#kybersää maaliskuu 2018

#kybersää kertoo kuukauden merkittävistä tietoturvapoikkeamista ja -ilmiöistä. Tarkoituksena on antaa lukijalle nopea kokonaiskuva siitä, mitä kyberturvallisuuskentällä on kauden aikana tapahtunut. Tilanne voi olla:

rauhallinen

huolestuttava

vakava

#kybersää 03/2018

Palvelunestot

- Ilmoitettujen hyökkäysten määrä oli maaliskuun aikana Suomessa vähäinen.
- Helmikuussa alkanut memcached-palveluiden käyttö hyökkäysten vahvistamisessa on laantunut päivitysten ja suojausten myötä.

Haittaohjelmat & haavoittuvuudet

- Meltdown- ja Spectre-haavoittuvuuksien korjauspäivitysten ongelmat ovat jatkuneet.
- Drupal-sisällönhallintaohjelmiston haavoittuvuus mahdollistaa sivuston täydellisen haltuunottamisen.

Huijaukset & kalastelut

- Murrettujen sähköpostitilien kautta lähetettiin tuhansittain sähköposteja suomalaisille.
- Viestin sisältönä oli PDF-liite, joka tarjosi linkkiä kalastelusivulle.

Vakoilu

- SUPO: kyberhyökkäykset ovat arkipäivää myös Suomessa
- Yhdysvallat syyttää Venäjää energia-alaan kohdistuneista hyökkäyksistä
- Kaspersky paljasti Yhdysvaltain armeijan kyberoperaation

Verkkojen toimivuus

- Hieman tavallista vähemmän merkittäviä häiriöitä.
- Vuoden 2017 kaikkien häiriöiden lukumäärä oli poikkeuksellisen korkea, koska yksi teleyritys on madaltanut tilastointinsa kynnysarvoja.

IoT

- Iso-Britannian Secure by Design -periaatteet
- Tietoturvayhtiö Dragos peräänkuuluttaa kyberuhkien ennakointia teollisuusautomaatiossa
- Markkinoille tulee tuotteita IoT-laitteiden ennakoivan huollon koneoppimiseen

Maaliskuussa 2018 korostuivat erilaiset huijaukset ja tietojenkalastelut

Meltdown- ja Spectre –haavoittuvuuksien paikkaus jatkuu. Kuukauden aikana nähtiin myös epäonnistuneita päivitysyrityksiä.

Viestintävirasto julkaisi Tietoturvan vuosi 2017 -katsauksen https://www.viestintavirasto.fi/tilastotjatutkimukset/katsauksetjaartikkelit/2018/tietoturvanvuosi2017-julkaisu0012018j.html

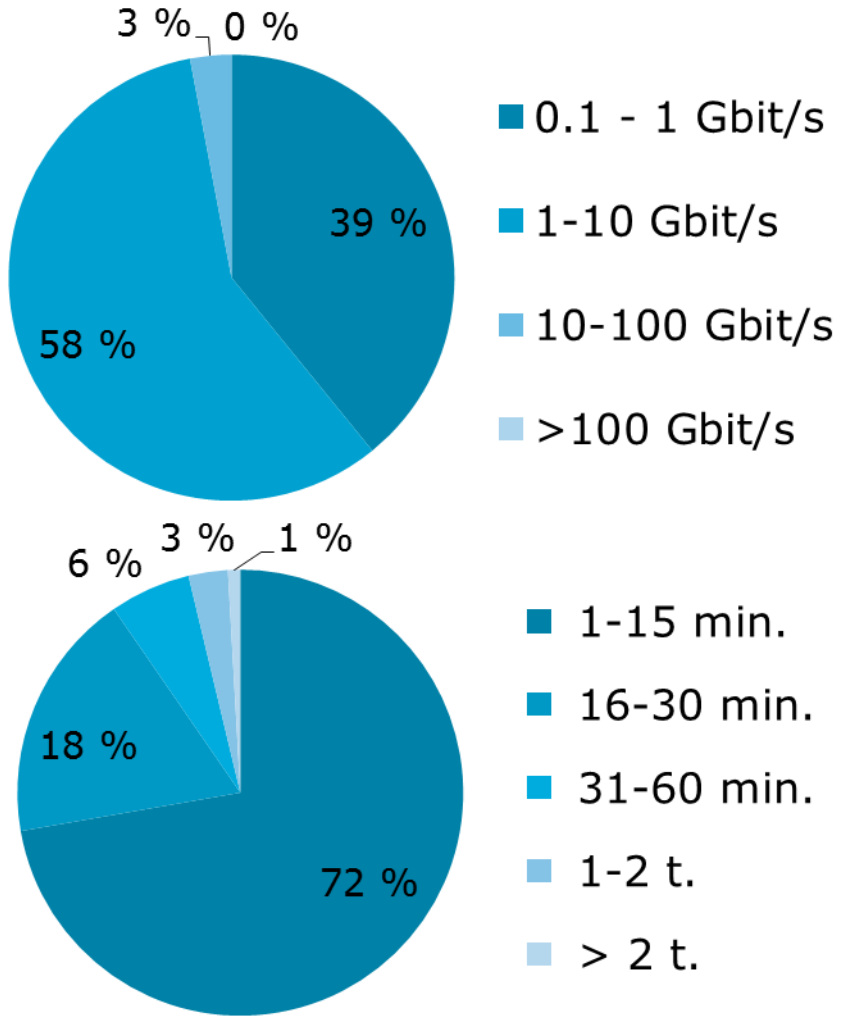
Palvelunestot

Palvelunestohyökkäykset ja niillä uhkailu: tilastojen valossa

- Lyhyet alle 15 min hyökkäykset ovat yleisimpiä (72 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin 60 % 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 viimeaikoina havaittuja palvelunestohyökkäyksiä. Lähde: teleyritykset

2018/Q1:	**2017/Q4:**	**2017/Q3:**
n. 35 Gbit/s (kesto 7 min)	n. 57 Gbit/s (kesto alle 10 min)	n. 30 Gbit/s (kesto 12 min)



volyymit ja kestot 2018/Q1. Lähde: Telia.

Palvelunestohyökkäykset ja niillä uhkailu: ajankohtaista

- Maaliskuussa kyberturvallisuuskeskukseen raportoitiin vähän palvelunestohyökkäyksiä
  - Eräässä hyökkäyksessä oli käytetty suuren volyymin sijaan sovelluspalvelinta raskaasti kuormittavia kyselyitä, joita oli lähetetty usean viikon ajan.
- Helmikuussa alkanut memcached-palveluiden käyttö hyökkäysten vahvistamisessa on laantunut päivitysten ja suojausten myötä
  - Helmikuussa maailmalla nähtiin historian suurin hyökkäys 1,7 Tbit/s.
  - Kyberturvallisuuskeskus kartoitti yhdessä teleyritysten kanssa Suomessa internetiin näkyviä memcached-palveluita ja tiedotti niiden ylläpitäjille palvelun suojaamisen tärkeydestä.

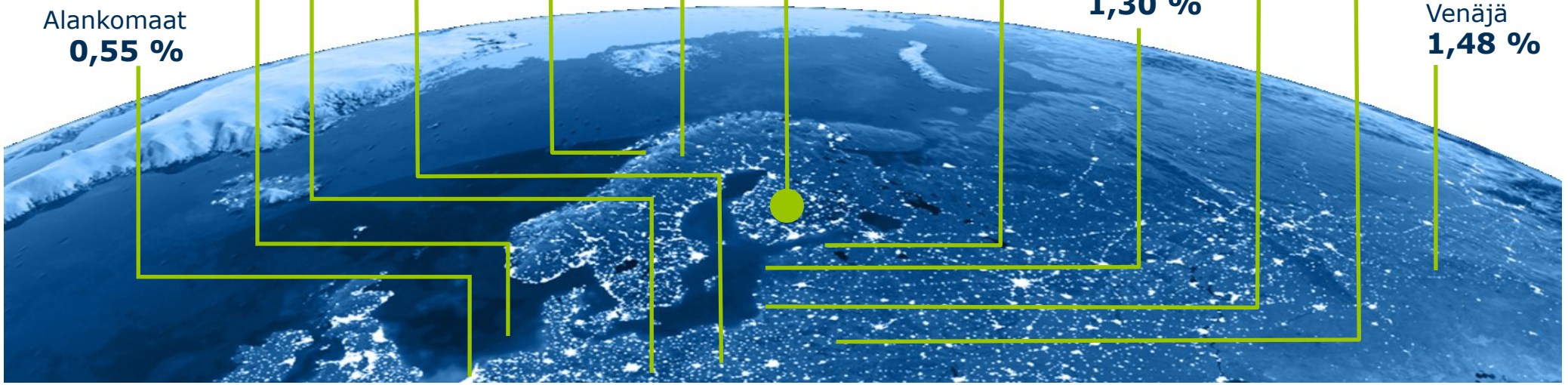
Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl

Suomi
0,29 %

2018
Havainnot
tammi-maaliskuu
19 604 kpl



Havaintojen määrä oli vuonna 2017 samalla tasolla vuoden 2016 kanssa.

Haittaohjelmat ja haavoittuvuudet

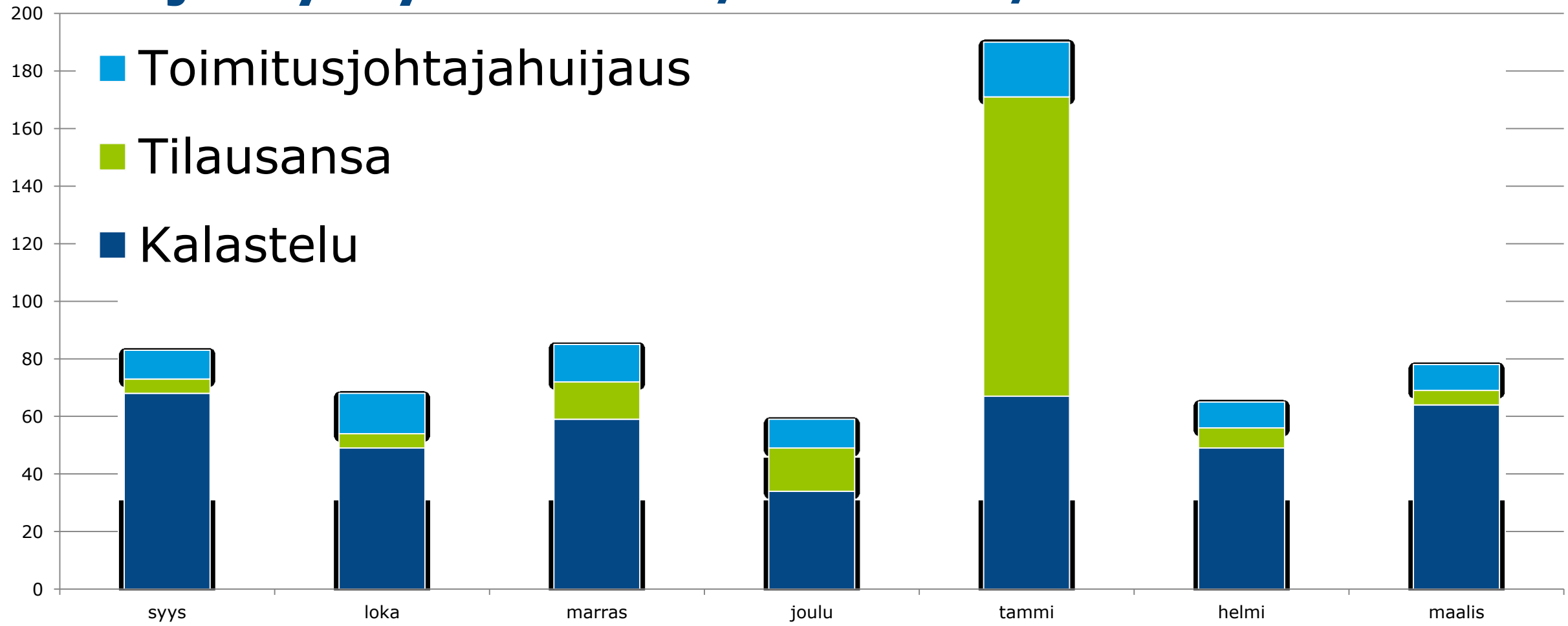
- Meltdown- ja Spectre-haavoittuvuuksien korjauspäivitysten ongelmat ovat jatkuneet
  - Windows 7:n tammikuussa julkaistussa Meltdown-haavoittuvuuden päivityksessä oli virheitä, jotka on korjattu Microsoftin maaliskuun päivityspaketissa
  - Intel tuo yhä uusia prosessoriperheitä päivitysten piiriin
- Drupal-sisällönhallintaohjelmiston versioissa 8, 7 ja 6 on havaittu haavoittuvuus, joka mahdollistaa hyökkääjän komentojen suorittamisen kohdejärjestelmässä ja sivuston täydellisen haltuunottamisen.
  - Haavoittuvuuksien korjaamiseksi järjestelmät on päivitettävä viipymättä.
- WannaMine-haittaohjelma tarttui Suomessa helmikuussa useiden organisaatioiden palvelimiin
  - Leviämistapa on liki identtinen NotPetyan kanssa.
  - WannaMinen pääasiallinen käyttötarkoitus on virtuaalivaluutan louhiminen, mutta varastaa myös käyttäjätunnuksia ja salasanoja.
- Rikolliset ovat siirtymässä levittämään virtuaalivaluuttoja louhivia haittaohjelmia kiristyshaittaohjelmien sijaan.

Huijaukset & kalastelut

Huijaukset maaliskuussa

- Sähköpostilla levitettiin PDF-dokumenttia, jonka avulla kalasteltiin mm. Dropbox-, Gmail- ja Office 365-tunnuksia.
  - Murrettujen sähköpostitilien kautta lähetettiin tuhansittain sähköposteja suomalaisille toimijoille eri organisaatioissa. Viestin sisältönä oli PDF-liite, joka tarjosi linkkiä kalastelusivulle.
  - Tietojenkalastelu toisinaan myös onnistuu. Sen seurauksena rikolliset saavat haltuunsa yritysten tai muiden organisaatioiden käytössä olevia oikeita sähköpostitilejä, joita voi käyttää monenlaiseen rikolliseen toimintaan.
- Tietoja yritetään kalastella tunnettujen pankkien nimissä.
  - Teemoina S-pankki, OP, Aktia, Nordea, Danske, Bank of America, ...
- Toimitusjohtajahuijauksia yhdistyksiin ja muihin organisaatioihin
  - Yritysten lisäksi kaikenlaiset yhdistykset, liitot, oppilaitokset, säätiöt, julkishallinnon laitokset ja muut organisaatiot ovat olleet laskutushuijareiden hampaissa. Organisaatioiden taloushenkilöille lähetetään tekaistuja laskuja.

Huijausyritykset 2017/09–2018/03



Vakoilu

Verkkovakoilutilanteessa ajankohtaista

SUPO:n vuosi 2017	Suojelupoliisin tietoon tuli vuonna 2017 useita tapauksia, joissa suomalaisyritykseen kohdistuneen kyberhyökkäyksen takana oli valtiollinen taho.
Hyökkäyksiä energia-yhtiöihin	Yhdysvallat syyttää Venäjää useista energia-alan yrityksiin kohdistuneista kyberhyökkäyksistä vuonna 2017
Yhdysvaltain asevoimien kyber-operaatio	Kaspersky paljasti vuosia kestäneen kyberoperaation, jonka uskotaan olevan Yhdysvaltain erikoisjoukkojen tekemä
9 iranilaista syytteeseen hyökkäyksistä	Yhdysvaltain oikeusministeriö syyttää 9 iranilaista erityisesti yliopistoihin kohdistuneista tietomurroista

Havainnointi- ja varoitusjärjestelmän (HAVARO) havainnot

Vuosi 2017

Vakavuus	Lukumäärä
Punainen	597
Keltainen	1 128
Vihreä	62 294
Yhteensä	**64 019**

Vuosi 2018
(tammi-maaliskuu)

Vakavuus	Lukumäärä
Punainen	225
Keltainen	830
Vihreä	4245
Yhteensä	**5300**

Massapostituksina levitetyt huijaukset ja tunnusten kalastelut näkyvät HAVARO:ssa vierailuina haitallisiksi tiedetyillä sivustoilla.

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

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

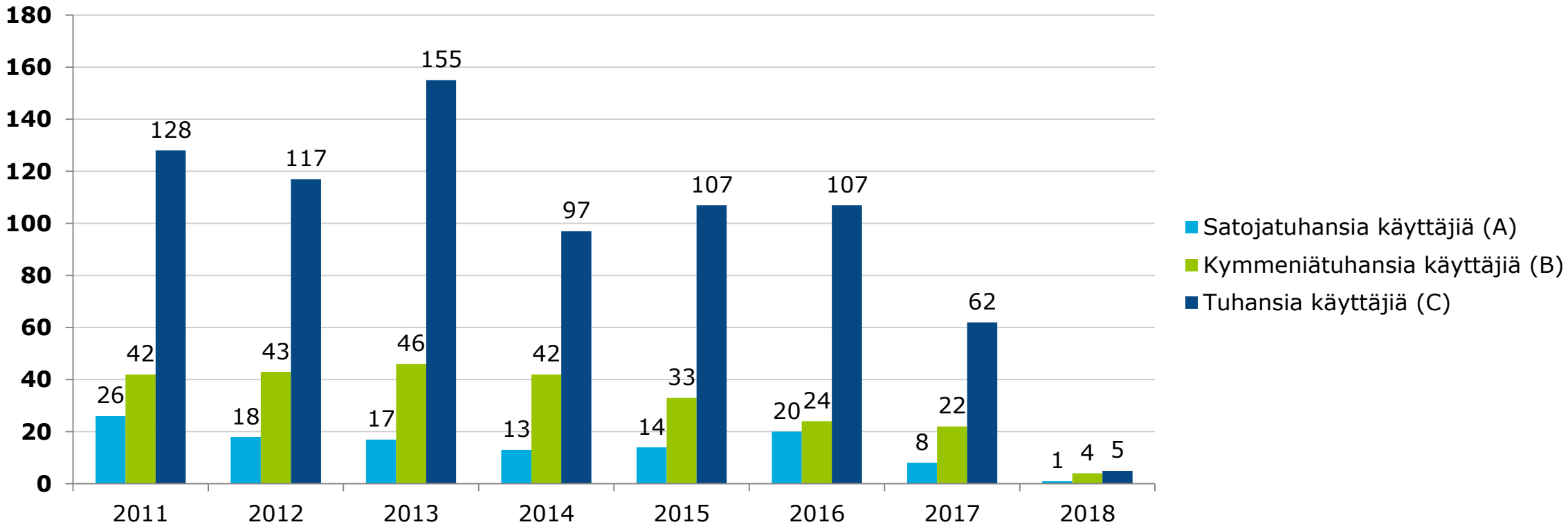
Vuosi 2018
(tammi-helmikuu)

Vakavuus	Lukumäärä
A-luokka	1
B-luokka	4
C-luokka	5
Kaikki häiriöt	**Ei tiedossa**

Ensimmäisen vuosineljänneksen tilasto kaikista häiriöistä valmistuu huhtikuun lopussa.

Vuoden alussa tykkylumen aiheuttamista sähkönjakelun häiriöistä johtuneista viestintäverkkojen häiriöistä selvittiin hyvällä viranomaisten ja yritysten yhteistyöllä.

Viestintäverkkojen toimivuus



Tässä tilastossa on esitetty ainoastaan A-, B- ja C-vakavuusluokkien toimivuushäiriöt. Niitä on vuosittain 100–200. Pienempiä häiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–350 000 vuodessa.

IoT

Esineiden internet (IoT) maaliskuun yhteenveto

- **Iso-Britannian Secure by Design -periaatteet**
  - https://www.gov.uk/government/publications/secure-by-design
  - Luonnos Iso-Britannian hallituksen linjauksiksi kuluttajille myytävien IoT-tuotteiden tietoturvan vähimmäistasosta.
  - Linjauksia on kritisoitu mm. siitä, ettei niistä tule heti velvoittavia.
- **Tietoturvayhtiö Dragosin vuosikatsaus automaatiojärjestelmien tietoturvaan**
  - https://www.dragos.com/yearinreview/2017/
  - Katsaus automaatiojärjestelmistä paljastuneisiin haavoittuvuuksiin
  - Katsaus uhkiin ja uhkatoimijoihin
  - Tarve siirtyä tietoturvapoikkeamiin reagoinnista hyökkääjien ennakointiin
- **Tekoäly ja internetiin kytkettyjen esineiden ennakoiva huolto**
  - https://www.tivi.fi/CIO/tekoaly-tuo-valtavat-saastot-koneet-huolletaan-jo-ennen-niiden-rikkoutumista-6706990
  - Ennakoivaa huoltoa on jo vuosia tehty kalliille laitteille, kuten kaivosteollisuuden koneille. Nyt esimerkiksi Hitatchi on tuonut markkinoille teollisen internetin alustatuotteen, jossa ennakoivan huollon koneoppimiseen on valmiita työkaluja.

Tietoturva-alan kehitys

Ajankohtaiset lakiasiat

- NIS-direktiivin täytäntöönpanon valmistelu jatkuu kotimaassa ja EU:ssa
  - HE 192/2017 vp laeiksi Euroopan Unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta on käsiteltävänä eduskunnassa
  - EU:n komissio antoi 30.1.18 täytäntöönpanoasetuksen (EU) 2018/151 digitaalisten palveluiden turvallisuuden riskihallinnasta ja poikkeamien merkittävyyden arvioinnista. Asetusta sovelletaan pilvipalveluihin, verkon markkinapaikkoihin ja hakukoneisiin 10.5.2018 alkaen.
  - Jäsenvaltioiden yhteistyötä kehitetään muun muassa CSIRT-verkostossa
- Viestintävirasto valmistelee siirtymäaikataulun jatkamista TUPAS-tunnistuksen muutoksille
  - Tunnistukseen on lisättävä sanomatason salaus
  - Tämä tehdään muuttamalla kevään aikana määräystä 72/2016
  - Valmisteluun toivotaan erityisesti sähköisten asiointipalveluiden osallistumista, koska muutokset vaikuttavat niihin
  - Lisätietoja hankkeesta ja osallistumisesta: https://www.viestintavirasto.fi/ohjausjavalvonta/lausuntopyynnottiedoksiannotkyselyt/lausuntopyynnot/viestintavirastonkommenttipyyntokutsujamuistiotunnistusmaarayksen72tupas-muutoksesta.html

Ajankohtaiset lakiasiat

- Hallitus on esittänyt uuden tietosuojalain säätämistä henkilötietojen käsittelyä koskevaksi yleislaiksi (http://oikeusministerio.fi/artikkeli/-/asset_publisher/tietosuojalaki-taydentaisi-eu-n-tietosuoja-asetusta)
  - Tietosuojalaki täydentäisi EU:n yleistä tietosuoja-asetusta (GDPR)
- Tiedustelulakipakettia koskevat hallituksen esitykset ovat valiokuntakäsittelyssä (HE 198/2017 vp, HE 202/2017 vp ja HE 203/2017 vp)
- Mm. rajavartiolain ja ulkomaalaislain muuttamista koskeva hallituksen esitys on valiokuntakäsittelyssä (HE 201/2017, http://intermin.fi/hybridiuhat)
  - Säädettäisiin mm. valtuuksista puuttua miehittämättömiin ilma-aluksiin ja lennokkeihin
- Puolustusministeriön työryhmämietintö miehittämättömän ilmailun lainsäädännön kehittämisestä turvallisuuden näkökulmasta ollut lausuttavana 31.1.2018 asti
  - https://www.defmin.fi/ajankohtaista/tiedotteet/2017/puolustusministerion_tyoryhmamietinto_miehittamattoman_ilmailun_lainsaadannon_kehittamisesta_turvallisuuden_nakokulmasta_valmistui.8915.news

Kyberasioihin liittyvää uutisointia maailmalta

MyFitnessPal-palvelun käyttäjätietoja vuotanut tietomurron yhteydessä. MyFitnessPal on joutunut tietomurron kohteeksi. Noin 150 miljoonan käyttäjän käyttäjätunnuksia, sähköpostiosoitteita ja salasanatiivisteitä on päätynyt ulkopuolisten haltuun.

Kyberturvallisuus on keskeinen osa suomalaisen yhteiskunnan turvallisuutta ja kilpailukykyä. Teknologisen kehityksen ja digitalisoitumisen syvenemisen myötä kyberturvallisuuden merkitys kasvaa ja kyberturvallisuuden strateginen johtaminen korostuu todetaan Jyväskylän yliopiston ja Aalto-yliopiston tutkijoiden laatimassa raportissa.

Yhdysvallat syyttää yhdeksää iranilaista tietomurroista ja tietovarkauksista satoihin yliopistoihin kymmenissä maissa, myös Suomessa.

Valtionvarainministeriö on käynnistänyt mobiilin viranomaisverkkoratkaisun (MoVi) kehitystyön.
Työn tarkoituksena on toteuttaa seuraavan sukupolven viranomaisten viestintäratkaisu Virve 2.0 vuoteen 2025 mennessä.

Viestintävirasto
Kyberturvallisuuskeskus

cert@ficora.fi

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi