



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Huhtikuu 2020

14.5.2020

#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 huhtikuu 2020

Tietomurrot ja -vuodot

- ▶ Office 365 –tietomurtojen määrä on noussut takaisin alkuvuoden tasolle.
- ▶ Kalastetulla haltuun saatuja O365 - tunnuksia käytetään myös muihin tietomurtoihin.



Huijaukset ja kalastelut

- ▶ Edistyneissä huijauksissa käytetään uhrin oikeita henkilötietoja, tilitietoja, sähköpostia ja tekstiviestejä.
- ▶ Kaapattua tiliä käytetään yhdessä salasananpalautustoiminnon kanssa varastamaan monien palveluiden salasanoja.



Haaitaohjelmat ja haavoittuvuudet

- ▶ Kuukauden aikana paljon kriittisiä haavoittuvuuksia, uusia hyväksikäyttömenetelmiä ja hyökkäykselle alttiita palveluita.
- ▶ Älä laiminlyö kriittisiä päivityksiä, varsinkin jos palvelu on avoinna Internetiin.



Automaatio

- ▶ Kyberturvallisuuskeskuksen vuosittainen selvitys suomalaisten tietoverkkojen suojaamattomista automaatiolaitteista meneillään.
- ▶ Päivittämättömiä laitteita, kuten teollisuusautomaatio- tai lääkintälaitteita on saastunut tunnetuilla haittaohjelmilla.



Verkkojen toimivuus

- ▶ Toimivuushäiriöitä oli tavanomaista enemmän ja ne vaikuttivat laajasti.
- ▶ Telian internetyhteyksien häiriö 25.4. vaikutti moniin yhteiskunnan toimintoihin.
- ▶ Huhtikuu oli palvelunestohyökkäysten osalta rauhallinen.

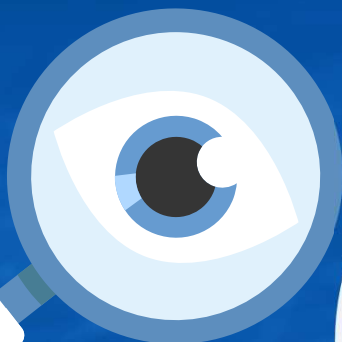


Vakoilu

- ▶ Koronavirukseen liittyviin teemoihin, kuten rokote- ja muuhun tutkimukseen voi kohdistua vakoilua.
- ▶ Myös valtioiden päätöksenteko ja sen valmistelu ovat perinteisiä kohteita, jotka ovat ajankohtaisia myös pandemia-aikana.



Kuukauden tunnuslukuja



**5 H
45 MIN**

**PISIMMÄN MERKITTÄVÄN YLEISTEN
VIESTINTÄPALVELUIDEN
TOIMIVUUSHÄIRIÖN KESTO.**

**TELIAN KIINTEÄN JA
MATKAPUHELINVERKON
INTERNETYHTEYSPALVELUSSA OLI
MAANLAAJUINEN HÄIRIÖ
LAUANTAINA 25.4.**



N.3700

**HENKILÖÄ VASTASI VAPPUVISAAMME
KALASTELUSIVUJEN TUNNISTAMISESTA.**

**SAAMISSAMME VASTAUKSISSA NÄKYI,
ETTÄ KALASTELUSIVUN TUNNISTAMINEN
PELKÄN ULKOASUN PERUSTEELLA ON
VAIKEAA.**



25+

**HAAVAKOOSTEISSAMME OLI TIETOA
YLI 25 ERI VALMISTAJAN
OHJELMISTOJEN KRIITTISISTÄ
HAAVOITTUVUUKSISTA.**

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Haavoittuvuuksien hyväksikäyttö nopeutuu, mikä vaatii nopeita päivityksiä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet sekä ylläpito ovat puutteellisia.

2

Tietojenkalastelu on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdennetuissa hyökkäyksissä ja vakoilussa.

3

Laajavaikutteiset kiristyshyökkäykset uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Puutteet lokien tarkkailussa vaikeuttavat uhkien havaitsemista.

5

Organisaatiot eivät osaa hallita kyberriskejään. Uhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Palautumissuunnitelmissa on puutteita.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

1

Haavoittuvuuksien hyväksikäyttö nopeutuu, mikä vaatii nopeita päivityksiä. Verkkoon jätetään auki laitteita ja palveluita, joiden tietoturvaa ei ole huomioitu ja suojaustoimet sekä ylläpito ovat puutteellisia.

- ▶ Rikolliset kehittävät hyväksikäyttömenetelmiä nopeasti heti ohjelmistopäivitysten ilmestyttyä ja iskevät kohteisiin, joita ei ole päivitetty. Erityisesti tietoturvatuotteissa olevat haavoittuvuudet ovat vakavia, sillä ne on yleensä sijoitettu muutenkin hyökkäyksille alttiin tietojärjestelmien kohtiin.
- ▶ Hyökkäyksissä käytetyt järjestelmähaavoittuvuudet ovat usein olleet 2-6 kk vanhoja haavoittuvuuksia, joihin on ollut saatavilla korjaus jo pitkään, mutta syystä tai toisesta haavoittuvuutta ei ole korjattu.
- ▶ Mitä pidempään haavoittuvuuden korjaamisessa kestää tai korjausta siirretään myöhemmäksi, sitä korkeammaksi hyväksikäyttämisen riski kasvaa.

CASE

Palvelinten ylläpitoon käytetystä Saltstack Salt -hallintakehikosta korjattiin kriittisiä haavoittuvuuksia huhtikuun lopulla. Ensimmäiset automatisoidut hyökkäykset havaittiin vain pari päivää myöhemmin. Hyökkääjä asensi virtuaalivaluutta louhivan haittaohjelman kaikkiin hallinnan piirissä oleviin palvelimiin. Verkkoon auki olevia palveluita löytyi yli 6000.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

2

Tietojenkalastelu on erittäin yleistä, ja viestin vastaanottajan voi olla vaikea havaita huijausta. Tätä hyödynnetään myös kohdistetuissa hyökkäyksissä ja vakoilussa.

- ▶ Tietojenkalastelu on ollut hyvin yleistä pidemmän aikavälin tarkastelulla. Tyypillisesti rikolliset kalastelevat suomalaisilta Office 365 -tuotteiden ja sähköpostin käyttäjätunnuksia ja salasanoja.
- ▶ Typosquatting / domainsquatting liittyvät myös ilmiöön: kirjoitusvirheillä höystetyillä verkkotunnuksilla voidaan tehostaa huijauksen vaikuttavuutta.
- ▶ Henkilökunnan koulutuksella on suuri merkitys. Tutkimusten mukaan tietojenkalastelua opitaan tunnistamaan koulutuksen avulla ja tämä auttaa siihen, että tietojenkalastelu jää vain yritykseksi.

CASE

Vappuvisassa tunnistettiin huijauksia

Kyberturvallisuuskeskus julkisti vappuviikolla leikkimielisen kuvavisailun, jonka takana oli kuitenkin vakava asia: huijauksiin tehdyt tietojenkalastelusivut.

Lähes 3700 vastaajaa yritti tunnistaa kuvista, onko verkkosivu aito vai huijarin tekemä tietojenkalastelusivu. Kuten vastaajat saivat huomata, pelkästä kuvasta on vaikea tunnistaa petkutusta, vaan rinnalle tarvitaan muutakin tietoa.

Lue lisää artikkelistamme:

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vappuvisan-tulokset-petkuhuiputusta-vaikea-tunnistaa>

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

3

Laajavaikutteiset kiristyshyökkäykset (Big Game Hunting) uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

- ▶ Tapauksia myös Suomessa. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan seurauksena.
- ▶ Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja. Jos rikolliset havaitsevat huonosti suojatun ympäristön kiristämisen arvoiseksi, siihen saatetaan kohdistaa Big Game Hunting –toimintaa.
- ▶ Uusia ilmoituksia laajoista kiristyshaittaohjelmatarunnoista tulee kansainvälisesti viikoittain. Lisäksi uusia toimijoita tulee jatkuvasti. Esimerkkinä tästä on ICS-toimijoihin kohdistuva EKANS.
- ▶ Kiristyshyökkäysten uutena ilmiönä uhataan julkaista hyökkääjän haltuun saamia tietoja lunnasvaatimuksen tehostamiseksi.

CASE

Norjassa Norsk Hydroon kohdennettu kiristyshaittaohjelma pääsi leviämään tuotantojärjestelmään asti. Toimintahäiriöt kestivät kuukausia ja koskettivat yrityksen useita eri toimipisteitä.

Norsk Hydro arvioi omilla sivuillaan kiristyshaittaohjelman kokonaiskustannukseksi noin 60 miljoonaa euroa.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa. Puutteet lokien tarkkailussa vaikeuttavat uhkien havaitsemista.

- ▶ Epäselvä vastuunjako ICT-palveluiden hankinnassa ja tuotannossa heikentää tietoturvan hallintaa. Tämä pätee myös organisaatioiden sisällä, jos tietoturvariskien omistajuus ja tietoturvavastuut eivät ole selkeästi määriteltyjä.
- ▶ Yleinen puute on jättää keräämättä ja tarkkailematta tietoturvalokeja. Lokien jatkuvan tarkkailun avulla tietojärjestelmän omistaja voi havaita lievät tietoturvaloukkaukset ja järjestelmän heikkoudet ennen kuin kukaan ehtii käyttää niitä suurempaan vahingontekoon. Lokeja tarvitaan myös loukkausten selvittämiseen jälkikäteen.
- ▶ Lisäksi käytöstä poistuvien palveluiden alasajo tulee tehdä huolella. Jos alasajotoimenpiteitä ei tehdä johdonmukaisesti loppuun asti, voi taustalle jäädä pyörimään käyttämättömiä palveluita, jotka voivat aiheuttaa merkittäviä tietoturvariskejä organisaatiolle.

Korona-aikana epäselvän vastuunjaon lisäksi nousee esille resurssien riittävyys sekä erilaisten varautumissuunnitelmien tärkeys. Pandemian aikana henkilöstöllä on keskeinen rooli, jotta toiminnot saadaan pidettyä yllä ja resurssien tulee olla riittävät kaikissa tilanteissa. Vaikutuksia saattaa olla myös tuotantoketjuissa, jolloin normaalisti saatava tuote jääkin tulematta, millä on vaikutuksia organisaation toimintaan.

CASE

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

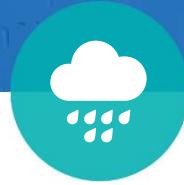
5

Organisaatiot eivät osaa hallita kyberriskejään. Uhkien vaikutuksia toimintaan ei osata ennakoida, minkä vuoksi riskit aliarvioidaan. Palautumissuunnitelmissa on puutteita.

- ▶ Tietoturvaloukkauksista toipumista ei usein suunnitella huolellisesti ennakoon. Suunnitelmat ovat vain luokkaa "palautetaan tiedot varmuuskopioista". Palautumisen tärkeysjärjestyksiä, resursseja ja aikajänteitä ei mietitä ennakoon.
- ▶ Häiriön iskiessä palautumisen monimutkaisuus ja työläys yllättävät. Jos palautuminen olisi suunniteltu ennakolta paremmin, myös varautuminen häiriöihin ja niiden ennaltaehkäisyyn olisi parempaa.
- ▶ Kyberturvallisuuskeskus on julkaissut yritysten hallituksille suunnatun kyberturvallisuutta käsittelevän oppaan. Kyberturvallisuus ja yrityksen hallituksen vastuu -opas antaa työkaluja ja tukea organisaation kyberturvallisuuden parantamiseen.
- ▶ Lue lisää:
<https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas>

CASE

Organisaatioiden kyvyssä hallita kyberriskejään on selviä puutteita. Tyypillisesti organisaatiot eivät osaa ennalta arvioida kyberuhkien toteutumisen vaikutuksia päivittäiseen toimintaan. Tämän seurauksena on, että kyberriskit ja niiden vaikutukset aliarvioidaan eikä niiden hallintaan osoiteta riittävästi resursseja.



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

- ▶ Kyberturvallisuuskeskukseen ilmoitettujen Office 365 -tietomurtojen määrä on noussut takaisin alkuvuoden tasolle.
 - ▶ Osa tietomurroista on tapahtunut SOTE-alan ja muiden kriittisten toimijoiden järjestelmiin.
 - ▶ Kyberturvallisuuskeskus on julkaissut ohjeen Office 365 -ympäristön koventamisesta. Se on saatavilla suomen-, ruotsin- ja englanninkielisenä.
 - ▶ Ohje löytyy osoitteesta: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/organisaatio-torju-office-365-tunnusten-kalastelu-oppaamme-avulla>

ANALYYSI

- ▶ Tietomurron kohteeksi joutuminen voi aiheuttaa taloudellisten menetysten lisäksi myös merkittävän mainehaitan. Useissa tapauksissa murrettua sähköpostitiliä on käytetty uusien huijausviestien lähettämiseen.
- ▶ Monivaiheisella tunnistautumisella voitaisiin estää suurin osa tietomurroista.



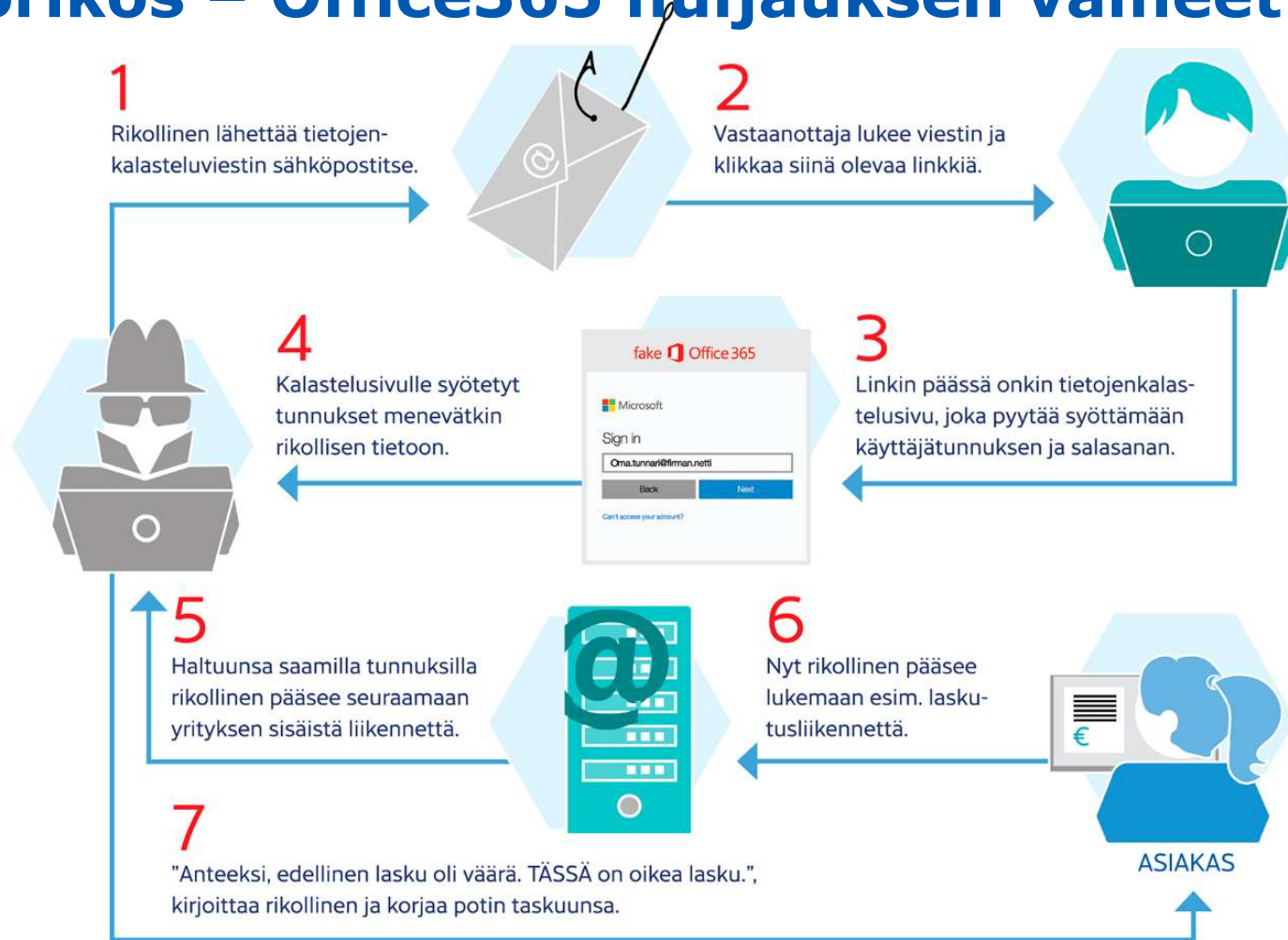
Tietomurrot ja vuodot

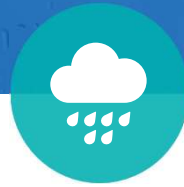
- ▶ Office 365 -kalastelulla haltuun saatuja tunnuksia käytetään myös muihin tietomurtoihin.
 - ▶ Huhtikuussa onnistuneella kalastelulla haltuun saatuja tunnuksia käytettiin kahden eri organisaation henkilöstöhallinnon itsepalveluportaaliin kirjautumiseen.
 - ▶ Portaalissa työntekijöiden palkkatilitietoja onnistuttiin muokkaamaan siten, että palkka ohjautui muulitilien kautta ulkomaille.
 - ▶ Asia huomattiin, kun osa työntekijöistä ei saanut palkkaa ajallaan. Organisaatioiden taloudelliset tappiot olivat noin 30 000–50 000€.

ANALYYSI

- ▶ Käyttäjätunnukset ja salasanat ovat verkkorikillisille kauppatavaraa, joita pyritään hyödyntämään mahdollisimman tehokkaasti.
- ▶ On tärkeää, että eri järjestelmissä käytetään eri tunnuksia ja salasanoja. Näin vältetään laajemmat vahingot yhden salasanan päätyessä väärin käsiin.

Tietojenkalastelu – yleisin yrityksiin osuva verkkorikos – Office365 huijauksen vaiheet:





Huijaukset ja kalastelut

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



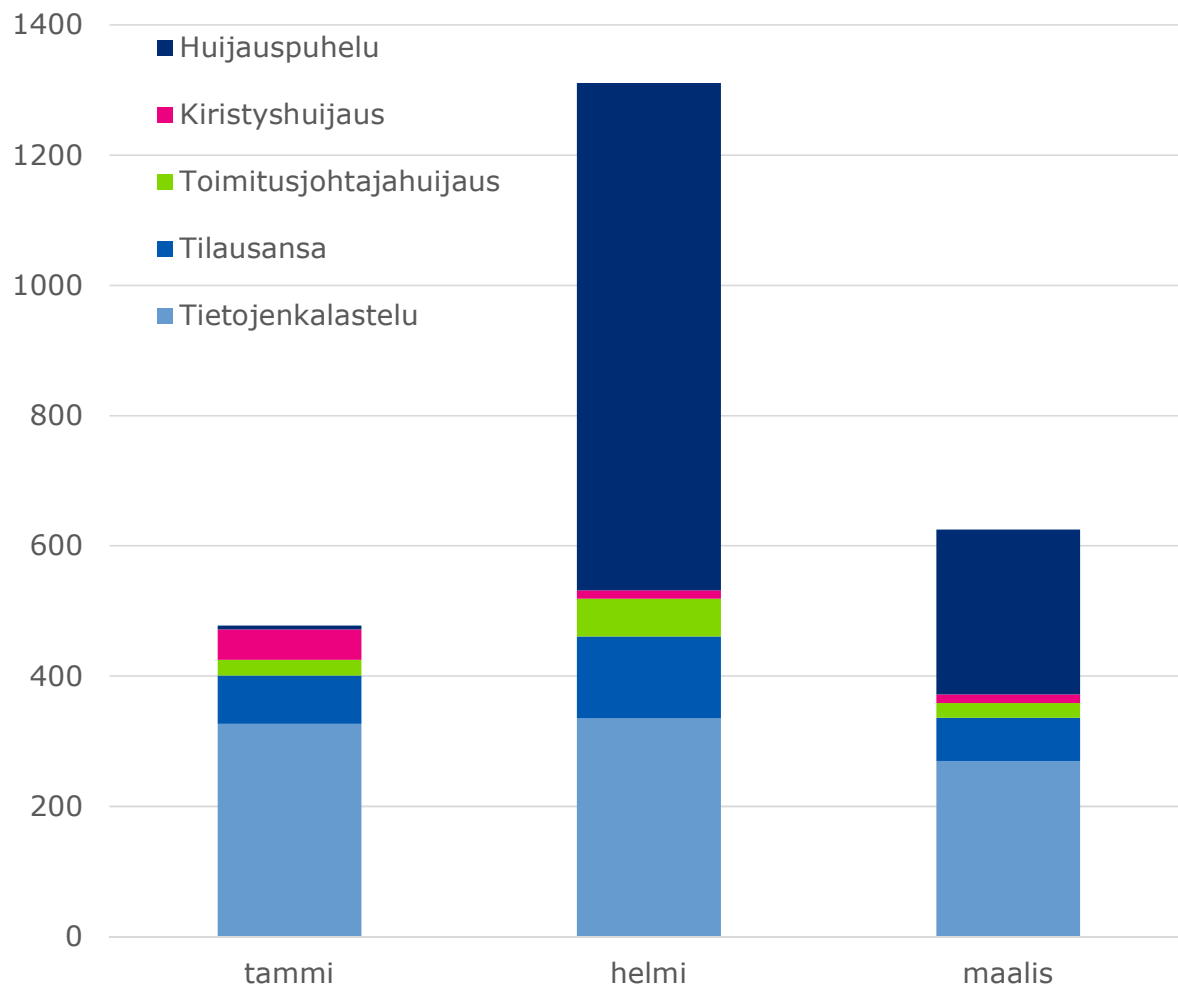
Huijaukset ja kalastelut

- ▶ Murrettuja verkkosivuja käytetään säännöllisesti sekä kotimaisten pankkitunnusten että suosittujen palveluiden käyttäjätunnusten kalasteluun.
- ▶ Edistyneissä huijauksissa nimettyä tekstiviestiä seuraa sähköposti ja linkin päässä kalastellaan pankkitunnuksia. Huijauksia tehostetaan uskottavammiksi oikeilla henkilötiedoilla.
- ▶ Korona-teemaisia huijauksia on huhtikuussa raportoitu paljon.
- ▶ Kryptovaluuttasijoitushuijauksissa käytetään luvatta mediatalojen ulkoasuja ja tunnettuja henkilöitä.

ANALYYSI

- ▶ Unohdetun salasanan palautustoimintoa käytetään yhdessä kaapatun sähköpostitilin kanssa: Kaapatun tilin avulla voi päästä käsiksi moniin muihin palveluihin.
- ▶ Väärennetyt sähköpostiviestit ovat keskeinen huijausväline. Organisaation nimissä väärennetyt viestit aiheuttavat myös mainehaittaa. Huijauksia voi estää SPF/DKIM/DMARC-asetuksilla. Asetuksilla voidaan estää organisaation osoitteiden väärentäminen ja luvaton käyttö. Asetuksia kannattaa käyttää myös vastaanotettavan postin suodatuksessa.
- ▶ Verkkosivun salaus ja sertifikaatti eivät kerro verkkosivun luotettavuudesta: salaussertifikaatti on kunnossa 73 %:lla kaikista alasotetuista haitallisista verkkosivuista.

Käsiteltyjä huijaustapauksia Q1/2020



- ▶ Alkuvuoden 2020 näkyvin trendi ovat olleet huijauspuhelimet:
- ▶ Helpdesk-huijari yrittää saada uhrin tietokoneen haltuunsa ja varastaa siten tietoja ja rahaa.
- ▶ Hälärihuijauksissa uhri yritetään saada soittamaan takaisin kalliiseen ulkomaan numeroon tai satelliittipalveluun.
- ▶ Kiristyshuijaukset ovat sähköposteja, joissa huijari uhkailee jollain tai väittää saaneensa uhrin koneen haltuunsa ja vaatii lunnaita.
- ▶ Toimitusjohtajahuijaukset kohdistuvat yrityksiin ja organisaatioihin. Väärennetyt viestit tähtäävät laskutuspetokseen.
- ▶ Tilausansoja suunnataan kaikille kuluttajille esiintyen mm. Postin, Gigantin, tai muiden tuotemerkkien nimissä. Useimmat tekstiviestihuijaukset johtavat tilausansa.
- ▶ Tietojenkalastelut ovat tavallisin tapa murtautua yrityksen verkkoon: Kalastellaan tunnuksia ja salasanoja, joilla järjestelmiin pääsee.

Q1/2020 - tilasto päivitetään kvartaaleittain



Haittaohjelmat ja haavoittuvuudet

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



Haaitaohjelmat ja haavoittuvuudet

- ▶ Haitallista sisältöä levitetään jälleen sähköpostitse eri organisaatioiden nimissä. Lähettämiseen käytetään murrettuja tilejä tai väärennetyjä lähettäjätietoja.
 - ▶ Huhtikuussa on nähty mm. Opetushallituksen nimissä levitettyjä viestejä, jossa liitteenä haitallinen tiedosto.
- ▶ Maailmalta raportoitu useita, esimerkiksi energia-alaan kohdistuvia kiristyshaittaohjelmatapauksia mm. Berkine ja EDP sekä IT-palveluntarjoajaan kohdistunut hyökkäys, Cognizant.

ANALYYSI

- ▶ Haitallisten tiedostojen levittämiseen käytetään ajankohtaisia teemoja, koska ne ovat tehokkaita.
- ▶ Teknisten kontrollien lisäksi tietoisuuden lisääminen auttaa haitallisen sisällön tunnistamisessa.



Haittaohjelmat ja haavoittuvuudet

- ▶ SaltStack Salt –hallintakehikossa, jota käytetään palvelinten ylläpidossa, on kriittisiä haavoittuvuuksia (Haavoittuvuus 13/2020):
<https://www.kyberturvallisuuskeskus.fi/fi/saltstack-salt-hallintakehikossa-kriittisia-haavoittuvuuksia>
- ▶ Tiedossa olevien hyökkäysten yhteydessä murretuille palvelimille on asennettu ainakin kryptovaluutan louhijoita.
- ▶ Haavoittuvuuden hyväksikäytön yhteydessä on myös potentiaalia laajamittaisiin ja pahoihin vahinkoihin, kuten esimerkiksi kiristyshaittaohjelman asentamiseen organisaation laajuisesti.

ANALYYSI

- ▶ Päivitä SaltStack Salt versioon 3000.2 tai 2019.2.4 mahdollisimman pian.
- ▶ Jos haavoittuvuutta on hyödynnetty, tulee koko ympäristö tarkistaa huolellisesti myös muiden haittaohjelmien varalta.
- ▶ Erityisesti pilviympäristöissä olevat hallintaratkaisut on suojattava asianmukaisesti.



Haittaohjelmat ja haavoittuvuudet

- ▶ Liferay Portal –julkaisujärjestelmä on aktiivisen hyökkäyksen kohteena.
 - ▶ Kyseessä on organisaatioille suunnattu portaaliratkaisu, josta löydettyyn haavoittuvuuteen on julkaistu hyväksikäyttökoodi maaliskuussa.
 - ▶ Kyberturvallisuuskeskus on saanut sekä eurooppalaisilta että kotimaisilta yhteistyökumppaneilta tietoja Liferay Portal -julkaisujärjestelmään kohdistuvista hyökkäyksistä. Tiedossa olevissa tapauksissa murrettuun järjestelmään on ujutettu Perl-pohjainen haittaohjelma, jonka avulla palvelin on valjastettu SSH-palvelinten murtoyrityksiin.

ANALYYSI

- ▶ Päivittämättömät asennukset on syytä päivittää pikaisesti. Vanhempiin, ei tuettuihin versioihin ei saa välttämättä enää päivitystä, mutta haavoittuvan toiminnon voi poistaa käytöstä (JSONWS).
- ▶ Lisätietoa Liferayn sivuilta: https://portal.liferay.dev/learn/security/known-vulnerabilities/-/asset_publisher/HbL5mxmVrnXW/content/id/117954271

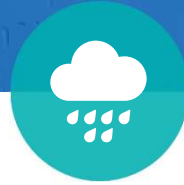


Haaitaohjelmat ja haavoittuvuudet

- ▶ Laitteiden internetiin avoimet etäyhteyspalvelut altistavat organisaatiot tietomurroille.
 - ▶ Kyberturvallisuuskeskus on huhtikuun aikana paikallistanut useita avoimia RDP-palveluja ja ottanut yhteyttä ylläpitäjiin ja suositellut jatkotoimenpiteitä.
 - ▶ Yritysten tulisi arvioida etätöön mahdollistavat ratkaisut tietoturvan näkökulmasta. Huolehdi, etteivät etätöjärjestelyt vaaranna yrityksen tietoturvaa.

ANALYYSI

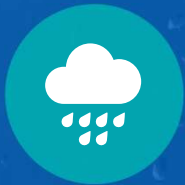
- ▶ Kyberturvallisuuskeskus on havainnut merkittävää kasvua internetiin avointen palveluiden määrässä.
 - ▶ Avoimien etäyhteyspalvelujen, esimerkiksi avoimien etätöpöytäyhteyksien ja tiedostonjakopalvelujen (esim. RDP, VNC ja SMB) määrä on kasvanut: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/suojattomien-etatyopoyta-ja-verkkoyhteyspalveluiden-maara-kasvoi-maaliskuussa>
 - ▶ Lisätietoa ja ohjeita esim. VPN-yhteyksistä: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vpn-yhteyksien-kapasiteetin-varmistaminen>



Automaatio

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

Automaatiojärjestelmiä käytetään ohjaamaan ja monitoroimaan esimerkiksi erilaisia yksittäisiä tehtäviä tai vastaavan tuotantolaitoksen palveluita tai laitteita.

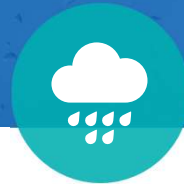


Automaatio

- ▶ Kyberturvallisuuskeskuksen vuosittainen selvitys suomalaisten tietoverkkojen suojaamattomista automaatiolaitteista tehdään viikkojen 18–21 aikana. (Tietoturva nyt! 27.4.): <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskus-kartoittaa-suojaamattomia-automaatiojarjestelmia>
- ▶ Kyberturvallisuuskeskuksen tietoon on kevään aikana tullut tapauksia, joissa suljetuissa ympäristöissä olevia päivittämättömiä laitteita, kuten teollisuusautomaatio- tai lääkintälaitteita on saastunut tunnetuilla haittaohjelmilla.
 - ▶ Kansainvälisissä uutisissa on tietoja esimerkiksi Israelin vesihuoltoon kohdistuneista tunkeutumisyrityksistä.
- ▶ Automaatiolaitteiden useista kriittisistä haavoittuvuuksista esimerkkinä Sierra Wireless AirLink ALEOS -verkkolaitteista löydetty haavoittuvuus. (ICSA-19-122-03)

ANALYYSI

- ▶ Etähallintayhteyksien avaaminen tulee tehdä huolellisen riskiarvion pohjalta.
- ▶ Laitteiden päivityksistä ja verkkojen eristämisestä tulee huolehtia.



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

- ▶ Yleisissä viestintäpalveluissa oli huhtikuussa seitsemän merkittävää häiriötä.
 - ▶ Häiriöiden määrä oli tavanomaista suurempi ja moni häiriöstä vaikutti suureen käyttäjämäärään. Häiriöiden yleisin syy oli palvelun ohjelmistovika.
 - ▶ Valtakunnallinen häiriö Telian kiinteän ja matkapuhelinverkon internetyhteyspalvelussa 25.4. aiheutti lauantapäivästä huolimatta haittaa monen tölle.
 - ▶ Kokonaisuudessaan yleiset viestintäpalvelut ovat kestäneet hyvin poikkeusoloista johtuneen tietoliikenteen lisäyksen.

ANALYYSI

- ▶ Toimivuushäiriö osuu melko harvoin yksittäisen käyttäjän kohdalle. Tällaisen tilanteen tullessa kohdalle käyttäjä voi ottaa mahdolliset ennalta valmistelemansa viestinnän varakeinot käyttöön tai sietää tilannetta, kunnes teleyritys saa häiriön poistettua.
- ▶ Kannattaa arvioida ennakolta, miten pitkiä viestintäpalveluiden katkoja organisaation keskeiset toiminnot sietävät.
- ▶ Häiriöihin voi varautua mm. eri teleyrityksiltä hankituilla liittymillä. Huoltovarmuuskriittiset yritykset voivat käyttää VIRVEä.



Verkkojen toimivuus

- ▶ Koronan seurauksena vallitsevissa poikkeusoloissa tehdään paljon etätöitä, jolloin esimerkiksi VPN-palvelun toimivuus ja kapasiteetin riittävyys ovat kriittisiä.
- ▶ Yksi mahdollinen ratkaisu tähän ongelmaan on muokata päätelaitteen reititysasetuksia, jolloin osa verkkoliikenteestä kulkee VPN-tunnelin kautta organisaation sisäverkkoon ja osa suoraan internetiin. Tätä kutsutaan VPN split -tunneloinniksi.
- ▶ Lisätietoja Tietoturva nyt! -artikkelissa:
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vpn-yhteyksien-kapasiteetin-varmistaminen>

ANALYYSI

- ▶ VPN split -tunneloinnissa voidaan parantaa etätöihin liittyvien resurssien kapasiteettia hyvinkin nopealla aikataululla.
- ▶ VPN split -tunneloinnin käyttöönotto tulee tehdä ainoastaan silloin kun organisaatiolla on tiedossa, että se pystyy tekemään sen turvallisesti.
- ▶ Lisäksi VPN split -tunnelointia harkitessa organisaatioiden on suoritettava oma riskiarviointinsa siitä, mitä tietoa ne voivat siirtää suljetun VPN-tunnelin ulkopuolelle.



Palvelunestohyökkäykset

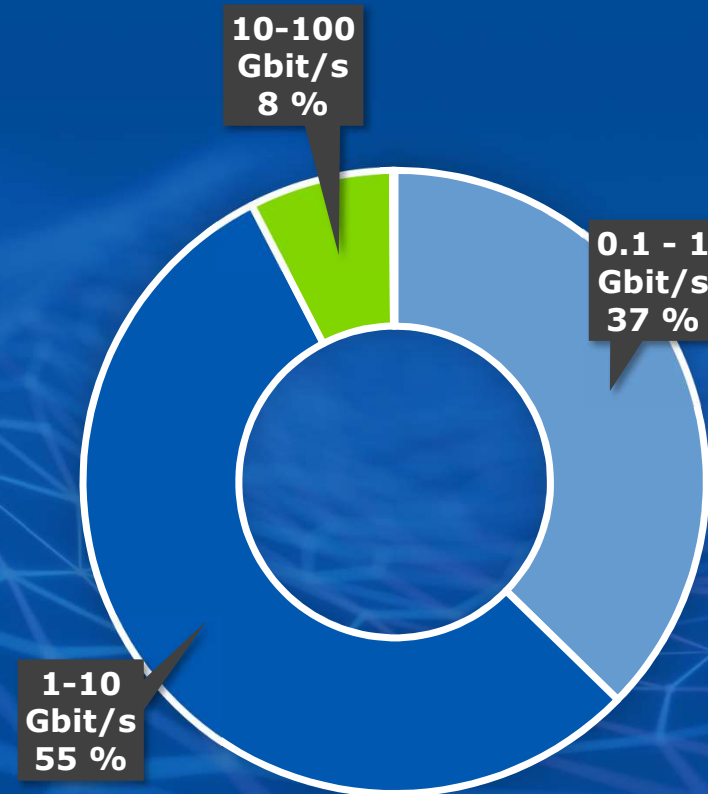
- ▶ Huhtikuu oli palvelunestohyökkäysten osalta melko rauhallinen. Raportoiduilla hyökkäyksillä ei pääasiassa ollut vaikutuksia palveluiden toimintaan.
 - ▶ Raportoiduissa hyökkäyksissä on käytetty vanhoja tuttuja TCP SYN- ja UDP-reflektiotekniikoita. UDP-puolella mm. LDAP-, CLDAP- ja NTP-palvelimet ovat suosittuja vahvistuksen lähteitä.
- ▶ Verkko-opiskeluympäristöihin tehtyt hyökkäykset lisääntyivät maaliskuussa, mutta huhtikuussa Kyberturvallisuuskeskuksen tietoon ei ole tullut uusia näihin kohdistuneita hyökkäyksiä.
- ▶ Maaliskuussa nähtiin palvelunestohyökkäyksiä, jotka vaikuttivat organisaation työntekoon häiritsemällä Skypeä ja muita sisäisiä työkaluja. Huhtikuussa tällaisia hyökkäyksiä ei raportoitu.

ANALYYSI

- ▶ Koronan seurauksena vallitsevissa poikkeusoloissa tehdään paljon etätöitä, jolloin esimerkiksi VPN-palvelun toimivuus on kriittistä.
- ▶ Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei yleensä ole vaikutuksia palveluiden toimivuuteen.

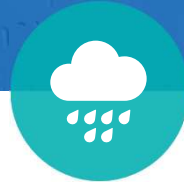
Palvelunestohyökkäysten tunnuslukuja

- 161 Gbit/s oli suurin Suomessa nähty palvelunestohyökkäys alkuvuonna 2020.
- Noin 80% hyökkäyksistä oli pituudeltaan alle 15 minuuttia.
- Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.



SUOMEEN
KOHDISTUNEIDEN
PALVELUNESTO-HYÖKKÄYSTEN
VOLYYMIT (Q1/2020 -
TILASTO PÄIVITETÄÄN
KVARTAALITTAIN.)

14.5.2020



Vakoilu

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



Vakoilu

- ▶ COVID-19-tautiin liittyvät teemat, kuten rokote- ja muu tutkimus, ovat valtioiden kasvavan kiinnostuksen kohteena. Tämä heijastuu myös kybervakoiluun, jonka keinoin esimerkiksi Kiinaan liitettyjen toimijoiden on syytetty pyrkivän edistämään maan rokotetutkimusta.
- ▶ Esimerkiksi Yhdysvallat ja Iso-Britannia ovat varoittaneet terveydenhuoltosektoriin ja koronavirukseen ja sen hoitoon liittyvään tutkimukseen ja tietoon kohdistuvasta valtiollisesta kybervakoilusta.
- ▶ Myös valtioiden päätöksenteko ja sen valmistelu ovat perinteisiä kybervakoilun kohteita, jotka ovat ajankohtaisia myös pandemia-aikana.

ANALYYSI

- ▶ COVID-19-aiheiden parissa työskentelevien organisaatioiden on syytä olettaa olevansa kasvavan ulkopuolisen kiinnostuksen kohteina – myös laittomien tiedonhankintakeinojen osalta. Kiinnostus voi kohdistua niin rokote- ja lääketutkimukseen kuin diagnostiikkaan ja muuhun tutkimus- ja tuotekehitystietoon.
- ▶ Työntekijöitä on myös syytä ohjeistaa tarkkaavaisuuteen kohdistetun tietojenkalastelun tai tietomurtoyritysten varalta sekä ilmoittamaan havainnoistaan matalalla kynnyksellä.



Vakoilu

- ▶ Myöskään koronavirus- ja COVID-19-aiheiden hyödyntämisen mahdollisuus tietomurtojen valmistelussa ja toteuttamisessa ei ole uhkana poistunut.
 - ▶ Ulkomailla on kevään aikana raportoitu mm. käyttäjätunnusten ja salasanojen kalastelusta sekä haittaohjelmien jaosta koronavirusteemalla myös valtiollisiin toimijoihin liitetyissä kampanjoissa.
 - ▶ Ainakin Kiinaan, Pohjois-Koreaan ja Venäjään liitettyjen ryhmien on uutisoitu hyödyntäneen koronavirusteemaa tavalla tai toisella.

ANALYYSI

- ▶ Organisaatioiden on hyvä ohjeistaa työntekijöitään erityiseen tarkkaavaisuuteen tilanteissa, joissa vastaanotetaan materiaalia tai viestejä uuteen, runsaasti huomiota herättävään aiheeseen liittyen.
- ▶ Ilmiö itsessään ei ole uusi, vaan kertoo pikemminkin siitä, että sekä kybervakoilussa että -rikollisuudessa hyökkäyksiä tehostetaan ajankohtaisilla ja kiinnostavilla teemoilla harhauttamalla.



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

- ▶ Liikenne- ja viestintävirasto Traficom antoi 4.5.2020 uuden määräyksen (M71) verkkotietojen ja verkon rakentamissuunnitelmien toimittamisesta. Määräyksen vaatimukset kohdistuvat sektorirajat ylittäen viestintä-, energia-, vesihuolto- ja liikenneverkkotoimijoihin.

ANALYYSI

- ▶ Määräyksen tarkoituksena on ennen kaikkea vähentää maanrakennustöistä verkkoinfrastruktuurille aiheutuvia vikatilanteita sekä edistää verkkojen yhteisrakentamista ja -käyttöä.
- ▶ Määräys tulee voimaan 1.6.2020. Fyysistä infrastruktuuria ja aktiivisia verkon osia koskevat velvoitteet tulevat kuitenkin voimaan vasta 1.10.2022, jolloin tietojen tulee olla toimitettu Sijaintitietopalveluun.
- ▶ Tutustu tarkemmin määräykseen ja sen perusteluihin:
<https://www.finlex.fi/fi/viranomaiset/normi/480001/45988>

Arjen kyberturvallisuus – huhtikuu on kuukaudesta hakkeroiduin

Vappuvisa toi esille tunnistamisen vaikeudet

- ▶ Kalastelua tehdään käytännössä lähes kaikkien palveluiden nimissä jatkuvasti. Huijausta ei aina voi tunnistaa ulkonäöltä.
- ▶ Lue lisää vappuvisan tuloksista:
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vappuvisan-tulokset-petkuhuiputusta-vaikea-tunnistaa>
- ▶ Lue lisää neuvoista epäilyttävien sivujen tunnistamiseksi:
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-epailyttavien-sivujen-tunnistamiseksi>

Kiristyshuijauksia liikkeellä runsaasti – älä usko huijarien väitteitä

- ▶ Huijarit ovat jälleen aktivoituneet aikuisviihdeemaisten kiristysviestien lähettelyssä.
- ▶ Viestit ovat huijausta, eikä huijareille pidä missään nimessä maksaa lunnaita.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kiristyshuijauksia-liikkeella-runsaasti-ala-usko-huijarien-vaitteita>

Team Whackin uusi kausi julkaistu

- ▶ Ylen dokumenttisarjassa Team Whack - kaikki on hakkeroitavissa, kolme ammattihakkeria paljastaa, kuinka sinunkin elämäsi voidaan sekoittaa.
- ▶ Toisella kaudella kohteeksi joutuvat yksityiset älylaitteet, pelistriimi ja vakuutusyhtiö. Tämä kaikki tehdään kohteiden luvalla.
- ▶ Tavoitteena ammattihakkereilla on auttaa suojautumaan oikeilta hyökkäyksiltä.
- ▶ <https://areena.yle.fi/1-4664681>

Kutsumattomia vieraita linjalla

- ▶ Etäkokouksissa, tapahtumissa ja nettikonserteissa on nähty kutsumattomia vieraita, jotka levittävät haitallista sisältöä tavalla tai toisella.
- ▶ Striimaustapahtumia on häiritty ja oikeita linkkejä yritetään vaihtaa hyökkääjien omiin linkkeihin, jotka johtavat kalastelusivuille ja tilausansoihin.
- ▶ Etäkokouksen asetukset on hyvä tarkistaa, ettei mukaan pääse kutsumattomia osallistujia:
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/valitse-videoneuvotteluratkaistu-kayttotarpeen-ja-tiedon-luottamuksellisuuden-mukaan>



Ajankohtaista Kyberturvallisuuskeskuksesta

Osataanko teillä torpata tietoturvauhkia? Kyberharjoittelusta hyötyvät kaikki

- ▶ Astu matkaan kun teemme mielikuvitusreissun tavalliseen toimistotyöpäivään Kyberilän vesihuollossa.
- ▶ Matkan aikana huomaamme, että uhkaavien tilanteiden kyberharjoittelu on yksi halvimista ja helpoimmista tavoista ylläpitää turvallisuutta.
- ▶ Artikkelin lopusta löytyvät Kyberturvallisuuskeskuksen Kyberharjoitusopas ja -skenaariot.
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/osataanko-teilla-torpata-tietoturvauhkia-kyberharjoittelusta-hyotyvat-kaikki>

Toimi näin, jos havaitset tietoturvapoikkeaman

- ▶ Kun tietoturvapoikkeama osuu kohdalle, siitä on hyvä ilmoittaa sekä viranomaisille että IT-tuelle. Ilmoituksesi avulla viranomaiset voivat selvittää tapausta ja olla tukenasi asian käsittelyssä.
- ▶ Viranomaisena toimintamme perustuu luottamukseen. Siksi tietoturvailmoituksen yhteydessä kysymme, voiko Kyberturvallisuuskeskus vaihtaa tapauksesta tietoja Poliisin kanssa.
- ▶ Luvan avulla tapauksen selvittäminen helpottuu ja nopeutuu.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/toimi-nain-jos-havaitset-tietoturvapoikkeaman>

Yhteistyö varmistaa yhteiskunnan digitaalisen turvallisuuden

- ▶ Kyberturvallisuuskeskus, Digipooli ja Huoltovarmuuskeskus tuottavat poikkeustilan aikana yhteistyössä digialan tilannekuvaa.
- ▶ Yhteistyössä saatua tietoa raportoidaan yritysten ja valtionhallinnon käyttöön. Raportit käsitellään ja tilannekuvan muodostumista seurataan säännöllisesti yhteisissä etätapaamisissa.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/yhteistyo-varmistaa-yhteiskunnan-digitaalisen-turvallisuuden>



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)