TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Heinäkuu 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 heinäkuu 2019

Verkkojen toimivuus

- Kolme merkittävää toimivuushäiriötä, mikä on keskimääräistä vähemmän
- Paikannusjärjestelmä Galileo ei toiminut viikkoon
- Palvelunestohyökkäyksien vaikutukset onnistutaan torjumaan aiempaa paremmin.

Vakoilu

- Pohjois-Korean väitetään anastaneen yhteensä 2 miljardia US dollaria kyberhyökkäyksin ydinaseohjelman rahoittamiseksi
- Kiinalaisryhmittymä Winnti on vakoillut vuosien ajan useita saksalaisia korkean teknologian yrityksiä

Haittaohjelmat ja haavoittuvuudet

- Applen iMessage-sovelluksessa useita vakavia haavoituvuuksia.
- VxWorks-käyttöjärjestelmästä löydetty useita vakavia haavoittuvuuksia, jotka vaikuttavat kriittisiin sovelluksiin
- BlueKeep-haavoittuvuus voi johtaa haittaohjelmaepidemiaan.

Tietomurrot ja -vuodot

- Kokemäen kaupungin järjestelmiin kohdistui tietomurto ja kiristyshaittaohjelma.
- Tietomurto Capital One –pankkiin.
- Tietomurtojen kohteeksi joutuneet organisaatiot määrättiin maksamaan satoja miljoonia euroja uhreille.

Huijaukset ja kalastelut

- Lomakausi sijaisuuksineen on näkynyt jälleen lisääntyneinä toimitusjohtajahuijauksina
- O365-aiheinen kalastelu jatkuu edelleen runsaana ja johtaa onnistuneisiin tietomurtoihin.

IoT ja automaatio

- Sääntelyyn herätty Euroopan tasolla
- IoT-laitteiden hyväksikäyttö kohdentuu organisaatioihin, hyödyntäen organisaatioiden kasvaa varjo-IT:tä.

Big Game Hunting eli kohdennetut tietomurrot ja kiristäminen

Maailmalla on keväällä 2019 yleistynyt ilmiö, jota kutsutaan nimellä *Big Game Hunting*. Toiminnalle ominaista on, että rikollinen **tunkeutuu** organisaation tietojärjestelmiin, **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. Suomessa on myös havaintoja ilmiöstä.

Samaan ilmiöön liittyy useita eri kiristyshaittaohjelmia, kuten LockerGoga, SamSam, Ryuk ja MegaCortex. Organisaation järjestelmiin tunkeutuminen voi alun perin tapahtua internetiin avointen haavoittuvien palveluiden, haitallisten sähköpostin liitetiedostojen tai esimerkiksi onnistuneen tietojenkalastelun avulla.

Ilmiö on syytä huomioida riskiarvioissa erityisenä uhkana. 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.

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. Kyberturvallisuuskeskus julkaisi 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 todella hyvin 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

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

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

3

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

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

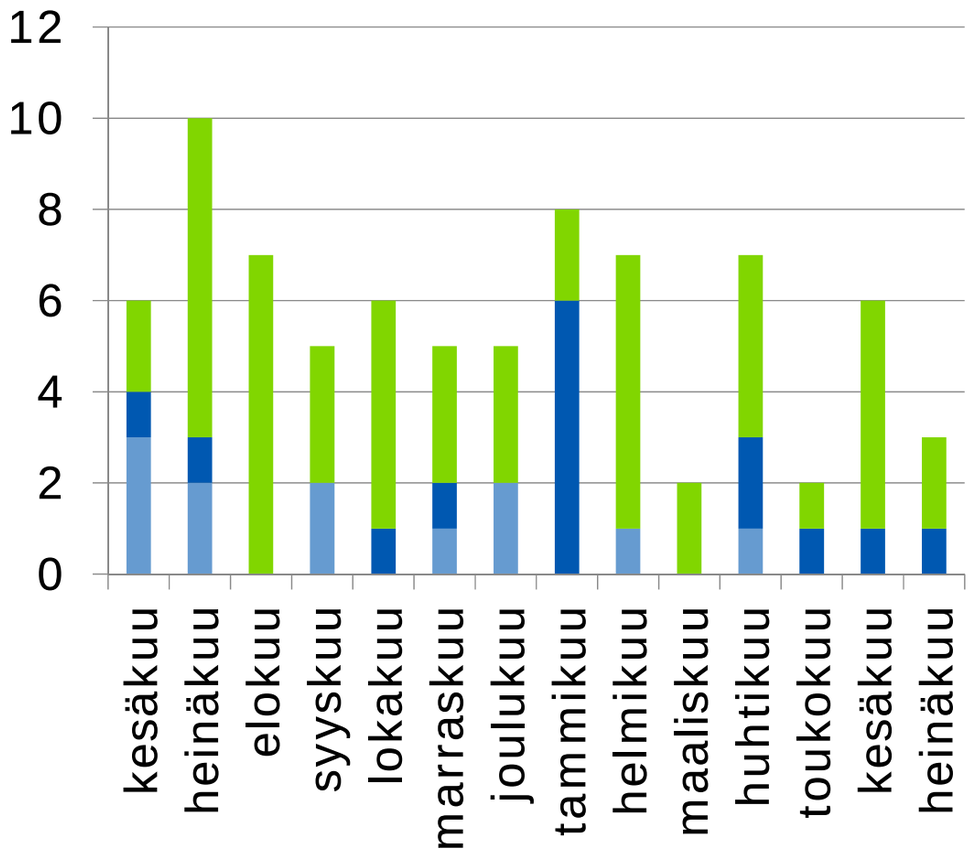
Verkkojen toimivuus

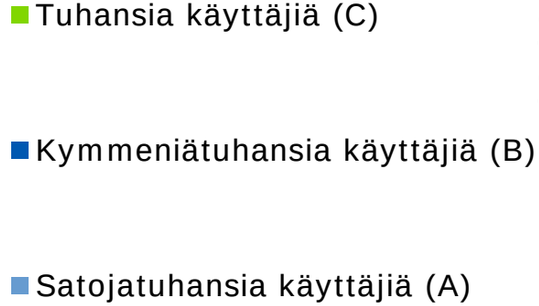
- Heinäkuussa kolme merkittävää yleisten viestintäpalveluiden toimivuushäiriötä
  - Merkittäviä häiriöitä oli keskimääräistä vähemmän
  - Tampereella DNA:n matkaviestinverkon palveluissa muutaman tunnin kestänyt häiriö tiedonsiirtokuitujen katkeamisen johdosta
- Eurooppalainen satelliittipaikannusjärjestelmä Galileo oli epäkunnossa viikon ajan
  - Järjestelmän maa-asemien laitteistoissa oli yhtäaikainen toimivuushäiriö https://www.gsa.europa.eu/newsroom/news/galileo-initial-services-have-now-been-restored
- Käyttäjien ja organisaatioiden kannattaa miettiä vaihtoehtoisia keinoja tärkeiden ihmisten tavoittamiseen niissä tilanteissa, kun tavallisesti käytetyssä viestintäpalvelussa on häiriö
  - Kemin kaupungin tietoverkossa useita tunteja kestänyt häiriö http://www.kemi.fi/ajankohtaista/2019/07/11/kemin-kaupungin-tietoliikenneverkon-hairion-syy-ei-ollut-ulkopuolinen-hairinta/
  - Facebook ja Twitter ilmoittivat ympäri maailmaa vaikuttaneista häiriöistä palveluissaan

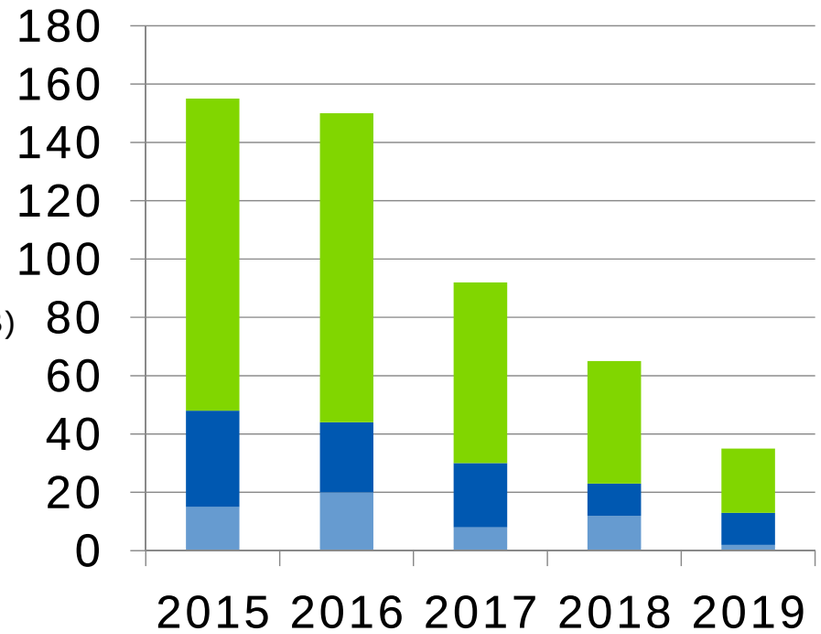
Verkkojen toimivuus

- Verraten rauhallinen palvelunestohyökkäysten heinäkuu
  - Kuukauden lopulla saatiin useita peräkkäisiä havaintoja pienikokoisista palvelunestohyökkäyksistä, jotka eivät kuitenkaan haitanneet palveluiden toimivuutta.
  - Verkon kuormitukseen ja palvelunestohyökkäyksiin varaudutaan paremmin kuin aikaisemmin. Liikenteen pesuripalvelut ja hyökkäysten torjuntatoimet ovat parantaneet verkkopalveluiden toimintavarmuutta hyökkäystilanteissa.

Merkittävien toimivuushäiriöiden määrä



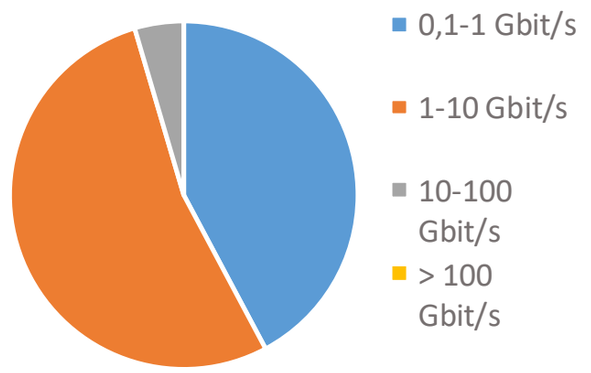




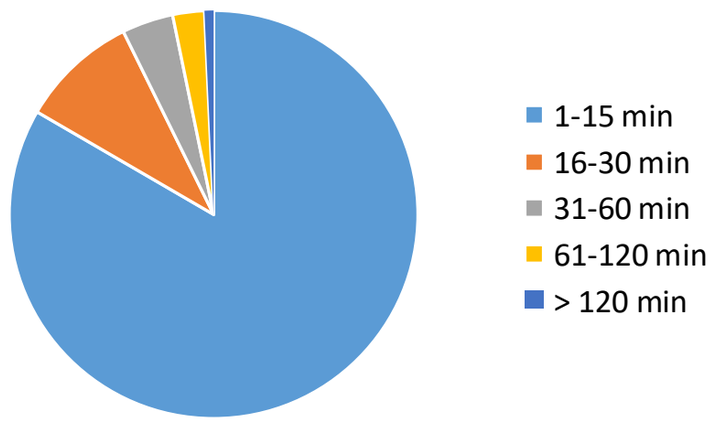
Tässä tilastossa on esitetty ainoastaan yleisten viestintäpalveluiden merkittävät toimivuushäiriöt. Niitä on vuosittain 70–200 ja määrä on laskenut useiden vuosien ajan. Pieniä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 kappaletta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



Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.



Suomeen kohdistuneiden palvelunestohyökkäysten kesto.

Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä (lähde: teleyritykset)

2019/Q2:	2019/Q1:	2018/Q4:
n. 79 Gbit/s	n. 162 Gbit/s	n. 45 Gbit/s
(kesto 4 min)	(kesto 9 min)	(kesto 6 min)

Vakoilu

Vakoilutilanteessa ajankohtaista

Pohjois-Korea on anastanut 2 miljardia USD kyberhyökkäyksin

YK raportin mukaan Pohjois-Korean tiedustelupalvelun hakkerit ovat viime vuosien aikana anastamaan pankeilta ja kryptovaluuttojen käsittelijöiltä 2 miljardin USD arvosta rahaa, jotka on käytetty maan ydinaseohjelman rahoittamiseen.

Kiinalainen Winnti on vakoillut vuosia saksalaisia yrityksiä

Saksalaisten tutkijoiden journalistien mukaan hakkeriryhmä Winnti on vakoillut jo vuosia erityisesti saksalaisten korkean teknologian yritysten yrityssalaisuuksia. Artikkelissa on mainittu yritykset Gameforge, Valve, Henkel, Covestro, Bostik, Shin-Etsu Chemical, Sumimoto Electric, Roche, BASF, Siemens, Thyssenkrupp, Teamviewer, Bayer.

DNS-nimipalveluinfrastruktuurin kaappaamiset jatkuvat

Nimipalvelukyselyjen kaappaamiseen ja liikenteen uudelleenohjaamiseen erikoistunut Sea Turtle jatkaa toimintaansa käyttäen uutta vaikeammin havaittavaa menetelmää. Uhrien joukossa oli myös Kreikan maatunnusta (.gr) ylläpitävä taho.

Haittaohjelmat ja haavoittuvuudet

Haittaohjelmahavaintomme

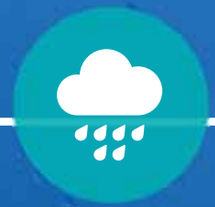
Haittaohjelmatyyppi	Tilanne	
IoT-haittaohjelmat	Muodostavat merkittävän osan Suomessa tehdyistä havainnoista	
Kiristyshaittaohjelmat	Muutamia havaintoja kiristyshaittaohjelmista	
Etähallittavat haittaohjelmat (RAT)	Etähallittavia haittaohjelmia yritetään levittää aktiivisesti	
Louhijat	Louhijoita levitetty edelleen haavoittuvuuksien avulla palvelimille	
Tietoja varastavat haittaohjelmat	Levittämisyrityksistä jonkin verran havaintoja. Käyttäjätunnuksia kuitenkin kalastetaan aktiivisesti ja myös kohdistetusti.	
Mobiilihaittaohjelmat	Mobiilihaittaohjelmatapauksista on joitain havaintoja	

Haittaohjelmat

- Big game hunting -toimijat hyödyntävät laajasti levitettäviä haittaohjelmia päästäkseen sisälle kohdeorganisaation verkkoon.
  - Myös Suomessa on tehty onnistuneita hyökkäyksiä.
- Sähköpostitse jaettujen tai linkitettyjen haittaohjelmien levitys on aktiivista.
- Tarpeettomasti julkiseen verkkoon avoimet palvelut lisäävät riskiä. Yhtenä riskikohteena ovat esimerkiksi etätyöpöytäyhteydet (RDP).
- Verkkosivuilta luottokorttitietoja keräävää Magecart-kampanjaa on havaittu myös Suomessa.
  - StealthWorker-bottiverkkoa hyödynnetty ainakin salasanojen arvaamiseen yleisesti käytetyissä julkaisu- ja verkkokauppa-alustoissa

Haavoittuvuudet

- VxWorks on yleisesti käytössä oleva tosiaikakäyttöjärjestelmä (RTOS), josta on löydetty useita kriittisiä haavoittuvuuksia. Niistä osaa voi hyödyntää helposti myös verkon yli. Päivittäminen voi olla vaikeaa.
- Applen iMessage-sovelluksen useat haavoittuvuudet mahdollistavat jopa laitteen kaappaamisen lähettämällä siihen viestin. Päivitys iOS 12.4 – versioon korjaa useita näistä haavoittuvuuksista.
- Microsoftin etätyöpöytäratkaisun kriittiseen RDS/RDP-haavoittuvuuteen (BlueKeep) on saatavilla julkinen palvelunestotilan mahdollistava esimerkkikoodi. Lisäksi on olemassa ei-julkisia hyväksikäyttömenetelmiä, joilla palvelimella saadaan suoritettua haitallista koodia verkon yli järjestelmätason oikeuksin. Useissa yleisesti käytetyissä ohjelmistoissa on julkaistu haavoittuvuuksia.



Tietomurrot ja -vuodot

Tietomurrot ja -vuodot

- Kokemäen kaupunki joutui heinäkuussa tietomurron ja kiristyshaittaohjelman uhriksi. https://yle.fi/uutiset/3-10899982
  - Kiristyshaittaohjelma aiheutti laajaa haittaa kaupungin tietoverkossa ja palveluiden järjestämisessä.
  - Kaupungin palveluiden järjestämistapaa jouduttiin osittain muuttamaan toistaiseksi ja vaihtoehtoisia tapoja asioiden hoitamiseen on jouduttu keksimään.
  - Vaikutuksia on ollut mm. kaupungin maksu- ja sähköpostiliikenteeseen sekä kirjastopalveluihin.
- Kyberturvallisuuskeskukselle tulee edelleen ilmoituksia päivittäin Microsoft O365-tietomurroista.
- Heinäkuussa uutisoitiin tietomurtojen aiheuttamista korvauksista ja sakoista. Korvaukset nousivat suurimmillaan satoihin miljooniin dollareihin. Kuten mainituista summista voi laskea, oletus on, että vain murto-osa uhreista tulee hakemaan korvauksia. http://www.enforcementtracker.com/

Tietomurrot ja -vuodot

- Heinäkuussa monet tahot maailmalla joutuivat tai raportoivat jo aiemmin joutuneensa tietomurtojen kohteiksi: Yhteensä kymmenien miljoonien käyttäjien tietoja oli vuotanut rikollisille.
- Yhdysvaltalainen Capital One -pankki huomasi 19.7. joutuneensa maaliskuussa 2019 tietomurron kohteeksi paljastaen tietoja lähes 106 miljoonan henkilöltä. https://yle.fi/uutiset/3-10898706
- Venäjän turvallisuuspalvelu FSB:n yhteistyökumppanin järjestelmiin murtauduttiin. https://www.forbes.com/sites/zakdoffman/2019/07/20/russian-intelligence-has-been-hacked-with-social-media-and-tor-projects-exposed/
- IBM:n tutkimuksen mukaan keskimääräisen tietomurron kustannukset ovat uhrille 3,92 miljoonaa dollaria ja keskimääräinen kesto 279 päivää. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

Suojautumisohjeita tietomurtojen varalta

- Käytä eri salasanaa jokaisessa palvelussa.
- Muista päivittää käyttöjärjestelmä ja käyttämäsi ohjelmistot.
- Säilytä salasanoja turvallisesti.
- Vaihda salasanasi, jos epäilet tai tiedät sen joutuneen vääriin käsiin.
- Käytä monivaiheista tunnistamista, jos käyttämissäsi palveluissa sellainen on mahdollista.
- Käytä tekniikoita, jotka nopeuttavat tietomurtojen huomaamista. Kuten monet tämän kuun uutiset kertoivat, murtojen huomaaminen voi kestää kauan.
- Mieti ja harjoittele etukäteen miten toimia, jos tietomurto tapahtuisi suojautumisesta huolimatta.

Huijaukset ja kalastelut

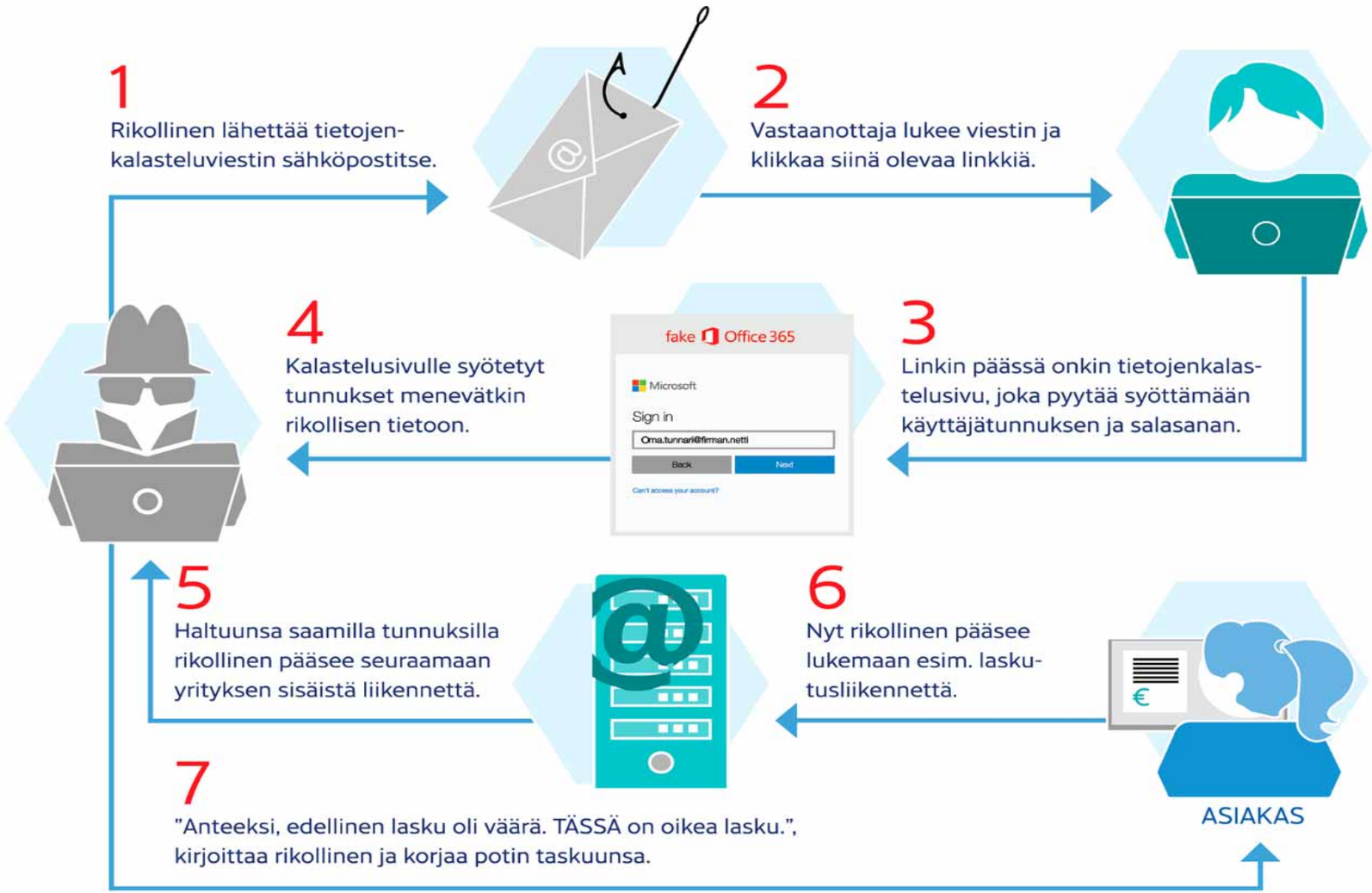
Huijaukset ja kalastelut

- Toimitusjohtajahuijauksia on ilmoitettu Kyberturvallisuuskeskukselle tasaisesti koko kesän ajan.
  - Toimitusjohtajahuijaukset yleistyivät kesäkaudella, kun maksuja hyväksyvät sijaiset tai kesätyöntekijät.
  - Toimitusjohtajahuijauksissa johtajan nimiin väärennetyillä viesteillä yritetään saada organisaation tilinhaltijaa siirtämään rahaa huijarin tilille.
  - Myös palkanlaskentaan kohdistuu huijausyrityksiä, joissa huijari pyytää vaihtamaan johtajan tai työntekijän palkanmaksutilin omakseen.
- Pornokiristyksiä yritetään jatkuvasti, kohteena sekä yritysosoitteet että yksityishenkilöt
  - Huijari käyttää uhkailuun vanhoja salasanavuotoja, väärennettyä sähköpostia tai muita keinoja, mutta väitteet ovat valetta.

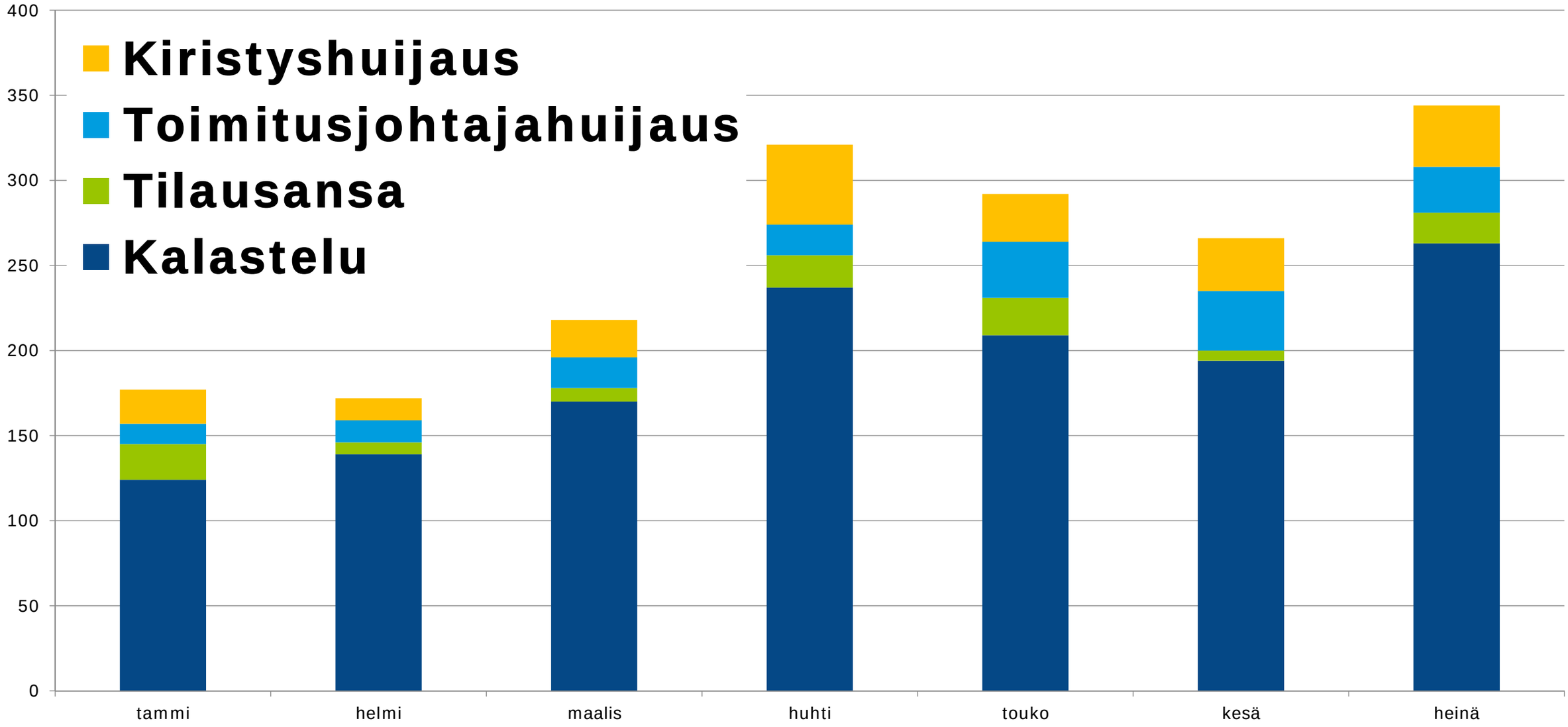
Huijaukset ja kalastelut

- Microsoft Office 365 -palvelun tunnusten tietojenkalastelulla tehdään aktiivisesti tietomurtoja
  - Kyberturvallisuuskeskuksen jo vuoden voimassa ollut varoitus on edelleen ajankohtainen.
  - Kattava ohje Office 365 -ympäristön suojaamiseen: https://www.kyberturvallisuuskeskus.fi/fi/node/2532
  - Tiedostonjakopalveluita käytetään levittämään vilpillisiä PDF-tiedostoja ja linkkejä kalastelusivuille.
- Eri pankkien ja tuotemerkkien nimissä kalastellaan käyttäjätunnuksia, salasanoja ja maksukorttitietoja
  - Viestit tulevat sekä sähköpostitse että tekstiviestitse.
- Mediatalojen nimissä tehdään uskottavan näköisiä valeuutissivustoja, joissa mainostetaan epämääräisiä sijoituspalveluita. Huonojen sijoitusvinkkien jakaminen ei vaaranna kyberturvallisuutta, mutta toiminta voi rikkoa muita lakeja ja hyviä markkinointitapoja.

Office 365 –huijauksen vaiheet



Käsiteltyjä huijaustapauksia 2019/01–07



IoT ja automaatio

IoT ja automaatio

- Kolmannes Mirai-haittaohjelmien kohteista yritysten IoT-laitteita
  - IoT-laitteet usein havaitsematon osa organisaation varjo-IT:tä, jonka riskejä haastavaa arvioida.
    - https://www.darkreading.com/mirai-groups-target-business-iot-devices/d/d-id/1335308
- Leivänpaahtimiakin käytetään hyväksi hyökkäyksissä
  - Hyökkääjää kiinnostaa sen hyödyntäminen osana suurempaa hyökkäystä. Turvattomat älylaitteet ovat pääsy kotiverkkoon, jossa muut asiat voi olla hoidettu hyvin.
  - Kyberturvallisuuskeskuksen mukaan uusien sovellusten tietoturvaa ei ole säädelty juuri lainkaan. Asiaan on havahduttu Euroopassa aivan hiljattain.
  - EU:n kuluttajasuojasta vastaavan ECCG:n (European Consumer Consultative Group) toimesta.
  - Esimerkiksi Iso-Britannia on aktiivinen tietoturvavaatimusten standardisoimiseksi ETSI:ssä.
- Yhdysvalloissa julkaistu luonnos IoT-tuotteiden tietoturvan vähimmäisvaatimuksista: https://csrc.nist.gov/publications/detail/nistir/8259/draft

Tietoturva-alan kehitys

Oikeudelliset asiat

- Suomi aloitti EU:n neuvoston puheenjohtajana 1.7.2019 → https://eu2019.fi/fi
  - Liikenne- ja viestintäministeriön puheenjohtajuuskauden teemoihin voi tutustua videolla: https://www.youtube.com/watch?v=AATacCzAKfo
- Sähköisen viestinnän palveluista annetun lain (917/2014) uudistaminen EU:n sähköisen viestinnän säännöstön (”EECC”) voimaansaattamiseksi jatkuu
  - https://valtioneuvosto.fi/hanke?tunnus=LVM004:00/2019
- Liikenne- ja viestintävirasto Traficomin ohjeluonnos 211/2019 O Sähköisen tunnistuspalvelun arviointiohje on lausuttavana 16.8. saakka
  - Luotu mm. arviointikriteeristö mobiilisovelluksille, joita käytetään osana vahvaa sähköistä tunnistuspalvelua
  - https://www.kyberturvallisuuskeskus.fi/fi/sahkoinen-tunnistaminen (Valmisteluasiakirjat-otsikon alla)
- Traficomin määräysluonnos 71/2019 M verkkotietojen ja verkon rakentamissuunnitelmien toimittamisesta on lausuttavana 30.8. saakka
  - https://www.traficom.fi/fi/ajankohtaista/lausuntopyynto-maarays-verkkotietojen-ja-verkon-rakentamissuunnitelmien

Kyberasioihin liittyvää uutisointia maailmalta

Iran ja Kiina liittoutuivat USA:ta vastaan kybermaailmassa

- Iran ja Kiina pitävät Yhdysvaltain ylivaltaa kybermaailmassa uhkana. Maiden ministerit ovat keskustelleet yhteistyön lisäämisestä.
- Maat suunnittelevat yhteistyötä tietotekniikan saralla sekä kybermaailman uhkien tutkimisessa ja torjunnassa.
- Taustalla vaikuttavat jännitteet Yhdysvaltain suhteissa erityisesti Venäjään ja Kiinaan.
- https://www.forbes.com/sites/zakdoffman/2019/07/06/iranian-cyber-threat-heightened-by-chinas-support-for-its-cyber-war-on-u-s/

Vakuutusyhtiö kieltäytyi maksamasta korvauksia kybervakuutuksesta, koska se tulkitsi hyökkäyksen sotatoimeksi

- Yhdysvaltalainen elintarvikealan yritys Mondelez pyysi vakuutusyhtiö Zurich Americanilta yli 100 miljoonan dollarin vakuutuskorvausta.
- Vakuutusyhtiö pitää NotPetya-haittaohjelman levittämistä sotatoimena. Perusteena se, että mm. Yhdysvaltain hallitus syytti hyökkäyksistä suoraan Venäjää.
- https://www.theregister.co.uk/2019/07/26/do_insurance_war_exclusion_clauses_apply_to_cyberattacks/

Kyberrikollisuus aiheutti yli 37 mrd € kulut ja tappiot vuonna 2018

- Internet Societyn Online Trust Alliancen tekemän selvityksen mukaan kyberrikollisuus aiheutti koko maailmassa vähintään 37 miljardin euron kulut ja tappiot.
- Kiristyshaittaohjelmat aiheuttivat vajaan viidesosan kuluista ja tappioista. Osuus on kasvussa.
- Internet Society arvioi, että 95 % tietoturvaloukkauksista oltaisiin voitu estää.
- https://www.internetsociety.org/resources/ota/2019/2018-cyber-incident-breach-trends-report/

Kybersään johtopäätökset

Tietoturvan edistyminen

1. Merkittävien tietoturvaloukkausten uhrit ovat avoimella tiedottamisellaan edistäneet koko yhteiskunnan valmiutta parantaa kyberturvallisuutta.

2. Toimitusjohtajahuijaukset tunnistetaan entistä paremmin, ja niitä osataan välttää hyvin myös kesälomakaudella.

3. Käyttäjät tunnistavat käyttäjätunnusten kalastelun entistä paremmin. Ilmoitukset tietomurroista ovat vähentyneet samalla, kun havainnot kalastelusta ovat lisääntyneet.

Tietoturvan kehitystarpeet

1. Poikkeamahavaintoihin reagointia on parannettava. Monesti lokitietoja tallennetaan, mutta kukaan ei seuraa niitä.

2. Tietoturvaan pitää panostaa enemmän myös kuntasektorilla.

3. Kaikkien organisaation verkossa olevien laitteiden tulee olla tiedossa ja hallinnassa