TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Lokakuu 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 lokakuu 2019

Verkkojen toimivuus

- Normaali määrä merkittäviä yleisten viestintäpalveluiden häiriöitä. Runsaasti muita ICT-häiriöitä.
- Suomalaisia palvelimia kuormittunut, kun niitä on hyödynnetty ulkomaille suuntautuvan palvelunesto-hyökkäysliikenteen peilaamiseen.

Vakoilu

- Suomalaisten korkeakoulujen työntekijöiden tunnuksia kalastellaan tutkimustietoon pääsemiseksi.
- Intialaiseen ydinvoimalaan kohdistuneessa tietomurrossa pyrittiin todennäköisesti varastamaan ydinteknologiaa.

Haittaohjelmat ja haavoittuvuudet

- Verkkotallennuslaitteisiin leviävästä QSnatch-haittaohjelmasta on tehty Suomessa noin 200 havaintoa.
- Haittaohjelmien levittäminen sähköpostin avulla on tuplaantunut syyskuusta.

Tietomurrot ja -vuodot

- Office 365 -tietomurtojen määrä kasvussa.
- NordVPN:n Suomessa sijaitsevaan palvelimeen kohdistui tietomurto.

Huijaukset ja kalastelut

- Sosiaalinen media ja pikaviestipalvelut ovat nousseet sähköpostin rinnalle toimitusjohtajahuijauksien välineinä.
- Office 365 -tilien kalastelu johtaa edelleen tietomurtoihin päivittäin.

IoT ja automaatio

- Kansainvälisen automaatioalan kyselytutkimuksen mukaan 1 % organisaatioista vastasi tietoturva-häiriöiden johtaneen hengen menetykseen.
- Automaatiolaitteiden testauksen suurin tapahtuma Yhdysvalloissa.

Top 5 kyberuhat - merkittävät pidemmän aikavälin ilmiöt

1

Haavoittuvuuksien hyväksikäyttö nopeutuu, mikä vaatii nopeita päivityksiä.

2

Tietojenkalastelu ja sen avulla huijatuilla tunnuksilla tehdyt tietomurrot ovat erittäin yleisiä.

3

Laajavaikutteiset kiristyshyökkäykset uhkaavat liiketoiminnan jatkuvuutta.

4

Epäselvä vastuunjako palvelutoimittajan, alihankkijoiden ja tilaajan välillä heikentää tietoturvan hallintaa ja poikkeamien havaitsemista.

5

Organisaatiot eivät osaa ennakoida kyberuhkien vaikutuksia toiminnalleen, minkä vuoksi riskit aliarvioidaan ja palautumis-suunnitelmat ovat puutteellisia.

Verkkojen toimivuus

Verkkojen toimivuus

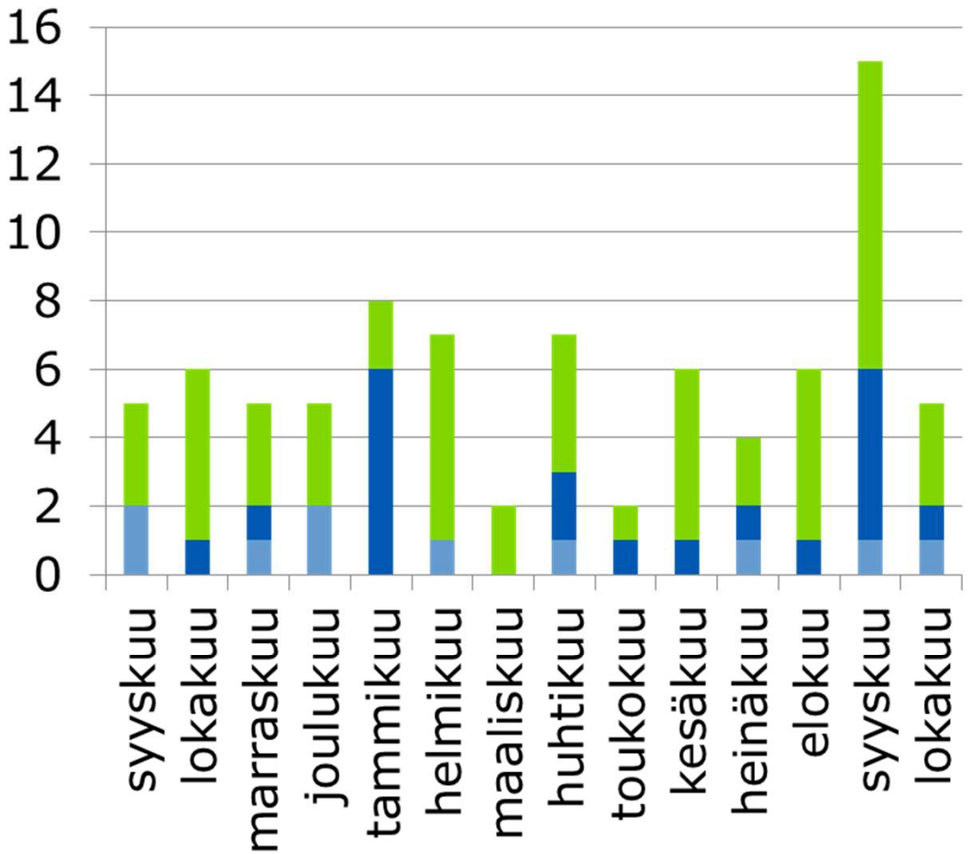
- **Syyskuuhun verrattuna yleisissä viestintäpalveluissa vähemmän merkittäviä häiriöitä**
  - Yksittäiset häiriöt olivat lokakuussa vakavampia.
- **Julkishallinnon ICT-palveluissa oli useita häiriöitä**
- **Nesteen IT-häiriö laski väliaikaisesti yhtiön osakkeen arvoa**

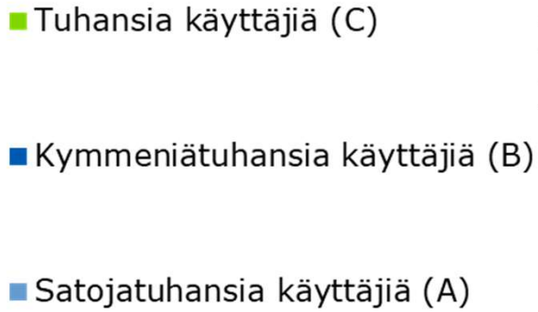
Verkkojen toimivuus

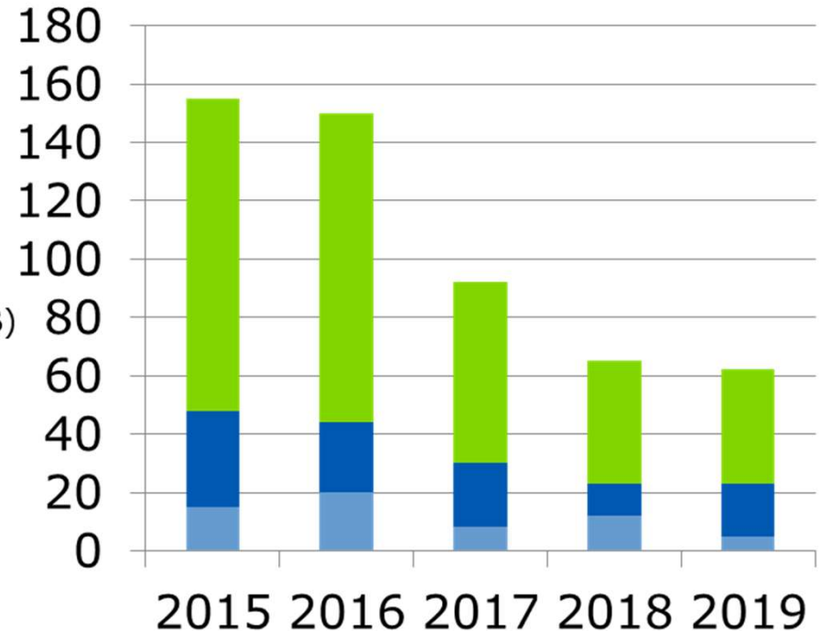
- **Palvelunestohyökkäyksillä uhkailu on jälleen nostanut päätään ulkomailla**
  - Lokakuussa osa uhkauksista johti merkittäviin palvelunestohyökkäyksiin, vaikka yleensä näitä hyökkäyksiä ei toteuteta.
  - Tiedossamme ei ole kotimaisia uhkailutapauksia tältä syksyltä.

- **Kuun loppupuolella yleistyneet peilatut TCP SYN –hyökkäykset näkyivät myös Suomessa**
  - Suomalaisia palvelimia hyödynnettiin peilaamaan palvelunestoliikennettä ulkomaille suuntautuvassa hyökkäyksessä, vaikka ne eivät olleet varsinaisen hyökkäyksen kohteena.
  - Hyökkääjät kuormittavat lukuisia kohteen verkkolohkon IP-osoitteita samaan aikaan, mikä tekee torjumisesta vaikeampaa.

Merkittävien toimivuushäiriöiden määrä







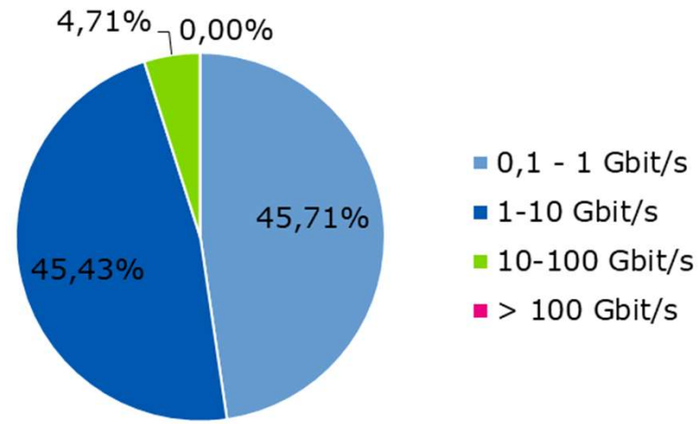
Näissä tilastoissa on esitetty yleisten viestintäpalveluiden merkittävät toimivuushäiriöt, joita on vuosittain 70–200. Määrä on laskenut useiden vuosien ajan. Teleyritykset korjaavat satoja pieniä toimivuushäiriöitä päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 vuodessa. Niiden määrä riippuu teleyrityksen tilastointitavasta.

Palvelunestohyökkäykset ja niillä uhkailu

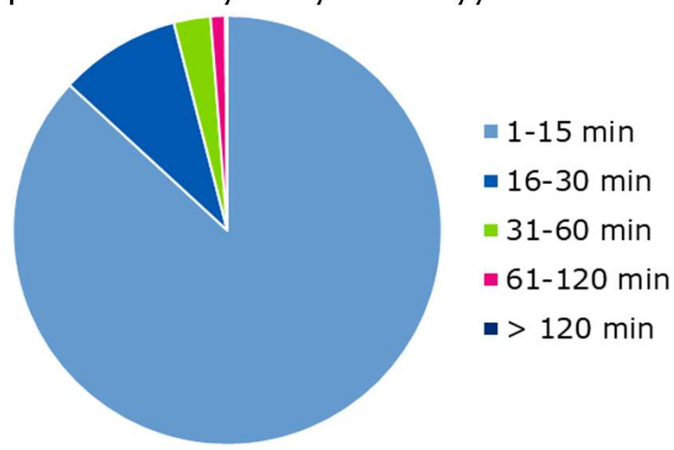
- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (87 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin puolet havainnoiduista yli 100Mbit/s hyökkäyksistä on volyymiltään 1-10 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Yli 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/Q3:	2019/Q2:	2019/Q1:
n. 39 Gbit/s	n. 79 Gbit/s	n. 162 Gbit/s
(kesto 64 min)	(kesto 4 min)	(kesto 9 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymi.



Suomeen kohdistuneiden palvelunestohyökkäysten kesto.

Vakoilu

Vakoilun ajankohtaiset

Turla vakoili kohteita toisen ryhmän operaation kautta

Venäjään liitetyn Turla-ryhmän kerrotaan vakoilleen ulkomaisia kohteita siten, että ryhmä soluttautui toisen toimijan operaatioon ja sai sitä kautta pääsyn sen uhreihin. Tämä tekee myös hyökkääjän tunnistamisesta vaikeampaa.

Korkeakoulut tietojenkalastelun kohteena

Suomalaisten korkeakoulujen työntekijöiden käyttäjätunnuksia ja salasanoja on pyritty kalastelemaan kohdennetusti. Varastettuja tunnuksia voidaan hyödyntää esimerkiksi erilaisiin tutkimustietokantoihin pääsemiseksi.

Tietomurto intialaiseen ydinvoimalaan

Intialaisen ydinvoimalan järjestelmistä löydettiin haittaohjelma, jonka epäillään olevan pohjoiskorealaista alkuperää. Haittaohjelman avulla on mahdollisesti pyritty saamaan tietoja ydinteknologiasta, sillä tapahtumaan liitetty toimija tunnetaan erityisesti teollisuusvakoilusta.

Haittaohjelmat ja haavoittuvuudet

Haittaohjelmahavaintomme

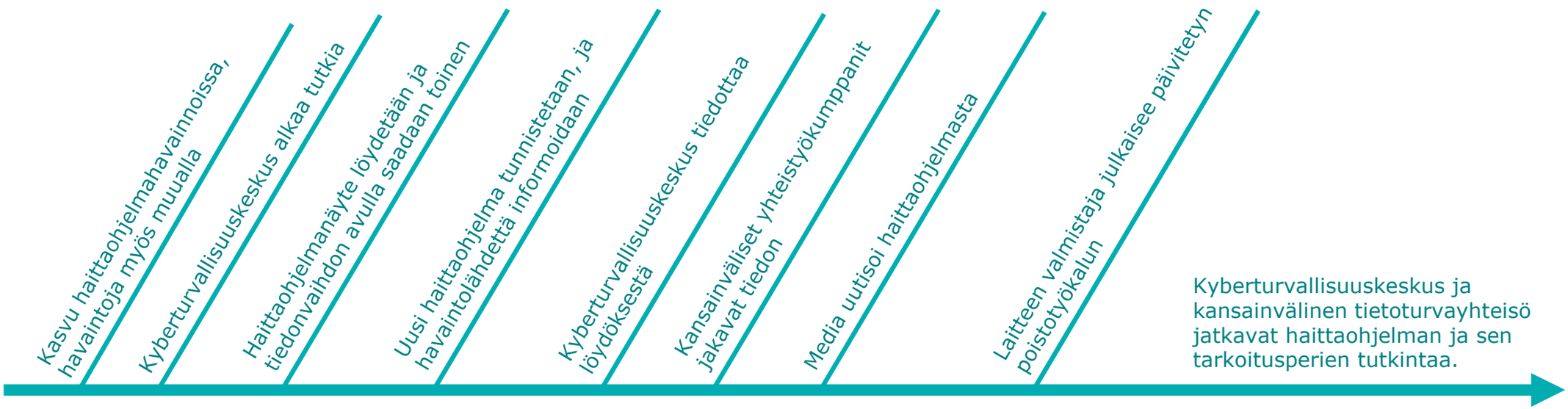
Haittaohjelmatyyppi	Tilanne	
IoT-haittaohjelmat	Muodostavat merkittävän osan Suomessa tehdyistä havainnoista. QSnatch-haittaohjelma havaittu lukuisissa QNAP-verkkotallennuslaitteissa Suomessa.	
Kiristyshaittaohjelmat	Kiristyshaittaohjelmien osalta tilanne Suomessa rauhallinen.	
Etähallittavat haittaohjelmat (RAT)	Etähallittavia haittaohjelmia yritetään levittää aktiivisesti mm. sähköpostin välityksellä.	
Louhijat	Ei merkittäviä louhijahavaintoja tässä kuussa.	
Tietoja varastavat haittaohjelmat	Levittämisyrityksistä jonkin verran havaintoja. Käyttäjätunnuksia kuitenkin kalastetaan aktiivisesti ja myös kohdistetusti.	
Mobiilihaittaohjelmat	Mobiilihaittaohjelmatapauksista on joitain havaintoja.	

Haittaohjelmat

- **QSnatch-haittaohjelma on saastuttanut QNAP-verkkotallennuslaitteita Suomessa ja maailmalla vähintään vuoden verran**
  - Lokakuussa analysoimme ja nimesimme tämän aiemmin huonosti tunnetun haittaohjelman QSnatchiksi.
- **Sähköpostin avulla yritetty levittää aiempaa enemmän haittaohjelmia**
  - Kyberturvallisuuskeskukselle on raportoitu sähköpostin avulla levitettävistä haittaohjelmista noin kaksi kertaa syyskuuta enemmän.
  - Usein ensimmäinen tartunta on etäkäytön mahdollistava haittaohjelma, kuten Emotet.
  - Rikolliset hyödyntävät tartuntaa asentamalla esimerkiksi kiristävän tai tietoja varastavan haittaohjelman.
- **Murretuille verkkosivuille ujutetuista ja siten leviävistä haittaohjelmista on edelleen havaintoja**
  - Muun muassa vanhoja WordPress-julkaisualustan päivittämättömiä lisäosia (plug-in) on murrettu.

QSnatch – suomalainen haittaohjelmalöydös ja osoitus kansainvälisen yhteistyön toiminnasta

- Asiantuntijamme löysivät lokakuussa aiemmin tunnistamattoman, QNAP-verkkolevylaitteisiin tarttuvan haittaohjelman.
- Kyseessä kehittynyt haittaohjelma, joka muun muassa varastaa salasanoja ja voi luoda väylän laitteelle tallennettuihin tiedostoihin.
- Suomessa havaintoja oli päivittäistasolla noin 200, mutta muualla Euroopassa puhuttiin tuhansista.
- Tutkinnan tuloksena maailmaa pystyttiin varoittamaan laajasta tartunnasta – tieto levisi nopeasti verkostoissa ja mediassa.



Haavoittuvuudet

- **Chrome-selaimessa vakavia haavoittuvuuksia**
  - Pahimmillaan on mahdollista ohittaa hiekkalaatikkosuojaus ja ottaa tietokone haltuun.
  - Riittää, että uhri vierailee haitallisella verkkosivulla, jossa haavoittuvuutta hyödynnetään.
  - Verkkorikolliset ovat hyödyntäneet ainakin yhtä haavoittuvuuksista.
  - On harvinaista, että Chromesta löytyy näin vakavia haavoittuvuuksia, joita myös hyödynnetään.
- **Haavoittuvuus verkkosivujen palvelinohjelmiston toteutuksessa (NGINX PHP-FPM)**
  - Ohjelmisto on yleisesti käytössä.
  - Haavoittuvuutta hyödyntämällä palvelin on mahdollista ottaa haltuun.
  - Verkkoon avoinna olevien palveluiden haavoittuvuudet ovat vakavia, ja tällaiset palvelut tulisi päivittää viipymättä.

Tietomurrot ja -vuodot

Tietomurrot ja -vuodot

- **Meille ilmoitettujen Office 365 -tietomurtojen määrä lisääntyi taas hieman**
  - Sähköpostitileiltä varastettuja tietoja käytetään muun muassa taitavasti laadituissa laskutuspetoksissa, joissa väärennetty lasku laditaan ja välitetään eteenpäin hyödyntämällä aitoa laskua käsittelevää viestiketjua.
  - Yhdessä tapauksessa onnistuttiin kalastamaan pilviympäristön pääkäyttäjätason tunnukset. Tunnusten avulla luotiin uusia tunnuksia sekä korotettiin käyttöoikeuksia. Suosittelemme, että myös pilvipalveluiden ylläpidossa käytetään päivittäiskäytöstä erillisiä tunnuksia.
- **VPN-palvelutarjoaja NordVPN:n Suomessa sijaitseva palvelin joutui tietomurron kohteeksi maaliskuussa 2018**
  - Tietomurrossa käytettiin hyväksi verkkoon auki ollutta ylläpitoliittymää.
  - NordVPN ja suomalainen konesalipalvelutoimittaja syyttävät julkisuudessa toisiaan tapahtumasta.
- **Toistuvasti tietomurtoja verkkojulkaisujärjestelmiin ja verkkokauppasovelluksiin**
  - Suurin osa tietomurroista johtuu päivittämättömistä tai väärin konfiguroiduista järjestelmistä.

Suojautumisohjeita tietomurtojen varalta

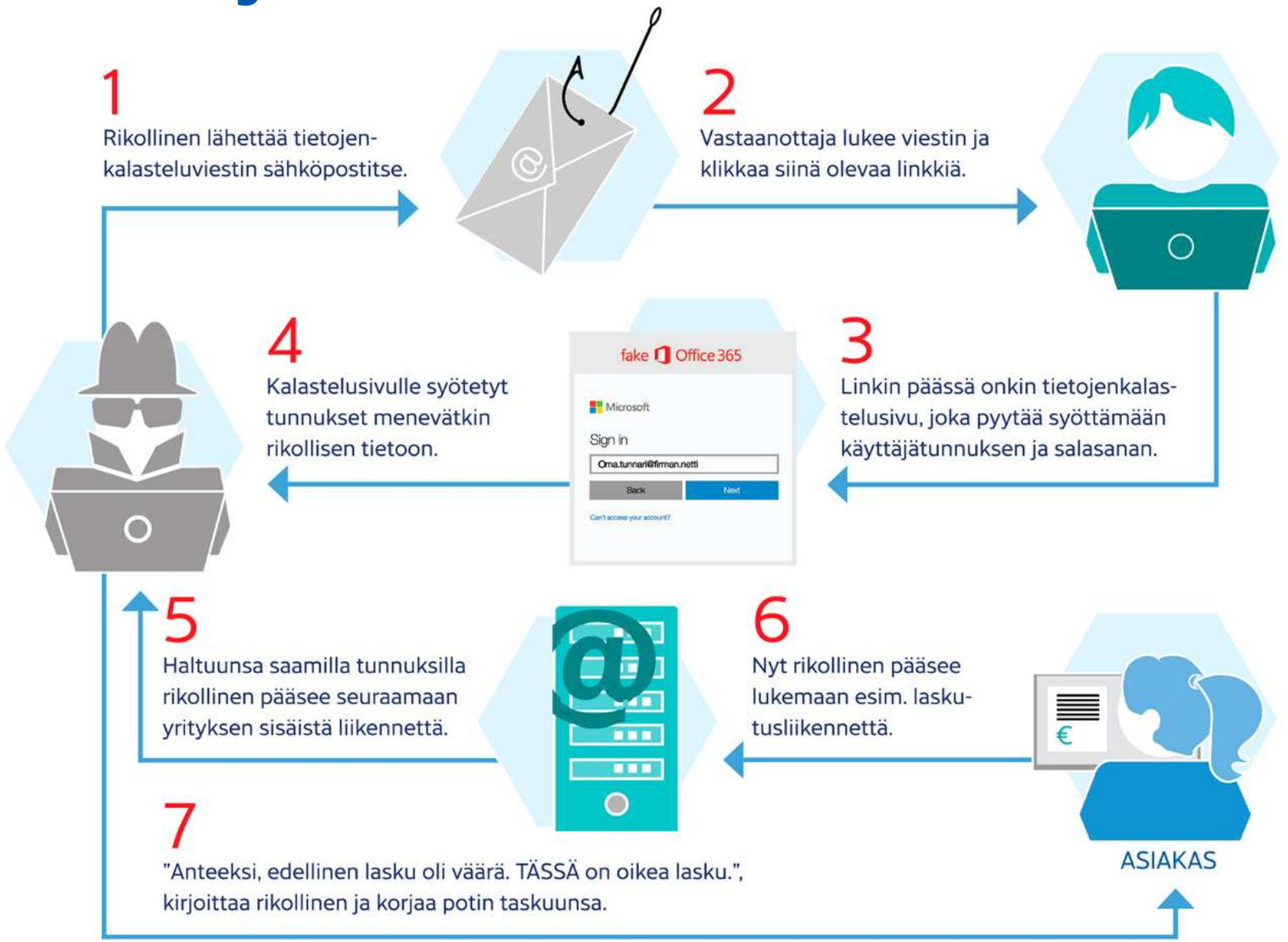
- Käytä eri salasanaa jokaisessa palvelussa.
- Muista päivittää käyttöjärjestelmä ja käyttämäsi ohjelmistot.
- Säilytä salasanoja turvallisesti.
- Vaihda salasanasi, jos epäilet tai tiedät sen joutuneen vääriin käsiin.
- Käytä monivaiheista tunnistamista, jos käyttämissäsi palveluissa sellainen on mahdollista.

Huijaukset ja kalastelut

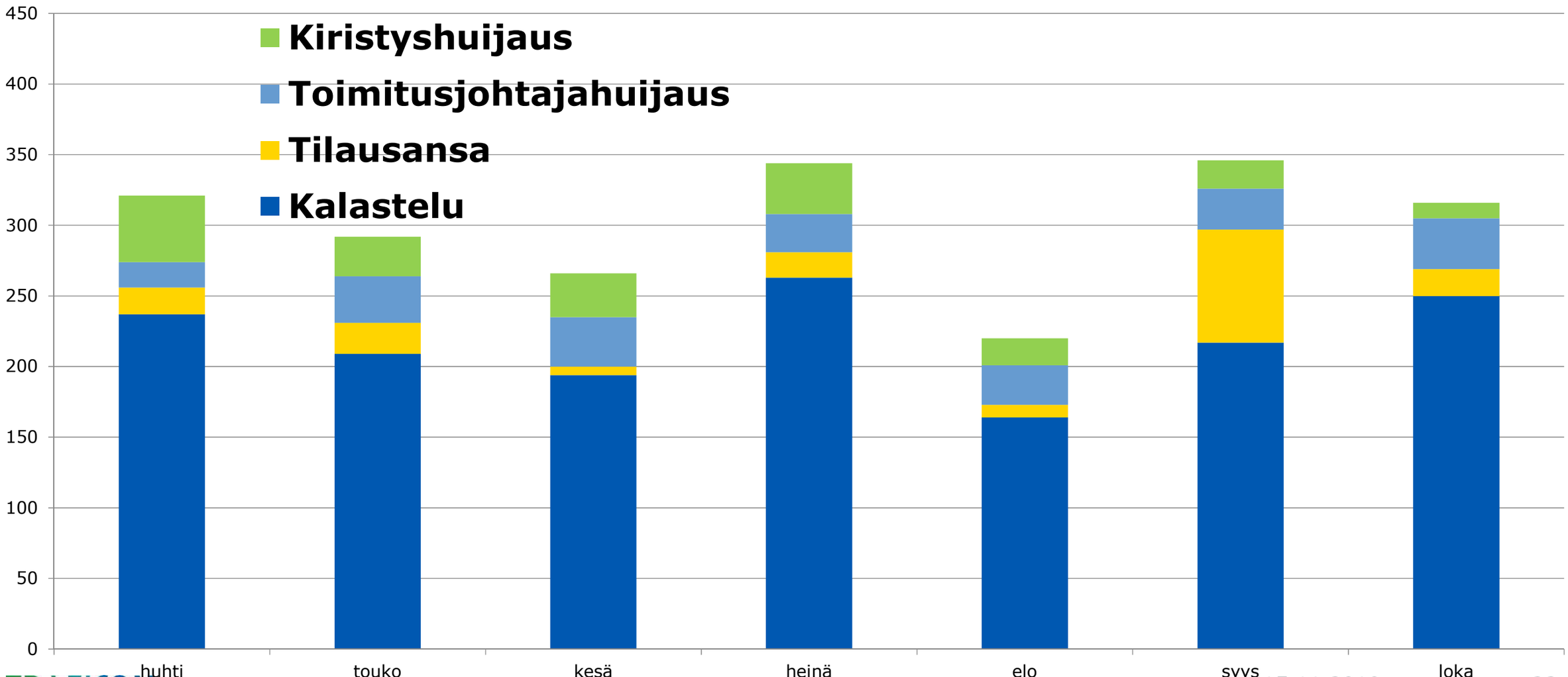
Huijaukset ja kalastelut

- **Sosiaalisen median ja pikaviestintäpalveluiden profiileja käytetään toimitusjohtajahuijauksiin**
  - Osa profiileista on aitoja johtajan tilejä, jotka oli murrettu ja käytetty huijaukseen.
  - Osa profiileista on huijarin laatimia valeprofiileja.
- **Petollisiin tarkoituksiin rekisteröidään valedomaineja**
  - Huijarit rekisteröivät oikean näköisiä verkko-osoitteita, joista he lähettävät väärennettyjä sähköposteja eri organisaatioihin Suomessa ja ulkomailla.
- **Office 365 -kalastelut johtavat edelleen tietomurtoihin lähes päivittäin**

Office 365 –huijauksen vaiheet



Käsiteltyjä huijaustapauksia 2019/04–10



IoT ja automaatio

IoT ja automaatio

- **Automaation laaja kansainvälinen kyselytutkimus**
  - Tutkimuksessa 1 % vastaajista (n=300) kertoi tietoturvahäiriöiden johtaneen hengen menetykseen viimeisen vuoden aikana.
- **Pwn2Own järjestää Yhdysvalloissa ensimmäistä kertaa automaatiolaitteiden testaustapahtuman valkohattuhakkereille**
  - Tapahtuma on historian suurin, ja sen palkkiot liikkuvat kymmenissä tuhansissa dollareissa.

Tietoturva-alan kehitys

Oikeudelliset asiat 1/2

- **Hallitus antoi 7.10.2019 eduskunnalle esityksen laiksi hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi (HE 32/2019)**
  - Hallinnon yhteisistä sähköisen asioinnin tukipalveluista annettuun lakiin lisättäisiin Digi- ja väestötietovirastolle (nyk. VRK) mahdollisuus tunnistaa ulkomaalainen henkilö suomi.fi- tunnistuspalvelun tarjoamisen yhteydessä myös eIDAS-asetuksen mukaisilla notifioiduilla ulkomaisilla tunnistusmenetelmillä.
  - Väestötietojärjestelmästä ja väestörekisterikeskuksen varmennepalveluista annettuun lakiin lisättäisiin Digi- ja väestötietovirastolle tehtäväksi tarjota ulkomaalaisen tunnistuspalvelua. Se olisi tarkoitettu henkilöille, joilla ei ole suomalaista henkilötunnusta ja jotka eivät siksi voisi saada tunnistuslain mukaista vahvan sähköisen tunnistamisen välinettä. Edellytyksenä olisi myös, ettei henkilö voi saada eIDAS-asetuksen mukaista ulkomaista vastavuoroisesti hyväksyttävää tunnistusvälinettä.

Oikeudelliset asiat 2/2

- **Euroopan unionin tuomioistuin on antanut tuomion evästekäytännöistä (C-673/17, 1.10.2019)**
  - Perehdymme tuomioon ja arvioimme tarvetta muuttaa antamaamme tulkintalinjausta asiassa.
  - http://curia.europa.eu/juris/document/document.jsf;jsessionid=E3ED23BA3350CED65CE2760D9E47CFEE?text=&docid=218462&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=1703328

Kyberuutisointia maailmalta

Urheilu- ja antidoping-organisaatiot kohteena

- Microsoft kertoi lokakuussa havainneensa niin kansallisiin kuin kansainvälisiin urheilu- ja antidoping-organisaatioihin kohdistuneita kyberhyökkäyksiä ja niiden yrityksiä.
- Yhtiö ei täsmennä, millaisista hyökkäyksistä oli kyse, mutta kertoo osan niistä onnistuneen.
- Hyökkäysten tekijäksi yhtiö nimeää Venäjään liitetyn ryhmän, joka tunnetaan mm. APT28:na ja Fancy Bearina.
- https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

Kiristyshaittaohjelmatapauksia nähtiin maailmalla runsaasti

- Useita merkittäviin organisaatioihin kohdistuneita kiristyshaittaohjelma-tapauksia tuli ilmi myös lokakuussa, eikä laajavaikutteisten kiristys-tapausten uhka ole poistunut.
- Kohteiksi joutuivat esimerkiksi saksalainen automaatiotekniikka-valmistaja Pilz ja ranskalainen TV-kanava M6.
- https://www.zdnet.com/article/major-german-manufacturer-still-down-a-week-after-getting-hit-by-ransomware/
- https://www.zdnet.com/article/m6-one-of-frances-biggest-tv-channels-hit-by-ransomware/

Facebook haastoi NSO Groupin oikeuteen WhatsApp-murroista

- Sosiaalisen median jätti haastoi israelilaisfirma NSO Groupin oikeuteen.
- Facebookin mukaan yhtiö oli osallisena pikaviestipalvelu WhatsAppin käyttäjien vakoilussa kehittämällään vakoilutyökalulla, joka hyödynsi pikaviestisovelluksessa ollutta haavoittuvuutta.
- Facebook syyttää yritystä WhatsAppin käyttöehtojen rikkomisesta.
- https://thehackernews.com/2019/10/whatsapp-nso-group-malware.html

Kybersään johtopäätökset

Tietoturvan edistyminen

1. EU:n kyberturvallisuuskuukausi kiinnitti huomion arjen kybertaitojen parantamiseen.

2. Hackathonit tukevat tuotteissa ja järjestelmissa olevien tietoturva-aukkojen tunnistamista ja korjaamista.

3. Kansallisen teknologiateollisuuden kiinnostus tuotearviointeihin ja -hyväksyntöihin on kasvanut.

Tietoturvan kehitystarpeet

1. Palvelunestohyökkäysten torjunnassa ei tehokkaasti varauduta tilanteisiin, joissa organisaatio kärsii hyökkäyksestä sen vuoksi, että hyökkääjä heijastaa liikennettä varsinaiseen kohteeseensa tämän kautta.

2. Vakavastikin haavoittuvia järjestelmiä jää päivittämättä kasvavista riskeistä huolimatta.

3. Vikatilanteet huolto- ja korjaustöiden yhteydessä aiheuttavat merkittäviä katkoja palveluihin.

Kiitos!

kyberturvallisuuskeskus.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus