#kybersää 11/2018

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

rauhallinen

huolestuttava

vakava

Kybersään lähteinä ovat vastaanottamamme ilmoitukset, omat järjestelmämme, kansainvälinen tiedonvaihto, uutiset ja muut julkiset lähteet

Varoitus 03/2018: Office 365 -tunnuksia kalastellaan aktiivisesti

- Suomalaisten yritysten ja organisaatioiden työntekijöiden sähköpostitunnuksia ja -viestejä on kuluvan vuoden aikana varastettu. Vakava varoitus aiheesta on edelleen voimassa. Varoituksen taso laskettiin lokakuussa kriittisestä (punainen) vakavaksi (keltainen).
- Käyttäjätunnuksia ja salasanoja on kalasteltu sähköpostitse ja huijaussivujen avulla. Lokakuun lopulla nähtiin viestejä, joissa kalastelulinkki toimitettiin pdf-liitetiedoston sisällä.
- Hyökkääjät voivat ohittaa käyttäjän monivaiheisen tunnistamisen (MFA), jos ylläpitäjät ovat asettaneet Office 365:n tukemaan kirjautumista myös vanhoilla sovelluksilla (ns. legacy support).
- Hyökkääjät kirjautuvat käyttäjätileille ja seuraavat yritysten sähköpostiliikennettä. He pyrkivät saamaan tietoa organisaatioiden liikesalaisuuksista tai maksuliikenteestä sekä kalastelemaan muiden työntekijöiden tai yhteistyökumppanien tunnuksia.
- Kyberturvallisuuskeskus antoi asiasta varoituksen 11.6.2018. Lisätietoja: https://www.viestintavirasto.fi/2018/varoitus-2018-03

#kybersää 11/2018

Palvelunestot

- Palvelunestohyökkäys, jonka jälkeen vaadittiin kiristysviestillä virtuaalivaluuttaa jatkohyökkäyksen estämiseksi.
- Sähköpostin avulla tehty palvelunestohyökkäys.

Haittaohjelmat & haavoittuvuudet

- Hotelliketjun tietomurrossa vaarantui 500 miljoonan matkailijan maksu- ja henkilötiedot.
- Android-laitteisiin on murtauduttu internetiin auki jääneiden vianselvitysporttien avulla.

Huijaukset & kalastelut

- Office 365 -tietojenkalastelulla on vakavia seurauksia.
- Tietojenkalastelu- ja tilausansalinkkejä lähetetään paljon myös tekstiviestitse.

Vakoilu

- APT29 eli Cozy Bear aktivoitui uudelleen. Kalasteluviestien kohteina olivat muun muassa yhdysvaltalaisviranomaiset ja ajatushautomot.
- Tsekin turvallisuuspalvelu yhdistää maan ulkoministeriön tietomurron Venäjään.

Verkkojen toimivuus

- Vakavia häiriöitä on ollut enemmän kuin viime vuonna, mutta niiden kestot ovat lyhentyneet.
- Merkittävien häiriöiden kokonaismäärä laskussa.

IoT

- Saksan viranomaiset (BSI) ovat kehittäneet reitittimille tietoturvakriteeristön.
- DigiCertin tutkimuksen mukaan IoT-laitteiden turvallisuus on yritysjohtajien korkea prioriteetti.
- YLE uutisoi IoT-laitteiden haasteista.

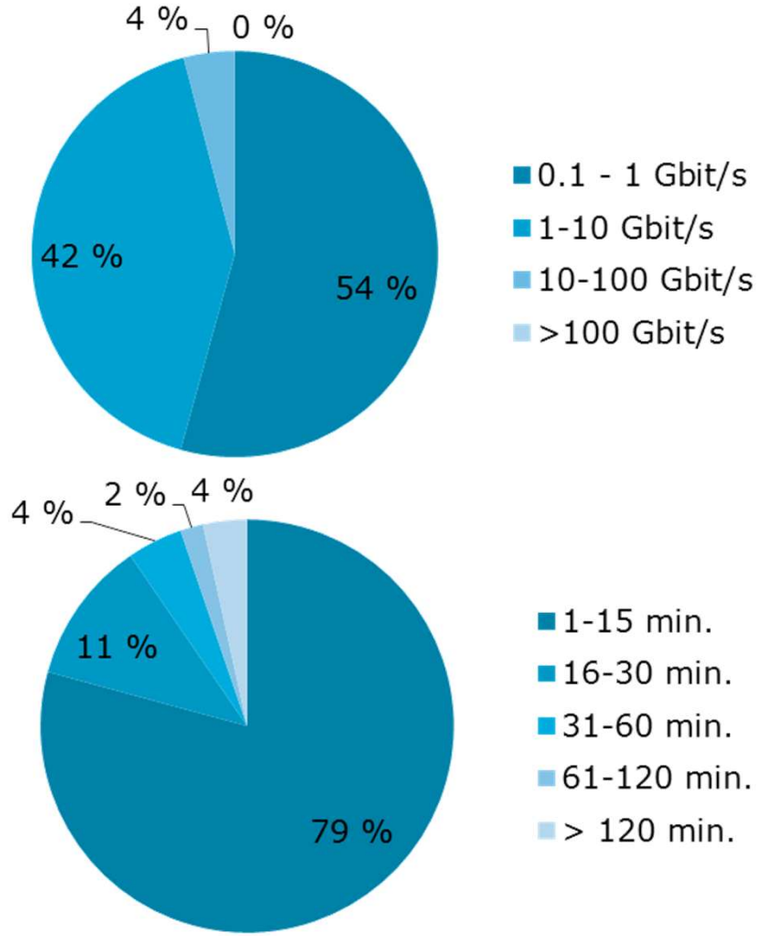
Palvelunestot

Palvelunestohyökkäykset ja niillä uhkailu:

- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (71 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin 57 % kaikista nähdyistä hyökkäyksistä ovat volyymiltään yli 1 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Myös yli 10 Gbit/s hyökkäyksiä nähdään Suomessa useita viikoittain.
- Palvelunestohyökkäysten kuvaajat kerätään suoraan teleyrityksiltä, koska Viestintävirastoon ilmoitetaan vain murto-osa tapahtuneista palvelunestohyökkäyksistä.

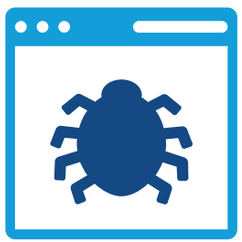
Suurimpia Suomessa viime aikoina havaittuja palvelunestohyökkäyksiä. Lähde: teleyritykset

2018/Q3:	**2018/Q2:**	**2018/Q1**
n. 89 Gbit/s (kesto 30 min)	n. 37 Gbit/s (kesto 8 min)	n. 35 Gbit/s (kesto 7 min)



Suomeen kohdistuneiden palvelunestohyökkäysten volyymit ja kestot 2018/Q3. Lähde: Telia.

Palvelunestohyökkäykset ja niillä uhkailu

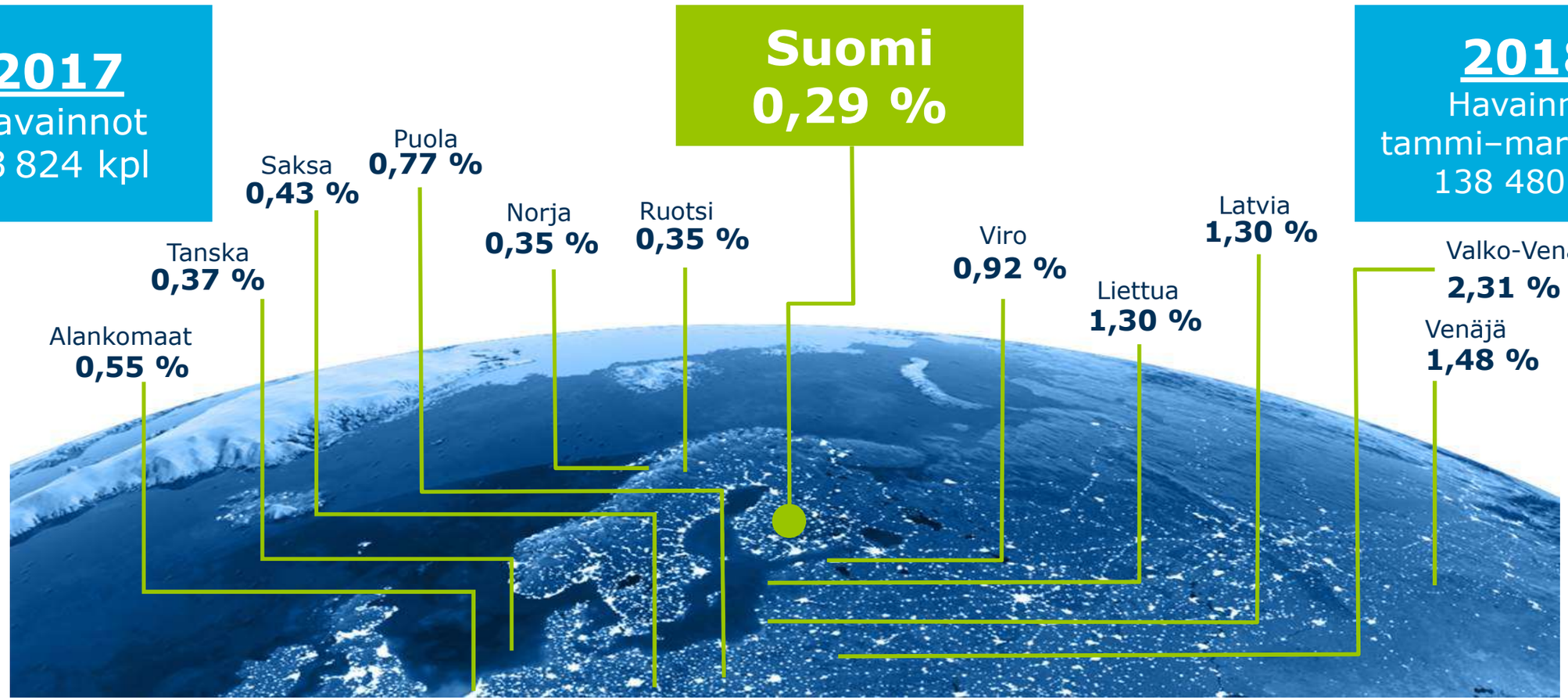


- **Suomalaiseen organisaatioon tehtiin palvelunestohyökkäys lukuisten sähköpostien avulla**
  - Sähköpostit saapuivat aidoilta sähköpostipalvelimilta. Viestit oli saatu lähtemään verkkosivujen uutiskirjeen tilausomaisuuden avulla.
- **Suomessa havainto palvelunestohyökkäyksestä, johon liittyi kiristysviesti**
  - Kohteeseen tehtiin ensin näytösluontoinen hyökkäys, jonka jälkeen vaadittiin 50 Monero-virtuaalivaluuttaa jatkohyökkäysten estämiseksi.
  - Rikollisille ei pidä maksaa, vaan panostaa parempaan suojautumiskykyyn palvelunestohyökkäyksiä vastaan. Omalta palveluntarjoajalta paras apu.
- **Palvelunestohyökkäyksiä tehdään nyt enemmän niin sanotulla HTTP FLOOD -tekniikalla, jossa WWW-palvelinta kuormitetaan suurella määrällä HTTP-kyselyitä**
  - Torjuminen on perinteisiä hyökkäystekniikoita haastavampaa, sillä HTTP FLOOD -kyselyt näyttävät normaalilta selainliikenteeltä. HTTP FLOOD -hyökkäyksellä voidaan myös kuormittaa palvelinta tavanomaista hyökkäystä tehokkaammin.
  - Myös perinteiset amplifikaatiohyökkäykset ovat yhä yleisiä. Viime aikoina on näkynyt erityisen paljon memcached- ja DNS-amplifikaatiotekniikoilla toteutettuja hyökkäyksiä.

Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

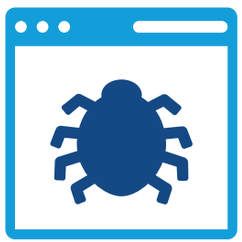
2017
Havainnot
93 824 kpl



2018
Havainnot
tammi–marraskuu
138 480 kpl

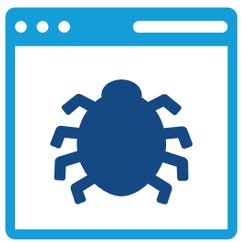
Vuoden 2018 tietoturvapoikkeamien havaintomäärää nostaa pienreitittimien haittaohjelmatartunnat

Haittaohjelmat



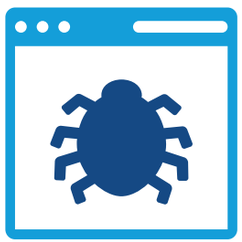
- **Suomessa määrällisesti eniten havaintoja kotireitittimiin ja muihin IoT-laitteisiin tarttuneista haittaohjelmista**
  - Havainnot liittyvät erityisesti muutaman teleyrityksen tiettyihin reititinmalleihin.
- **Haittaohjelmat ovat saastuttaneet Android-laitteita internetiin auki jääneiden vianselvitysporttien (ADB) avulla**
  - Haittaohjelmalla on louhittu mm. virtuaalivaluuttaa.
- **Magento-verkkokauppa-alustoja murretaan edelleen, ja murretuissa verkkokaupoissa käytetyt maksukorttitiedot päätyvät rikollisille**
  - Erään tietoturvatutkijan mukaan n. 7 000 Magento-alustaa käyttävää verkkokauppaa on murrettu viimeisen 6 kuukauden aikana. Julkisuuteen ovat tulleet muun muassa Ticketmaster, British Airways ja Newegg.
  - Kyberturvallisuuskeskuksen tiedossa on yksi havainto myös Suomesta.

Haavoittuvuudet



- **Useiden valmistajien SSD-kiintolevyjen tarjoamat salausratkaisut eivät ole luvatun vahvuisia**
  - » Tämä vaikuttaa myös oletusasetuksin käyttöönotettuun Windowsin BitLocker-salaukseen, joka luottaa kiintolevyn tarjoamaan salaukseen.
- **Rikolliset skannaavat jatkuvasti internetiin kytkettyjä laitteita**
  - » Laitteista pyritään löytämään haavoittuvuuksia tai vääriä asetuksia, joiden avulla laitteisiin pyritään tekemään tietomurto.
  - » Haavoittuva internetiin kytketty laite voidaan löytää ja ottaa haltuun jopa muutamassa tunnissa
- **Tammikuussa julkaistujen Spectre- ja Meltdown –haavoittuvuuksien jälkeen suorittimien sivukanavahyökkäyksiä on tutkittu enemmän ja vastaavia haavoittuvuuksia on löytynyt jatkuvasti lisää**
  - » Erilaisia suorittimien sivukanavahyökkäyksiä tunnetaan jo useita kymmeniä.
  - » Haavoittuvuutta hyväksikäyttämällä voi saada esille esimerkiksi salausavaimia.
  - » Käytännössä uhka on vakavin yhteiskäyttöisille alustoille, kuten pilvipalveluille ja muille yhteiskäyttöisille alustoille.

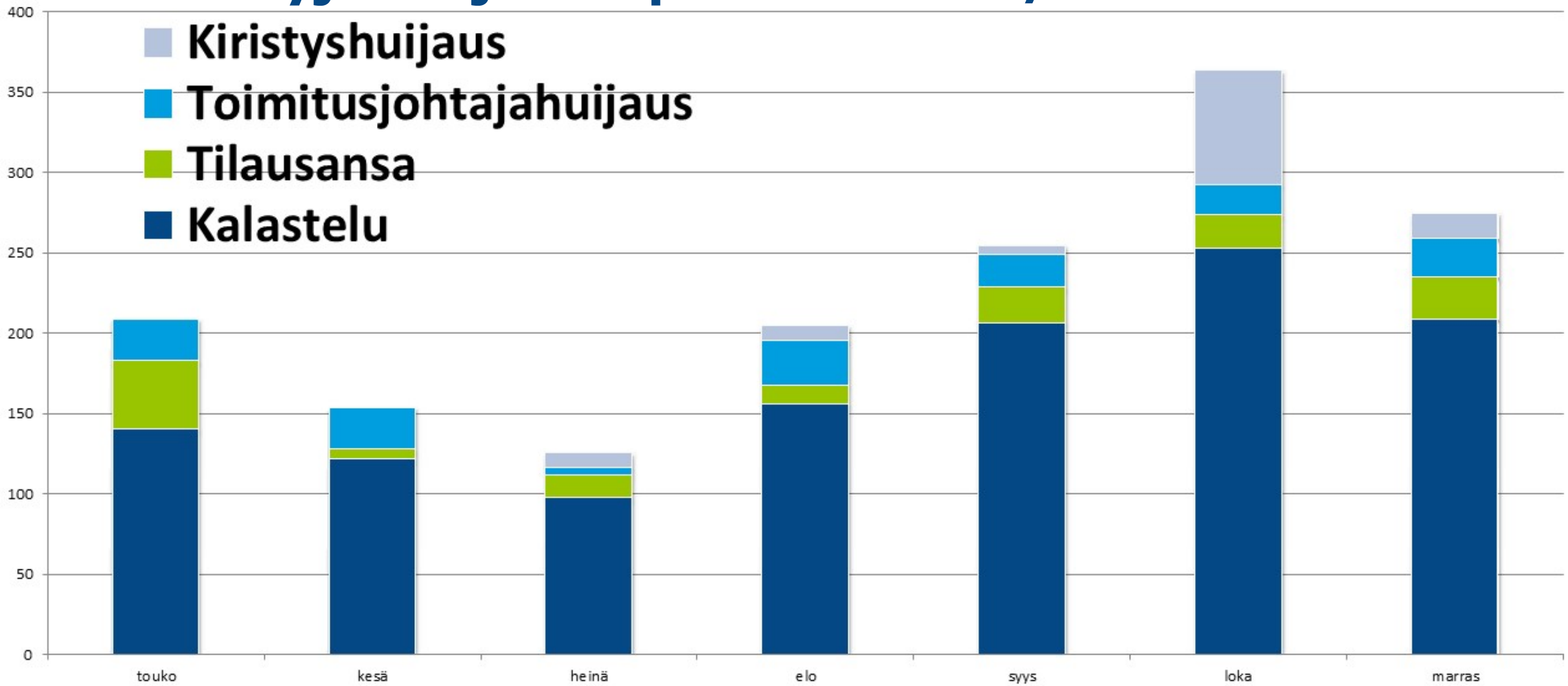
Tietomurrot ja tietovuodot



- **Marriottin omistaman hotelliketju Starwoodin asiakastietojärjestelmään on ollut luvaton pääsy vuodesta 2014 alkaen**
  - » Paljastuneissa tiedoissa on voinut olla 500 miljoonan asiakkaan luottokorttinumeroita, passin tietoja sekä syntymäaikoja.
- **Quora-verkkopalvelusta on voinut vuotaa noin 100 miljoonan asiakkaan tietoja**
  - » Paljastuneissa tiedoissa on voinut olla nimi, sähköposti, salasanan tiiviste ja muita tietoja.
- **Statcounter-verkkoanalytiikkapalvelun tietomurron seurauksena noin 700 000 verkkosivustoa altistui hyökkääjän ohjelmakoodille**
  - » Hyökkäyksen varsinainen kohde oli yksi virtuaalivaluutan kauppapaikka, josta hyökkääjät pyrkivät varastamaan virtuaalivaluuttaa.

Huijaukset & kalastelut

Käsiteltyjä huijaustapauksia 2018/05–11



Huijaukset marraskuussa

- **Office 365 -tunnusten kalastelu jatkuu**
  - Suomalaisten yritysten sähköpostitileille on murtauduttu kalastelluilla tunnuksilla.
  - Kalasteluun käytetään myös organisaatioiden omia turvapostiviestejä sekä sellaiseksi naamioituja väärennettyjä turvaposti-ilmoituksia.
  - Kalastelun avulla haltuun saatuja sähköpostitilejä käytetään mm. huijauksiin, vakoiluun ja uusien kalasteluviestien lähetykseen.
  - Kaksivaiheinen kirjautuminen suositellaan ottamaan käyttöön pakotetusti niin, ettei Office 365:n Modern Authentication -kirjautumistapaa voi kiertää vanhemmilla päätelaitteilla.

- **Kiristyshuijauksia aikuisviihdeteemalla**
  - Muutaman kuukauden jatkunut kiristyshuijauskampanja on jatkunut marraskuussakin.
  - Kiristyksen uhreja säikytellään väittämällä, että kiristäjä on saanut pääsyn uhrin laitteeseen ja vakoillut tämän tekemisiä. Kiristäjä väittää saaneensa käsiinsä arkaluontoista materiaalia, mutta se on kaikki huijausta.
- **Tekstiviestihuijaukset johtavat tilausansaan**
  - Ulkomaisesta numerosta tulleissa tekstiviesteissä on ollut linkkejä tilausansaan, jossa kuluttajia huijataan IPhone-arvonnalla.
  - Perinteisten sähköpostihuijausten lisäksi tekstiviestejä käytetään yhä enemmän huijausviesteihin.
- **Tietoja yritetään kalastella tunnettujen pankkien ja tuotemerkkien nimissä**
  - Apple ID –tunnuksia on jälleen kalasteltu runsaasti. Myös pankkien ja Netflixin nimissä kalasteltiin maksukorttitietoja.
  - Tilausansoihin houkuteltiin kuluttajia paljon mm. Ikean ja Gigantin tuotenimillä.

Vakoilu

Verkkovakoilutilanteessa ajankohtaista

APT29-ryhmä aktivoitui jälleen

Tietoturvayhtiöt CrowdStrike ja FireEye raportoivat APT29-ryhmän aktivoitumisesta. Myös Cozy Bearina tunnetun ryhmän kerrotaan lähettäneen kalasteluviestejä USA:ssa muun muassa viranomaisille ja ajatushautomoihin.

Tsekki syyttää venäläisryhmää ministeriönsä vakoilusta.

Tsekin turvallisuuspalvelu yhdistää vuosiraportissaan maan ulkoministeriön järjestelmiin vuonna 2017 kohdistuneen tietomurron Venäjään. Raportin mukaan hyökkääjä pääsi käsiksi yli sadan henkilön sähköpostilaatikoihin.

Saksassa raportoitiin uudesta vakoiluyrityksestä

Lehtitietojen mukaan saksalaisviranomaiset ovat havainneet uuden, parlamenttiin, armeijaan ja lähetystöihin kohdistetun kyberhyökkäyksen. Tekijäksi nimetty Snake- eli Turla-ryhmä yhdistettiin Saksassa myös aiemmin tänä vuonna havaittuun hyökkäykseen.

Verkkojen toimivuus

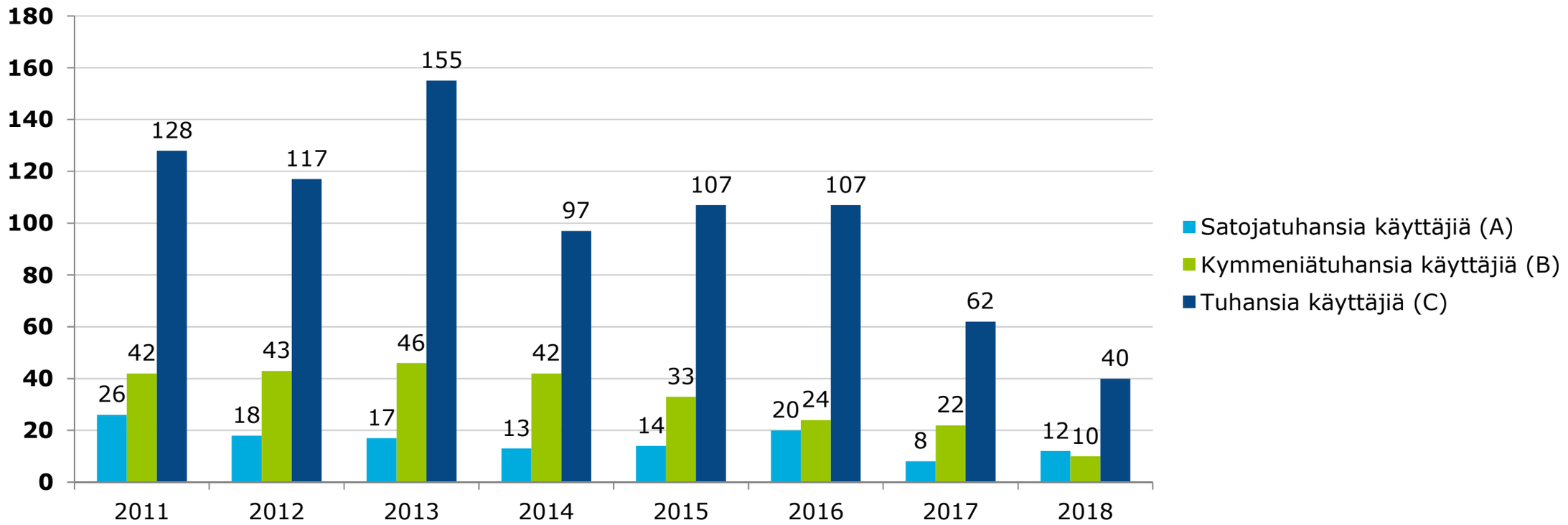
Viestintäverkkojen toimivuus

Vuosi 2017	
Vakavuus	**Lukumäärä**
A-luokka	8
B-luokka	22
C-luokka	62
Kaikki häiriöt	**460 075**

Vuosi 2018 (tammi–marraskuu)	
Vakavuus	**Lukumäärä**
A-luokka	12
B-luokka	10
C-luokka	40
Kaikki häiriöt (Q1–Q3)	**287 723**

Merkittävien häiriöiden määrä jatkaa laskemistaan. Vakavimpia A-luokan häiriöitä on ollut kesän aikana paljon, mutta se vaikuttaa sattumalta.

Viestintäverkkojen toimivuus



Tässä tilastossa on esitetty ainoastaan A-, B- ja C-vakavuusluokan toimivuushäiriöt. Niitä on vuosittain 80–200. Pienempiä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 vuodessa.

IoT

Esineiden internet (IoT), marraskuun yhteenveto

- **Saksan viranomaiset (BSI) ovat kehittäneet reitittimille tietoturvallisuuskriteeristön**
  - » Maaliskuun alussa julkaistu kriteeristö reitittimien tietoturvallisuudelle (BSI TR-03148) ei velvoita valmistajia noudattamaan ohjeen kriteeristöä. Noudattamisesta saa merkiksi tarran, joka auttaa kuluttajaa.
  - » Kriteeristö joutui nopeasti CCC:n (Chaos Computing Club) arvostelun kohteeksi, sillä teknisessä ohjeessa oli lukuisia tietoturvaa mahdollisesti heikentäviä kohtia.
- **DigiCertin tutkimuksen mukaan IoT-laitteiden turvallisuus on yritysjohtajien korkea prioriteetti**
  - » Yritysjohtajat pitävät laitteiden turvallisuutta erittäin tärkeänä (92 % uskoo sen olevan erittäin tärkeää seuraavan 2 vuoden aikana).
  - » Tutkijat muistuttavat, että heikoimmat valmistajat kärsivät suurimmat tappiot.
- **YLE uutisoi IoT-laitteiden haasteista**
  - » Haasteet ovat sekä lainsäädännön että tietoturvan hitautta.
  - » IoT-laitteiden riskejä havainnollisti KTK:n erityisasiantuntija Saana Seppänen, F-Securen asiantuntijat sekä Tietosujavaltuutettu Reijo Aarnio.

Tietoturva-alan kehitys

Ajankohtaiset oikeudelliset asiat: EU

- **EU:n televiestintäuudistus ("EECC-direktiivi")**
  - Hyväksyttiin 14.11. parlamentissa ja 4.12. neuvostossa. Toimielinten on määrä allekirjoittaa se 12.12. ja se julkaistaneen 17.12. EU:n virallisessa lehdessä. Säädös tulee voimaan 3 päivän kuluttua julkaisemisesta ja voimaantulosta alkaa pääsääntöisesti 2 vuoden täytäntöönpanoaika.
  - Samalla hyväksyttiin ns. BEREC-asetus eli asetus Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimestä.
  - Kansallisesti tarvittavat muutokset tehdään pääasiassa sähköisen viestinnän palveluista annettuun lakiin (917/2014) LVM:n käynnistämässä säädöshankkeessa.
- **"Kyberturvallisuusasetus"**
  - Asetus käsittäisi säännökset EU:n laajuisesta ICT-tuotteiden tietoturvasertifioinnin puitekehyksestä sekä EU:n verkko- ja tietoturvavirasto ENISA:n pysyvästä mandaatista.
  - Asetusehdotus annettu syksyllä 2017; nyt käynnissä parlamentin, neuvoston ja komission väliset neuvottelut asetuksen sisällöstä; tavoitteena hyväksyminen keväällä 2019.
- **Sähköisen viestinnän tietosuoja-asetus ("ePrivacy-asetus")**
  - Liittyy tiiviisti jo sovellettavaan EU:n yleiseen tietosuoja-asetukseen (GDPR).
  - Asetuksen valmistelu etenee hitaasti; jäsenvaltioilla hyvin erilaisia näkemyksiä mm. evästeiden käsittelyn oikeudellisesta perusteesta.

Ajankohtaiset oikeudelliset asiat: kotimaa

- **Eduskunnassa muun muassa:**
  - U-kirje eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi verkossa tapahtuvan terroristisen sisällön levittämisen estämisestä (U 98/2018)
    - Asetusehdotuksen mukaan säilytyspalvelun tarjoajien olisi muun muassa poistettava terroristinen sisältö tai estettävä siihen pääsy tunnin kuluessa toimivaltaisen viranomaisen antaman poistamismääräyksen vastaanottamisesta. Ollut myös Viestintäviraston lausuttavana.
  - U-jatkokirje asetusehdotuksesta sähköistä todistusaineistoa rikosasioissa koskevista eurooppalaisesta esittämismääräyksestä ja säilyttämismääräyksestä ja direktiiviehdotus yhdenmukaisista säännöistä koskien laillisten edustajien nimittämistä todistusaineiston keräämiseksi rikosasioissa (UJ 28/2018; ns. e-evidence-säädöshanke)
    - Ehdotuksilla mahdollistettaisiin lainvalvontaviranomaisen rajat ylittävä pääsy sähköiseen todistusaineistoon. Asiaa on käsitelty eduskunnassa aikaisemmin syksyllä U 33/2018 -kirjelmän johdosta.
  - Hallituksen esitys eduskunnalle laeiksi sähköisen viestinnän palveluista annetun lain ja julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain muuttamisesta (HE 226/2018)
    - Lakimuutoksilla mahdollistetaan laajakaistainen viranomaisviestintäpalvelu, jolla korvataan nykyinen viranomaisradioverkkoon (VIRVE) perustuva kapeakaistainen viranomaisviestintäpalvelu.
  - Tunnistus- ja luottamuspalvelulain muutos (HE 264/2018)
    - Marraskuun lopussa annetussa hallituksen esityksessä selkeytetään vahvan sähköisen tunnistamisen luottamusverkostoon kuuluvien palveluntarjoajien sopimuksentekovelvoitetta ja ehdotetaan enimmäishinnan alentamista tukkutasolla.

Ajankohtaiset oikeudelliset asiat: kotimaa

- **Hyväksytyt ja vahvistetut lait:**
  - » Tietosuojalaki (1050/2018) ym.
    - Täydentävät EU:n yleistä tietosuoja-asetusta (GDPR); tulevat voimaan 1.1.2019.
  - » Laki Liikenne- ja Viestintävirastosta (935/2018) ja muut LVM:n hallinnonalan virastouudistukseen kuuluvat lait
    - Ns. voimaanpanolaki (937/2018) tuli voimaan 27.11.2018 ja muut kokonaisuuteen kuuluvat yli 80 lakia tulevat voimaan 1.1.2019.
    - Viestintävirasto, Liikenteen turvallisuusvirasto Trafi sekä Liikenneviraston tietyt toiminnot yhdistyvät Liikenne- ja viestintävirasto Traficomiksi 1.1.2019.
    - Kyberturvallisuuskeskus toimii organisatorisesti ja toiminnallisesti erillisenä suoraan pääjohtajan alaisuudessa ja vastaa valtakunnallisista tietoturvallisuustehtävistä (laki Liikenne- ja Viestintävirastosta, 5 §).
- **Viestintävirastossa:**
  - » Tunnistuspalveluiden arviointikriteeristön päivitys käynnistetty
    - Viestintävirasto on antanut vahvan sähköisen tunnistuspalvelun tarjoajien vaatimustenmukaisuuden arvioinnista kaksi ohjetta. Ohjeessa 211/2016 on mallikriteeristö ja ohjeessa 215/2016 ohjeet tarkastuskertomuksen laatimiselle.
    - Viestintävirasto käynnisti marraskuun lopussa ohjeiden päivityksen. Mallikriteeristöön lisätään mobiilisovelluksien kriteeristö.
    - Päivitystyöhön on kutsuttu kaikille avoin työryhmä, ks. lisää https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/11/ttn201812030958.html

Kyberasioihin liittyvää uutisointia maailmalta

Iso-Britannian parlamentaarinen komitea varoittaa kohonneesta kyberhyökkäyksen mahdollisuudesta kriittistä infrastruktuuria kohtaan. Komitean raportin mukaan vihamieliset valtiot muodostavat suurimman uhkan, mutta myös rikollisjärjestöjen kyvykkyydet kasvavat jatkuvasti.

Iso-Britannian hallinto ei kerro kaikista havaituista haavoittuvuuksista ohjelmistovalmistajille. Maan tiedusteluviranomaiset sekä kyberturvallisuuskeskus arvioivat tapauskohtaisesti haavoittuvuuden aiheuttamaa uhkaa kansalliselle turvallisuudelle sekä sen hyödyntämisen etuja tiedustelutoiminnassa.

Puola liittyy Liettuan käynnistämään PESCO-kyberyhteistyöhankkeeseen. Puolan puolustusministeri Mariusz Blaszczak allekirjoitti aiesopimuksen Liettuan vierailullaan. Liettuan aloite tähtää kiertävällä vastuulla toimivien "Cyber Rapid Response" -ryhmien perustamiseen. Ryhmät koostuisivat toimintaan osallistuvien maiden asiantuntijoista.

Oikeus- ja kuluttaja-asioista vastaava **komissaari Vera Jourova varoittaa, että Venäjän propaganda ja kyberhyökkäykset saattavat vaikuttaa europarlamenttivaaleihin.** Komissaarin mukaan jäsenvaltioille on annettu erityisiä ohjeita vaalien turvallisuuden takaamiseksi.

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi