TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybersää

Marraskuu 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 marraskuu 2019

Verkkojen toimivuus

- Telian matkapuhelinverkossa laaja häiriö 22.11. esti osan hätäpuheluista.
- Palvelunestohyökkäysten näkökulmasta rauhallinen marraskuu.

Vakoilu

- Suojelupoliisin mukaan ulkomaisten tiedustelupalveluiden kiinnostus Suomen kriittiseen infrastruktuuriin ja strategisiin investointeihin on lisääntynyt.

Haittaohjelmat ja haavoittuvuudet

- SSD-levyjen laiteohjelmistoissa olevien ohjelmointivirheiden vuoksi tietoja on menetetty.

Tietomurrot ja -vuodot

- Monivaiheinen tunnistautuminen ehkäisisi suurimman osan Office 365 -tietomurroista.
- Marraskuussa tuli ilmi suuri, noin 1,2 miljardia tietuetta sisältänyt tietovuoto.

Huijaukset ja kalastelut

- Black Friday –aiheiset huijaukset jäivät yrityksiksi.
- Joulun läheisyys alkaa näkyä: huijarin osoitteeksi on väärennetty "Real Santa".

IoT ja automaatio

- Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa. **Tietoturvamerkki** auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja.

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

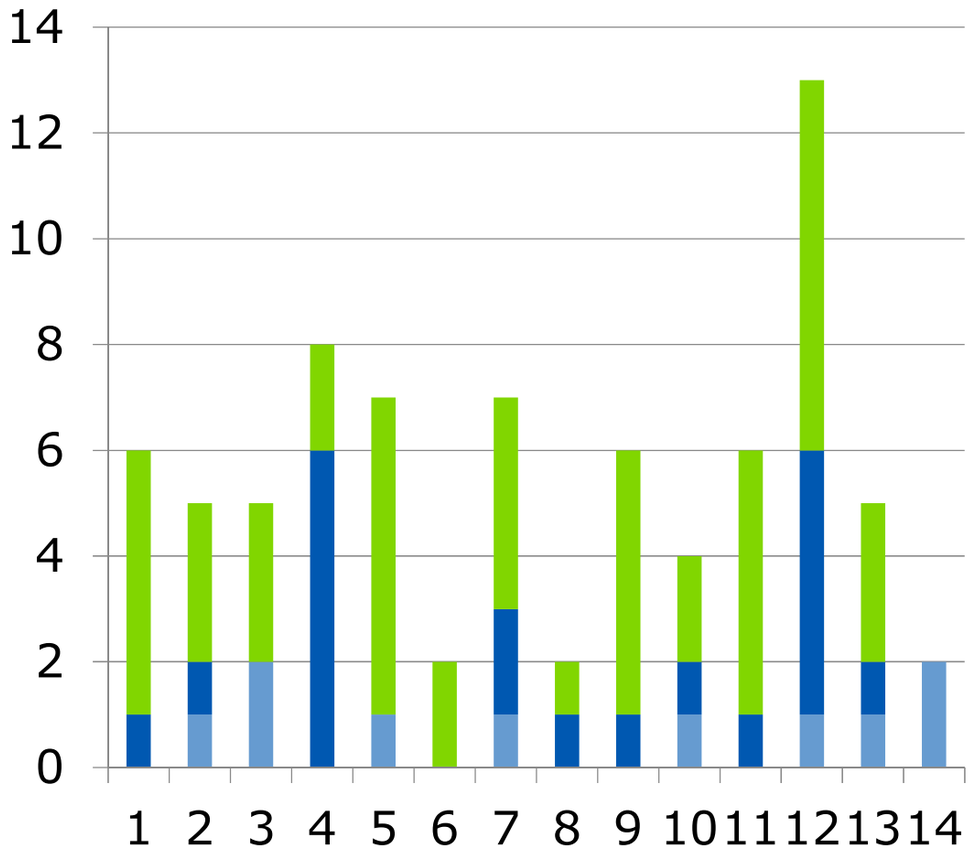
Verkkojen toimivuus

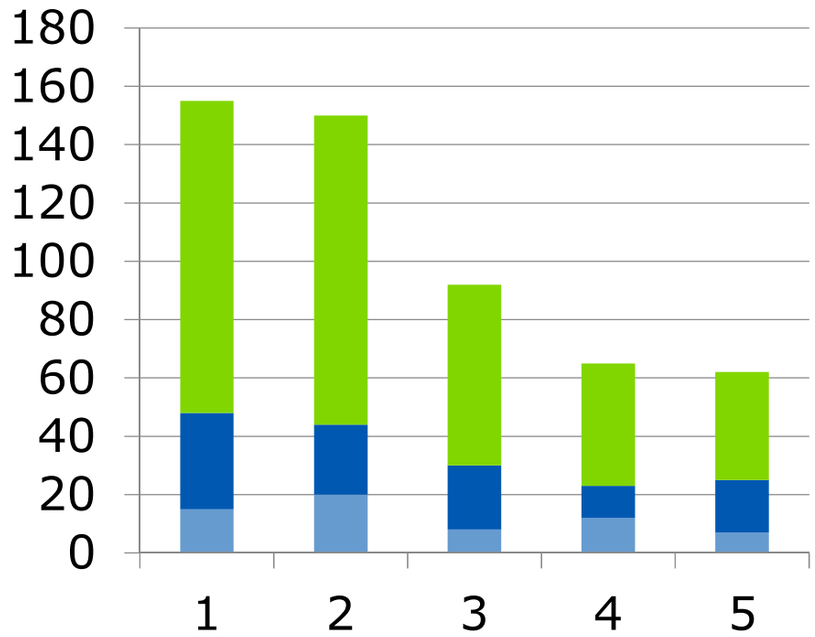
- Kaksi merkittävää toimivuushäiriötä:
  - 22.11. Telian matkaviestintäpalveluissa valtakunnallinen vika
    - Osa puheluista, internetyhteyksistä ja tekstiviestien toimittamisesta epäonnistui.
    - Hätäpuheluiden soittamisessa Telian verkosta oli ongelmia. Hätäkeskuslaitos julkaisi vaaratiedotteen.
    - Jos hätäpuhelu ei onnistu normaalisti soittamalla, käynnistä puhelin uudestaan ja soita hätäpuhelu ennen PIN:n syöttämistä: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/nain-soitat-hatapuhelun-verkon-hairiotilanteessa
  - 12.11. tietyt maksulliset TV-kanavat eivät näkyneet Digitan antenni-TV-verkossa.
- Tampereen kaupungin tietoverkoissa huomattavia häiriöitä 6. ja 11.11.

Verkkojen toimivuus

- Palvelunestohyökkäyksissä tilanne on ollut kohtuullisen rauhallinen
  - Vain muutama ilmoitus vähemmän merkittävistä tapauksista.
- Tietoturvayhtiö Kasperskyltä päivitetty palvelunestohyökkäysraportti
  - Sen mukaan 97.75 % hyökkäyksissä käytetyistä bottiverkoista toimii Linux-pohjaisissa järjestelmissä.
  - Arviomme mukaan suuri osa näistä laitteista on erilaisia IoT-laitteita ja muita kodin verkkolaitteita.
  - Kuluttajien tulisi kiinnittää huomiota internetiin kytkettävien laitteiden tietoturvaan jo laitetta valitessa.

Merkittävien toimivuushäiriöiden määrä





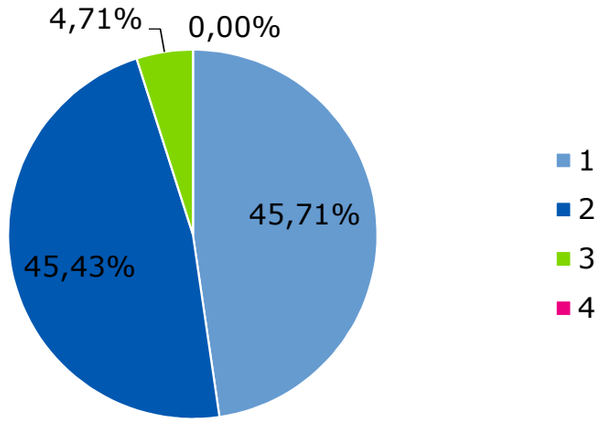
Tässä tilastossa on esitetty ainoastaan yleisten viestintäpalveluiden merkittävät toimivuushäiriöt. Niitä on vuosittain 70–200 ja määrä on laskenut useiden vuosien ajan. Pieniä toimivuushäiriöitä teleyritykset korjaavat satoja päivittäin. Kaikkien häiriötilanteiden määrä on 200 000–450 000 kappaletta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

Palvelunestohyökkäykset ja niillä uhkailu

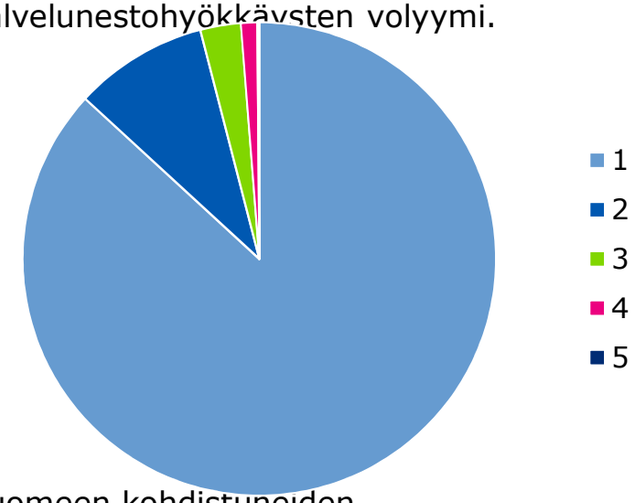
- Lyhyet alle 15 minuutin hyökkäykset ovat yleisimpiä (87 %). Kappalemääräisesti niitä nähdään tuhansia vuodessa.
- Noin puolet havainnoiduista yli 100Mbit/s hyökkäyksistä on volyymiltään 1-10 Gbit/s. Organisaatioiden kannattaakin varautua vähintään tämän volyymin hyökkäyksiin riskiarviossaan.
- Yli 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

Vakoilutilanteessa ajankohtaista

Suomen kriittinen infrastruktuuri tiedustelupalvelujen kiinnostuksen kohteena

Suojelupoliisi varoittaa, että ulkomaisten tiedustelupalveluiden kiinnostus Suomen kriittistä infrastruktuuria ja strategisia investointeja kohtaan on lisääntynyt. Erityisesti Suomi kiinnostaa Kiinan ja Venäjän tiedustelupalveluita.

Kiinalaisryhmä havittelee poliittisten vaikuttajien tekstiviestejä

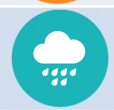
Tietoturvayhtiö FireEye kertoo kiinalaisryhmän pyrkineen vakoilemaan valikoitujen, geopoliittisiin intresseihin liittyvien henkilöiden tekstiviestejä ja liittymä- ja puhelutietoja. Kohteena olivat muun muassa toisinajattelijat, toimittajat ja korkea-arvoiset diplomaatit.

Pahamaineinen iranilaisryhmä teollisuusautomaatio-toimittajien kimpussa

Microsoft on havainnut Iraniin liitetyn APT33-ryhmän yrittäneen saada haltuunsa teollisuusautomaatiovalmistajien ja -toimittajien työntekijöiden kirjautumistietoja. Toiminnan motiivista ei ole tietoa, mutta ryhmän on aiemmin arveltu kehittäneen kybervakoiluun ja tuhoaviin kyberiskuihin liittyviä kyvykkyyksiään.

Haittaohjelmat ja haavoittuvuudet

Haittaohjelmahavaintomme

Haittaohjelmatyyppi	Tilanne	
IoT-haittaohjelmat	QSnatch-haittaohjelma muodostaa edelleen merkittävän osan Suomessa tehdyistä havainnoista. Monia laitteita ei ole puhdistettu tai saatu puhdistettua.	
Kiristyshaittaohjelmat	Kiristyshaittaohjelmissa tilanne Suomessa rauhallinen.	
Etähallittavat haittaohjelmat (RAT)	Etähallittavia haittaohjelmia yritetään levittää edelleen sähköpostin avulla, mutta tilanne rauhallisempi kuin lokakuussa.	
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

- Haittaohjelmia jaetaan sähköpostin välityksellä tavalliseen tapaan
  - Haittaohjelman sisältävä tiedosto näyttää usein laskuliitteeltä, saapumisilmoitukselta tai muulta viattomalta dokumentilta.
  - Kyberrikoksia tehtaileva ryhmä TA505 on lähettänyt suomalaisiin yrityksiin haitallisia lyhytlinkkejä sisältäviä sähköposteja. Linkin klikkaaminen johtaa haitallisen tiedoston lataukseen – useimmiten jonkin Office-tiedoston.
- Kansainvälisesti on havaittu paljon kiristyshaittaohjelmahyökkäyksiä
  - Julkisuudessa hyökkäyksestä kertoneita uhreja ovat olleet muun muassa Everis ja espanjalainen mediayhtymä sekä Yhdysvalloissa Louisianan osavaltion hallinto.

Haavoittuvuudet

- Kriittisiä ohjelmointivirheitä korjattu HPE:n SSD-levyjen laiteohjelmistoista (Haavoittuvuus 21/2019)
  - Vikasietoisuudestaan (RAID) huolimatta, levyjärjestelmissä olleiden ongelmien vuoksi tietoja on menetetty.
  - Päivittämätön levy muuttuu tietyn ajan kuluttua käyttökelvottomaksi. Vastaavaa saattaa esiintyä muissakin kuin HPE:n tuotteissa. (Tietoturva nyt! 28.11.2019)
- Intel julkaisi päivityksiä yhteensä 77 haavoittuvuuteen, jotka liittyvät muun muassa etähallintaan ja sivukanavahyökkäyksiin
  - Tässä kaksi esimerkkiä:
    - Intelin TPM-toteutus on haavoittuvainen sivukanavahyökkäyksille, mistä voit seurata, että hyökkääjä pääsee käsiksi tallennetuihin salausavaimiin.
    - Intel julkisti merkittäviä päivityksiä prosessoreissa oleviin haavoittuvuuksiin, joita hyödyntämällä hyökkääjä pystyisi lukemaan toisten prosessien tietoja.

Tietomurrot ja -vuodot

Tietomurrot ja -vuodot

- Office 365 –tietomurtoja ilmoitetaan edelleen päivittäin
  - Suurin osa tietomurroista olisi vältettävissä monivaiheisella tunnistautumisella.
  - Yksittäisen tietomurron selvittäminen johtaa usein useamman muun tietomurron havaitsemiseen, koska kalasteluviestit tulevat usein murretusta osoitteesta.
  - Murrettuja sähköpostitilejä käytetään petoksiin, tietovuotoihin ja uusien tietomurtojen valmisteluun tietojenkalastelulla.
- Verkkoon avoinna olevien palveluiden huonot konfiguraatiot aiheuttivat useita tietovuotoja
  - Osa tietovuodoista johtui haavoittuvista järjestelmistä, joita ei oltu päivitetty.
- Noin 1,2 miljardin tietueen tietovuoto, jossa paljastui yli 600 miljoonaa henkilötietoa
  - Vuotaneet tiedot sisältävät sähköposteja, puhelinnumeroja sekä LinkedIn- ja Facebook-tunnuksia.
  - HaveIBeenPwned.com-palvelusta voi tarkistaa, löytyykö oma sähköposti vääriin vuotolistoilta. Jos sähköpostin tiedot ovat vuotaneet, suosittelemme salasanojen vaihtamista niissä palveluissa, joissa sähköpostiosoitetta käytetään.
  - Vuoto liittyy tietoja keräävän ja myyvän yrityksen (PDL, People Data Labs) tietoihin. PDL ei todennäköisesti itse ole vuotaja, vaan tiedot ovat päätyneet julkisuuteen joltakin sen asiakkaalta.

Suojautumisohjeita tietomurtojen varalta

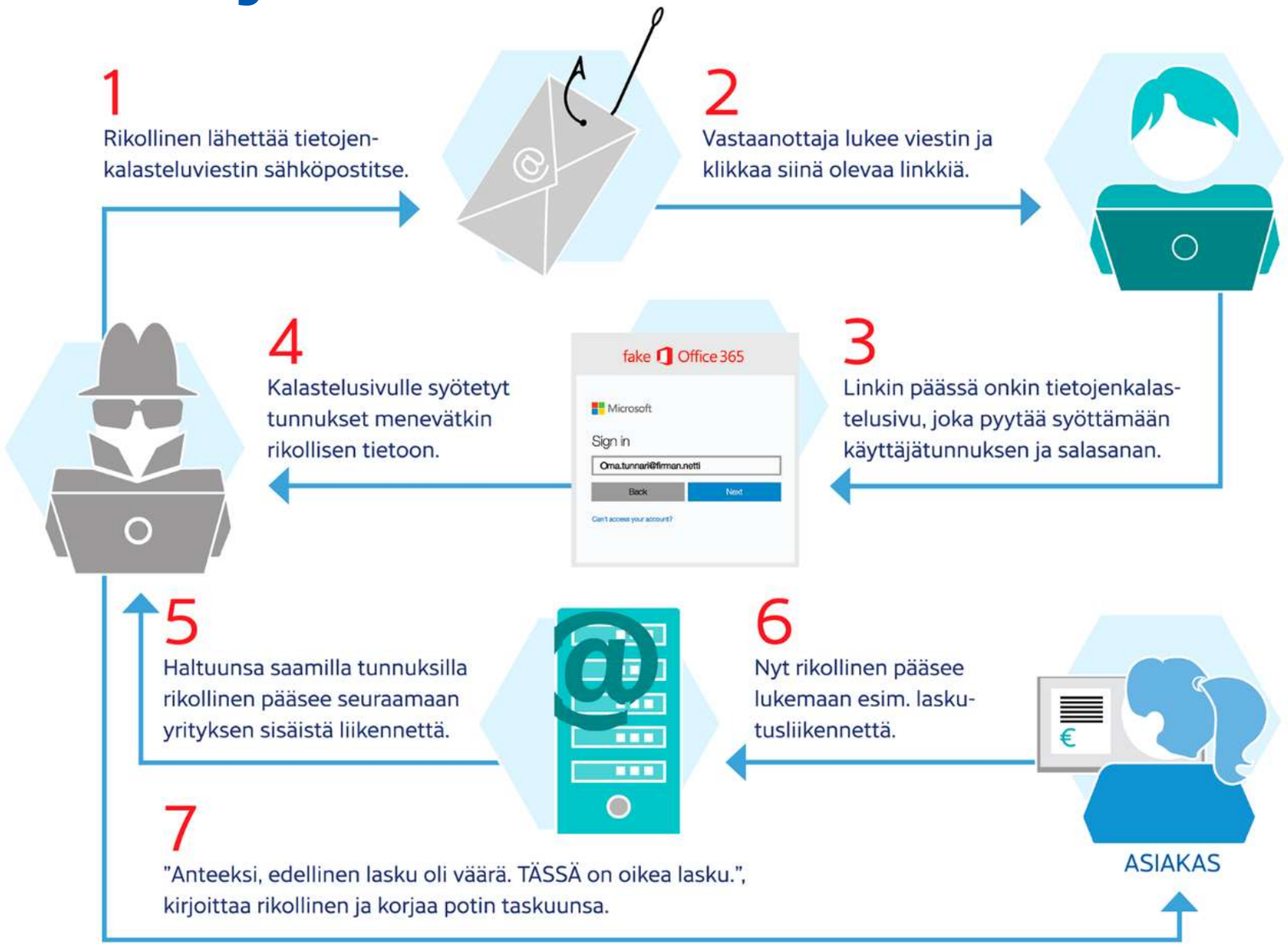
- Käytä eri salasanaa jokaisessa palvelussa.
- Muista päivittää käyttöjärjestelmä ja käyttämäsi ohjelmistot.
- Säilytä salasanoja turvallisesti.
- Vaihda salasanasi, jos epäilet tai tiedät sen joutuneen vääriin käsiin.
- Käytä monivaiheista tunnistamista, jos käyttämissäsi palveluissa sellainen on mahdollista.

Huijaukset ja kalastelut

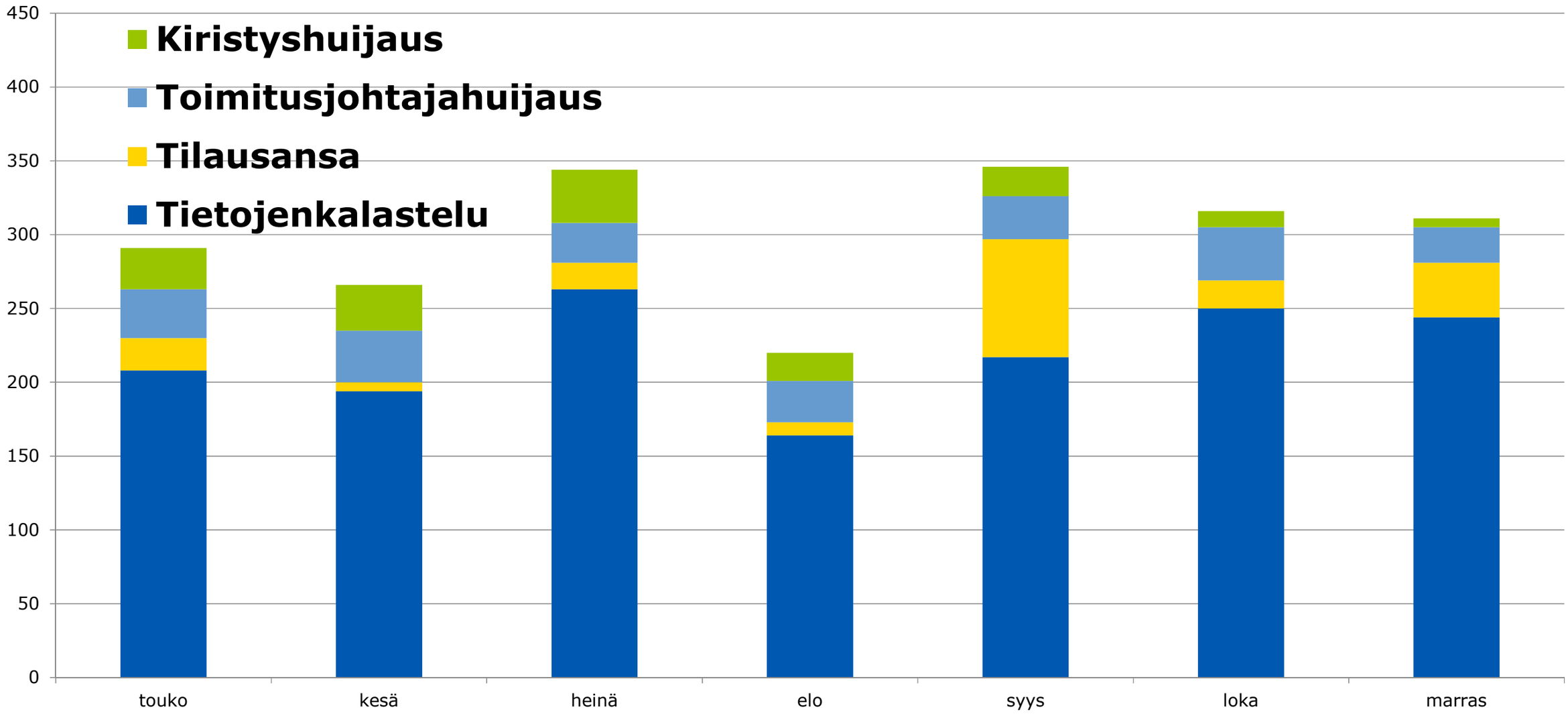
Huijaukset ja kalastelut

- Office 365 -kirjautumistunnusten kalastelu jatkui marraskuussa kiivaana ja johti uusiin tietomurtoihin päivittäin
  - Kaksivaiheinen tunnistautuminen auttaa suojautumaan tietomurtoja vastaan.
- Pankkitunnuksia kalastellaan päivittäin melkein kaikkien Suomessa toimivien pankkien nimissä
- Yleisiä huijausten ja tietojenkalastelun teemoja ovat myös suositut tuotemerkit
  - Esimerkiksi Netflix, Paypal, Gigantti, DHL, Apple, R-kioski, Power, Niken kengät ja Applen kellot.
- Huijausviesteissä näkyy huijareiden pyrkimys välttää huijausviestien automaattiset suodatukset
  - Avainsanoja on kirjoitettu vähän väärin ja kiristysviestien Bitcoin-lompakoita on pilkottu. Myös leipäteksteihin on lisätty erilaisia osioita frekvenssianalyysiä sekoittamaan.

Office 365 –huijauksen vaiheet



Käsiteltyjä huijaustapauksia 2019/05–11



IoT ja automaatio

IoT ja automaatio

- Suomi aloittaa älylaitteiden turvallisuuden varmistamisen ensimmäisenä Euroopassa – uusi Tietoturvamerkki auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja (Tietoturva nyt! 26.11.)
  - Myös Australia julkaisi luonnoksen IoT:n tietoturvavaatimuksista. Vaatimuslista olisi toteutuessaan vapaaehtoinen hyvä käytäntö tuotteiden valmistajille.
- ABB julkaisi marraskuun alussa PGIM–järjestelmissä olevan kriittisen haavoittuvuuden
  - Ollut yrityksen tiedossa jo viisi vuotta.
  - Hyökkääjä voi haavoittuvuutta hyödyntämällä saada käyttäjätunnukset ja salasanat haltuunsa.
  - CVE-2019-18250
- Yhdysvaltalainen energia-alan yritys sPower joutui alkuvuodesta hyökkäyksen kohteeksi
  - Hyökkääjä hyödynsi päivittämätöntä palomuuria ja onnistui katkaisemaan valvomon yhteyden tuotantoon.
  - Kyseessä on ensimmäinen energiantuotannon automaatiojärjestelmään läpi mennyt kyberhyökkäys Yhdysvalloissa.

Tietoturva-alan kehitys

Oikeudelliset asiat 1/2

- **1.1.2020 astuvat voimaan laki julkisen hallinnon tiedonhallinnasta (906/2019) ja valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019)**
  - Tulevat uudistamaan viranomaisten tiedonhallintaa sekä muun muassa salassa pidettävien tietojen luokittelu- ja suojauskäytäntöjä.
- Teletoiminnan häiriötilanteita koskeva **määräys (M66) on päivitetty**
  - Uudistetun määräyksen merkittävimmät muutokset ovat
    - Virastolle ilmoittamisen vaatimusten soveltamisalan yhdenmukaistaminen kaikissa joukkoviestintäpalveluissa niiden toteutustekniikasta riippumatta ja tilastointivaatimusten keventäminen.
    - Määräyksen perustelumuistio sisältää listauksen tehdyistä muutoksista, niiden syistä ja vaikutusarvioinneista.
- Euroopan unionin tuomioistuimen 1.10.2019 antamasta tuomiosta johtuen **Traficom on tarkentanut evästeohjeistustaan** suostumuksen antamiselle sekä käyttäjän evästeiden toiminta-ajasta ja kolmannen osapuolen mahdollisuudesta käyttää evästeitä
  - Tarkennetun ohjeistuksen mukaan evästeiden käytön hyväksyminen on edelleen mahdollista selainasetusten kautta eikä erillistä ponnahdusikkunaa vaadita.

Oikeudelliset asiat 2/2

- **Liikenne- ja viestintäministeriö pyytää lausuntoja luonnoksesta hallituksen esityksestä, jolla muutettaisiin sähköisen viestinnän palveluista annettua lakia ja eräitä siihen liittyviä lakeja**
  - Lausuntoja pyydetään viimeistään keskiviikkona 16.1.2020.
  - Ehdotuksella pannaan täytäntöön sähköistä viestintää koskeva teledirektiivi (1972/2018 EU) ja audiovisuaalisia mediapalveluita koskeva AVMS-direktiivi (1808/2018 EU).
  - Lisäksi esityksessä ehdotetaan yksittäisiä muita, kansallisista tarpeista lähteviä muutoksia.
- **Komissio on 17.10.2019 antanut päätöksiä tietojen käsittelyä koskevista soveltamissäännöistä:**
  - KOMISSION PÄÄTÖS (EU, Euratom) 2019/1961, annettu 17 päivänä lokakuuta 2019, luokkiin CONFIDENTIEL UE/EU CONFIDENTIAL ja SECRET UE/EU SECRET kuuluvien tietojen käsittelyä koskevista soveltamissäännöistä
  - KOMISSION PÄÄTÖS (EU, Euratom) 2019/1962, annettu 17 päivänä lokakuuta 2019, luokkaan RESTREINT UE/EU RESTRICTED kuuluvien tietojen käsittelyä koskevista soveltamissäännöistä
  - KOMISSION PÄÄTÖS (EU, Euratom) 2019/1963, annettu 17 päivänä lokakuuta 2019, yhteisöturvallisuutta turvallisuusluokiteltujen hankintasopimusten yhteydessä koskevista soveltamissäännöistä

Kyberasioihin liittyvää uutisointia maailmalta

5G:n turvallisuus kiinnostaa maailmalla

- Liikenne- ja viestintävirasto Traficom järjesti maailman ensimmäisen 5G:n kyberturvallisuutta koskevan hackathonin Oulussa 29.11.-1.12.2019. Hackathon keräsi kiinnostusta myös ulkomailla.
- https://www.wsj.com/articles/hackers-in-finland-test-5g-networks-devices-in-security-exercise-11576146601?tpl=cybersecurity

EU:n yhteinen kyberharjoitusympäristö

- Cyber Ranges Federation -projektissa rakennetaan EU:n laajuinen suljettu kyberharjoitteluympäristö jäsenmaiden puolustushallintojen käyttöön. Tarkoituksena on kehittää jäsenmaiden valmiuksia ja harjoittelua, jolla ne varautuvat kyberuhkatilanteisiin.
- https://eu2019.fi/artikkeli/-/asset_publisher/cyber-ranges-federation-yhteistyolla-kohti-parempaa-kyberkyvykkyytta

Viranomaisten yhteistyö estää terroristisen propagandan välittäminen verkossa

- 12 EU-maata ja yhdeksän kaupallista toimijaa yhdistivät voimansa marraskuussa, kun yli 26 0000 terroristista verkkopropagandaa levittäviä kohdetta poistettiin verkosta.
- https://www.europol.europa.eu/newsroom/news/eu-law-enforcement-and-judicial-authorities-join-forces-to-disrupt-terrorist-propaganda-online

Kybersään johtopäätökset

Tietoturvan edistyminen

1. Julkaisimme maailman ensimmäisen Tietoturvamerkin. Se auttaa kuluttajia tekemään turvallisempia kodin älylaitehankintoja.

2. Lapset ja heidän vanhemmat voivat harjoitella kybertaitoja uuden Spoofy-pelin avulla. Pelistä on hyötyä myös aikuisille.

3. Tietoturvallisuuden puutteiden etsinnän yhteisöllistäminen auttaa kaikkia.

Tietoturvan kehitystarpeet

1. Turvallisuus ja käytettävyys eivät aina kulje käsi kädessä. Monivaiheinen tunnistautuminen turvaa tietosi mutta hidastaa palvelun käyttöä.

2. Organisaatiot eivät tunnista kybervakoilun vaikutuksia liiketoiminnalle.

3. Liian suuri yhteen toimittajaan tai tuotteeseen tukeutuminen voi vikatilanteessa aiheuttaa peruuttamattomia vahinkoja.

Kiitos!

kyberturvallisuuskeskus.fi

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus