



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Tammikuu 2020

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



rauhallinen



huolestuttava



vakava

Kybersää tammikuu 2020

Tietomurrot ja -vuodot

- ▶ Tietomurtoja käytetään kiristyshaittaohjelmien asentamiseen
- ▶ Office 365 –tietomurrot jatkuvat entiseen tapaan



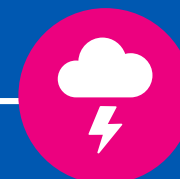
Huijaukset ja kalastelut

- ▶ Organisaatioihin kohdistuvat laskutushuijaukset ovat aiheuttaneet tuntuvia rahan menetyksiä
- ▶ Henkilökunnan kouluttaminen auttaa suojautumaan huijauksia vastaan



Haittaohjelmat ja haavoittuvuudet

- ▶ Kriittisten päivitysten laiminlyönti vaarantaa yritystoiminnan jatkuvuuden



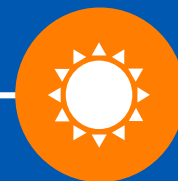
Automaatio

- ▶ Tutkimuksen mukaan eri valtiolliset toimijat ovat aktivoituneet energiasektorilla Yhdysvalloissa viime aikoina



Verkojen toimivuus

- ▶ palvelunestohyökkäyksillä ei ollut merkittäviä vaikutuksia palveluiden toimintaan
- ▶ Määräys teletoiminnan häiriötilanteista uudistettiin

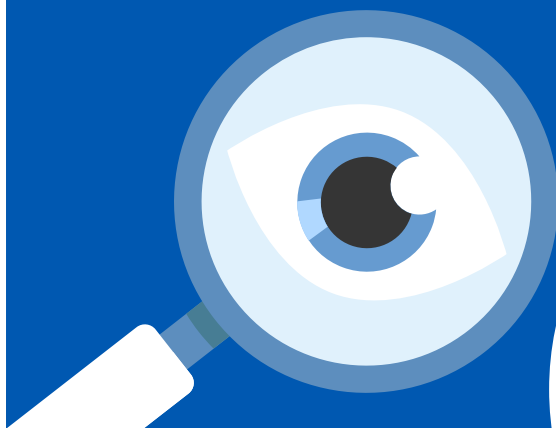


Vakoilu

- ▶ Vakoilu kohdistuu valtioiden lisäksi myös yrityksiin



Kuukauden tunnuslukuja



130 000€

TAMMIKUUN AIKANA
KYBERTURVALLISUUSKESKUS ON
SAANUT ILMOITUKSIA
LASKUTUSPETOKSIIN LIITTYEN.

ONNISTUNUT PETOS VOI TULLA
KALLIIKSI, KUTEN TODELLINEN
ESIMERKKILUKU KERTOO.



56 %

YLI PUOLET
KYBERTURVALLISUUSKESKUKSELLE
RAPORTOIDUISTA TIETOMURTO-
TAPAUKSISTA KOSKEE OFFICE-365
TIETOMURTOJA.

TRENDI ON OLLUT PYSYVÄ JA
OFFICE-365-TAPAUKSET OVAT UUSI
NORMAALI.



1

TAMMIKUUN AIKANA
OLI VAIN YKSI VAKAVA
VERKKOJEN
TOIMIVUUSHÄIRIÖ

Top 5 kyberuhat - merkittävät pitkän 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 kohdistetuissa 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 pitkän 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 tietoturvaluottoissa 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 korjaus ollut saatavilla jo pitkään, mutta syystä tai toisesta haavoittuvuutta ei ole korjattu.
- ▶ Mitä pidempään haavoittuvuuden korjaamisessa kestää tai korjausta siirretään myöhemmäksi, sitä korkeammaksi hyväksikäyttämisen riski kasvaa. Esimerkkejä on lukuisia, esim. Pulse Secure VPN:n haavoittuvuus oli tiedossa jo viime huhtikuussa ja korjaus saatavilla elokuussa, mutta vielä tammikuussakin sitä käytetään hyökkäyksiin.

CASE

Pulse Secure VPN:stä korjattiin kriittinen haavoittuvuus huhtikuussa 2019. Haavoittuvuuden hyväksikäyttömenetelmä julkaistiin elokuussa, jonka jälkeen hyödyntämisyrityksiä alettiin näkemään. Silti vielä tammikuussa 2020 haavoittuvuus on useissa kohteissa päivittämättä, ja sitä hyödynnetään yhä mm. laajavaikutteisissa kiristyshyökkäyksissä.

Top 5 kyberuhat – merkittävät pitkän 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 käyttäjätunnuksia ja salasanoja Office 365 -tuotteisiin ja sähköpostiin.
- ▶ 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.

Top 5 kyberuhat – merkittävät pitkän 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 sattumalta.
- ▶ Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja. Jos rikolliset havaitsevat huonosti suojatun ympäristön kiristämisen arvoiseksi, siihen saatetaan kohdistaa Big Game Hunting –toimintaa.
- ▶ Yhdysvalloissa tilannetta voi kuvata jo epidemiaksi. Uusia ilmoituksia laajoista kiristyshaittaohjelmatarunnoista tulee kansainvälisesti viikoittain.

CASE

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

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

Top 5 kyberuhat – merkittävät pitkän 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.

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja>

<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kaytosta-poistuvien-palveluiden-alasajo-tulee-tehda-huolella>

OHJE

Top 5 kyberuhat – merkittävät pitkän 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 ennakkoon. Suunnitelmat ovat vain luokkaa "palautetaan tiedot varmuuskopioista". Palautumisen tärkeysjärjestyksiä ja resursseja ja aikajänteitä ei mietitä ennakkoon.
- ▶ 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.

▶ <https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas>



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



Tietomurrot ja -vuodot

Osiossa käsitellään suojauskeinoja sekä tietoomme tulleita trendejä tietomurroista ja -vuodoista. Tietomurroilla voidaan aiheuttaa esimerkiksi kohteena olevalle organisaatiolle taloudellisia tappiota. Myös kohteen maine voi kärsiä.



Tietomurrot ja vuodot

- ▶ Tietomurtoja käytetään kiristyshaittaohjelmien asentamiseen
 - ▶ Tietomurrot ovat verkkorikollisille yleinen tapa tavoitella taloudellista hyötyä.
 - ▶ Tietomurto tarjoaa usein pääsyn kohteeksi joutuneen organisaation järjestelmiin.
 - ▶ Esimerkiksi valuutanvaihtoyritys Travelexin koko verkkoliiketoiminta oli suljettu koko tammikuun
 - ▶ <https://www.tekniikkatalous.fi/uutiset/valuutanvaihtojatilta-petti-pahasti-tietoturva-asiakkaiden-lomasaastot-teilla-tietymattomilla-hakkerikiristajilta-lunnasvaade/b24aa5fd-8dd0-4e13-b0e7-4a6d2ae656a3>

ANALYYSI

- ▶ Tietomurtojen avulla tehty kiristyshaittaohjelma on ns. Big Game Hunting -toimintaa.
- ▶ Kiristyshaittaohjelma salaa kohdeorganisaatiolle tärkeää tietoa. Salauksen purkamisesta pyydetään lunnaita. Lunnasvaatimusta saatetaan tehostaa uhkaamalla julkaista sensitiivistä tietoa, jota on kopioitu kohdeympäristöstä ennen tietojen salaamista.
- ▶ Tietomurron kohteeksi joutuminen voi haitata merkittävästi organisaation toimintaa ja aiheuttaa merkittävän maineriskin.



Tietomurrot ja vuodot

- ▶ Office 365 –tietomurrot jatkuvat päivittäin
 - ▶ Office 365 –tietomurroissa pyritään mm. saamaan haltuun luottamuksellista tietoa, väärentämään laskutusliikennettä tai levittäytymään muihin organisaatioihin. (kts. kalvo 16)
 - ▶ Kyberturvallisuuskeskus on julkaissut ohjeen Office 365 –ympäristön koventamisesta. Ohje löytyy osoitteesta: <https://www.kyberturvallisuuskeskus.fi/fi/ohjeet>

ANALYYSI

- ▶ Tällä hetkellä saamme päivittäin useamman ilmoituksen Office 365-tietomurrosta. Määrä on kasvanut kuluneen vuoden aikana, eikä merkkejä ilmiön laantumisesta ole. Tietomurto haittaa käytettävyyttä ja voi aiheuttaa taloudellisia menetyksiä.
- ▶ Monet Office 365 -tietomurron yritykset tehdään aiemmin murrettua tiliä hyödyntäen. Siksi on syytä olla tarkkana myös tutun lähettäjän epätavallisen sähköpostin suhteen.
- ▶ Monivaiheinen tunnistautuminen estäisi suurimman osan Office 365 -tietomurroista.



Huijaukset ja kalastelut

Osiossa käsitellään muun muassa käyttäjätunnusten ja salasanojen kalastelua, laskutuspetoksia, yrityshuijauksia ja kiristyksiä. Osio sisältää asiaa myös pankkitunnus- ja maksukorttikalastelusta sekä muista geneerisistä yksittäisten uhrien huijauksista.



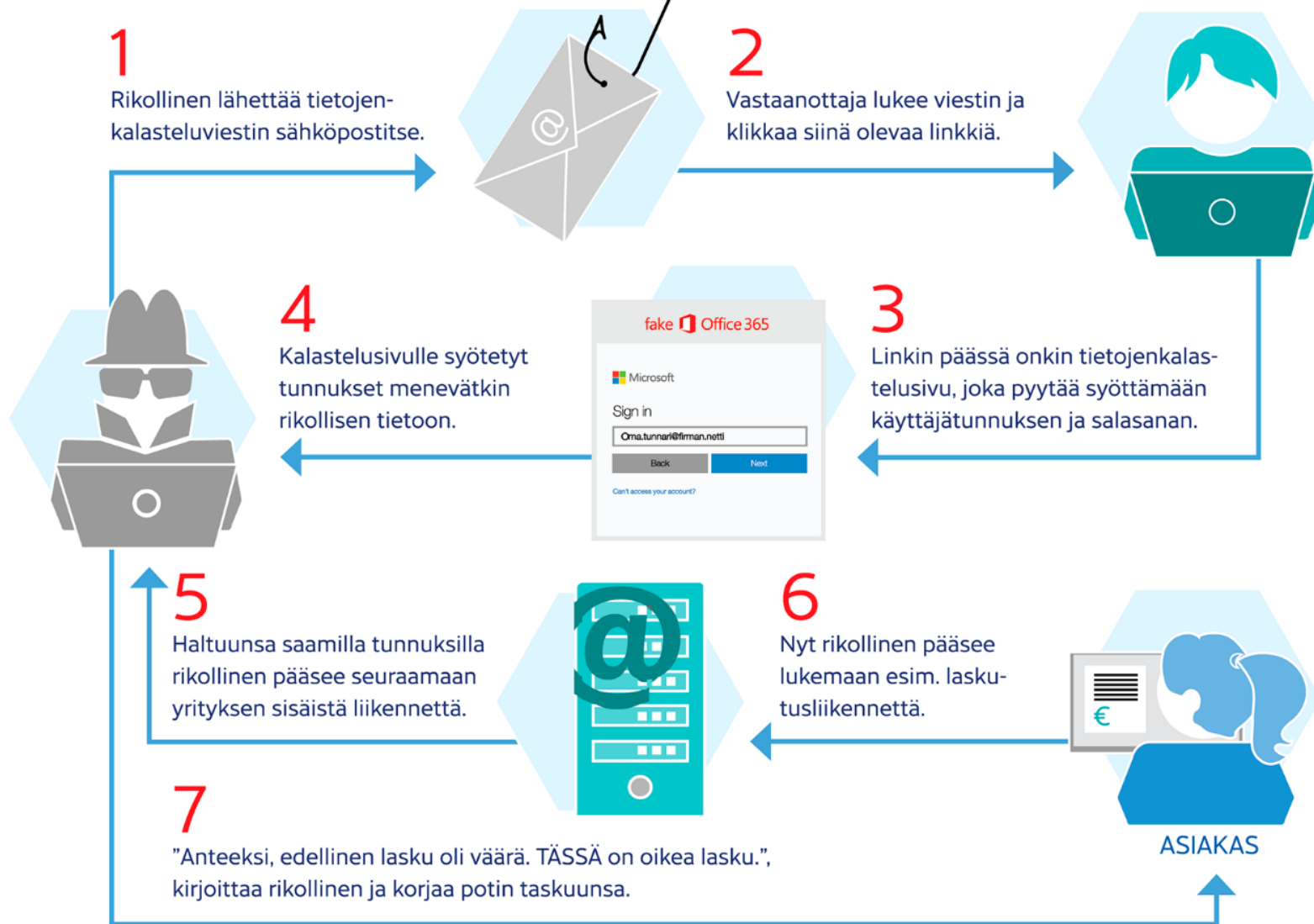
Huijaukset ja kalastelut

- ▶ Organisaatioihin kohdistuvat laskutushuijaukset ovat aiheuttaneet tuntuvia rahan menetyksiä
 - ▶ EU-kilpailutusten julkisia tietoja on käytetty huijauksiin. Tietojen julkisuus ja kilpailutusten läpinäkyvyys on periaattellisesti hyvä asia, mutta se auttaa myös huijareita laatimaan erityisen uskottavia laskutuspetoksia.
- ▶ 50 % Kyberturvallisuuskeskuksen tietoon tulleista Office 365 -kalasteluyrityksistä johtaa tietomurtoon

ANALYYSI

- ▶ Tekniset keinot eivät kokonaan pysty torjumaan alati muuntuvia huijauksia, joten laskuliikennettä käsittelevän henkilökunnan kouluttaminen auttaa paremmin suojautumaan huijauksia vastaan.
 - ▶ Pelisäännöt ja hyväksyntäprosessit selviksi ulkoistettujen laskutuspalveluiden kanssa. Vastuuta ei voi ulkoistaa, se on aina omistajalla.
 - ▶ Laskutuspetokset huomataan usein vasta viikkoja vahingon jälkeen, jolloin rahojen palauttaminen on merkittävästi vaikeampaa.

Tietojenkalastelu – yleisin yrityksiin osuva verkkorikos – Office365 huijauksen vaiheet:





Haittaohjelmat ja haavoittuvuudet

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



Haittaohjelmat ja haavoittuvuudet

- ▶ Etäkäyttöratkaisussa olevia haavoittuvuuksia hyödynnetään aktiivisesti tietomurroissa, haittaohjelmien levittämiseen ja big game hunting -toimintaan
 - ▶ Esimerkiksi Microsoft Remote Desktop Gatewayn haavoittuvuus on merkittävä riski, mikäli päivittämättä ja käytössä
 - ▶ <https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus-microsoft-remote-desktop-gatewayssa>

ANALYYSI

- ▶ Haavoittuvuuden hyödyntäminen on usein vain ensimmäisiä vaiheita hyökkäyksessä. Onnistuessaan tämä voi johtaa esimerkiksi tietomurtoon ja tiedostojen salaukseen.
- ▶ Jos päivittäminen on viivästynyt niin pyri varmistumaan, ettei haavoittuvuutta ole jo hyödynnetty!
- ▶ On hyvä muistaa, että eri ilmiöt liittyvät toisiinsa ja niiden vaiheet voivat olla eri toimijan toteuttamia.



Haittaohjelmat ja haavoittuvuudet

- ▶ Mittavia lunnaita vaativan big game hunting -ilmiön uhreja on useita myös Suomessa
 - ▶ Suomalaisissa yrityksissä havaittu Sodinokibi-haittaohjelmatartuntoja, joissa haittaohjelmaa levitetään hyökkääjän toimesta organisaatiossa mahdollisimman laajalle ja lopuksi salataan organisaation tiedot samanaikaisesti.
 - ▶ Tiedostojen palauttamisesta hyökkääjä vaatii huomattavia lunnaita, tyypillisesti satojatuhansia euroja.

ANALYYSI

- ▶ Hyökkääjät ovat tunkeutuneet kohteisiin käyttäen internetiin avoimia, päivittämättömiä palveluita. Esimerkkejä tarkistettavista ovat Citrix ja Pulse Secure VPN, Sharepoint.
- ▶ Kriittisten päivitysten laiminlyönti vaarantaa yritystoiminnan jatkuvuuden
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuuspaivitykset-juoksukisa-hyvaksikayttoa-vastaan>



Haittaohjelmat ja haavoittuvuudet

- ▶ Kriittinen nollapäivähaavoittuvuus Internet Explorerissa ja Windows 7 -käyttöjärjestelmän sekä useiden muiden tuotteiden tuki päättynyt
 - ▶ Kyberturvallisuuskeskus suosittelee vanhentuneiden käyttöjärjestelmien ja ohjelmien pikaista päivittämistä, jos se vain on mahdollista.
 - ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/windows-7-kayttojarjestelman-seka-useiden-muiden-tuotteiden-tuki-paattyy-tanaan>
 - ▶ <https://www.kyberturvallisuuskeskus.fi/fi/kriittinen-nollapaivahaavoittuvuus-internet-explorerissa-cve-2020-0674>

ANALYYSI

- ▶ Tuen päätyttyä käyttöjärjestelmät ovat aiempaa alttiimpia tietomurroille ja muille pahantahtoïsille toimille, koska uusia niistä löydettyjä haavoittuvuuksia ei enää korjata.
- ▶ Internet Explorerin sijaista suosittelemme käyttämään muita selaimia.



Haittaohjelmamat ja haavoittuvuudet

- ▶ SHA-1-tiivistefunktio on lopullisesti murrettu
 - ▶ SHA-1-tiivistefunktiota vastaan on julkaistu käytännöllinen hyökkäys, minkä vuoksi sitä ei tule enää käyttää eheyden varmistamiseen.
 - ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/sha-1-tiivistefunktio-lopullisesti-murrettu>

ANALYYSI

- ▶ Tietotekniikassa käytetään tiedon oikeudellisuuden tarkastamiseksi erilaisia tarkastussummia.
- ▶ Vanhentunut algoritmi SHA-1 on edelleen laajalti käytössä varmenteissa ja useissa sovelluksissa, mutta sen käytöstä pitäisi luopua, koska tiedon eheyteen ei voida enää luottaa.
- ▶ Jos SHA-1 on vielä käytössä niin on syytä siirtyä käyttämään turvallisempia vaihtoehtoja kuten SHA-2-tiivistefunktioiden variantteja tai uudempaa SHA-3-standardia.



Automaatio

Tämä osio sisältää alan uutisia ja ilmiöitä kotimaasta ja ulkomailta. Automaatiojärjestelmiä käytetään ohjaamaan sekä monitoroimaan esimerkiksi erilaisia yksittäisiä tehtaan tai muun vastaavan tuotantolaitoksen palveluita tai laitteita.



Automaatio

- ▶ Dragosin tutkimuksen mukaan eri valtiolliset toimijat ovat aktivoituneet Yhdysvalloissa viime aikoina
 - ▶ Samat ryhmät voivat kohdistaa toimintansa muuallekin
 - ▶ Ryhmät ovat tutkimuksen mukaan laajentamassa mm. energiasektorilla sen eri liiketoimiin, öljyn- ja kaasuntuotantoaloilta sähköntuotantoon.

ANALYYSI

- ▶ On syytä huomioida, että ryhmät keskittyvät välillä laajemminkin saman toimialan eri osa-alueisiin, jolloin organisaatioiden yhteistyön ja tiedonvaihdon tärkeys on hyvä huomioida.
- ▶ Huomiota on hyvä alihankintaketjuihin, esimerkiksi etähallintayhteyden turvallisuutta parantaviin VPN-ratkaisuihin on kohdistettu hyökkäyksiä, jonka onnistuessa hyökkääjä pääsee sisään. Organisaation korkeaksi riskiksi on syytä priorisoida ulkoistukset.



Verkkojen toimivuus

Osio sisältää tietoa kotimaisista yleisten viestintäpalveluiden merkittävistä toimivuushäiriöistä, muiden ICT-palveluiden huomattavista häiriöistä ja palvelunestohyökkäyksistä Suomessa ja ulkomailla.



Verkkojen toimivuus

- ▶ Tammikuussa vain yksi merkittävä toimivuushäiriö: kuitukatko Elisan verkossa
 - ▶ Lisäksi DNA:n ja Telian yhteisverkossa oli Pohjois-Suomessa laaja häiriö 7.1. Vika korjattiin niin nopeasti, ettei se ehtinyt aiheuttaa merkittävää haittaa.
 - ▶ Teleyritykset kykenevät entistä paremmin rajaamaan häiriöiden vaikutuksia ja korjaamaan häiriöt nopeasti.

ANALYYSI

- ▶ Merkittävien toimivuushäiriöiden määrä on laskenut vuosien ajan. Pieniä häiriöitä tapahtuu ja korjataan kuitenkin päivittäin satoja tai tuhansia. Ne vain nykyään harvoin kumuloituvat alueeltaan laajoiksi ja pitkäkestoisiksi.
- ▶ Merkittävien häiriöiden määrän laskeminen ei tarkoita, etteikö käyttäjien yhä pitäisi varautua häiriöihin. Pienikin palvelun häiriö voi haitata käyttäjää vakavasti, kun se sattuu sopivaan aikaan sopivassa paikassa.



Verkkojen toimivuus

- ▶ Traficomın määräys 66 teletoiminnan häiriötilanteista uudistettiin
 - ▶ Keskeisimmät muutokset: teleyrityksille asetetut vaatimukset häiriöiden tilastoinnista kevenivät. Myös automatisoidun palvelunestohyökkäyksistä ilmoittamisen periaatteista säädettiin.

ANALYYSI

- ▶ Palvelunestohyökkäyksiä koskeva automaattinen tietojenvaihto edellyttää vielä tietojärjestelmäkehitystä sekä teleoperaattoreilta että Traficomilta. Tehokkaan tiedonvaihdon myötä Kyberturvallisuuskeskus voi tukea entistä paremmin sekä palvelunestohyökkäysten kohteita että teleoperaattoreita.
- ▶ Määräys 66: <https://www.finlex.fi/fi/viranomaiset/normi/480001/42167>



Palvelunestohyökkäykset

- ▶ Tammikuussa raportoiduilla hyökkäyksillä ei ollut vaikutusta palveluiden toimivuuteen hyvän varautumisen vuoksi.
- ▶ Volyymiltään hyökkäykset ovat tyypillisesti 1-10 Gbit/s luokkaa, mutta myös suurempia nähdään säännöllisesti.
- ▶ Palvelunestohyökkäysellä kiristämistä nähdään säännöllisesti.
 - ▶ Tekijästä riippuen kyse on vain hämäyksestä, mutta välillä niihin liittyy oikeita demonstraatiohyökkäyksiä.

ANALYYSI

- ▶ Raportoiduissa hyökkäyksissä on käytetty vanhoja TCP SYN- ja UDP reflektio -tekniikoita. Vaikeammin torjuttavia sovellustason hyökkäyksiä nähtiin muutamassa tapauksessa osana muuta hyökkäystä. Pahimmillaan yksitaiseen palveluun kohdistunut palvelunestohyökkäys voi sivuvaikutuksena estää yrityksen koko internetliikenteen.
- ▶ Jos organisaatio on etukäteen varautunut hyökkäyksiin, palvelunestohyökkäyksillä ei tyypillisesti ole vaikutuksia palveluiden toimivuuteen. Volymetrysten hyökkäysten lisäksi kannattaa huomioida myös sovellustason hyökkäyksiin varautuminen.

Palvelunestohyökkäykset ja niillä uhkailu 1/2

- ▶ Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (85 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- ▶ Yli puolet havainnoiduista yli 100Mbit/s hyökkäyksistä on volyymiltään 1-10 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- ▶ Yli 10 Gbit/s hyökkäyksiä havaitaan Suomessa päivittäin.
- ▶ **Varautumisessa kannattaa arvioida lyhyenkin palvelukatkoksen toiminnalle mahdollisesti aiheuttamia haittoja.**

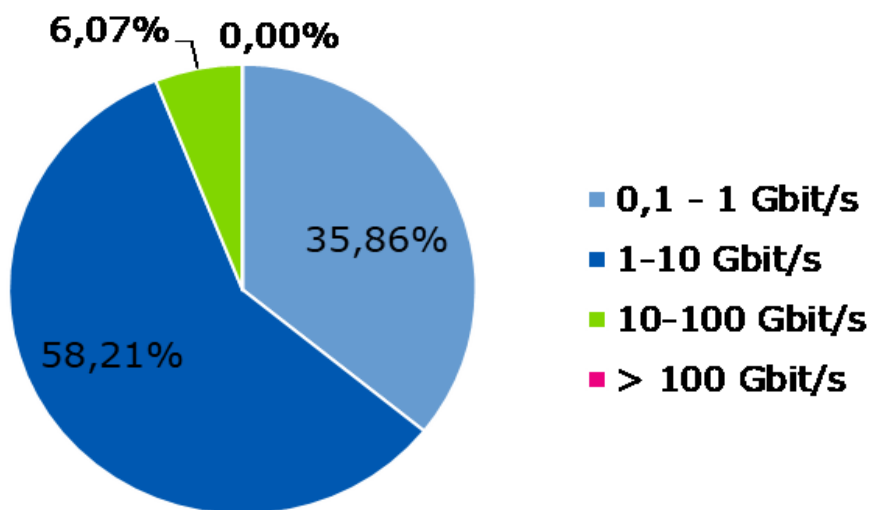
Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä (lähde: teleyritykset)

2019/Q4:
n. 54 Gbit/s
(kesto 8 min)

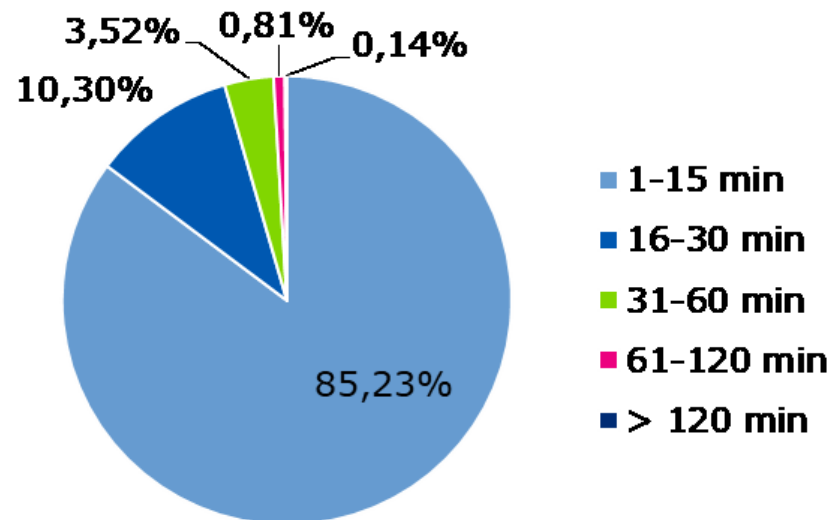
2019/Q3:
n. 39 Gbit/s
(kesto 64 min)

2019/Q2:
n. 79 Gbit/s
(kesto 4 min)

Palvelunestohyökkäykset ja niillä uhkailu 2/2



Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.



Suomeen kohdistuneiden palvelunestohyökkäysten kesto.

Huom! Tilastot päivitetään kvartaaleittain. Saamme tietoa palvelunestohyökkäyksistä teleyrityksiltä, koska Kyberturvallisuuskeskukselle ilmoitetaan vain murto-osa tapahtuneista palvelunestohyökkäyksistä.



Vakoilu

Osiossa käsitellään valtiollisten toimijoiden tai niihin liitettyjen ryhmien harjoittamaa kybervakoilua ja -vaikuttamista. Tavoitteena voi olla poliittinen tiedonhankinta, teollisuus- tai muu yritysvakoilu tai esimerkiksi tietojärjestelmien tuhoaminen tai sen valmistelu.



Vakoilu

- ▶ Teollisuusvakoilun tai muun tiedonkeruun lisäksi yrityksiin voi kohdistua myös sabotaasioperaatioita osana valtioiden välisiä konflikteja.
- ▶ Esimerkiksi bahrainilaiseen öljy-yhtiöön kohdistui tiettävästi joulukuun lopussa hyökkäys, jonka tarkoituksena oli tuhota järjestelmiä.
- ▶ Muun muassa APT33-nimellä tunnettu ryhmä*, joka on julkisuudessa liitetty Iraniin, on osoittanut kykynsä sabotaasioperaatioihin.

ANALYYSI

- ▶ Järjestelmiä tuhoavat haittaohjelmat tai operaatiot voivat lamauttaa yrityksen toiminnan tai haitata sitä vakavasti.
- ▶ Riski on kohonnut erityisesti Lähi-idän alueella toimivilla energia- ja petrokemian teollisuuden organisaatioilla: <http://www.fbcuae.fi/blog/2019/11/24/cyber-threats-can-be-regional>
- ▶ Myös muualla on havaittu yrityksiä murtautua kriittisen infrastruktuurin, kuten sähköalan yhtiöiden, tietojärjestelmiin (ks. lisää Automaatio-osiosta).

* APT-ryhmillä tarkoitetaan organisoituneita ryhmiä, jotka toiminnallaan edistävät jonkin valtion poliittisia tarkoitusperiä kyberoperaatioin.



Vakoilu

- ▶ Itävallassa paljastui valtionhallintoon kohdistunut vakava tietomurto
 - ▶ Julkisuudessa motiivina on arvioitu olevan valtiollinen vakoilu.
 - ▶ Tammikuun alussa tapahtuneen tietomurron kohteena oli Itävallan ulkoministeriö.
 - ▶ Hyökkäys havaittiin päivässä ja vastatoimiin ryhdyttiin nopeasti. Itävallan ulkoministeriö ei ole kertonut, mitkä hyökkäyksen lopulliset vaikutukset tai hyökkääjän tavoite oli.
 - ▶ <https://www.bbc.com/news/world-europe-50997773>

ANALYYSI

- ▶ Valtionhallintoon kohdistuva laitton tiedonhankinta on edelleen kybervakoilun yksi keskeinen tavoite.
- ▶ Tavoitteena on esimerkiksi hankkia tietoa poliittisesta päätöksenteosta, edistää omia poliittisia asemia tai arvioidaan varautumista ja kyvykkyyttä.
- ▶ Hyökkäysten nopea havaitseminen rajoittaa niiden vaikutuksia ja lisävahinkojen syntymistä.



Tietoturva-alan kehitys

Osio sisältää tietoa keskeisistä uudistuksista esimerkiksi alaa koskevan lainsäädännön tai asetusten päivityksiin liittyen. Kerromme kaikille tärkeää kyberturvallisuustietoa ja Kyberturvallisuuskeskuksen ajankohtaisista asioista.



Oikeudelliset asiat 1/2

- ▶ Lausunnolla hallituksen esityksen luonnos, joka koskee sähköisen viestinnän palveluista annetun lain uudistamista

- ▶ Ehdotuksella pannaan täytäntöön sähköistä viestintää koskeva teledirektiivi (1972/2018 EU) ja audiovisuaalisia mediapalveluita koskeva AVMS-direktiivi (1808/2018 EU). Lisäksi esityksessä ehdotetaan yksittäisiä muita, kansallisista tarpeista lähteviä muutoksia.
- ▶ Annetut 70 lausuntoa löytyvät linkistä:
<https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=36773abd-fb0b-4593-a36a-0d843e1af094>
- ▶ Uudistuksen seurantaryhmän seuraava kokous on pe 14.2. klo 13 ja seurattavissa YouTubessa: <https://www.youtube.com/watch?v=t8AsQoPCKk4>



Oikeudelliset asiat 2/2

- ▶ Sähköisen viestinnän palveluista annetun lain uudistuksella pantaisiin täytäntöön kyberturvallisuusasetuksessa jäsenvaltioille asetettu velvoite nimetä yksi tai useampi kansallinen kyberturvallisuussertifiointin myöntävä viranomainen. Velvollisuus toimia kansallisena kyberturvallisuussertifiointin valvontaviranomaisena lisättäisiin Liikenne- ja viestintäviraston erityisiin tehtäviin, sillä kyseiset tehtävät sijoittuvat luontevimmin Liikenne- ja viestintäviraston Kyberturvallisuuskeskukseen.
- ▶ Esityksellä katsotaan olevan myönteisiä tietoyhteiskuntavaikutuksia, sillä kyberturvallisuusasetuksen mukaisen sertifiointi-kehityksen tavoitteena on nostaa kyberturvallisuustasoa unionissa ja yhdenmukaistaa eurooppalaiset kyberturvallisuuden sertifiointijärjestelmät unionin tasolla.
- ▶ Sertifiointijärjestelmän tavoitteena on lisätä kansalaisten ja yritysten tietoturvaa. Liikenne- ja viestintäviraston nimeäminen asiasta vastaavaksi viranomaiseksi tukee tavoitetta.

Arjen kyberturvallisuus

Tietoturvan selviytymispakki koteihin ja toimistoihin - 3 uhkaa ja ratkaisua

- ▶ Jos tunnistat verkkohuijaukset, päivität älylaitteesi ja käytät hyviä salasanoja, tärkeät tietosi pysyvät turvassa. Työpaikalla oman tietoympäristön ja käytössä olevien sovellusten sekä järjestelmien tuntemus antavat hyvän pohjan kyberuhilta suojautumiseen.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvan-selviytymispakki-koteihin-ja-toimistoihin-3-uhkaa-ja-ratkaisua>

Tilausansa kuluttajan kiusana

- ▶ Kyberturvallisuuskeskus sai useita ilmoituksia tammikuun aikana. Tilausansoja on levitetty aktiivisesti ja usean toimijan tahosta. Tilausansa-sivuilla viitataan tunnettuihin tuotteisiin ja palveluihin. Tilausansa leviää nopeasti tekstiviestin ja sähköpostin välityksellä
- ▶ Ohje: Näin suojaudut nettihuijaukselta
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuujaukselta>

Yhteiskuntamme haavoittuvuuksia ei korjata vain keskustelemalla

- ▶ Vuoden 2020 ensimmäisessä Tietoturva nyt! -artikkelissamme käydään läpi kuluneen vuoden mieleenpainuvimpia kybertapahtumia.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/yhteiskuntamme-haavoittuvuuksia-ei-korjata-vain-keskustelemalla>



Suomalaisille lähetetään edelleen pornokiristysviestejä.

Kyberturvallisuuskeskus havaitsi tammikuussa viestipiikin, jossa suomalaisille lähetettiin pornokiristysviestejä. Ilmiö ei ole uusi, mutta tammikuun aikana viestejä on ollut jälleen jaossa poikkeuksellisen paljon.

- ▶ <https://www.is.fi/digitoday/art-2000006379822.html>

Uutisia Kyberturvallisuuskeskuksesta

10 tietoturvanäkymää vuodelle 2020

- ▶ Tietoturvan lähitulevaisuus näyttää melko poutaiselta. Arviomme mukaan esimerkiksi kyberturvallisuuden vaikutukset liiketoimintaan on selvästi huomattu
- ▶ Vuoden 2020 tietoturvanäkymät perustuvat Kyberturvallisuuskeskuksen ja yhteistyöverkostojemme yhteisarvioon. Ne ovat osa Tietoturvan vuosi 2019 - katsaustamme, joka julkaistaan helmikuussa.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/10-tietoturvanakymaa-vuodelle-2020>

Kyberharjoitusskenaariot 2020 harjoittelun suunnittelun tueksi

- ▶ Vihkonen sisältää 20 erilaista kyberturvallisuuden poikkeamaa, joita voidaan käyttää kyberharjoitusten tapahtumankuvauksina. Skenaariotperustuvat tosielämän kyberturvallisuuspoikkeamiin.
- ▶ Skenaario vihkonen täydentää 2019 vuonna ilmestynyttä Kyberturvallisuuskeskuksen harjoitteluohjetta
- ▶ <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kyberharjoitusskenaariot2020.pdf>

Kyberturvallisuus ja yrityksen hallituksen vastuu –opas

- ▶ Liikenne- ja viestintäviraston Kyberturvallisuuskeskus on julkaissut yritysten hallituksille suunnatun kyberturvallisuutta käsittelevän oppaan.
- ▶ Kyberturvallisuus ja yrityksen hallituksen vastuu -opas antaa työkaluja ja tukea organisaation kyberturvallisuuden parantamiseen.
- ▶ Opas on julkaistu suomeksi, ruotsiksi ja englanniksi.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuus-ja-yrityksen-hallituksen-vastuu-opas>



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)