa oleva perinteinen Exchange-sähköpostipalvelin. Osalla palvelin oli edelleen jossain marginaalisessa käytössä ja osalla se oli yksinkertaisesti unohdettu sulkea pilvimigraation lopuksi. Kaikkiin palvelimiin kuitenkin murtauduttiin. Tapaus on surullinen esimerkki siitä, kuinka loppumetreillä kesken jäänyt teknologiamuutos jättää ovet auki hyökkääjille.

4. Toimitus- ja palveluketjujen tietoturva on yhä kriittisempää

Alihankkijaketjun ymmärtäminen on organisaation oman kyberturvallisuuden kannalta keskeistä.

- ▶ Organisaatiot ostavat yhä enemmän palveluita ulkoisilta palveluntarjoajilta.
- ▶ Organisaatioiden olisi keskeistä ymmärtää omat alihankkijaketjunsä. On tärkeä ymmärtää kolmannen osapuolen tietoturvan taso. Esimerkiksi:
 - ▶ Konsultit ja heidän oman organisaation sisäiset järjestelmät.
 - ▶ Laitteistot ja palvelut joita voidaan käyttää joko osana omaa tuotetta tai palvelukokonaisuutena, tai ostettuna palveluna.
 - ▶ Organisaation tulee ymmärtää alihankinnanketju, myös alihankkija voi hankkia tuotteen/palvelun seuraavalta ketjussa olevalta palveluntarjoajalta.
- ▶ Organisaation tulisi kartoittaa, mistä osista sen eri palvelut muodostuvat, jotta ison kokonaisuuden voi hahmottaa. Erityisesti hankintavaiheessa tällaisen tekeminen on oleellista.
- ▶ On hyvä ymmärtää, että käytettävien palvelujen kautta voidaan murtautua organisaation, jos (kyber)turvallisuutta ei ole huomioitu.

CASE

Viime joulukuussa paljastunut Yhdysvaltojen hallintoon ja lukuisiin yrityksiin iskenyt SolarWinds-hyökkäys on merkittävä tietoturvatapaus. Tietomurron ja vakoilun mahdollistanut takaovi onnistuttiin levittämään tuhansiin organisaatioihin, joita oli myös Suomessa. Erilaiset toimitus- ja alihankintaketjut voivat mahdollistaa hyökkääjille keinon päästä huomaamattomammin varsinaiseen kohteeseensa tai saamaan samalla kertaa pääsyn laajaan kohdejoukkoon.

5. Etätyö tuli jäädäkseen – niin myös riskit

Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille. Ylläpitäjien on hyvä varmistaa etätyöntekijöiden laitteiden suojaukset ja palomuuriasetusten tarkoituksenmukaisuus.

- ▶ Vuonna 2020 siirryttiin kiireen vilkkaa etätöihin. Osa toimijoista rakensi etätyöjärjestelynsä kiireessä kirjavien viritysten varaan. Näiden väliaikaisten ratkaisujen kuntoon laittamisessa kestää vielä pitkään.
- ▶ Laaja siirtymä etätöihin näkyi maaliskuussa 2020 suojattomien laitteiden määrän selvänä kasvuna Suomen verkoissa. Verkkoon avoimilla laitteilla ja laitteiden suojattomilla etäyhteyspalveluilla tarkoitetaan tässä yhteydessä esimerkiksi avoimia etätyöpöytäyhteyksiä ja tiedostonjakopalveluja (esim. RDP, VNC ja SMB).
- ▶ Kesän 2021 jälkeen organisaatioissa ollaan todennäköisesti hybridiratkaisussa, jossa osa tekee töitä etänä ja osa toimistolla. Tässä tulee huomioida myös se, että koronan alussa tehdyt nopeat etätöyratkaisut tarkastellaan ja varmistetaan niiden tietoturvallisuus, jotta tietoturva huomioidaan ja voidaan taata pysyvämmässä mallissa.

CASE

Suojelupoliisin tiedote: Ulkomaiset tiedustelupalvelut käyttävät yritysten ja yksityishenkilöiden verkkoreitittimiä kybervakoiluun. Suojelupoliisi on havainnut, että suomalaista infrastruktuuria hyödyntävä kybervakoilu on lisääntynyt. Erityisesti autoritaaristen valtioiden tiedustelupalvelujen kybervakoiluoperaatioissa on käytetty hyväksi kymmeniä suomalaisten yksityishenkilöiden ja yritysten verkkolaitteita ja palvelimia liittämällä ne osaksi operaatiossa käytettävää infrastruktuuria.



Tietomurrot ja -vuodot

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



Tietomurrot ja -vuodot

- ▶ Suomalainen pörssiyhtiö kertoi tietomurrosta
 - ▶ Suomalainen kiinteistöyhtiö Adapteo tiedotti 6.9. joutuneensa tietomurron kohteeksi.
 - ▶ Tiedotteen mukaan kolmannen osapuolen tietomurto iski yhtiön järjestelmiin perjantaina 3. syyskuuta.
 - ▶ Isku vaikutti yhtiön palvelimiin ja liiketoiminnan ydinsovelluksiin, mutta tietomurron laajuus ei ole vielä selvillä.
 - ▶ Yhtiö kertoo tutkivansa ulkopuolisen kyberturva-asiantuntijan kanssa, mitkä tiedot ovat olleet tietomurron kohteena ja mihin toimenpiteisiin tietojen suojaamiseksi ja lisävahinkojen estämiseksi on ryhdyttävä.

Analyysi

- ▶ Kyberhyökkäykseen reagointia kannattaa harjoitella, jotta oikeassa tilanteessa toimintatavat ovat tuttuja.
- ▶ Kyberhyökkäys voi pahimmillaan lamauttaa liiketoiminnan kokonaan.
- ▶ Tietomurtojen torjunnan kannalta on erittäin tärkeää pitää järjestelmien ja laitteiden päivitykset ajan tasalla.
- ▶ Haavoittuvilla järjestelmillä on aina suurempi riski joutua tietomurron kohteeksi.



Tietomurrot ja -vuodot

- ▶ Hakkeriforumilla oli myynnissä suomalaisten organisaatioiden palomuurien ylläpitotunnuksia
 - ▶ Kyberturvallisuuskeskus sai kansainväliseltä yhteistyötaholta tiedon suomalaisten organisaatioiden ylläpitotunnusten myynnistä hakkerifoorumilla tarjolla olevassa kokoelmassa.
 - ▶ Mukana on noin kuusikymmentä eri organisaatiota, joiden Fortinet-palomuurien ylläpitotunnukset olivat päätyneet myyntiin.
 - ▶ Arviomme mukaan kaupattuja ylläpitotunnuksia voidaan käyttää esimerkiksi kiristyshaittaohjelmahyökkäysten valmisteluun.

Analyysi

- ▶ CISA julkaisi syyskuussa ohjeita VPN-laitteiden valintaan, koventamiseen sekä turvallisten etäyhteyksien ottamiseen.
- ▶ Lue lisää: <https://us-cert.cisa.gov/ncas/current-activity/2021/09/28/cisa-and-nsa-release-guidance-selecting-and-hardening-vpns>



Huijaukset ja kalastelut

Huijauksiin ja tietojenkalasteluun sisältyy käyttäjätunnusten ja salasanojen kalastelua, laskutuspetoksia, yrityshuijauksia, kiristyskiä ja muita vastaavia huijauksia. Lisäksi organisaatioihin voi kohdistua pankkitunnuskalastelua, maksukorttikalastelua ja muita geneerisiä yksittäisten uhrien huijauksia.



Huijaukset ja pankkikalastelut

- ▶ Pankkikalastelulla miljoonien rikoshyöty
 - ▶ Pankkitunnuksia kalastelemalla on viety rikoshyötynä suomalaisilta jo yli kahdeksan miljoonaa euroa vuonna 2021.
 - ▶ Poliisille on rekisteröity tänä vuonna yli 700 rikosilmoitusta pankkikalastelusta. Myös Kyberturvallisuuskeskukselle on kirjattu yli 900 ilmoitusta.
 - ▶ Verkkopankkien kirjautumistunnukset ovat rikollisille arvokasta riistaa, sillä rahan varastamisen lisäksi niitä voi käyttää myös vahvan tunnistautumisen välineinä.
 - ▶ Tunnistautumisvälineiden joutuminen väärin käsiin johtaa identiteettivarkauksiin.
- ▶ Erityisesti Nordean nimissä on kalasteltu pankkitunnuksia hyvin aggressiivisesti
 - ▶ Huijausviestien teemat ovat vaihdelleet tiheästi.

Analyysi

- ▶ Verkkopankkien lisäksi Omakannan hakutuloksia on väärennetty joihinkin hakukoneisiin. Selaimen osoitesivulle syötetty pelkkä pankin nimi tai vaillinainen verkko-osoite ei johdakaan oikealle verkkosivulle, vaan rikollisen väärentämään hakutulokseen.
- ▶ Väärennetty sivu voi näyttää pankin tai Omakannan oikealta kirjautumissivulta, mutta sinne syötetyt kirjautumistiedot menevät rikolliselle.
- ▶ Rikollinen syöttää hakukoneisiin linkkejä joko optimointimekanismeilla tai ostamalla hakukoneesta mainostilaa.



Huijaukset ja tietojenkalastelut

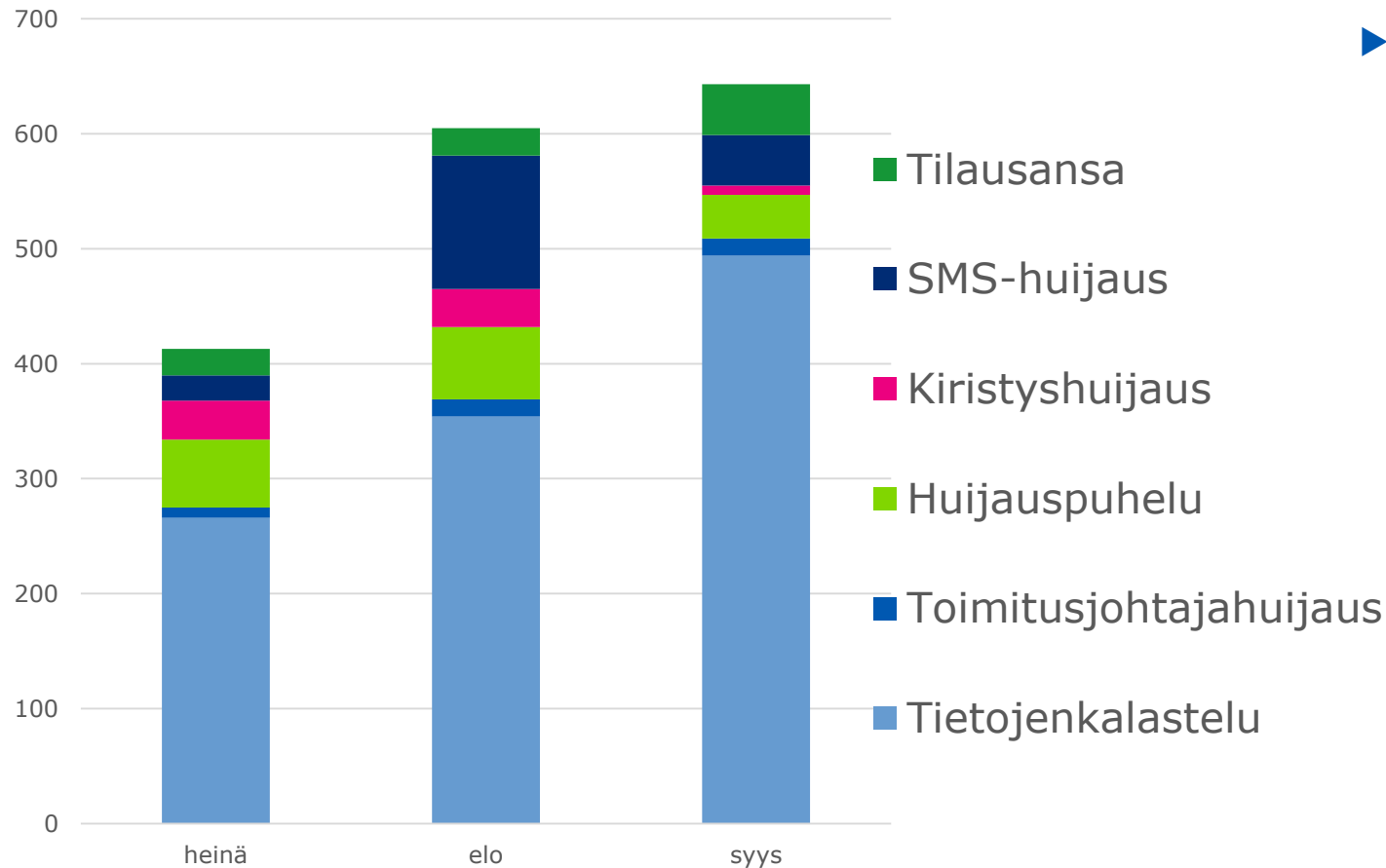
► Tietojenkalastelu jyllää voimakkaana

- Verkon myyntipaikkojen käyttäjiltä on kalasteltu maksukorttitietoja ja pankkitunnuksia.
- Vuosi sitten kiivaana riehunut Office 365 -tietojenkalastelu on hieman laantunut. Ilmoituksia tehdään edelleen huomattavasti, mutta ilmiö tuntuu olevan kurissa.
- Tilausansoihin on lähetetty tekstiviestejä K-markettien ja muiden päivittäistavarakauppojen nimissä.
 - Tilausansoja tehtailevat huijarit ovat ajan hermolla mainostamalla esimerkiksi Finnkinon nimissä lippuja uusimman James Bond -elokuvan näytöksiin.
- Lisäksi yrityksiä ja organisaatioita on lähestytty sekä toimitusjohtajahuijauksilla että sähköpostitilien kalastelulla.

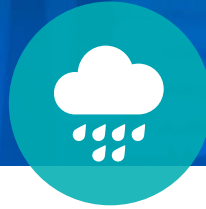
Analyysi

- Verkon kirpputoreilla ja myyntipaikoilla on raportoitu automatisoituja huijauksia.
- Osto-, myynti-, tai vuokraus-ilmoituksen laatineita käyttäjiä on lähestytty WhatsApp-viesteillä, jossa huijari väittää kiinnostuneensa ilmoituksen kohteesta ja olevansa valmis kauppoihin.
- Huijarin lähettämässä WhatsApp-viestissä on linkki, joka johtaa väärennetyille Postin sivuille.
- Väärennetyllä sivulla uhrilta kalastellaan maksukorttitietoja ja pankkitunnuksia.

Käsiteltyjä huijaustapauksia Q3/2021



- ▶ Vuoden 2021 kolmannen neljänneksen ilmiöitä ovat:
 - ▶ Tietojenkalastelutapauksia on ilmoitettu Kyberturvallisuuskeskukselle syksyn alettua merkittävästi kesää enemmän.
 - ▶ Tietojenkalasteluun pankkitunnusten kalastelu on aiheuttanut tasaista kasvua. Syyskuussa pankkikalasteluita ilmoitettiin 30 % enemmän kuin kesäkuukausina.
 - ▶ Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja järjestelmäpääsyn toivossa.



Haittaohjelmat ja haavoittuvuudet

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



Haittaohjelmat

- ▶ Autoreporterin 10 yleisimmän haittaohjelman kuvaukset
 - ▶ Sivulla esitellään yleisimpiä haittaohjelmia, joita Autoreporter-järjestelmämme on havainnut viimeisimmän vuosineljänneksen aikana.
 - ▶ Artikkelia päivitetään kerran vuosineljänneksessä mikäli kymmenen yleisimmän haittaohjelman joukkoon nousee uusi haittaohjelma.
 - ▶ Aiemmat havainnot jätetään myös näkyviin.
 - ▶ Ensimmäiset päivitykset on tehty vuoden 2021 kolmen ensimmäisen vuosineljänneksen osalta.
 - ▶ <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot>
 - ▶ Tilastoja on mahdollista tarkastella myös pidemmällä aikavälillä (ensimmäinen datapiste on vuodelta 2012), tätäkin sivua päivitetään vuosineljänneksittäin.
 - ▶ <https://www.traficom.fi/fi/tilastot/traficomin-haittaohjelmahavainnot>

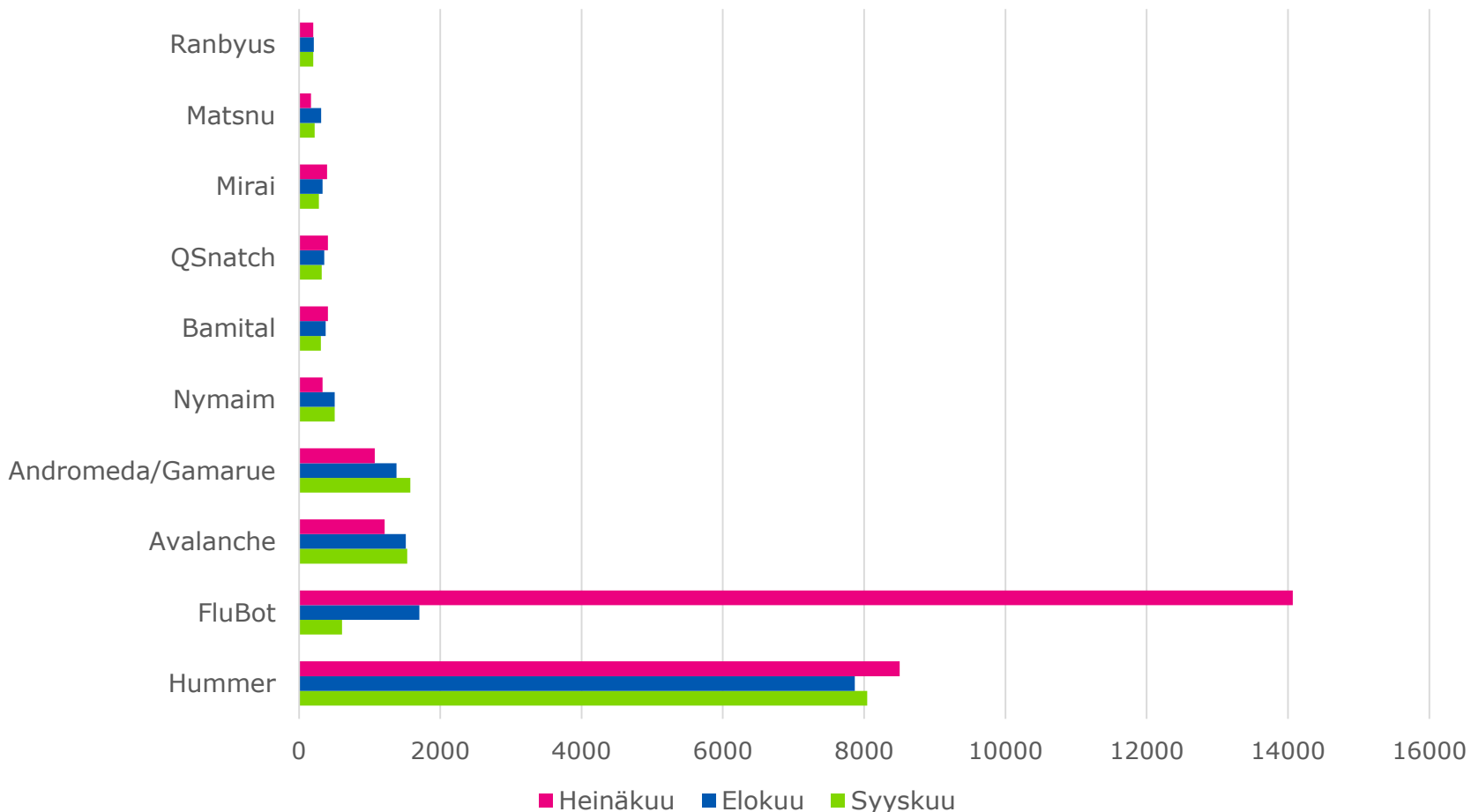
Analyysi

- ▶ Autoreporter-järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta.
- ▶ Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen.
- ▶ Sivuilla on mahdollisuuksien mukaan kuvattu haittaohjelmaa yleisesti, sen toimintaa, siihen varautumista ja mahdollista toipumista tartunnasta.

Autoreporterin haittaohjelmahavainnot



Haittaohjelmatyypit Q3/2021



Torjumme haittaohjelmia yhteistyössä teleyritysten kanssa Autoreporter-järjestelmän avulla. Järjestelmä saa tietoja Suomesta lähtöisin olevasta haittaohjelmaliikenteestä lähes kaikkialta maailmasta. Tiedot välitetään liittymiä ylläpitäville teleyrityksille, jotka ilmoittavat havainnoista asiakkailleen.

Tilastossa kerromme 10 yleisintä ja nimettyä haittaohjelmahavaintoa, jotka olemme saaneet Autoreporter-palvelun avulla. Niistä voi lukea tarkempia tietoja kotisivuiltamme:

<https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot>

Katso lisää tilastoja:

<https://www.traficom.fi/fi/tilastot/traficomin-haittaohjelmahavainnot>



Haavoittuvuus

► Microsoftin autodiscovery-toiminnon haavoittuvuutta käytetty hyväksi

- MS Exchangesta on todettu haavoittuvuus, jossa autodiscovery-toimintoa on voitu käyttää käyttäjätunnusten sieppaamiseen, kun Microsoftin tuotteisiin lisätään uusia kirjautumistietoja.
- Tietyt sovellukset ja protokollat käyttävät ennalta määriteltäviä verkkotunnusten nimiä uusien käyttäjien kirjautumiseen.
- Näiden määrättyjen verkkotunnusten päätyminen hyökkääjän hallintaan on voinut mahdollistaa tunnusten vuotamisen tai kaappaamisen.
- Haavoittuvuus on mahdollistanut sähköposti- ja toimialuetunnusten ja salasanojen kaappaamisen.
 - Tietoturvatutkijat ovat havainneet noin neljän kuukauden seurantajaksolla kymmenien tuhansien sähköpostitilien kirjautumistietojen ja satojen tuhansien toimialuetunnusten vaarantumisen haavoittuvuuden seurauksena.

Analyysi

- Haavoittuvuus vaikuttaa kaikkiin Microsoft Outlook -sovelluksen käyttäjiin, jotka käyttävät automaattista sähköpostitilin käyttöönottoavustinta.
- Pahimmillaan haavoittuvuus voi mahdollistaa käyttäjätilien salasanojen vuotamisen, joka voi johtaa tilien kaappaamiseen.



Kuukauden haavoittuvuusjulkaisut

- ▶ Microsoftin MSHTML-nollapäivähaavoittuvuus mahdollistaa komentojen suorittamisen etänä (26/2021)
- ▶ Apple korjasi haavoittuvuuksia iOS- ja iPadOS-käyttöjärjestelmistä - päivitä laitteesi heti (27/2021)
- ▶ Kriittinen haavoittuvuus Microsoftin Azure-pilvipalvelussa (28/2021)
 - ▶ Linux-palvelinten mallipohjissa on haavoittuva komponentti, joka ei päivity automaattisesti (koskee virtuaalikoneita)
 - ▶ Varmista, että komponentti on päivitetty!
- ▶ Kriittinen haavoittuvuus SonicWall SMA 100 -sarjan tuotteissa (29/2021)
- ▶ Apache korjasi aktiivisesti hyväksikäytetyn nollapäivähaavoittuvuuden (30/2021)
- ▶ Muistin korruptoitumishaavoittuvuus iOS- ja iPadOS-käyttöjärjestelmissä (31/2021)
 - ▶ Lue lisää: www.kyberturvallisuuskeskus.fi/fi/haavoittuvuudet

Analyysi

- ▶ Päivitykset tulee asentaa viipymättä, sillä haavoittuvuuksien hyväksikäyttö on todella nopeaa.
- ▶ Päivityssykklien ulkopuoliset päivitykset tulee myös huomioida, muutoin järjestelmään voi jäädä kriittisiä haavoittuvuuksia pitkäksi aikaa.



Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

- ▶ **Kyberturvallisuuskeskus vastaanottaa vuositasolla n.50 haavoittuvuuskoordinaatiotapausta**
 - ▶ Luku sisältää sellaiset ilmoitukset, jotka ovat vaatineet toimenpiteitä Kyberturvallisuuskeskukselta.
 - ▶ Haavoittuvuusilmoitusten luokat yleisesti: tiedoksi, pyydän apua tai koordinoitko haavoittuvuuden käsittelyn
- ▶ **Ilmoituksia tulee kansalaisilta, tutkijoilta ja organisaatioilta**
 - ▶ Vastaanotamme ilmoituksia myös anonyymeilta ilmoittajilta
- ▶ **Haavoittuvuustiedotteita tänä vuonna 32 kpl (tilanne 13.10.2021)**
 - ▶ Mukana mm. Microsoft Exchange Server ja etäkäyttötoteutusten haavoittuvuudet
- ▶ **Tilaamalla haavoittuvuuskoosteen saat tietoa erilaisista haavoittuvuuksista**
 - ▶ Kaikista haavoittuvuuksista ei julkaista suomenkielistä haavoittuvuustiedotetta
 - ▶ Kooste julkaistaan lähes päivittäin ja sen voi tilata sivuiltamme löytyvillä ohjeilla <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tilaa-uutiskirjeita>



Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

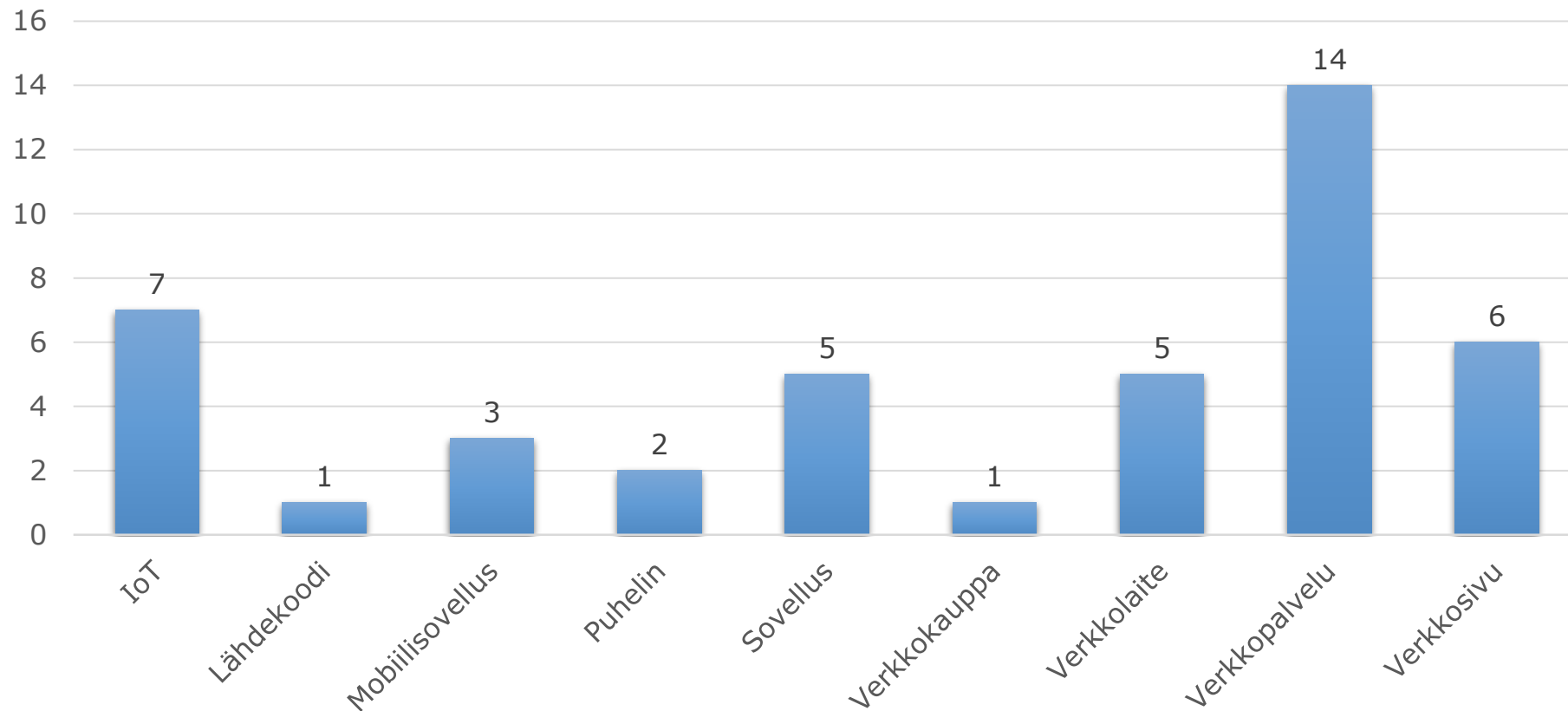
- ▶ Meille ilmoitetut haavoittuvuudet liittyvät usein verkkosivun tai -palvelun tietosuojaan. Helposti saatavilla oleva tieto voi olla sellaista, jonka ei tulisi näkyä muille. Tällaisia tietoja ovat esimerkiksi henkilötiedot tai erilaiset asiakastiedot.
- ▶ Vanhentuneet tai heikot salasanaikäytännöt ovat usein toistuva ongelma. Voi olla, että muutoin tietoturvallisesta tuotteesta löytyy kovakoodattu oletussalana. Erilaisissa verkkopalveluissa voi myös olla parannettavaa salasanaikäytännöissä esim. salasanan vaatimusten vai vaihtominaisuuksien osalta.
- ▶ IoT- ja verkkolaitteiden testaus on yleistä tietoturvatutkijoiden keskuudessa. Laitteiden turvallisuuden parantaminen on tärkeää verkossa ja kotona käytössä olevien laitteiden määrien jatkuvan kasvun vuoksi.
- ▶ Kyberturvallisuuskeskus saa haavoittuvuuksista ilmoituksia laidasta laitaan. Mikäli sinä tai organisaatiosi tarvitsette apua haavoittuvuuden löytyessä, haavoittuvuuden koordinoinnissa tai esimerkiksi CVE-tunnisteen haussa – olettehan yhteydessä Kyberturvallisuuskeskukseen.
- ▶ Ilmoita haavoittuvuudesta: <https://www.kyberturvallisuuskeskus.fi/fi/ilmoita>



Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio

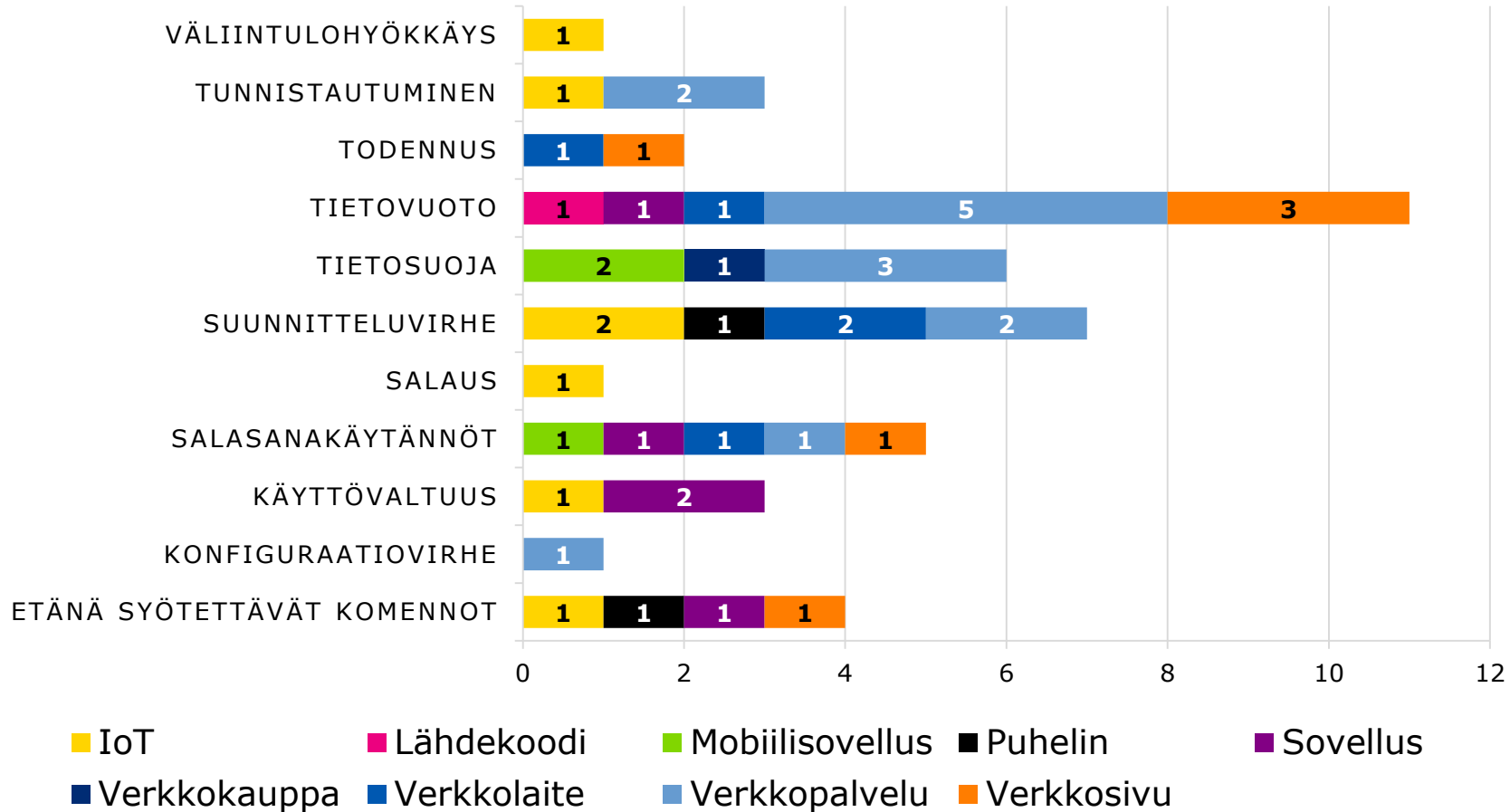


Haavoittuvuustyytit 01-06/2021





Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio



Taulukossa on esitetty Kyberturvallisuuskeskuksen haavoittuvuuskoordinaatio-tapaukset vuodelta 2021.

Tutustu aiheeseen tarkemmin:
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-haavoittuvuuskoordinaatio-pahkinankuoressa>



Automaatio ja IoT

Automaatio-osiossa ilmiöseurantaryhmä seuraa alan uutisia ja ilmiöitä maailmalla ja kotimaassa.

Automaatiojärjestelmiä käytetään ohjaamaan sekä monitoroimaan esimerkiksi erilaisia yksittäisiä tehtaan tai muun vastaavan tuotantolaitoksen palveluita tai laitteita.



Automaatio ja IoT

- ▶ Traficomin Kyberturvallisuuskeskus ja Singaporen kyberturvallisuusviranomaisen CSA julkaisivat yhteistyön IoT-tietoturvamerkkien vastavuoroisesta hyväksymisestä.
- ▶ Sopimus allekirjoitettiin Singaporen Cyber Weekin yhteydessä keskiviikkona 6.10.2021
- ▶ Tavoitteena on lisätä merkkien eurooppalaista ja kansainvälistä painoarvoa sekä antaa merkin saaneille valmistajille mahdollisuus kansainväliseen tunnustukseen tuotteidensa tietoturvatasosta
- ▶ Lue lisää Traficomin tiedotteesta: <https://www.trafficom.fi/fi/ajankohtaista/suomalaisen-yritysten-polku-turvallisten-alylaitteiden-markkinoille-helpottui>

Analyysi

- ▶ Kansainvälinen tietoisuus IoT-tuotteiden tietoturvaominaisuuksien merkityksestä kasvaa. Samalla lisääntyvät sekä vapaaehtoiset sertifiointit että pakottava lainsäädäntö.
- ▶ Kyberturvallisuuskeskus seuraa kehitystä ja pyrkii vaikuttamaan aktiivisesti tietoturvan tavoitetason määrittämiseen ja hyväksyttyihin todentamistapoihin.



Automaatio ja IoT

- ▶ Eri valmistajien koteihin tarkoitetuista IoT-laitteista löytyi vakavia haavoittuvuuksia
 - ▶ Victuren itkuhälyttimisestä löytyi haltuunoton ja salakatselun mahdollistava haavoittuvuus. Valmistaja ei ole kommentoinut haavoittuvuutta, eikä korjausta ole saatavilla.
 - ▶ Motorolan Halo+ -itkuhälyttimistä löytyi laitteen kaappaamisen mahdollistava haavoittuvuus. Korjaus on saatavilla.
 - ▶ Hikvisionin IP-kameroista löytyi komentojen mielivaltaisen suorittamisen mahdollistanut haavoittuvuus, joka on ollut laitteissa vuodesta 2016. Valmistaja on julkaissut korjauksen, mutta sitä ei välttämättä ole saatavilla kaikille laitteille.
 - ▶ Useista Netgearin reitittimistä löytyi vakava haavoittuvuus, joka mahdollistaa verkkoliikenteen manipuloimisen. Korjaus on saatavilla.

Analyysi

- ▶ Kun hankit laitetta, tarkista onko siihen saatavilla päivityksiä. Edullisestakin laitteesta tulee kallis, jos käyttöikä jää lyhyeksi puuttuvien päivitysten takia.
- ▶ Kun laite on käytössä, huolehdi että uusimmat päivitykset on asennettu.
- ▶ Jos päivitykset loppuvat, poista laite käytöstä tai varmista ettei se ole yhdistettynä internetiin.



Automaatio ja IoT

- ▶ Tietoturvayhtiö Guardara kertoi NanoMQ-viestinvälityskirjastossa löytyvästä puskurin ylivuodon mahdollistavasta haavoittuvuudesta
 - ▶ Heidän mukaan kyseinen kirjasto on käytössä jopa 100 miljoonassa IoT-laitteessa.
 - ▶ Kirjastoa hyödyntävien valmistajien korjauspäivitykset päätyvätkin laitteisiin todennäköisesti viiveellä ohjelmistopäivitysten muodossa. On mahdollista, että osa valmistajista ei julkaise korjausta lainkaan.
- ▶ Tietoturvayhtiö Claroty'n julkaiseman puolivuositaisen katsauksen mukaan automaatiojärjestelmistä löytyneet haavoittuvuudet jatkoivat kasvuaan vuoden 2021 ensimmäisellä puoliskolla
 - ▶ Edelliseen vuoteen verrattuna nousua nähtiin 41%.



Verkkojen toimivuus

Verkkojen toimivuus -osassa käsitellään yleisten viestintäpalveluiden merkittäviä toimivuushäiriöitä Suomessa, muiden ICT-palveluiden huomattavia häiriöitä Suomessa ja maailmalla, sekä palvelunestohyökkäyksiä Suomessa ja maailmalla.



Verkkojen toimivuus

- ▶ Syyskuussa yleisissä viestintäpalveluissa oli kaksi merkittävää toimivuushäiriötä
 - ▶ Vakavuusluokat: A: 0, B: 0, C: 2
- ▶ Facebookin, Instagramin ja WhatsAppin palveluissa raportoitiin maailmanlaajuisia käyttökatkoksia 4.10. usean tunnin ajan
 - ▶ Facebookin mukaan häiriön juurisyynä olivat virheelliset konfiguraatiomuutokset Facebookin runkoreitittimissä.
 - ▶ Komentojen varmistamiseen käytetyn sovelluksen virheen vuoksi Facebookin eri konesalien runkoreitittimet lopettivat BGP-reittien mainostamisen. Tämän seurauksena konesalien yhteydet muuhun internetiin katkesivat kokonaan.

Analyysi

- ▶ Yleisten viestintäpalveluiden toimivuus Suomessa on vuonna 2021 ollut keskimäärin hyvä.
- ▶ Kuukaudessa on keskimäärin vajaat kuusi merkittävää toimivuushäiriötä.
- ▶ Syyskuussa palvelukatkoksia oli myös AWS-palveluissa, Twitterissä ja Microsoft 365 -palvelun monivaiheisessa tunnistautumisessa.



Palvelunestohyökkäykset

- ▶ Syyskuussa Kyberturvallisuuskeskukselle raportoitin muutamia palvelunestohyökkäyksiä. Hyökkäyksillä oli myös vaikutuksia palveluihin.
 - ▶ Lyhytkestoisellakin hyökkäyksellä voi olla vaikutuksia palveluihin, jotka ovat palvelunestohyökkäyksen kohteena tai saavat osansa hyökkäyksestä välillisesti.
- ▶ Julkishallinnon palveluun osuu ajoittain palvelunestohyökkäyksiä, mutta ne pääsääntöisesti torjutaan tehokkaalla pakettipesuripalvelulla.
 - ▶ Palvelut kannattaa ottaa mukaan harjoituksiin ja testata niiden toimintakyky palveluntarjoajan kanssa - jotta ne kestävät yleisimmät palvelunestohyökkäystekniikat ja suuruusluokat.
- ▶ Noin 40% hyökkäyksistä Suomessa oli kooltaan yli 1 Gbit/s (Q3/2021). Tänä vuonna ilmoitettujen hyökkäysten perusteella skaala ulottuu jopa 260 Gbit/s tasolle asti.

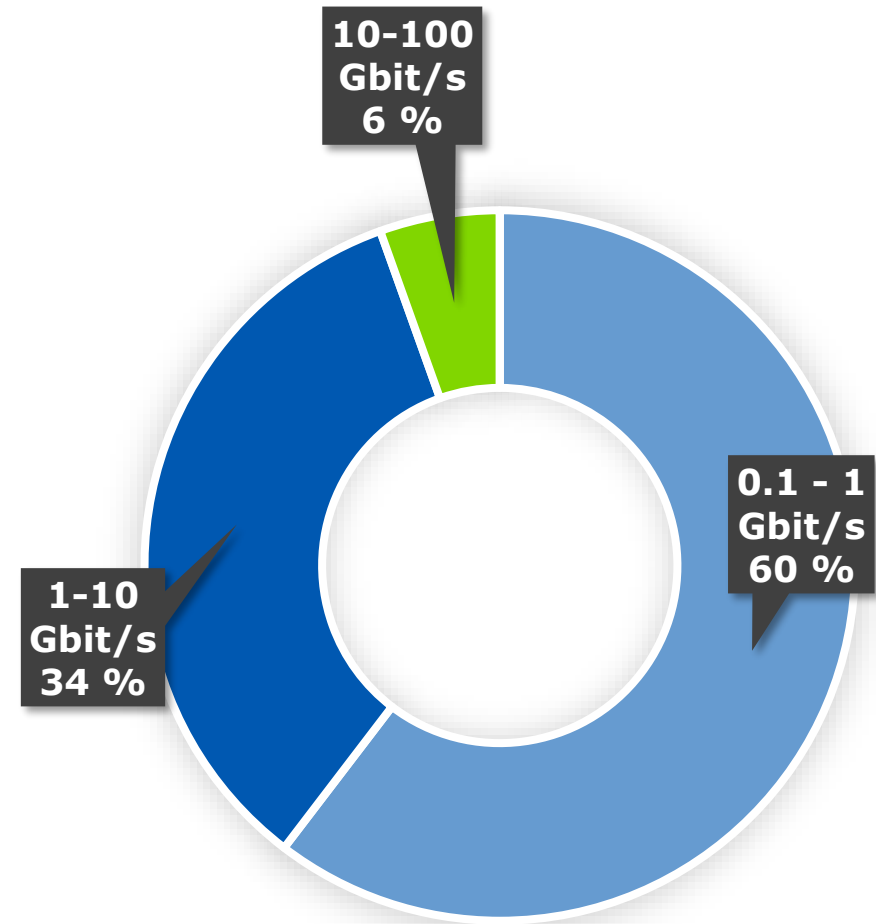
Analyysi

- ▶ Syksyn tulon huomaa myös hyökkäysten aktivoitumisesta oppimispalveluita ja opintohallintojärjestelmiä kohtaan.
- ▶ Koululaisille ja muille hakkeroinnin alkeisiin tutustuville on tärkeä muistuttaa, että tietoverkkojen häirintä on laitonta ja siitä koituvista rikosoikeudellisista seuraamuksista voi aiheutua harmia myöhemmin.
- ▶ Palvelunestohyökkäys voi myös välillisesti aiheuttaa muutakin haittaa kohteelle, jolloin vahinkoa ei aiheuteta pelkästään oppimispalveluihin.

Palvelunestohyökkäysten tunnuslukuja



- ▶ 99 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys Q3/2021.
- ▶ Noin 76% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- ▶ Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit
(Q3/2021 - tilasto päivitetään kvartaaleittain.)



Vakoilu

Vakoiluosiossa käsitellään valtiollisten toimijoiden tai niihin liitettyjen ryhmien harjoittamaa kybervakoilua ja -vaikuttamista. Tavoitteena voi olla poliittinen tiedonhankinta, yritysvakoilu tai esimerkiksi tietojärjestelmien tuhoaminen.



Vakoilu

- ▶ Saksa syyttää Venäjää maan parlamenttiin kohdistuneesta kyberhyökkäyksestä.
 - ▶ Saksan mukaan sillä on luotettavaa tietoa siitä, että ns. Ghostwriter-toiminta linkittyy Venäjään. Saksa yhdistää toiminnan Venäjän sotilastiedusteluun GRU:hun.
- ▶ Myös EU on tuominut jäsenvaltioihinsa kohdistuneet vaikuttamispyrkimykset ja yhdistää toiminnan Venäjään.
- ▶ Ghostwriter-toiminnan keskiössä on tähän asti ollut muun muassa luottamuksen heikentäminen sotilasliitto NATO:a kohtaan.
- ▶ Toiminnalle ominaista on ollut se, että siinä on yhdistelty tietomurtoja ja perinteisempää informaatiovaikuttamista, kuten vale uutisia.

Analyysi

- ▶ Ghostwriter-toiminta on jo useamman vuoden jatkunut informaatio-operaatio.
- ▶ Toimintaa on nähty aiemmin muun muassa Puolassa, Latviassa ja Liettuassa.
- ▶ Siinä on pyritty vaikuttamaan kohdemaassa muun muassa murtautumalla poliitikkojen, virkamiesten tai vastaavien toimijoiden sähköpostitileille tai henkilökohtaisille sosiaalisen median tileille.



Vakoilu

- ▶ Tietoturvatyöimija Mandiant raportoi ProxyShelliksi nimetyn haavoittuvuuskokonaisuuden hyödyntämisestä kohdistetuissa hyökkäyksissä.
 - ▶ Haavoittuvuuksien hyväksikäyttöön julkaistiin esimerkkikoodi elokuussa.
- ▶ ProxyShellillä tarkoitetaan sarjaa hyökkäyksiä, joissa hyödynnetään kolmea paikallisesti ylläpidetyissä (*on-premises*) Microsoft Exchange-palvelimissa olevaa haavoittuvuutta.
- ▶ Mandiantin mukaan ProxyShell-hyökkäyksiä on havaittu toimialoista ainakin koulutusalalla, valtionhallinnossa, liiketoimintapalveluissa ja televiestintäalalla. Havaintoja on tehty niin Yhdysvalloissa, Euroopassa kuin Lähi-idässä.

Analyysi

- ▶ Mandiant arvioi, että sen tunnistamien hyökkäysten taustalla on mahdollisesti Kiinasta käsin operoiva APT-toimija, jota ei tällä hetkellä pystytä linkittämään tunnettuihin kiinalaisiin APT-ryhmiin.
- ▶ Sähköpostipalvelimelle kohdistuva tietomurto voi mahdollistaa hyökkääjälle laajan pääsyn organisaation tärkeisiin tietoihin ja viestintään sekä antaa hyökkääjälle runsaasti tietoa organisaation rakenteista ja henkilöstöstä.



Vakoilu

- ▶ Suojelupoliisi nostaa kansallisessa uhka-arviossaan kybervakoilun keskeisimmäksi Suomeen kohdistuvaksi kyberuhaksi.
 - ▶ Kybervakoilu kohdistuu sekä poliittiseen päätöksentekoon että tuotekehitystietoon.
- ▶ Pääasiallisena järjestelmiin vaikuttamiseen liittyvänä kyberuhkana nostetaan esiin kiristyshaittaohjelmat, jotka voivat vakavasti haitata yhteiskunnan kriittisiä toimintoja.
 - ▶ Kriittisen infrastruktuurin suojaamisessa korostuu haavoittuvuuksien hallinta, liiketoiminnan jatkuvuuden varmistaminen sekä ulkoistettujen toimintojen suojaustasosta varmistuminen.
- ▶ Tiedustelullisesti Suomi kiinnostaa Suojelupoliisin mukaan erityisesti Venäjää ja Kiinaa.

Analyysi

- ▶ Suojelupoliisi nostaa kybervakoilun motiiveina esiin muun muassa tiedon hankkimisen päätöksenteon tueksi, kybervakoilun käyttämisen pelotteena sekä paremman aseman saavuttamisen globaaleilla markkinoilla.
- ▶ Tiedonhankintaan tähtäävän kybervakoilun arvioidaan jatkuvan pitkällä aikavälillä. Sen sijaan valtiolähtöistä, tietojärjestelmiin kohdistuvaa kybervaiikuttamista ei pidetä todennäköisenä.



Tietoturva-alan kehitys

Tietoturva-alan kehitys -osiossa kerromme keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.



Oikeudelliset asiat

- ▶ Hallituksen esitys eduskunnalle laeiksi Liikenne- ja viestintävirastosta annetun lain 3 §:n ja sähköisen viestinnän palveluista annetun lain 304 §:n muuttamisesta
 - ▶ Hallituksen esityksellä pannaan kansallisesti täytäntöön Euroopan parlamentin ja neuvoston asetus Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinoitavien verkoston perustamisesta (EU) 2021/887.
 - ▶ Liikenne- ja viestintäviraston kyberturvallisuuskeskuksen tehtäviin ehdotetaan lisättäväksi velvollisuus toimia asetuksen 6 artiklan mukaisena kansallisena koordinoitavien keskuksena. Uutena tehtävänä erityisesti kyberturvallisuusalan sidosryhmistä koottavan yhteisön rakentamisen koordinointi ja sekä toimiminen osaamisyhteisön yhteyspisteenä.
 - ▶ Kyberturvallisuuskeskukselle asetettuna tavoitteena mm. on edistää kyberturvallisuusklusterin rakentumista Suomeen, auttaa synnyttämään markkinoille kyberturvallisuuteen toimintansa perustavia yrityksiä sekä vahvistaa kyberturvallisuusosaamista. Lisäksi tavoitteena on edistää kansalaisyhteiskunnan, sidosryhmien ja elinkeinoelämän, kuten start up- ja pienten ja keskisuurten yritysten sekä akateemisten ja tutkimusyhteisöjen osallistumista rajat ylittäviin hankkeisiin kansallisella tasolla.
 - ▶ EU:n asetus on suoraan sovellettavaa oikeutta, joten tehtäviä ei erikseen luetella muutettavissa pykälissä. Kuitenkin perustuslain mukaan julkisen vallan käytön tulee perustua lakiin, joten tehtävän osoittamisesta Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselle tulee säätää kansallisesti.
 - ▶ Laki on tarkoitettu tulemaan voimaan syksyllä 2021, mutta kuitenkin viimeistään 28.12.2021.
- ▶ Lisätietoja: <https://finlex.fi/fi/esitykset/he/2021/20210157>



Oikeudelliset asiat

- ▶ Poliisille huomautus henkilötietojen lainvastaisesta käsittelystä kasvojentunnistusohjelmalla
 - ▶ Poliisi käsitteli erityisiin henkilötietoryhmiin kuuluvia tietoja lainvastaisesti kasvojentunnistusteknologian koekäytössä. Keskusrikospoliisin lasten seksuaalisen hyväksikäytön torjuntaan keskittyvä yksikkö oli kokeillut kasvojentunnistusteknologiaa mahdollisten uhrien tunnistamiseksi. Päätös koekäytöstä oli tehty poliisissa, eikä Poliisihallitus ollut tietoinen kokeilusta.
 - ▶ Poliisin henkilötietojen käsittelystä vastaava rekisterinpitäjä Poliisihallitus teki huhtikuussa 2021 tietosuojavaltuutetun toimistolle ilmoituksen tietoturvaloukkauksesta, jossa oli kyse kasvojentunnistusohjelman kokeilukäytöstä Keskusrikospoliisissa vuoden 2020 alussa. Poliisissa oli kokeiltu yhdysvaltalaista Clearview AI -palvelua lasten seksuaalisen hyväksikäytön mahdollisten uhrien tunnistamiseksi kasvokuvien avulla. Poliisi oli kokeillut samaan tarkoitukseen myös Arachnid-nimistä palvelua.
 - ▶ Poliisihallitus oli saanut tiedon Clearview AI -palvelun käytöstä yhdysvaltalaiselta BuzzFeed News -verkkosivustolta, joka oli 31.3.2021 ottanut yhteyttä Keskusrikospoliisiin.
 - ▶ Henkilötietojen käsittely kasvojentunnistusohjelmalla oli tapahtunut ilman rekisterinpitäjän eli Poliisihallituksen hyväksyntää tai valvontaa.
 - ▶ Apulaistietosuojavaltuutetun päätöksen mukaan henkilötietojen käsittely oli ollut lainvastaista. Huomautuksen lisäksi Poliisihallitus määrättiin ilmoittamaan henkilötietojen tietoturvaloukkauksesta niille rekisteröidyille, joiden henkilöllisyys on tiedossa.
- ▶ Lisätietoja: <https://finlex.fi/fi/viranomaiset/tsv/2021/20211023>

Arjen kyberturvallisuus

Euroopan kyberturvallisuuskuukausi - European Cyber Security Month

- ▶ Lokakuussa laitetaan kyberturvallisuuden ja tietoturvan perustaitoja kuntoon. Euroopan kyberturvallisuuskuukausi on loistoaika päivittää omat digitaidot ajantasaisiksi.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/euroopan-kyberturvallisuuskuukausi-european-cyber-security-month>

Rikolliset urkkivat suomalaisten pankkitunnuksia – ota talteen vinkit turvalliseen asiointiin

- ▶ Kela, Keskusrikospoliisi ja Kyberturvallisuuskeskus kehottavat huolellisuuteen verkkopalveluihin kirjautumisessa. Rikolliset kalastelevat pankkitunnuksia suomalaisten pankkien ja Omakanta-palvelun nimissä. Asioithan verkossa turvallisesti ja tunnista huijaukset. Kerro huijauksista myös läheisillesi.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/rikolliset-urkkivat-suomalaisten-pankkitunnuksia>

Tutustu Tietoturvamerkkiin

▶ Tietoturvamerkki on luotu auttamaan kuluttajaa tekemään turvallisia valintoja. Se kertoo, että tuote tai palvelu täyttää Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen asettamat tietoturvavaatimukset.

▶ Tutustu Tietoturvamerkkiin:
<https://tietoturvamerkki.fi/fi/kuluttajalle/>

CERT-FI 20 vuotta: Muistatko, kun palvelimet olivat rautaa ja Snowden heilutti maailmaa?

- ▶ Internetin ihmemaassa värähteli, kun millenium kääntyi ensimmäiselle vuosikymmenelleen. Esineiden internet oli tieteiskirjallisuutta ja Conficker-mato söi internetiä. Samoihin aikoihin Edward Snowden pysäytti tietovuodollaan kansainvälisen median ja samalla sai meidät kaikki pohtimaan tietoturvaa ja turvallista viestintää.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/cert-fi-20-vuotta-muistatko-kun-palvelimet-olivat-rautaa-ja-snowden-heilutti-maailmaa>



Uutisia Kyberturvallisuuskeskuksesta

Suomalaisten yritysten polku turvallisten älylaitteiden markkinoille helpottui

- ▶ Suomen ja Singaporen kyberturvallisuusviranomaiset tunnustavat ensimmäisinä maailmassa vastavuoroisesti toistensa myöntämät tietoturvamerkkit ja merkkien myöntämiseen liittyvät menetelmät. Kansainvälinen yhteistyön viranomaisten välillä helpottaa jatkossa suomalaisten yritysten mahdollisuuksia tarjota turvallisia älylaitteitaan muiden maiden älylaitemarkkinoille ja parantaa kodin älylaitteiden tietoturvasoa ja auttaa näin kuluttajia hallitsemaan kasvavia tietoturvariskejä.
- ▶ <https://www.traficom.fi/fi/ajankohtaista/suomalaisten-yritysten-polku-turvallisten-alylaitteiden-markkinoille-helpottui>

Evästeneuvontamme on uusittu

- ▶ Olemme julkaisseet uudistettua neuvontaa evästeiden ja muiden palvelun käyttöä kuvaavien tietojen tallentamisesta käyttäjän päätelaitteelle sekä näiden päätelaitteella olevien tietojen käytöstä. Näin tuemme sekä verkkopalvelujen tarjoajia että käyttäjiä evästekäytännöissä ja lainsäädännön soveltamisessa.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/evasteneuvontamme-uusittu>

Arvio mobiililaitteiden turvallisuuden selvityksestä

- ▶ Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on tutustunut Liettuan kyberturvallisuuskeskuksen tekemän selvityksen raporttiin kolmen älypuhelinvalmistajan mobiililaitteista. Kyberturvallisuuskeskus on todennut sen olevan pääosin sisällöllisesti paikkansa pitävä. Kyberturvallisuuskeskuksen arviolla kolmansien osapuolten verkkokaupoista voi olla kyberturvallisuuteen liittyviä vaikutuksia.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/arvio-mobiililaitteiden-turvallisuuden-selvityksesta>

Epäiletkö tietoturvaloukkausta?

- ▶ Jos teihin on kohdistunut tai epäilette teihin kohdistuneen tietoturvaloukkauksen, olkaa yhteydessä meihin.
 - ▶ Sähköinen lomake: <https://www.kyberturvallisuuskeskus.fi/fi/ilmoita>
 - ▶ Sähköposti: cert@traficom.fi
 - ▶ Puhelin: 0295 345 630 (arkisin klo 9-15)
- ▶ Muissa asioissa voitte olla meihin yhteydessä osoitteessa kyberturvallisuuskeskus@traficom.fi
- ▶ Kyberturvallisuuskeskuksen eri toimintojen ja hankkeiden yhteystiedot löydät keskitetysti täältä: <https://www.kyberturvallisuuskeskus.fi/fi/ota-yhteytta/yhteystiedot>