#kybersää 10/2018

#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. Syyskuussa yleistyivät turvapostilta näyttävät kalasteluviestit.
- 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 10/2018

Palvelunestot

- Kyberturvallisuuskeskukselle ei ole raportoitu merkittäviä palvelunestohyökkäyksiä.

Haittaohjelmat & haavoittuvuudet

- Useiden käyttöjärjestelmien verkkototeutuksista on löydetty kriittisiä haavoittuvuuksia.
- Magecart-hyökkäystä käytetään edelleen asiakas- ja luottokorttitietojen varastamiseen verkkokaupoista.

Huijaukset & kalastelut

- Suomalaisia hätyyteltiin suomenkielisellä pornokiristyshuijauksella.
- Office 365 -tietojenkalastelun varoitus laskettiin kriittisestä vakavaksi.

Vakoilu

- Venäjää syytetään useista kyberoperaatioista.
- Slovakian ulkoministeriö hyökkäyksen kohteena.
- Iso-Britanniaa syytetään vuonna 2013 julkisuuteen tulleesta tunkeutumisesta belgialaisoperaattorin järjestelmiin.

Verkkojen toimivuus

- Vakavimman luokan häiriöitä ollut enemmän kuin viime vuonna.
- Merkittävien häiriöiden kokonaismäärä laskussa.

IoT

- MikroTikin reitittimissä useita haavoittuvuuksia.
- Miljoonissa Xiongmain videovalvontalaitteissa haavoittuvuuksia, joiden seurauksena valvontakuvaa voi seurata pilvipalvelun kautta.
- Chalubo-botnet havaittu IoT-laitteisiin kohdistuvana uhkana.

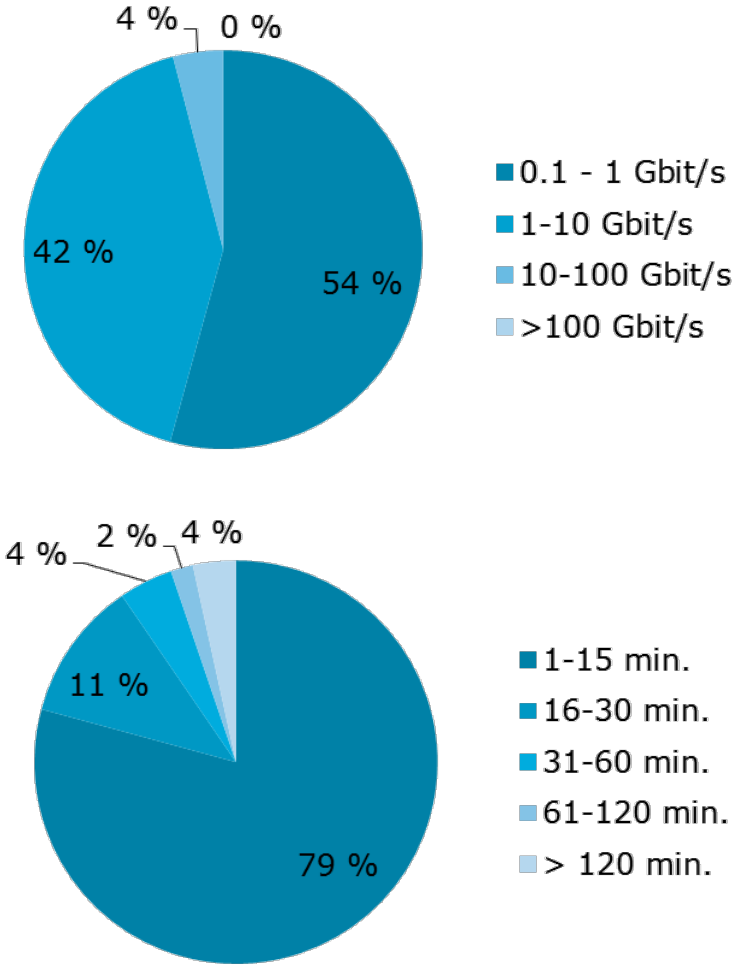
Palvelunestot

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

- **Palvelunestohyökkäykset ovat vaikuttaneet suomalaisiin kiinteistöautomaatiolaitteisiin**
  - Laitteita on luultavasti hyödynnetty hyökkäyksessä muita kohteita vastaan, mutta niille aiheutunut kuorma on häirinnyt automaatiolaitteiden toimintaa.
- **Valtionhallinnon palveluja vastaan ei ole lokakuussa tehty vakavia palvelunestohyökkäyksiä, jotka olisivat estäneet palveluiden käyttöä**
  - Oikeusministeriön ylläpitämässä Otakantaa.fi-verkkosivustossa olleeseen kesä- ja talviaikaa koskeneen kyselyyn annettiin runsaasti automaattisesti tehdyiksi tunnistettuja vastauksia. Automaattivaikuttamisen yritys ei vaarantanut kyselyn tuloksia.
- **Palvelunestohyökkäyksiä on 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.
  - Silti myös perinteiset amplifikaatiohyökkäykset ovat yhä yleisiä. Viime aikoina on näkynyt erityisen paljon memcached- ja DNS-amplifikaatiotekniikoilla toteutettuja hyökkäyksiä.

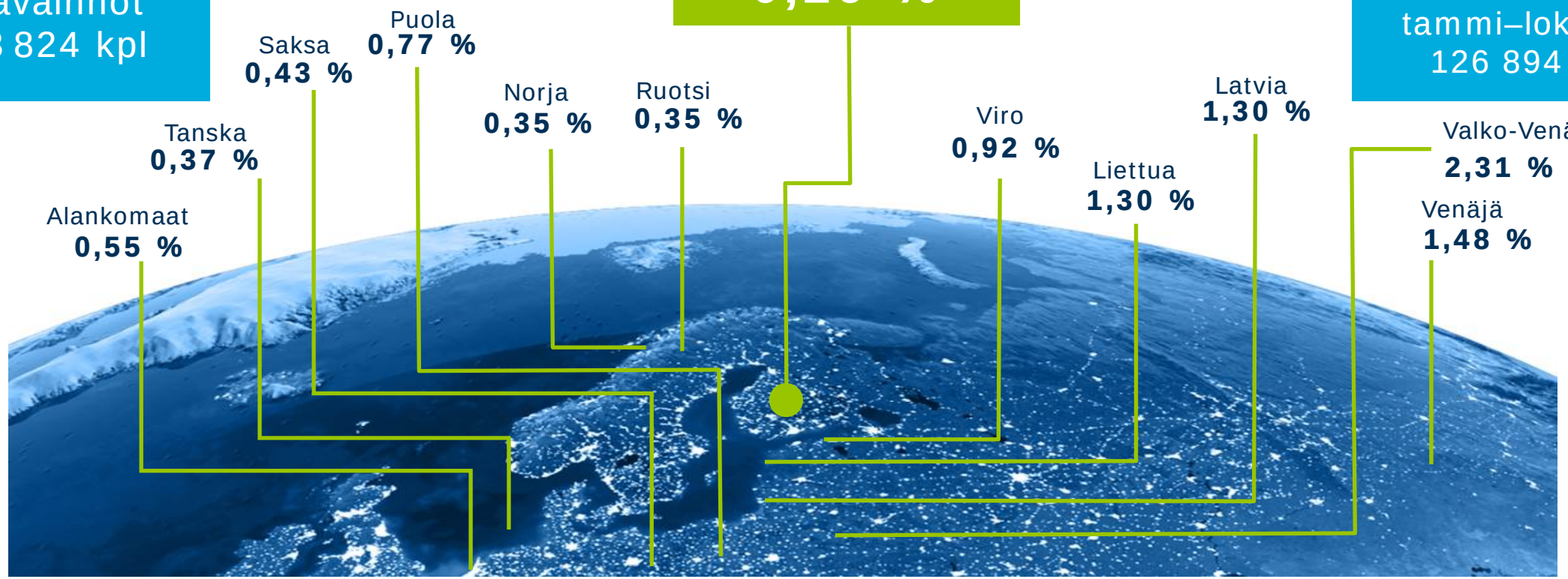
Haittaohjelmat & haavoittuvuudet

Tietoturvapoikkeamat suomalaisissa verkoissa

2017
Havainnot
93 824 kpl

Suomi
0,29 %

2018
Havainnot
tammi–lokakuu
126 894 kpl



Vuoden 2018 toukokuusta alkaen tietoturvapoikkeamahavaintojen määrä on kasvanut pienreitittimien haittaohjelmatartuntojen vuoksi

Haittaohjelmat

- **Ulkomailla Kovter- ja Emotet-haittaohjelmien havainnot ovat olleet kasvussa, ja tämä trendi näkyy myös Suomessa**
  - Kyberturvallisuuskeskuksen tiedossa ei ole erityisesti Suomeen kohdistunutta levityskampanjaa, vaan sivuosumia yleisesti levitettävistä haittaohjelmista.
- **Suomalaisten kotireitittimien haittaohjelmahavaintoja on selvitetty yhteistyössä tiettyjen teleyritysten kanssa**
  - Havainnot liittyvät muutaman teleyrityksen tiettyihin reititinmalleihin.
- **Ulkomaisia Magento-verkkokauppa-alustoja on edelleen murrettu, ja ne on laitettu varastamaan asiakas- ja luottokorttitietoja**
  - Tässä nk. Magecart-hyökkäyksessä verkkokauppaan asetetaan haitallinen ohjelmakoodi, joka oston yhteydessä siirtää asiakas- ja maksukorttitiedot kaupan lisäksi myös verkkorikollisille.
  - Erään tietoturvatutkijan mukaan n. 7 000 Magento-alustaa käyttävää verkkokauppaa on murrettu viimeisen 6 kuukauden aikana. Julkisuuteen ovat tulleet mm. Ticketmaster, British Airways ja Newegg.

Haavoittuvuudet

- **Applen macOS- ja iOS-käyttöjärjestelmän verkkototeutuksesta on korjattu haavoittuvuus, joka mahdollistaa laitteen kaatamisen tai komentojen suorittamisen kohdelaitteessa**
- **Useissa IoT-laitteissa käytetyn FreeRTOS-käyttöjärjestelmän verkkototeutuksesta on löydetty haavoittuvuuksia, joiden avulla voi muun muassa suorittaa ohjelmakoodia laitteessa**

- **Intelin suorittimien HyperThreading-rinnakkaissuorituksesta on löytynyt uusi haavoittuvuus, jonka avulla on mahdollista saada tietoja samalla suorittimella ajettavasta toisesta sovelluksesta**
  - » Haavoittuvuutta hyväksikäyttämällä voi saada esille esimerkiksi salausavaimia.
  - » Käytännössä uhka on vakavin yhteiskäyttöisille alustoille, kuten pilvipalveluille ja muille yhteiskäyttöisille alustoille.
  - » Haavoittuvuuden löysi Tampereen yliopiston tutkimusryhmä yhteistyössä Havannan yliopiston kanssa. Haavoittuvuus on saanut nimen Port Smash.

- **Useiden valmistajien SSD-kiintolevyjen tarjoamat salausratkaisut eivät ole luvatun vahvuisia**
  - » Tämä vaikuttaa myös oletusasetuksin käyttöönotettuun Windowsin BitLocker-salaukseen, joka luottaa kiintolevyn tarjoamaan salaukseen.

Tietomurrot ja tietovuodot

- **Facebookilta on viety noin 50 miljoonaa käyttäjätietoa syyskuussa**
  - » Tietomurrossa hyödynnettiin haavoittuvuutta Facebookin ominaisuudessa, jolla voi katsoa omaa profiilia toisen käyttäjän oikeuksin.
- **Bloombergin uutisoinnin mukaan kiinalaiset valmistajat ovat lisänneet SuperMicron emolevyihin ylimääräisiä komponentteja, joita voi käyttää vakoiluun**
  - » Amazon, Apple ja SuperMicro ovat jyrkästi kiistäneet nämä väitteet.
- **Cathay Pacific -lentoyhtiö paljasti tietovuodon, jossa 9,4 miljoonan asiakkaan tietoihin on päästy käsiksi maaliskuussa**

Huijaukset & kalastelut

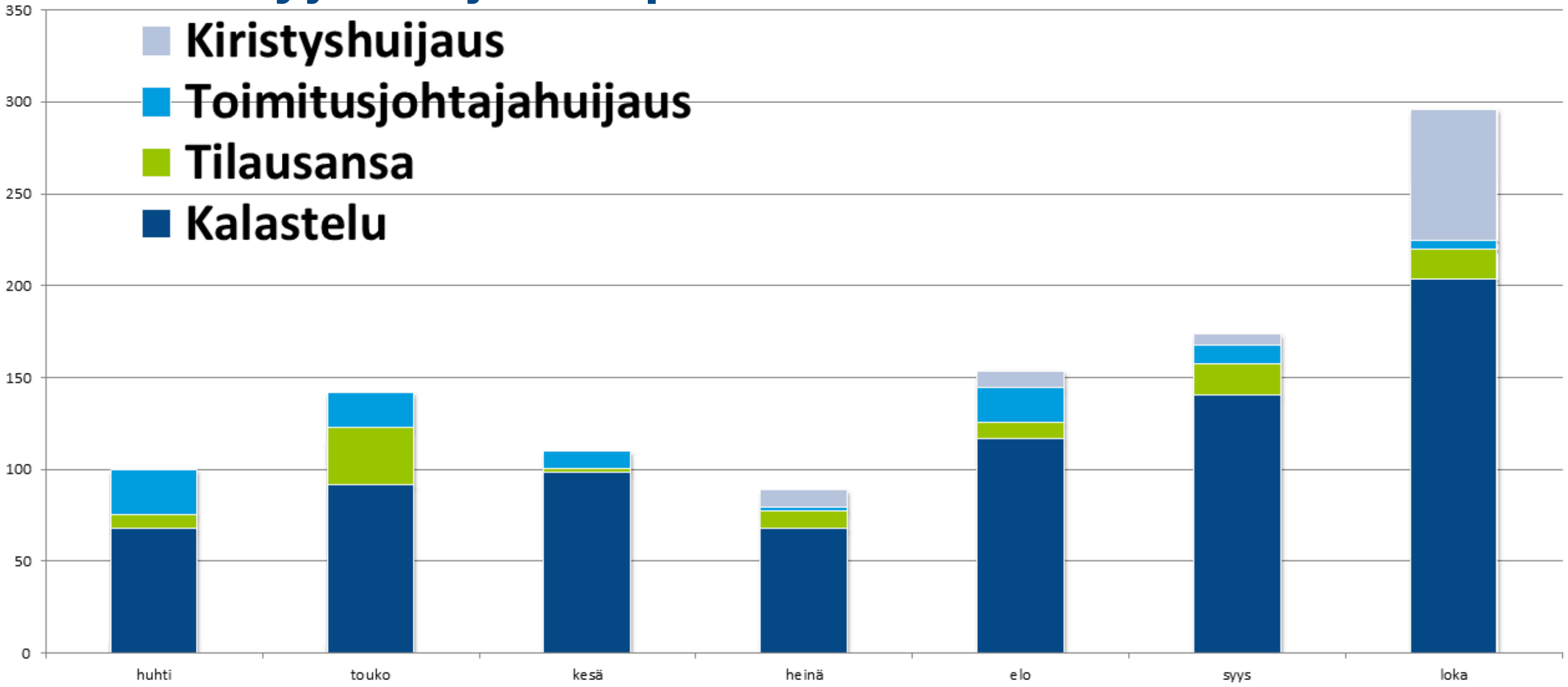
Huijaukset lokakuussa

- **Pornokiristyskampanja säikytteli suomalaisia**
  - Läpi kesän jatkunut kiristyshuijauskampanja alkoi lokakuussa suomenkieliseksi konekäännettynä.
  - Uusimmat kiristysviestit on väärennetty näyttämään siltä, että ne on lähetetty vastaanottajan omasta osoitteesta. Uhria säikytellään sillä, että kiristäjä olisi muka saanut uhrin sähköpostitilin haltuunsa ja voi lähettää siltä sähköpostia.
  - Liikkeellä oli eri versioita samasta huijausteemasta: kieliversioita, salasanavuotoja hyödyntäviä ja muita kiristysuhkailuja.

- **Office 365 -tunnusten kalastelu jatkuu**
  - Suomalaisten yritysten sähköpostitileille on murtauduttu kalastelluilla tunnuksilla.
  - Kalasteluun käytetään myös organisaatioiden omia turvapostiviestejä sekä sellaiseksi naamioituja väärennettyjä turvaposti-ilmoituksia.
  - Sähköposteja vakoillaan, ja niistä saatuja tietoja käytetään huijauksiin ja vakoiluun.
  - KTK:n varoitus tunnusten kalastelusta laskettiin lokakuussa jälleen punaisesta keltaiseksi.

- **Tekstiviestihuijaukset johtavat tilausansaan**
  - Finnkinon nimissä lähetetyissä tekstiviesteissä oli linkki, jonka takaa paljastui tilausansa.
  - Perinteisten sähköpostihuijausten lisäksi tekstiviestejä käytetään yhä enemmän huijausviesteihin.
- **Tietoja yritetään kalastella tunnettujen pankkien ja tuotemerkkien nimissä**
  - Apple ID -tunnusten kalastelu lisääntyi elo–syyskuussa. Myös pankkien ja Netflixin nimissä kalasteltiin maksukorttitietoja.
  - Tilausansoihin houkuteltiin kuluttajia paljon mm. Prisman, Gigantin, Finnkinon ja Shellin tuotenimillä.

Käsiteltyjä huijaustapauksia 2018/04–10



Vakoilu

Verkkovakoilutilanteessa ajankohtaista

Kiinalaisia syytteeseen tietomurroista	Yhdysvallat syyttää kiinalaisia tiedustelu-upseereja ja hakkereita suihkumoottoritietoihin kohdistuneesta teollisuusvakoilusta.
Slovakian ulkoministeriö hyökkäyksen kohteena	Slovakia on kertonut tutkivansa ulkomininisteriöönsä kohdistunutta kyberhyökkäystä.
Useat länsimaat syyttävät Venäjää kyber-operaatioista	Useat länsimaat syyttävät Venäjää kyberoperaatioista. Esimerkiksi Hollannin mukaan venäläiset yrittivät murtautua myrkkyiskua tutkineen järjestön järjestelmiin.
Iso-Britannia belgialais-operaattorin vakoilun takana	Belgialaislehden mukaan Belgia on löytänyt todisteita vuonna 2013 uutisoidusta Iso-Britannian tiedustelu- ja turvallisuuspalvelun tunkeutumisesta belgialaisoperaattorin järjestelmiin.

Verkkojen toimivuus

Viestintäverkkojen toimivuus

Vuosi 2017

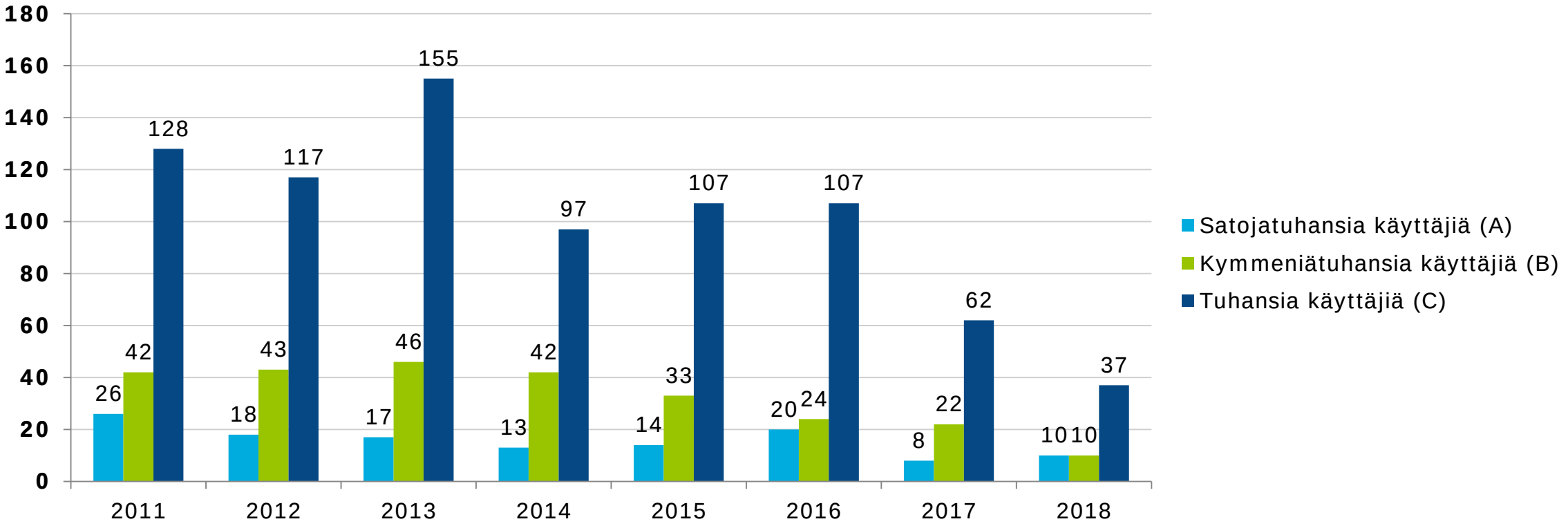
Vakavuus	Lukumäärä
A-luokka	8
B-luokka	22
C-luokka	62
Kaikki häiriöt	**460 075**

Vuosi 2018
(tammi–lokakuu)

Vakavuus	Lukumäärä
A-luokka	10
B-luokka	10
C-luokka	37
Kaikki häiriöt (Q1–Q2)	**208 238**

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), lokakuun yhteenveto

- **MikroTikin reitittimissä on useita haavoittuvuuksia**
  - » Vakavin haavoittuvuus mahdollistaa mielivaltaisen ohjelmakoodin suorittaminen tunnistetun käyttäjän käynnistämänä.
  - » Hyökkääjä hyötyy siitä, että usein reititinten ylläpitäjät jättävät vaihtamatta laitteiden oletusarvoisten käyttäjätilien oletusarvoiset salasanat. Lista auttaa IoT-tuotteiden tekijöitä välttämään tyypillisiä virheitä.
  - » Erityisesti pienet internetpalveluntarjoajat suosivat MikroTikin tuotteita.

- **Miljoonissa Xiongmain videovalvontalaitteissa on haavoittuvuuksia, joiden seurauksena kameroiden kuvaa voi seurata pilvipalvelun kautta**
  - » Moni käyttäjä ei vaihda ylläpitäjän salasanaa oletusarvostaan (tyhjä); laitteissa on dokumentoimaton käyttäjätunnus, jolla on kiinteä salasana.
  - » Valvontakameran omistajan on vaikea tietää onko hänen kameransa Xiongmain valmistama, sillä kameroita ei koskaan myydä Xiongmain nimellä.

- **Chalubo-bottiverkko uhkaa IoT-laitteiden turvallisuutta**
  - » Bottiverkkoja käytetään erityisesti palvelunestohyökkäyksiin.
  - » Botin ohjelmakoodiin on lainattu Mirain ja Xor.DDoS-haittaohjelmaperheiden lähdekoodia.
  - » Lisäksi siinä käytetään haittaohjelman tutkimista haittaavia tekniikoita.

Tietoturva-alan kehitys

Ajankohtaiset oikeudelliset asiat: EU

- **EU:n televiestintäuudistus ("EECC-direktiivi")**
  - » Parlamentti on 14.11. hyväksynyt säännöksen. Joulukuussa asia on tarkoitus hyväksyä ministerineuvostossa sekä julkaista EU:n virallisessa lehdessä.
  - » Voimaantulosta alkaa pääsääntöisesti 2 vuoden täytäntöönpanoaika.
  - » Muutokset tehdään pääasiassa sähköisen viestinnän palveluista annettuun lakiin (917/2014). Samalla on tarkoitus arvioida lain muut muutostarpeet ja tehdä sille kokonaisuudistus. LVM tulee käynnistämään säädöshankkeen, jossa kuullaan laaja-alaisesti toimialaa.
- **"Kyberturvallisuusasetus"**
  - » Asetus käsittäisi säännökset EU:n laajuisesta ICT-tuotteiden tietoturvasertifioinnin puitekehyksestä sekä EU:n verkko- ja tietoturvavirasto ENISA:n pysyvästä mandaatista.
  - » Komissio antoi asetusehdotuksensa syksyllä 2017; nyt käynnissä ovat parlamentin, neuvoston ja komission väliset trilogi-neuvottelut asetuksen sisällöstä, ja tavoitteena on asetuksen hyväksyminen keväällä 2019.
- **Sähköisen viestinnän tietosuoja-asetus ("ePrivacy")**
  - » Säädös liittyy tiiviisti jo sovellettavaan EU:n yleiseen tietosuoja-asetukseen (GDPR).
  - » Asetuksen valmistelu etenee hitaasti; jäsenvaltioilla on hyvin erilaisia näkemyksiä mm. evästeiden käsittelyn oikeudellisesta perusteesta (8 artikla) → edellyttääkö rekisteröidyn suostumusta vai ei?

Ajankohtaiset oikeudelliset asiat: kotimaa

- **Eduskunnassa:**
  - » Tiedustelulakipakettia koskevat esitykset
    - Täysistunto on hyväksynyt esityksen perustuslain 10 §:n muuttamisesta (HE 198/2017) kiireellisenä sekä itse ehdotuksen. Perustuslain muutos (817/2018) **tuli voimaan 15.10.2018**.
    - Muiden kokonaisuuteen kuuluvien esitysten valiokuntakäsittely on kesken: tiedustelutoiminnan valvonta (HE 199/2017), siviilitiedustelu (HE 202/2017) ja sotilastiedustelu (HE 203/2017)
  - » EU:n yleistä tietosuoja-asetusta täydentävää lainsäädäntöä koskeva esitys (HE 9/2018)
    - Eduskunta hyväksyi lakiehdotukset osittain muutettuna 13.11.2018.
  - » Esitys laiksi Liikenne- ja viestintäviraston perustamisesta ym. (HE 61/2018 ja 104/2018)
    - Eduskunta hyväksyi lakiehdotukset osittain muutettuna 23.10., ja niiden on tarkoitus tulla voimaan 1.1.2019. → https://www.lvm.fi/-/eduskunta-hyvaksyi-liikenne-ja-viestintaministerion-hallinnonalan-uudistuksen-986542
- **Lausuttavana ollut muun muassa:**
  - Luonnos hallituksen esitykseksi: Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttaminen*
  - Luonnos valtioneuvoston selonteoksi "Eettistä tietopolitiikkaa tekoälyn aikakaudella"*
  - Valtioneuvoston paikkatietopoliittinen selonteko VNS 2/2018 → https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/VNS_2+2018.aspx
  - Luonnos hallituksen esitykseksi laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi ("tiedonhallintalaki")*

* → ks. lausuntopalvelu.fi (suljetut)

Kyberasioihin liittyvää uutisointia maailmalta

Kiinan kautta kiertävä verkkoliikenne on herättänyt huolta monin paikoin. Tutkijat ovat jäljittäneet sarjan verkkoliikenteen uudelleenohjauksia, joissa esimerkiksi liikennettä Japanista Skandinaviaan on reititetty koukkaamaan kiinalaisten palvelimien kautta kuuden kuukauden ajan. Toiminta vaikuttaa tarkoitukselliselta tietoliikenteen kaappaamiselta ja voi vaarantaa salatun liikenteen luottamuksellisuutta.

Suomalaisyritys joutui kyberhuijauksen uhriksi – pankki esti suuremmat tappiot. Kyberrikolliset onnistuivat huijaamaan monialakonserni Algolilta 140 000 dollaria, kunnes pankki sulki rahahanat. Huijaus on vain yksi julkituotu esimerkki jatkuvista moninaisista huijausyrityksistä tietoverkoissa.

EU haluaa oikeuden määrätä pakotteita jäsenvaltioihinsa kohdistuneista kyberhyökkäyksistä. Uuden käytännön on tarkoitus astua voimaan ennen nykyisen EU-parlamentin kauden päättymistä tulevana keväänä. EU-komissio toivoo valmiita suunnitelmia joulukuuhun mennessä. Aloitteella on laaja tuki myös Suomelta.

Ilmainen verkkokurssi tietoturvasta käynnistyi jälleen. Helsingin Yliopiston ja F-Securen yhteistyönä tuottama, suuren suosion saanut **Cyber Security Base** -tietoturvakurssi käynnistyi jo kolmatta kertaa. Kurssin voi suorittaa verkossa kokonaan tai valita siitä haluamiansa osia.

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi