



TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Elokuu 2019

13.9.2019

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



rauhallinen



huolestuttava



vakava

Kybersää elokuu 2019



Verkkojen toimivuus

- ▶ Suomessa tavanomainen määrä toimivuushäiriöitä.
- ▶ Yli 100 British Airwaysin lentoa peruttiin IT-vian vuoksi.
- ▶ Palvelunestohyökkäyksillä lamautettiin muun muassa poliisin, verohallinnon ja rajavartiolaitoksen verkkosivuja.



Vakoilu

- ▶ Uusia vakoilukampanjoita, joissa on vakoiltu matkapuhelimia, paljastuu säännöllisesti.
- ▶ Myös esimerkiksi tutkijoita ja toimittajia vakoillaan.



Haittaohjelmat ja haavoittuvuudet

- ▶ Microsoftin etätyöpöytä-sovelluksen haavoittuvuuksia hyödynnetään tietomurroissa (Varoitus 2/2019).
- ▶ Useiden SSL VPN -toteutusten haavoittuvuuksia hyväksikäytetään paljon.



Tietomurrot ja -vuodot

- ▶ Kuntiin kohdistuvat tietomurrot jatkuivat. Muun muassa Kokemäki ja Pori uutisotsikoissa.
- ▶ Office 365 -tietomurrot päivittäisiä.



Huijaukset ja kalastelut

- ▶ 1500 valeverkkokauppaa poistettu verkosta.
- ▶ Tappouhkaukset uusin kiristyskeino.
- ▶ WhatsApp-profiilit nyt myös huijausvälineinä.



IoT ja automaatio

- ▶ Suomalainen IoT-tuotteiden tietoturvaleima julki ennen joulua.
- ▶ Automaatiojärjestelmien kyberturvallisuuden asiantuntijoista kova pula.
- ▶ IoT-tuotteiden tietoturva ei ole parantunut 15 vuodessa.

Varoitus 03/2018: Office 365-tunnuksia kalastellaan aktiivisesti



Suomalaisten yritysten ja organisaatioiden työntekijöiden sähköpostitunnuksia ja -viestejä varastetaan edelleen. Varoitus aiheesta on ollut voimassa kesästä 2018. Julkaisimme huhtikuun alussa oppaan Office 365 -tuotteiden tietoturvaominaisuuksista, joiden käyttöä suositellaan.

Hyökkääjät kirjautuvat käyttäjätileille ja seuraavat yritysten sähköpostiliikennettä. He pyrkivät saamaan tietoa organisaatioiden liikesalaisuuksista tai maksuliikenteestä tai kalastelevat muiden työntekijöiden tai yhteistyökumppanien tunnuksia.

Käyttäjätunnuksia ja salasanoja kalastellaan sähköpostitse ja huijaussivujen avulla. Yksi viimeaikainen menetelmä on Azuren pilvipalveluissa tehtävä kalastelu, joka on taitavasti toteutettu. Monivaiheinen tunnistaminen (MFA) voidaan myös ohittaa, jos Office 365 on asetettu tukemaan kirjautumista myös vanhoilla sovelluksilla (ns. legacy support).

Julkaisimme varoituksen 11.6.2018:

<https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota>

Julkaisimme oppaan uhkan torjumiseksi:

<https://www.kyberturvallisuuskeskus.fi/fi/node/2532>

Varoitus 02/2019: Windows RDS:n haavoittuvuuksia hyödynnetään tietomurroissa



Windows-käyttöjärjestelmän Remote Desktop Service -toteutuksesta (RDS, etätyöpöytäsovellus) on löydetty useita kriittisiä haavoittuvuuksia. Haavoittuvuudet tekevät mahdolliseksi **matomaisesti leviävien haittaohjelmien** toteuttamisen. Havaintoja haavoittuvuuksien hyödyntämisestä on tehty sekä Suomessa että ulkomailla.

Varoitus koskee Windows-palvelinten ja -työasemien **ylläpitäjiä** sekä organisaatioita, jotka käyttävät etätyöpöytäpalvelua. Ylläpitäjien tulee asentaa Windowsin **ohjelmistopäivitykset** viipymättä tai rajoittaa haavoittuvuuksien käyttömahdollisuuksia muilla keinoin.

Microsoft on julkaissut RDS-toteutusta koskevia tietoturvapäivityksiä: BlueKeep-haavoittuvuus korjattiin jo toukokuun 2019 käyttöjärjestelmäpäivitysten yhteydessä. Elokuun tietoturvapäivitysten yhteydessä korjattiin kaksi uutta kriittistä haavoittuvuutta RDS-toteutuksesta.

Julkaisimme varoituksen 14.8.2019:

<https://www.kyberturvallisuuskeskus.fi/fi/microsoftin-etatyopoyta-sovelluksen-haavoittuvuuksia-hyodynnetaan-tietomurroissa>

Julkaisuhetkellä Suomessa oli noin 4500 haavoittuvaa järjestelmää avoinna internetiin.

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 kohdistetuissa hyökkäyksissä ja vakoilussa.

3

Edistyneemmät rikollisryhmät etsivät kohteikseen isoja organisaatioita, joiden toimintaa haittaamalla voidaan yrittää kiristää rahaa.

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.



Verkkojen toimivuus

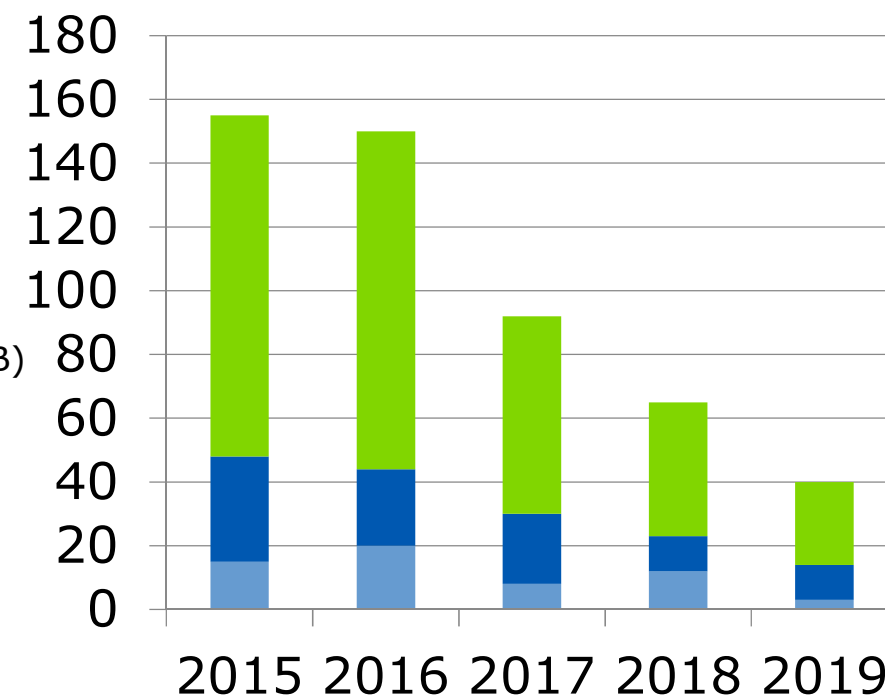
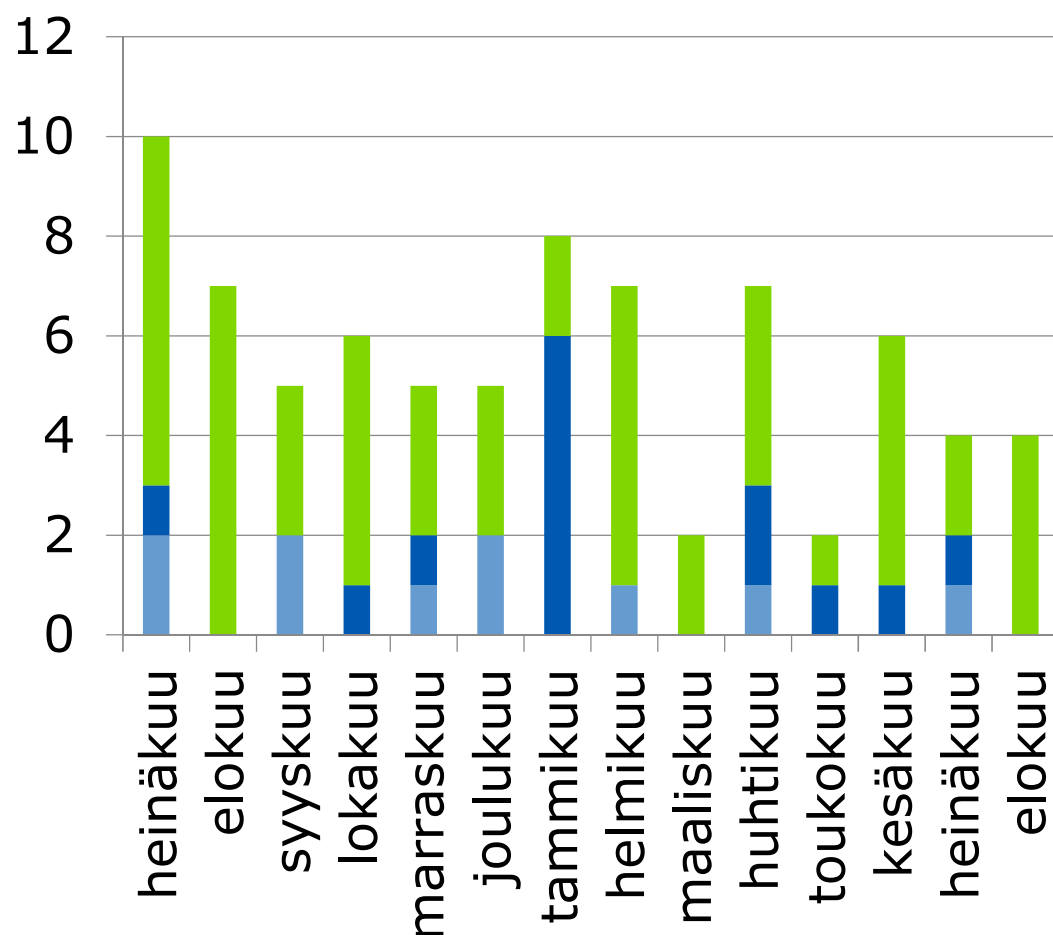
Verkkojen toimivuus

- ▶ Suomalaisissa yleisissä viestintäpalveluissa tavanomainen määrä häiriöitä.
- ▶ Yhdysvaltain FCC määräsi uhkasakot kolmelle teleyritykselle, koska niiden verkkolaitteet häiritsivät lentokentän säätutkia.
- ▶ T-Mobilen matkapuhelu- ja tekstiviestipalveluissa oli Yhdysvalloissa neljä tuntia kestänyt häiriö.
- ▶ Yli sata British Airwaysin lentoa peruttiin Iso-Britanniassa yhtiön tietojärjestelmissä esiintyneiden häiriöiden vuoksi.

Verkkojen toimivuus

- ▶ Laaja-alainen palvelunestohyökkäys julkispalveluihin 22.8.
 - ▶ Poliisin, verohallinnon, rajavartiolaitoksen ja julkisen tunnistautumispalvelun verkkosivuille kohdistui useita eri palvelunestohyökkäyksiä, joiden aikana verkkosivut eivät toimineet eikä palveluita voinut käyttää.
- ▶ Palvelunestohyökkäys tilannehuone.fi-palveluun 27.8.
 - ▶ Hälytystietoja kokoava tilannehuone.fi-sivusto kärsi verkko-ongelmista noin kahden tunnin ajan. Häiriön syynä oli palvelunestohyökkäys.

Merkittävien toimivuushäiriöiden määrä



Tässä tilastossa on esitetty ainoastaan yleisten viestintäpalveluiden merkittävät toimivuushäiriöt. Niitä on vuosittain 70–200 ja määrä on laskenut useiden vuosien ajan. Pieniä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 kappaletta vuodessa. Niiden määrä riippuu teleyrityksen tilastointitavasta.

Palvelunestohyökkäykset ja niillä uhkailu

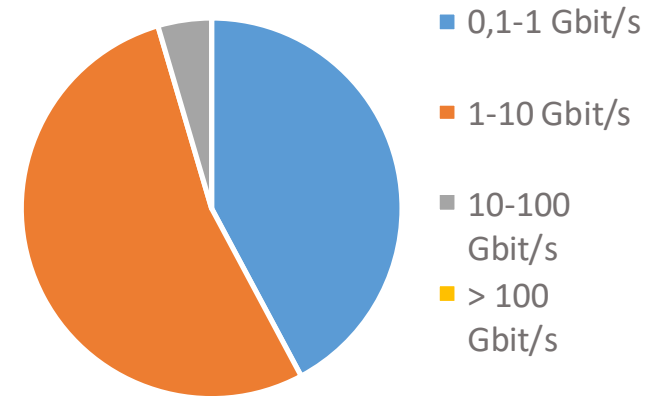
- ▶ Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (80 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- ▶ Noin puolet havainnoiduista yli 100Mbit/s hyökkäyksistä on volyymiltään 1-10 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- ▶ Yli 10 Gbit/s hyökkäyksiä havaitaan Suomessa liki päivittäin.
- ▶ Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska Kyberturvallisuuskeskukselle ilmoitetaan vain murto-osa tapahtuneista palvelunestohyökkäyksistä.

Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä (lähde: teleyritykset)

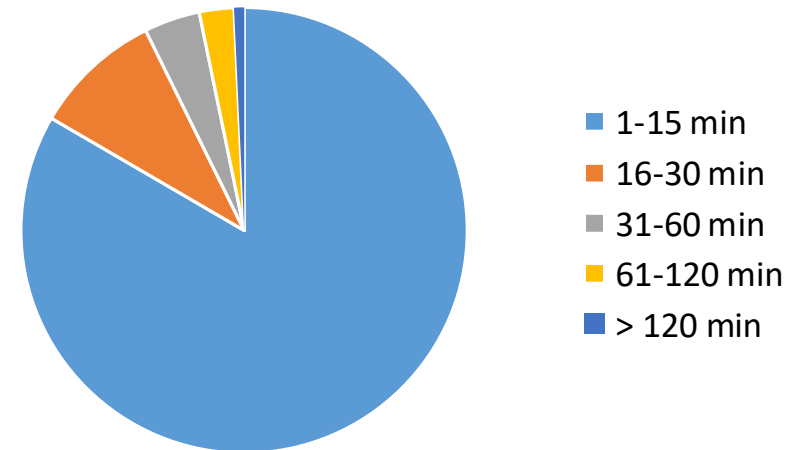
2019/Q2:
n. 79 Gbit/s
(kesto 4 min)

2019/Q1:
n. 162 Gbit/s
(kesto 9 min)

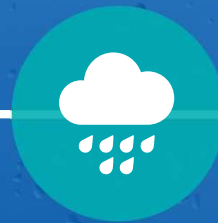
2018/Q4:
n. 45 Gbit/s
(kesto 6 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.



Suomeen kohdistuneiden palvelunestohyökkäysten kesto.



Vakoilu

Vakoilutilanteessa ajankohtaista



Matkapuhelinten vakoilu yleistyy

Matkapuhelimet ovat vakoilun kohteina samaan tapaan kuin perinteiset tietokoneet. Esimerkiksi elokuussa uutisoitiin Kiinan laajamittaisista pyrkimyksistä vakoilla uiguureja. Vakoilu kohdistui niin Android- ja iOS-puhelimiin kuin Windows-laitteisiin.

Toimittajat ja tutkijat vakoilun kohteena

Tutkimusyhteisö Bellingcat paljasti kalastelukampanjan, joka kohdistui joukkoon Proton Mail -sähköpostijärjestelmää käyttäneitä toimittajia, tutkijoita, aktivisteja ja kolmannen sektorin toimijoita. Bellingcatin mukaan kyse oli todennäköisesti laajemman vakoiluoperaation valmistelusta. Kohteita yhdisti työskentely Venäjään liittyvien aiheiden parissa.

Vakoilun ja kyberrikollisuuden välinen raja häilyy

Valtiollisen vakoilun ja taloudellista hyötyä tavoittelevan rikollisuuden tunnistaminen toisistaan vaikeutuu, kun samat toimijat ovat osallisina useammanlaisissa operaatioissa. Tietoturvayhtiö FireEye arvioi elokuussa, että esimerkiksi APT41:ksi nimetyllä kiinalaisryhmällä on kytköksiä sekä vakoiluun että kyberrikollisuuteen.



Haittaohjelmat ja haavoittuvuudet

Haittaohjelmahavaintomme

Haittaohjelmatyyppi	Tilanne	
IoT-haittaohjelmat	Muodostavat merkittävän osan Suomessa tehdyistä havainnoista.	
Kiristyshaittaohjelmat	Useita havaintoja kiristyshaittaohjelmatartunnoista.	
Etähallittavat haittaohjelmat (RAT)	Yritetään levittää aktiivisesti.	
Louhijat	Havainnot vähentyneet.	
Tietoja varastavat haittaohjelmat	Levittämisyrityksistä jonkin verran havaintoja. Käyttäjätunnuksia kuitenkin kalastellaan paljon, myös kohdistetusti.	
Mobiilihaittaohjelmat	Joitakin havaintoja.	

Haittaohjelmat

- ▶ Big game hunting -toimijat hyödyntävät laajasti levitettäviä haittaohjelmia päästäkseen sisälle kohdeorganisaation verkkoon
 - ▶ Suomalasetkin organisaatiot kärsineet hyökkäyksistä.
- ▶ Sähköpostiin liitettyjen tai linkitettyjen haittaohjelmien levitys yhä aktiivista
 - ▶ Sähköpostitse on jaettu muun muassa kiristyshaittaohjelmia ja tietoja varastavia haittaohjelmia sekä etäkäytön mahdollistavia haittaohjelmia.

Haavoittuvuudet

- ▶ **Microsoftin etätyöpöytä-sovelluksen haavoittuvuuksia hyödynnetään tietomurroissa (Varoitus 2/2019)**
 - ▶ Microsoftin Windows-käyttöjärjestelmän Remote Desktop Service -toteutuksesta on löytynyt useita kriittisiä haavoittuvuuksia.
- ▶ Useiden eri SSL VPN –toteutusten haavoittuvuuksia skannataan ja hyväksikäytetään aktiivisesti
 - ▶ Seurauksena voi olla VPN-laitteen haltuunotto, käyttäjätunnusten ja salasanojen urkinta, liikenteen kuuntelu sekä haittaohjelmien levitys.
 - ▶ Haavoittuvia laitteita: Pulse Secure SSL VPN, Palo Alto Global Protect SSL VPN, Fortigate SSL VPN
- ▶ Verkkopohjaisesta palvelinten hallintaan käytetystä Webmin-työkalusta on löydetty etähallinnan järjestelmänvalvojan oikeuksilla mahdollistava takaovi.

Big Game Hunting

Maailmalla on yleistynyt ilmiö, jota kutsutaan nimellä *Big Game Hunting* (suom. kirj. "suurriistan metsästys"). Toiminnalle ominaista on, että rikollinen toimija tunkeutuu organisaation järjestelmiin, levittäytyy organisaation verkossa ja käynnistää kiristyshaittaohjelman siten, että tiedostojen salaus haittaa organisaation toimintaa vakavasti tai jopa lamauttaa sen.

Salauksen jälkeen organisaatiolta kiristetään lunnaita salauksen purkamiseksi. Kohteita yhdistää perinteisesti hyvä maksukyky tai toiminnan jatkumisen aikakriittisyys. Esimerkiksi tammikuussa kohteiksi joutui ranskalainen Altran ja maaliskuussa norjalainen Norsk Hydro. Yhdysvalloissa useat kunnat ja aluehallinnot ovat myös olleet kohteina.

Samaan ilmiöön liittyy useita eri kiristyshaittaohjelmia, kuten LockerGoga, SamSam, Ryuk ja MegaCortex. Organisaation järjestelmiin tunkeutuminen puolestaan voi alun perin tapahtua käyttäen hyväksi haavoittuvia verkkoon avoimia palveluita, haitallisilla sähköpostien liitetiedostoilla tai esimerkiksi onnistuneen tietojenkalastelun avulla.

Ilmiö on hyvä huomioida riskiarvioissa. Muun muassa murtautumisen ja levittäytymisen havaitsemiseksi on hyvä varmistua siitä, että jo hankittujen ratkaisujen tietoturvaominaisuuksia hyödynnetään kattavasti. Varautumista suunnitellessa on syytä huomioida myös, että rikolliset voivat pyrkiä vaikeuttamaan toipumista salaamalla myös esimerkiksi varmuuskopiot ja käyttövaltuushallinnan.





Tietomurrot ja -vuodot

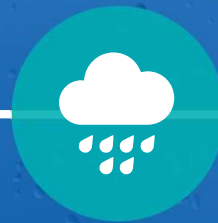
Tietomurrot ja -vuodot

- ▶ Porin kaupungin verkkoon kohdistui tietomurto
 - ▶ Haittaohjelma pääsi sisään Porin kaupungin opetusverkkoon todennäköisesti julkiseen verkkoon avoinna olleen päivittämättömän Windows 7- työaseman kautta. Tietomurron avulla päästiin käsiksi opetusverkon käyttäjätunnuksiin.
 - ▶ Tietomurron seurauksena noin 9000 käyttäjää joutui vaihtamaan salasanan.
 - ▶ Ei ole tiedossa, että vuotaneita tunnuksia olisi käytetty hyväksi.
 - ▶ <https://yle.fi/uutiset/3-10913191>
- ▶ Kokemäen tietomurron vaikutukset on pääosin saatu korjattua
 - ▶ Korjauksessa pystyttiin käyttämään hyväksi varmuuskopioita, vaikkei varmuuskopioiden palauttamista ollutkaan testattu ennalta.
- ▶ Fonectan järjestelmän pääsynhallintavirhe aiheutti laajan tietovuodon.
- ▶ Office 365 –tietomurtoja ilmoitetaan päivittäin
 - ▶ Esimerkiksi suuri suomalainen ammattijärjestö ilmoitti joutuneensa sähköpostimurron kohteeksi. Haltuun saatuja tunnuksia käytettiin kalasteluviestien edelleen lähettämiseen.

Suojautumisohteja tietomurtojen varalta

- ▶ Käytä eri salasanaa jokaisessa palvelussa.
- ▶ Muista päivittää käyttöjärjestelmä ja käyttämäsi ohjelmistot.
- ▶ Säilytä salasanoja turvallisesti.
- ▶ Vaihda salasanasi, jos epäilet tai tiedät sen joutuneen väärin käsiin.
- ▶ Käytä monivaiheista tunnistamista, jos käyttämässäsi palveluissa sellainen on mahdollista.
- ▶ Käytä tekniikoita, jotka nopeuttavat tietomurtojen huomaamista.
- ▶ Mieti ja harjoittele etukäteen tietomurroista palautumista. Säilytä varmuuskopiot erillään tuotantoympäristöstä.



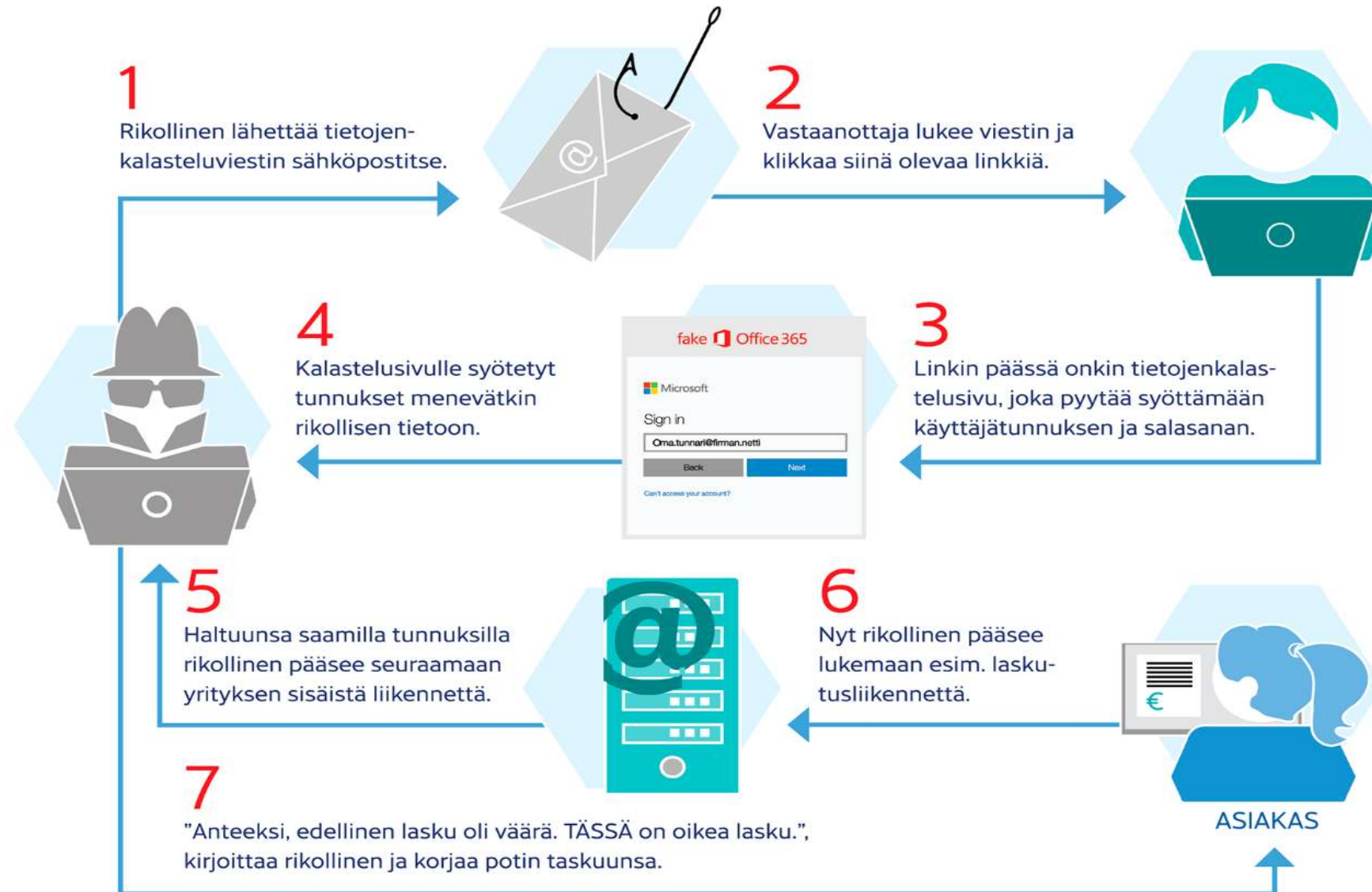


Huijaukset ja kalastelut

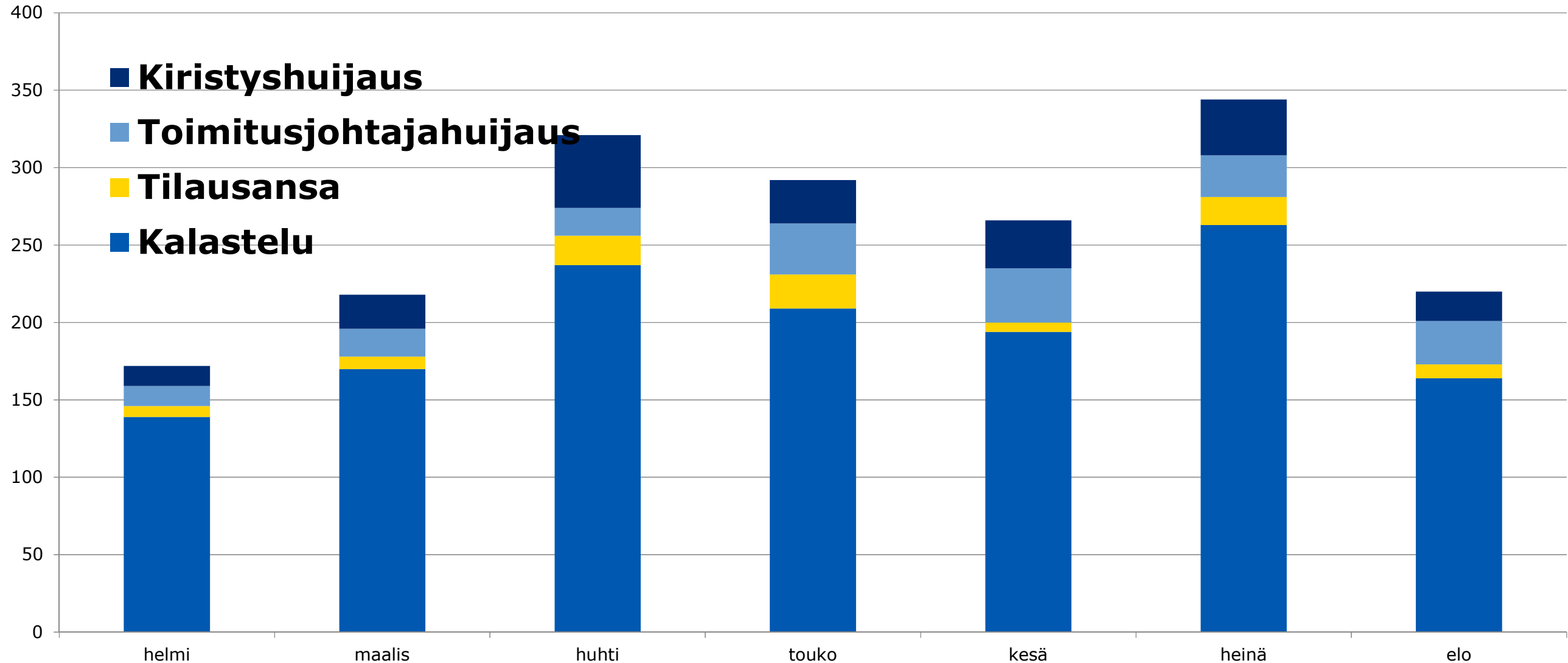
Huijaukset ja kalastelut

- ▶ Kiristyshuijauksissa uudenlainen ilmiö: tappouhkaus, jos et maksa.
- ▶ 1500 valeverkkokauppaa poistettu verkosta.
- ▶ Huijauksia monenlaisiin organisaatioihin, myös yhdistyksiin ja urheiluseuroihin.
- ▶ Väärennetty johtajan WhatsApp-profiili uutena huijausvälineenä.

Office 365 -huijauksen vaiheet



Käsiteltyjä huijaustapauksia 2019/02–08





IoT ja automaatio

IoT ja automaatio

- ▶ Suomalaisen IoT-laitteiden tietoturvaleiman valmistelu on edennyt aikataulussa, ja se lanseerataan ennen joulua.
- ▶ Automaatiojärjestelmien kyberturvallisuuden asiantuntijoista on maailmalla huutava pula. Osasyynä voi olla epärealistiset osaamisvaatimukset.
- ▶ IoT-tuotteiden tietoturva ei parane, mikä selvisi yli 6000 laiteohjelmistoa kattaneessa tutkimuksessa.



Tietoturva-alan kehitys

Oikeudelliset asiat

- ▶ EU:n sähköisen viestinnän tietosuojasta-asetuksen ("ePrivacy") valmistelu on kesken, ja sitä edistettäneen Suomen EU-puheenjohtajakaudella syksyllä 2019.
- ▶ LVM on julkaissut työryhmäselvityksen *Muiden kuin henkilötietojen vapaan liikkuvuuden esteet Suomessa*, joka liittyy asetukseen (EU) 2018/1807 muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa.
 - ▶ <https://julkaisut.valtioneuvosto.fi/handle/10024/161774>
- ▶ Laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) on vahvistettu ja se tulee voimaan 1.1.2020
 - ▶ Lain tarkoituksena on muun ohella varmistaa viranomaisten tietoineistojen tietoturvallinen käsittely
 - ▶ Tietoturvallisuudesta säädetään lain 4 luvussa.
 - ▶ Samanaikaisesti voimaan tulee viranomaisten toiminnan julkisuudesta annetun lain (621/1999, julkisuuslaki) muutos (907/2019)
 - ▶ Muun muassa uusi 16 a §, jonka perusteella muuhun kuin salassa pidettävään asiakirjaan voidaan tehdä merkintä "HARKINNANVARAISESTI ANNETTAVA".

Kyberasioihin liittyvää uutisointia maailmalta

Kuntasektorin kyberturvallisuus valokeilassa

- ▶ Suomalaisia kaupunkeja vastaan kesän aikana tehdyt tietomurrot ovat saaneet runsaasti huomiota.
- ▶ Kuntaliitto korosti Kuntalehden artikkelissa varautumisen ja harjoittelun tärkeyttä.
- ▶ Turvallisuuskomitea kehotti perehtymään ohjeisiin, pyytämään apua ja ilmoittamaan poikkeamista.
- ▶ <https://kuntalehti.fi/uutiset/lahti-kokemaki-pori-kyberiskut-ovat-jotaalla/>
- ▶ <https://turvallisuuskomitea.fi/tiedote-turvallisuuskomitean-kokous-2-9-2019/>

Valkohattuhakkeri on lahja

- ▶ Vastuullisesti tietoturva-aukkoja etsivä ja raportoiva hakkeri on lahja organisaation tietoturvalle, sillä vain havaitut aukot tietoturvassa voidaan korjata.
- ▶ Tuemme ja kannustamme valkohattuhakkereita ja organisaatioita vastuullisessa haavoittuvuuksien käsittelyssä.
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vinkkejä-valkohatuille-parempaan-jahelpompaan-yhteistyöhön>
- ▶ <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palveluistanne-loytyi-tietoturva-aukko>

Viestintäyhteyksiä katkaistaan maailman konflikteissa

- ▶ Tiedon levittämisen rajoittaminen on tehokas vallankäytön muoto.
- ▶ Esimerkiksi Intia on katkaissut puhelin- ja internetyhteydet Kashmirin laaksoon otettuaan haltuunsa Jammun ja Kashmirin osavaltiot.
- ▶ <https://www.hs.fi/ulkomaat/art-2000006209489.html>

Kybersään johtopäätökset

Tietoturvan edistyminen

1. Kyberturvallisuuden harjoittelu on lisääntynyt.
2. Kuntien kyberturvallisuutta on alettu kehittää järjestelmällisemmin.
3. Suomalaisen IoT-tietoturvamerkkin valmistelu etenee suunnitellusti.

Tietoturvan kehitystarpeet

1. Haavoittuvuuksien hyväksikäyttö nopeutuu entisestään – päivitysten asentamista täytyy nopeuttaa.
2. Kuntasektorin kyberturvallisuus vaatii lisää resursseja ja suoraviivaisia ohjeita.
3. Organisaatioiden kyky estää, havaita ja rajoittaa tietojenkalastelun vaikutuksia on puutteellinen.