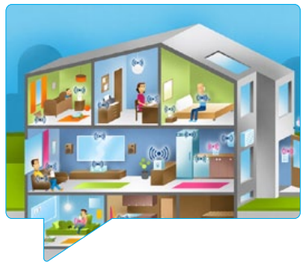
Tietoturvan vuosi 2016

Viestintäviraston julkaisu 001/2017 J

Viestintävirasto

4 TOP5-uhat ja -ratkaisut



18 Esineiden internet (IoT)

22 10 tietoturva näkymää vuodelle 2017

Sisällys

Toimivat tietoverkot rasvaavat yhteiskunnan rattaat

Monille meistä on mahdotonta kuvitella arkea ilman sähköisiä peruspalveluitamme. Riippuvuutemme tietoverkoista ja -järjestelmistä on ehdotonta. Viimeistään vuosi 2016 näytti, kuinka teknologian ja toimintamallien räjähdysmäinen kehitys vaikuttaa yhteiskunnan toimintavarmuuteen ja turvallisuuteen.

Alkuvuoden kaksi erittäin laajaa ja pitkäkestoista matkapuhelinverkon häiriötä olivat konkreettisia esimerkkejä uhkista, joita häiriöt aiheuttavat arjellemme. Arkisilta kuulostavilla vikatilanteilla oli huomattavia vaikutuksia koko yhteiskuntaan. Saamiemme yhteydenottojen mukaan useita suunniteltuja matkoja jäi tekemättä ja monia kauppoja solmimatta. Erityisen vakavia vaikutuksia nähtiin niissä organisaatioissa, jotka olivat järjestäneet ihmishengen kannalta kriittisiä palvelujaan toimivien matkapuhelinverkkojen varaan. Omassa elämässäni häiriö näkyi ja tuntui, kun ekaluokkalainen lapseni ei voinutkaan soittaa sovittua olen päässyt kotiin -puhelua. Huoli oli kova.

Yhtä vakava esimerkki nähtiin marraskuussa. Lämmönsyöttöä ohjanneisiin laitteisiin vaikuttanut verkkohyökkäys kylmensi asuntoja Lappeenrannassa. Automaatiolaitteet eivät olleet hyökkäyksen tai rikollisten kiinnostuksen kohteena. Ne olivat ainoastaan helposti hyödynnettävissä oleva väline Suomen ulkopuolelle suunnatun hyökkäyksen toteuttamiseen. Vaikutukset kohdistuivat kuitenkin välittömästi Suomeen ja suomalaisiin.

Uhkista huolimatta on tärkeää nähdä metsä puilta. Digikehitys muuttaa arkeamme ja haastaa jatkuvasti yksilöitä ja yhteiskuntaa rikkomalla vanhaa ja luomalla uutta. Muutos on aina vaikeaa ja joskus kivuliastakin. Uudet tavat voidaan ottaa käyttöön vain, jos ihmiset luottavat palvelujen turvallisuuteen ja toimintavarmuuteen. Myös yksityisyydensuojan merkitys on korostumassa. Luottamuksen rakentamiseksi tietoturvallisuus ja vastuulliset toimintamallit ovat erottamaton osa uusien palveluiden luomista.

Uskallan väittää, että antamalla käyttäjille yhä enemmän mahdollisuuksia arvioida eri palvelumalleja, heikommat palvelut poistuvat ja paremmat menestyvät. Tämä luo meille kaikille parempaa arkea.

Muutos on aina myös mahdollisuus.

Helsingissä 31.1.2017

Jarkko Saarimäki

Johtaja
Kyberturvallisuuskeskus
Viestintävirasto

TOP5-uhat ja -ratkaisut

TOP5-UHAT: Organisaatiot

Päivitysten laiminlyönti
Muutostenhallinta on monista syistä hankalaa. Päivittämättömät laitteet kaapataan resursseiksi haittakäyttöön.

Kiristyshaittaohjelmat
Työasemat ja verkkopalvelimet lukitaan lunnaita varten. Jälkien korjaaminen aiheuttaa pitkiä katkoksia toiminnassa.

Huijausviestit ja tietojen kalastelu
Laskutus- ja toimitusjohtajahuijaukset aiheuttavat suuria taloudellisia menetyksiä. Urkittuja tietoja käytetään uusiin rikoksiin.

Ulkoistusten ja laitehankintojen hallinta
Laitteet, ohjelmistot ja palvelut ostetaan eri paikoista. Vastuut, sopimukset ja tietoturva koetaan toisarvoisiksi hankintahetkellä. Kokonaisuuden riskejä on vaikea hallita.

Palvelunestohyökkäykset ovat internetin arkipäivää. Se on huomioitava organisaation riskiarvioissa joko hyökkäysten sietämisen tai varautumisen ja suojautumisen kannalta.

TOP5-RATKAISUT: Organisaatiot

Järjestelmien rutiininomainen päivitys
Ota päivittäminen kiinteäksi osaksi tietohallinnon prosesseja, niin pysyt järjestelmiesi kanssa ajan tasalla.

Koulutettu henkilöstö
Tarkkaavaiseksi koulutettu henkilökunta on paras suoja uhkia vastaan. Myös verkkoympäristön segmentointi auttaa pitämään syntyneet vahingot pieninä.

Varmuuskopiot
Tee varmuuskopioinnista säännöllistä ja harjoittele niiden palauttamista.

Lokien hallinta
Tapahtuneen selvittely, vahinkojen korjaaminen ja haavoittuvuuksien paikkaaminen onnistuvat vain, jos lokeista selviää, mitä on tapahtunut.

Tietoturvan hallittu johtaminen
Sovi etukäteen vastuut sekä oman väen että yhteistyökumppaneiden kanssa. Silloin akuutissa tilanteessa tiedetään, miten tulee toimia.

TOP5-UHAT: Yksityishenkilöt

Huijaukset ja tilausansat
Uskottava ulkoasu ja kieli saavat yhä useamman haksahtamaan huijauksiin.

Kiristyshaittaohjelmat leviävät älylaitteisiin
Lunnastroijalaiset lukitsevat tietokoneiden lisäksi muitakin laitteita, kuten televisioita ja tabletteja.

IoT tuli joka kotiin,
mutta tietoisuus sen riskeistä ei tullut samassa paketissa.

Yksityisyys somemaailmassa
Kaikki jakamasi ja tekemäsi siirtyy markkinoijan käyttöön, halusit sitä tai et.

Salasanojen kierrätys
Koska moni käyttää samoja vanhoja salasanoja eri palveluissa, yhteen palveluun murtautuminen vaarantaa muidenkin palveluiden käytön.

TOP5-RATKAISUT: Yksityishenkilöt

Mieti ennen kuin klikkaat
Varmista, että linkki tai tiedosto, jota olet avaamassa, on sitä mitä väittää olevansa. Älä aukaise, jos epäilet huijausta.

Salasanojen hallinta
Käytä vahvoja salasanoja, vaihda ne säännöllisesti äläkä käytä samoja salasanoja eri palveluissa.

Päivitä verkossa olevat laitteet ja käyttämäsi ohjelmistot säännöllisesti.
Ajan tasalle päivitetyt ohjelmistot ja käyttöjärjestelmä ovat paras turva tietoturvauhkia vastaan.

Varmuuskopiot tärkeistä tiedoista
Ota tavaksi säännöllinen varmuuskopiointi.

Käytä tietoturvaohjelmistoja
Pidä tietoturvaohjelmistosi ajan tasalla ja ota selaimen varoitukset vakavasti.

Nettihuijaus- ja kalastelubisnes kukoistaa

Verkkorikollisille on arvoa kaikella tiedolla, jota voi käyttää rahan ansaitsemiseen. Erilaisilla nettihuijauksilla viedään suomalaisilta miljoonia euroja vuosittain. Uhreiksi päätyvät niin suuryritykset, yksityiset kansalaiset ja kaikki siltä väliltä. Viestintäviraston Kyberturvallisuuskeskus taistelee yhdessä poliisin kanssa huijauksia vastaan.

Tarkista laskujen oikeellisuus ennen kuin hyväksyt

Vuoden 2016 aikana, ennen lähinnä satunnaiset ja loma-aikoihin keskittyvät, yritykset lypsää rahaa valelaskuilla ja toimitusjohtajahuijauksilla arkipäiväistyivät.

Toimitusjohtajahuijauksessa rikollinen lähestyy uhriaan sähköpostitse tai puhelimitse, tekeytyy yrityksen johtajaksi ja koettaa saada talousosaston siirtämään rahaa tililleen. Apuna käytetään väärennettyjä sähköpostiosoitteita tai aidon näköisiä verkkotunnuksia.

Uskottavalla huijauskampanjalla rikollisten saama hyöty voi nousta kymmeniin tuhansiin euroihin kerralla. Valelasku muistuttaa toimitusjohtajahuijausta, mutta on usein vain pelkkä lasku, joka koetetaan saada maksuprosesseista läpi vauhdikkaasti. Kertasummat ovat pienempiä kuin toimitusjohtajahuijauksissa.

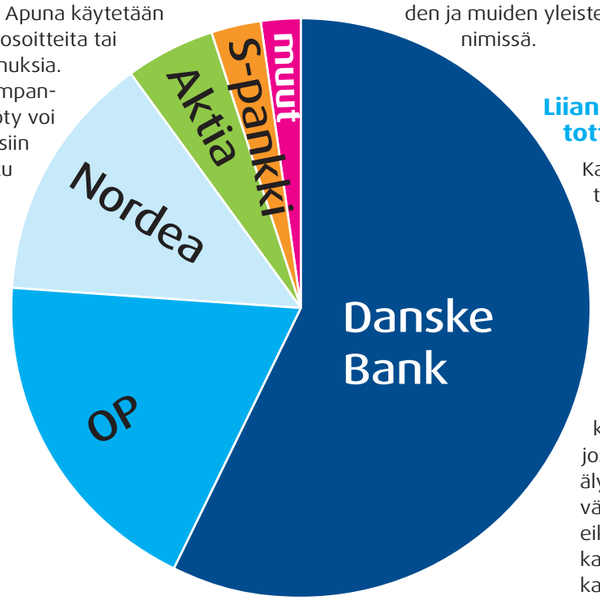
Katkaise huijarin ansaintamalli

Moniin huijauksiin on selvästi käytetty aikaa, vaivaa ja rahaa, koska se kannattaa. Rikollisen on kannattanut panostaa huijaamiseen, koska huolellisemmin tehty huijaus tuottaa enemmän voittoa. Siksi tietoisuuden lisääminen tiedottamisella ja valistamisella toimii tehokkaasti huijareita vastaan. Rikollisuus vähenee, jos ei siitä koidu huijareille rikoshyötyä.

Yksittäisiä kuluttajia koetetaan saada lankaan monin tavoin. Puhelin- ja sähköpostiviesteillä kuluttaja houkutellaan verkkoon pystytetylle valesivustolle, joilla kalastellaan luottokorttinumeroita, pankkitunnuksia, henkilötietoja, käyttäjätunnuksia, tai yhteystietoja uusien kalasteluviestien uhreiksi. Kaikki jollain tavoin rahaksi muutettava kelpaa.

Pankkipalvelut huijausten ytimessä

Eniten suomalaisilta kalastellaan tietoja pankkien nimissä. Kaikkien Suomessa toimivien liikepankkien nimiä hyödynnetään huijauksissa, mutta vuonna 2016 Viestintävirastolle ilmoitetuista pankkikalastelusivustoista valtaosa yritti huijata Danske Bankin asiakkaita. Monenlaisia huijausviestejä lähetetään myös postin, poliisin, verottajan, verkkokauppojen, kuriiripalveluiden ja muiden yleisten verkkopalvelujen nimissä.



Viestintävirastolle ilmoitetut pankkihuijaukset vuonna 2016

Liian hyvää ollakseen totta

Kalastelujen lisäksi kuluttajia kiusataan kasvavassa määrin tilausansoilla. ”Vain sinulle” kohdistettu lähes ilmainen älylaite houkuttelee syöttämään luottokorttitiedot postitusta varten, mutta sitookin tilaajan kymmenien eurojen jatkuvaan kuukausiveloitukseen, josta ei pääse irti. Luvattua älylaitetta kuluttaja ei välttämättä koskaan saa, eikä erehdyksessä tilattu kaupanpäällinen palvelukaan ole toivotunlainen.

Suomalaisia kiusanneet huijaukset ja kalastelut ovat olleet melko kömpelöitä ja helppoja tunnistaa huijaukseksi, mutta vuoden 2016 loppua kohti huijausten laatu on kohentunut ja esiin on tullut entistä taitavampia harhautuksia.

Nettihuijausten ja kalastelun aikajana

Tammikuu	13.1.2016	Toimitusjohtajahuijaukset riehuvat sähköposteissa.
Helmikuu	5.2.2016	Varoitus! Tietojenkalastelukampanjoita eri pankkien, postin ja poliisin nimissä.
	16.2.2016	Valelaskuja tekstiviestillä puhelinoperaattorien nimissä.
Maaliskuu	21.2.2016	Tietojenkalastelua verottajan nimissä.
Huhtikuu	1.4.2016	Pankkitietojen kalastelua Danske Bankin ja Nordean nimissä.
	22.4.2016	Pankkitietojen kalastelua Aktian nimissä.
Toukokuu	21.6.2016	Varastettujen iPhone-puhelimien tunnuslukujen kalastelua tekstiviestillä.
Kesäkuu	22.6.2016	Varoitus! Aktiivinen toimitusjohtajahuijauskampanja hyödynsi alkanutta lomakautta.
Heinäkuu	4.7.2016	Euromegawins-huijauksia tekstiviesteinä tuhansille suomalaisille.
	19.8.2016	Toimitusjohtajahuijaukset jatkuivat Euroopan lomakaudella.
Elokuu	15.9.2016	Toimitusjohtajahuijauksia jälleen liikkeellä.
Syyskuu	4.10.2016	Uusia tilausansoja pankkien, Gigantin ja Verkkokaupan nimissä.
	5.10.2016	Huijauslaskun mukana kiristyshaittaohjelma ensimmäistä kertaa.
Lokakuu	18.10.2016	Uusia toimitusjohtajahuijauksia hyvällä suomen kielellä.
Marraskuu	1.11.2016	Varoitus! Satoja suomalaisia luottokorttinumeroita ja verkkopankkitunnuksia huijannut Apple ID -kampanja jatkui koko loppuvuoden.
Joulukuu	10.11.2016	Veronpalautuksiin liittyvillä huijausviesteillä kalasteltiin luottokorttitietoja.

Uhka-arvio: **Huijaukset ja kalastelut**

	Kansalaiset	Yritykset	Valtio
Huomio/Häirintä		Maineongelmat Asiakkaiden luottamus	Maineongelmat Kansalaisten luottamus
Raha	Laskutus ja maksu-liikenne	Laskutus ja maksu-liikenne	Palveluiden saatavuus ja kiristäminen
Tieto	Käyttäjätunnukset, salasanat, pankkitunnukset, maksukortit	Käyttäjätunnukset, salasanat, yritystiedot	Käyttäjätunnukset, salasanat, yritystiedot
Väliresurssi	Yhteystietoja käytetään huijaukseen.	Tietoja hyödynnetään rikollisuudessa.	Tietoja hyödynnetään rikollisuudessa.

Ei uhkaa · Lievä uhka · Haittaava uhka · Vakava uhka

Oikean alakulman väri kertoo vuoden 2015 tilanteen.

Haavoittuvuudet ja haittaohjelmat

Vuosi 2016 oli tiedostot salaavien kiristyshaittaohjelmien vuosi. Erilaisten kiristyshaittaohjelma-muunnosten määrä on vuoden aikana kasvanut yli kuusinkertaiseksi.

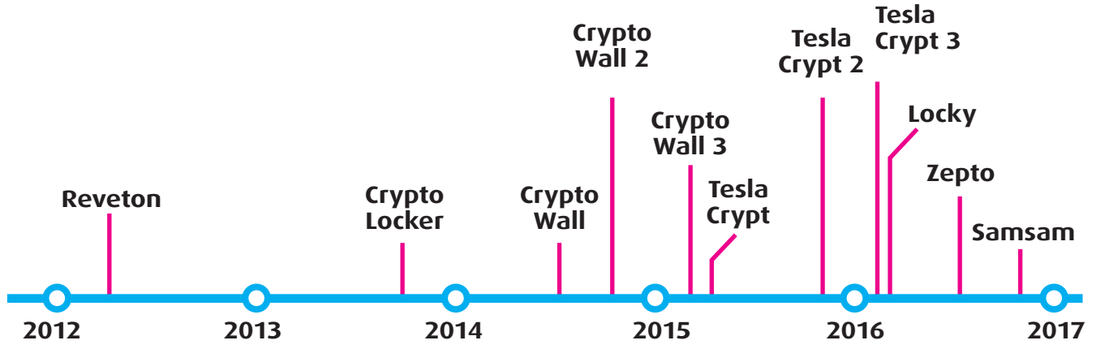
Kiristyshaittaohjelmat hallitsivat vuotta

Suurin osa haittaohjelmia levittävistä roskapostiviesteistä ja murretuista sivustoista levittää nyt kiristyshaittaohjelmia. Myös tartuntojen määrä kasvoi moninkertaiseksi vuoteen 2015 nähden. Suomessa levitettiin eniten Lockya, ja se myös aiheutti eniten kiristyshaittaohjelmatartuntoja.

Useimmiten kiristyshaittaohjelma tarttuu tietokoneeseen, koska käyttäjä on uskonut huijaussähköpostiviestiä ja avannut liitetiedoston tai haittaohjelmatiedostoon osoittavan linkin. Tartuttamiseen ei siis yleensä käytetä ohjelmistojen haavoittuvuuksia, vaan tietokoneen käyttäjä houkutellaan ja hämätään asentamaan haittaohjelma itse. Haittaohjelmien kehitys on nopeaa, ja aina jokin muunnelma haittaohjelmasta pääsee torjuntaohjelmienkin seulasta läpi.

Kyberrikolliset tekevät kiristyshaittaohjelmilla myös kohdennettuja iskuja yrityksiin. Vuoden aikana maailmalla kohistiin erityisesti sairaaloita vastaan tehdyistä kyberhyökkäyksistä. Rikolliset murtautuivat sairaalan tietojärjestelmiin ja asensivat kiristyshaittaohjelmia paikkoihin, joissa ne aiheuttaisivat mahdollisimman paljon haittaa sairaalan päätehtävälle, potilaiden hoitamiselle. Esimerkiksi yhdysvaltalainen sairaala Hollywood Presbyterian Medical Center maksoi 17000 dollarin lunnaat saadakseen salatut tiedostot jälleen auki. Tyypillinen lunnasvaatimus massoittain levitetyissä kiristyshaittaohjelmissa on muutaman sadan dollarin luokkaa.

Joulukuussa Suomessakin sattui kohdennettu kiristystapaus. Samsam-nimistä kiristyshaittaohjelmaa käyttävät rikolliset iskivät suomalaiseen yritykseen ja aiheuttivat merkittävää haittaa yrityksen toiminnalle.



Suomessa havaittuja kiristyshaittaohjelmia ja niiden muunnoksia.

Shadow Brokers vuoti verkkovakoilun työkaluja

Vuoden merkittävin ohjelmistohaavoittuvuustapaus oli Shadow Brokers -ryhmän elokuussa tekemä kyberhyökkäystyökalujen paljastus, joka samalla paljasti uusia haavoittuvuuksia useiden verkkolaitevalmistajien tuotteissa. Rikolliset alkoivat heti etsiä haavoittuvia laitteita internetistä, mikä näkyi skannausliikenteenä.

Seurauksena verkkolaitevalmistajat joutuivat julkaisemaan korjaavia ohjelmistopäivityksiä pikavauhtia. Haavoittuvuuksien massapaljastuksia lienee luvassa jatkossakin niiden merkityksen kasvaessa pimeillä markkinoilla.

Haavoittuvuuksia brändätään

Heartbleedistä vuonna 2014 alkanut haavojen brändäys on alkanut vakiintua. Hauskat nimet kuten Badlock, Blacknurse ja DROWN herättävät huomiota ja saavat ihmiset paikkaamaan ongelmia. Toisaalta joidenkin haavoittuvuuksien näkyvä markkinointi saattaa ohjata ihmisten huomion pois muista kriittisistä ongelmista, joille ei ole keksitty vetävää nimeä.

Haavoittuvuuksien aikajana 2016

Tammikuu

8.1.2016 Juniper tiedotti, että sen ScreenOS-reititintuotteiden satunnaislukugeneraattorin ohjelmakoodissa on luvattomasti tehtyjä muutoksia, jotka heikensivät laitteiden tietoturvaa.

Helmikuu

1.3.2016 SSLv2-protokollan DROWN-haavoittuvuus tuli julki. Viestintävirasto selvitti, missä suomalaisissa verkkopalveluissa on käytössä haavoittuva ohjelmisto ja otti yhteyttä niiden ylläpitäjiin.

Maaliskuu

16.3.2016 Android-laitteiden Stagefright-haavoittuvuuden uusi hyväksikäyttömenetelmä Metaphor tuli julki. Haavoittuvan laitteen voi ottaa etähallintaan, jos käyttäjä vierailee hyökkääjän hallitsemalla verkkosivulla.

Huhtikuu

7.4.2016 Badlock-haavoittuvuuden ennakkotietojen valossa Viestintävirasto selvitti suomalaisissa verkoissa olevia Samba-palvelimia, havaitsi useiden olleen jopa vuosia päivittämättä ja otti yhteyttä niiden ylläpitäjiin.

Toukokuu

Kesäkuu

12.5.2016 Uutisen mukaan rikolliset murtautuivat suomalaisten jäähallien jäähdytyksen suojaamattomiin etähallintajärjestelmiin ja lähettivät tekstiviestejä maksullisiin palveluihin.

Heinäkuu

16.5.2016 Viestintävirasto aloitti vuosittaisen selvityksen suojaamattomista automaatiojärjestelmistä suomalaisissa verkoissa. Löydökset olivat samankaltaisia kuin edellisvuosina.

Elokuu

Syyskuu

17.8.2016 Cisco julkaisi päivityksiä verkkolaitteidensa ohjelmistoihin, jotka korjasivat The Shadow Brokersin paljastamien hyökkäystyökalujen hyödyntämiä haavoittuvuuksia.

Lokakuu

Marraskuu

7.11.2016 Kahden kerrostalon lämmitys katkesi, koska niiden automaatiojärjestelmiä käytettiin palvelunestohyökkäyksen välikappaleina. Automaatiojärjestelmät eivät kestäneet kasvanutta liikennettä.

Joulukuu

Haittaohjelmien aikajana 2016

Tammikuu

9.1.2016 Useat lähteet vahvistivat, että Ukrainassa 23.12.2015 tapahtuneet sähkökatkokset aiheutettiin BlackEnergy-haittaohjelman välityksellä.

12.1.2016 Suomessa levitettiin runsaasti sähköpostiviestejä, joista saattoi saada Jsocket RAT -tartunnan. Viestien levityksessä oli käytetty suomalaisia murrettuja sähköpostitilejä. Poliisi aloitti tapauksen tutkinnan.

Helmikuu

25.1.2016 Viestintävirasto otti sähköpostilla yhteyttä henkilöihin, joiden oli selvitetty saaneen Jsocket RAT:ia levittäviä sähköpostiviestejä.

Maaliskuu

17.2.2016 Lockyä levitettiin erityisesti laskuiksi naamioitujen tiedostojen välityksellä.

26.2.2016 Kahden saksalaisen sairaalan kiristyshaittaohjelmatartunnat uutisissa.

27.2.2016 CTB-Lockerin uutisoitiin leviävän maailmalla nopeasti. Suomessa kiristyshaittaohjelmista näkyi lähinnä TeslaCryptiä ja Lockyä.

Huhtikuu

22.3.2016 Kanadalaisessa sairaalassa ”hätätila” kiristyshaittaohjelmatartunnan vuoksi.

23.3.2016 Samsam-kiristyshaittaohjelman uutisoitiin kohdistuvan maailmalla erityisesti terveydenhuollon organisaatioihin.

Toukokuu

28.3.2016 Yhdysvaltalainen MedStar-sairaala suljettiin kiristyshaittaohjelmatartunnan vuoksi.

10.4.2016 Useiden uutissivustojen verkkomainosten kautta levitettiin haittaohjelmia Suomessa ja muualla maailmalla.

Kesäkuu

18.5.2016 TeslaCryptin kehittäjät löivät hanskat tiskiin ja julkaisivat yleisavaimen salauksen purkamiseen.

1.6.2016 Dridexin ja Lockyn levitys väheni rajusti maailmanlaajuisesti, kun niiden levityksessä käytetty Necurs-bottiverkko lakkasi yllättäen toimimasta.

Heinäkuu

28.6.2016 Locky palasi levitykseen.

22.7.2016 Viestintävirasto selvitti kyselyllä kiristyshaittaohjelmien vaikutuksia Suomessa.

Elokuu

8.8.2016 Oracle ilmoitti, että sen valmistaman MICROS-kassajärjestelmän lähdekoodiin oli istutettu haitallista ohjelmakoodia.

13.8.2016 Shadow Brokers -niminen ryhmä julkaisi hyökkäystyökaluja useita verkkolaitteita vastaan. Ryhmä väitti niiden olevan varastettu Equation Group -nimiseltä ryhmältä, jonka uskotaan toimivan Yhdysvaltain laskuun.

Syyskuu

16.9.2016 Pääasiassa huonosti suojatuista älylaitteista koostunutta Mirai-bottiverkkoa käytettiin hajautettuun palvelunestohyökkäykseen KrebsOnSecurity-verkkosivustoa vastaan. Hyökkäyksen volyymi oli ennätyksellisesti yli 600 Gbit/s.

Lokakuu

13.10.2016 Mirai-bottiverkkoon kuuluvista laitteista Suomessa tehtiin noin 300 havaintoa.

22.10.2016 Ranskalaista palvelintilayritystä vastaan tehtiin hajautettu palvelunestohyökkäys IoT-laitteista kootulla bottiverkolla. Hyökkäyksen volyymi oli ennätyksellisesti lähes 1 Tbit/s.

Marraskuu

25.11.2016 Mirai-botti alkoi levitä uudella tavalla ja tarttui laajakaistamodeemeihin laajasti Suomessa ja maailmalla. Viikonlopun aikana Suomessa noin 16000 tartuntaa.

29.11.2016 Viestintävirasto julkaisi punaisen varoituksen Mirai-tartuntojen takia.

Joulukuu

2.12.2016 Viestintävirasto sai ilmoituksen suomalaisesta Samsam-tartunnasta.

Maailman suurin digitaalinen pankkiryöstö Bangladeshissa

Pankit ovat suurine rahavirtoineen ilmiselviä kohteita rikollisille. Huijauksilla saadaan vähällä vaivalla tavalliselta kansalta koottua pienistä rahavirroista suuria summia, mutta onnistuneella haittaohjelmahyökkäyksellä suoraan pankin järjestelmiin voivat kertasummat nousta suuriksi

Helmikuussa Bangladeshin keskuspankista yritettiin ryöstää liki miljardi Yhdysvaltain dollaria väärentämällä pankkien välistä rahaliikennettä. Pankkien välisiä rahansiirtoja tehdään järjestelmän nimeltä SWIFT kautta. Ryöstäjien oli onnistunut ujuttaa etähallittavia haittaohjelmia Bangladeshin keskuspankin SWIFT-järjestelmään kytkettyihin tietokoneisiin. Ryöstäjät ehtivät viedä Bangladeshin keskuspankista noin 81 miljoonaa dollaria, ennen kuin ryöstäjien tekemä näppäilyvirhe johti transaktion väärään paikkaan paljasten operaation ja keskeyttäen ryöstäjien toiminnan.

Bangladeshin tapaus osoittaa, että rikollisetkin seuraavat aikaansa: kun rahan käsittely on digitaalista, myös rikollista hyötyä haetaan digitaalisesti. Tapaus osoittaa myös, että vaikka murtautuminen Bangladeshissä SWIFT-päätteelle oli suhteellisen helppoa, rikolliset tarvitsivat yhä paljon aikaa, vaivaa ja resursseja kyetäkseen väärentämään rahansiirtoja. Lisäksi ryöstö havaittiin normaalin käytännön mukaisella rahojen alkuperän tarkastuksella.

Bangladeshin tapauksen vanavedessä on paljastunut muutamia vastaavia ryöstöjä tai ryöstön yrityksiä muualla maailmassa. SWIFT-viestinvälitystä ylläpitävä yhtiö on sanonut, että ryöstöjen syynä on ollut yksittäisten pankkien huono tietoturvataso. SWIFT on lisännyt ja parantanut ohjeistustaan pankeille.

Uhka-arvio: **Haavoittuvuudet ja haittaohjelmat**

	Kansalaiset ⬆	**Yritykset** ⬆	**Valtio** ➡
Huomio/Häirintä	Epäluottamus digitaalisia palveluita kohtaan	Maineongelmat palvelun/tuotteen haavoittuvuuksista	Maineongelmat palveluiden haavoittuvuuden vuoksi
Raha	Kiristäminen ja maksukorttien tietoja varastavat haittaohjelmat	Palveluiden saatavuus ja kiristäminen	Palveluiden saatavuus ja rahan käsittelyä koskevia tietoja varastavat haittaohjelmat
Tieto	Käyttäjätunnukset, salasanat ja tiedostot	Vakoilu	Vakoilu
Väliresurssi	Tietokoneiden ja laitteiden valjastaminen bottiverkkoihin	Verkkosivujen valjastaminen haittaohjelmien levitykseen	Tietojen hyödyntäminen haittaohjelmien levityksessä

Ei uhkaa · Lievä uhka · Haittaava uhka · Vakava uhka

Oikean alakulman väri kertoo vuoden 2015 tilanteen.

Uhka-arvion muutokset: Kiristyshaittaohjelmat ovat yleistyneet merkittävästi ja ovat vakava uhka sekä yksittäisten ihmisten että organisaatioiden tietojen käytettävyydelle.

Esimerkki kohdistetun hyökkäyksen kulusta

Verkkovakoilu ja kohdistetut hyökkäykset koskevat yhä useampaa

Kohdistetut haittaohjelmahyökkäykset kehittyivät ja monipuolistuvat vuonna 2016. Laittoman tiedonhankinnan lisäksi niitä käytettiin maailmalla myös informaatiovaikuttamiseen. Suomessa verkkovakoiluun tarkoitettujen haittaohjelmien levitysyrityksiä havaittiin valtiollisten toimijoiden ja yritysten tietojärjestelmiin. Ulkoasiain- ja puolustushallinnot ovat todennäköisimpiä kohdistettujen hyökkäysten kohteita. Nähtävissä on poliittisen päätöksentekokoneiston nousu merkittäväksi kohdistettujen hyökkäysten kohteeksi.

Yksityissähköpostia ja perheenjäseniä hyödynnetään levityksessä

Vuoden 2016 havaintojen perusteella vakoiluun räätälöidyn haittaohjelman saamiseksi kohdeverkkoon käytettiin kahta tyypillistä keinoa: joillekin verkon käyttäjille lähetetään sähköpostiviesti, joka sisältää joko haitallisen liitetiedoston tai linkin, joka johtaa haitalliselle verkkosivustolle.

Itse sähköpostiviestit sisälsivät vastaanottajan työtehtävien kannalta mielenkiintoisia teemoja ja ne lähetettiin selkeästi ennalta huolellisesti valituille henkilöille. Verkkosivut, joihin linkit osoittivat, saattoivat olla tuttuja ja luotettuja työtehtävien tai arkisten asioiden hoitamisessa. Nämä sivustot kuitenkin oli murrettu ja valjastettu haitalliseen käyttöön. Kohdistettujen hyökkäysten kohdistus on sananmukaisesti tarkkaa.

Uutena ilmiönä havaittiin, että työsähköpostien lisäksi, haittaohjelmaa yritettiin levittää kohdehenkilöiden yksityissähköpostien ja esimerkiksi heidän perheenjäsentensä sähköpostiosoitteiden kautta. Yksityissähköpostin käytön havainnointimekanismit ja postin käyttötavat ovat löyhempiä työsähköpostiin verrattuna. Hyökkääjät pyrkivät jatkuvasti kehittämään uusia menetelmiä löytääkseen heikoimmalla suojauksella varustetun reitin kohdehenkilön tietoihin.

Informaatiovaikuttaminen mukaan tavoitteisiin

Maailmalla tehtyjen havaintojen perusteella voidaan sanoa, että kohdistettuja haittaohjelmia käytetään myös informaatiovaikuttamiseen, esimerkiksi vaalien yhteydessä. Myös kohdistettujen ohjelmien käyttö on laajentunut perinteisestä toimistotietotekniikasta verkon aktiivilaitteisiin, älylaitteisiin sekä teollisuusautomaatiojärjestelmiin. Lisäksi kohdistettujen hyökkäyksien tekniikoita on hyödynnetty kybersabotaaseissa. Vuoden 2016 aikana asiaan herättiin maailmanlaajuisesti analysoitaessa vuoden 2015 lopun Ukrainan sähköverkko-operaattoreihin kohdistunutta verkkoinfrastruktuurin lamautusoperaatiota.

Nollapäivähaavoittuvuuksia käytettiin hyökkäysmenetelminä aktiivisesti, vaikka valtaosa kohdistetuista hyökkäyksistä toteutetaan yleisesti tunnettuja haavoittuvuuksia hyödyntämällä. Useissa tunnetuissa tapauksissa hyökkäys perustui täysin vastaanottajan harhauttamiseen, eikä haavoittuvuuksien hyödyntäminen ollut hyökkääjälle välttämättä tarpeellista.

Verkkovakoilua ja kohdistettujen hyökkäysten yrityksiä on havaittu Suomessa lähes yhtä paljon kuin vuonna 2015. Tapauksia ilmenee muutamia kymmeniä vuodessa. Viestintäviraston kotimainen ja kansainvälinen yhteistyö tapausten selvittelyssä jatkui tiiviinä. Hyökkäysten torjunnassa suurin ongelma on edelleen organisaatioiden oman syvän havainnointikyvyn puute.

Kehityssuuntia

Hyökkäyksissä käytettyjen haittaohjelmien, hyökkäysinfrastruktuurien sekä työkalujen kehitys tulee jatkumaan. Haittaohjelmista pyritään tekemään entistä vaikeammin havaittavia. Yksi kehityssuunta ovat muistinvaraiset haittaohjelmat, joista ei jää kohdetietojärjestelmän levyjärjestelmiin mitään jälkiä.

Kohdistettujen hyökkäysten käyttö osana informaatiovaikuttamista lisääntynee. Kansalaisjärjestöt, poliittiset puolueet sekä poliittiset päätöksentekijät ovat yhä todennäköisemmin hyökkäysten kohteita.

Uhka-arvio: **Verkkovakoilu**

	Kansalaiset	Yritykset	Valtio
Huomio/Häirintä	Ei kohdistu kansalaisiin	Yritysten häirintään ei tehokkain keino	Informaatiovaikuttaminen haittaa valtionhallinnon toimintaa onnistuessaan.
Raha	Ei kohdistu käyttäjien rahoihin	Välilliset seuraukset näkyvät kilpailutusten epäonnistumisena ja tuotekilpailussa.	Rahalliset tavoitteet valtionhallintoon eivät tyypillisiä
Tieto	Ei kohdistu kansalaisten tietoihin	Kilpailutukset, innovaatiot ja asiakastiedot voivat olla ulkopuoliselle hyödyllistä tietoa.	Tieto ensisijainen tavoite poliittisen päätöksenteon tueksi
Väliresurssi	Yksityissähköpostien ja läheisten hyödyntäminen organissatioihin hyökätessä	Merkittävät asiakkaat lisäävät yrityksen riskiä väliresurssina hyödyntämiseksi.	Valtionhallinto ensisijainen kohde, johon pyritään väliresurssien avulla

Ei uhkaa · Lievä uhka · Haittaava uhka · Vakava uhka

Oikean alakulman väri kertoo vuoden 2015 tilanteen.

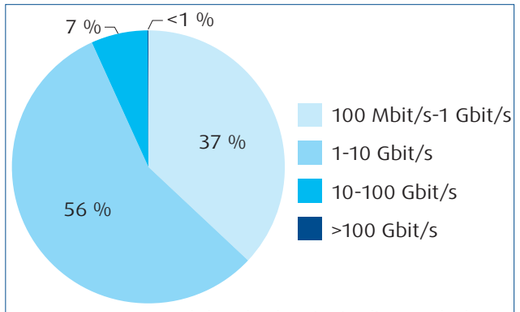
Palvelunestohyökkäykset

Palvelunestohyökkäysten voimakkuudet ovat kasvaneet vuonna 2016. Lisäksi viime vuosina on yleistynyt rahan kiristäminen palvelunestohyökkäysuhkailuilla.

Volyymiennätykset uusiksi

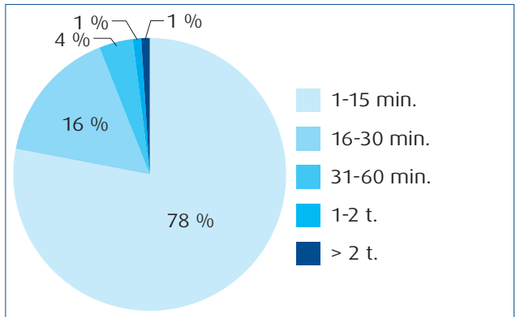
Mirai-bottiverkon tekemät hyökkäykset lokakuussa 2016 saivat kansainvälisesti paljon huomiota lyömällä aiemmat palvelunestohyökkäysliikenteen volyymiennätykset yli terabitin sekuntinopeudella toimivilla hyökkäyksillään. Mirai aiheutti häiriöitä mm. erään suurikapasiteettisten nimipalveluiden tarjoajan toiminnassa, joka näkyi monien kansainvälisesti tunnettujen verkkosivujen, kuten Twitterin, Redditin ja Netflixin toimimattomuutena.

Myös Suomeen osui muutamia erittäin voimakkaita, liikennevolyymiltään yli 100 gigabittiä sekunnissa, olevia palvelunestohyökkäyksiä (kuva 1). Tyypillinen



Kuva 1. Suomessa nähdään kuukausittain yli 500 palvelunestohyökkäystä, joista yli puolet on voimakkuudeltaan yli 1 Gbit/s. (Lähde: Telia Company)

hyökkäys on kooltaan muutamia gigabittejä sekunnissa. Tällaisia nähtiin vuonna 2016 Suomessa tuhansia. Suurin osa hyökkäyksistä oli lyhytkestoisia eli alle 15 minuuttisia. Vain noin 2 % Suomessa nähdyistä palvelunestohyökkäyksistä kesti yli tunnin. Toisaalta lyhytkestoisia hyökkäyksiä voidaan tehdä useita peräkkäin, jolloin niiden aiheuttama kokonaisvaikutus saattaa olla pidempikestoinen. Pitkiä hyökkäyksiä saattaa siis olla enemmän kuin kuvasta 2 käy ilmi.



Kuva 2. Suomessa nähdyistä palvelunestohyökkäyksistä suurin osa kestää alle 15 minuuttia. Pidempikestoisia hyökkäyksiä osuu kuitenkin säännöllisesti myös Suomeen. (Lähde: Telia Company)

Pienempien palvelunestohyökkäysten tarkkaa lukumäärää on vaikea laskea, koska niitä on vaikea erottaa epätavallisen vilkkaasta normaalista verkkoliikenteestä.

Valtionhallinto palvelunestohyökkäysten kohteena

Suomessa nähtiin keväällä kaksi valtionhallintoa vastaan suunnattua palvelunestohyökkäysten sarjaa, joiden takana epäillään olevan eri tekijät. Hyökkäykset aiheuttivat häiriöitä mm. valtion virastojen ja ministeriöiden verkkosivujen toimintaan. Poliisi on ottanut molempien palvelunestohyökkäyssarjojen takana olevat epäillyt kiinni. Lokakuussa valtionhallinnon palveluita vastaan hyökättiin kolmannen kerran, kun mm. Vetuma-tunnistuspalvelussa ja Kelan Kanta-palvelussa oli palvelunestohyökkäysten aiheuttamia ongelmia, jotka häiritsivät myös sähköisten reseptien toimintaa.

Palvelunestohyökkäykset huomioitava riskiarvioissa

Palvelunestohyökkäyksen tekeminen on rikollisille helppoa, mutta niiden torjuminen on kohteena oleville organisaatiolle kallista. Palvelunestohyökkäykset eivät onneksi vaaranna palvelun sisältämiä tietoja, joten pysyvää teknistä tai tiedollista haittaa niistä ei koidu. Sen sijaan palvelukatkon aiheuttamat imagolliset ja rahalliset haitat voivat olla merkittäviä. Koska palvelunestohyökkäyksiä nähdään Suomessakin päivittäin, on yritysten ja muiden organisaatioiden syytä ottaa ne huomioon omassa riskiarviossaan.

Palvelunestohyökkäyksiltä suojautuminen on tehokkainta tehdä jo verkkopalveluiden suunnitteluvaiheessa. Lisätietoja palvelunestohyökkäyksistä suojautumisesta voi lukea Viestintäviraston Kyberturvallisuuskeskuksen Ohjeesta 3/2016.

https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohje32016palvelunestohyokkaystenehkaisyjatorjunta.html

Palvelunestohyökkäyksen anatomia

Tyypillisesti palvelunestohyökkäykset toteutetaan suuntaamalla kohteeseen tarkoitettu hyökkäysliikenne lähtemään lukuisista lähteistä samaan aikaan. Liikenteen lähteenä on yleensä tavallisten kotikäyttäjien ja organisaatioiden verkkoon kytkemiä laitteita, jotka on joko otettu haltuun tietomurron avulla tai niiden tarjoamien verkkopalveluiden toiminnallisuuksia käytetään välikappaleena hyökkäyksessä.

Tietomurron avulla haltuun otetuista tietokoneista tai muista älylaitteista koostuvien laitteiden joukkoa kutsutaan bottiverkoksi. Esimerkiksi Mirai-bottiverkko koostuu kymmenistä tuhansista eri maissa haltuun otetuista esineiden internet -laitteista (IoT), kuten verkkokameroista.

Palvelimen normaalien toiminnallisuuksien, kuten DNS:n tai Wordpress pingback:n hyödyntämistä hyökkäyksen välikappaleena kutsutaan reflektiohyökkäykseksi. Reflektiohyökkäyksessä palvelimille lähetetään kysely, jonka lähettäjäksi on väärennetty uhrina oleva kohde. Palvelin luulee siis vastaavansa normaaliin kyselyyn, mutta koska lähdeosoite on väärennetty, todellisuudessa vastaus menee uhrina olevaan tietojärjestelmään. Reflektoreihin ei siis ole murtauduttu, vaan niiden normaalia toiminnallisuutta vain käytetään väärin. Reflektiohyökkäyksessä suositaan protokollia, joiden vastauspaketit ovat huomattavasti kyselyitä suurempia, jolloin reflektoreina olevat palvelimet vahvistavat hyökkäystehoa.

Uhka-arvio: **Palvelunestohyökkäykset**

	Kansalaiset	**Yritykset**	**Valtio**
Huomio/Häirintä	Käyttäjille palvelunestohyökkäykset häiritsevät arkea palvelujen saatavuuden häiriintymisenä.	Otettava riskiarviossa huomioon	Otettava varautumisessa huomioon
Raha	Voi vaikuttaa hetkellisesti rahan saatavuuteen verkkopalveluiden kautta, mutta ei uhkaa rahaa.	Kiristysyrityksiä on, mutta eivät vuonna 2016 johtaneet hyökkäyksiin. Verkkopalvelun käytön estyessä voi vaikuttaa kaupankäyntiin.	Kiristysyrityksiä on, mutta eivät vuonna 2016 johtaneet hyökkäyksiin.
Tieto			
Väliresurssi	Käyttäjien suojaamattomat IoT-laitteet muodostavat isot volyymit.	Suojaamattomat IoT-laitteet	Suojaamattomat IoT-laitteet

Ei uhkaa · Lievä uhka · Haittaava uhka · Vakava uhka

Oikean alakulman väri kertoo vuoden 2015 tilanteen.

Verkkojen häiriöt

Kotimaisten viestintäverkkojen yleistilanne on melko hyvä. Viestintävirasto sai teleyrityksiltä ilmoitukset yhteensä 151 merkittävästä toimivuushäiriöstä. Niistä vakavimpia ja laajimpia oli noin 20, mikä on selvästi enemmän kuin vuonna 2015.

Vikaantuneet laitteet yleisin häiriön syy

Vikaantuneet laitteet aiheuttavat eniten häiriöitä, yli kaksi kertaa enemmän kuin sähkökatkot tai ohjelmistoviat, jotka ovat seuraavaksi yleisimpiä syitä. Myös kaapelikatkot sekä päivitys- ja muutostyöt olivat melko yleisiä häiriöiden syitä.

Vakavista häiriöistä kärsivät eniten kaapeli- ja antenni-TV-palvelut sekä matkaviestinverkon palvelut (puhe, data, tekstiviestit). Alkuvuodesta hätätekstiviestien toimivuudessa havaittiin vakavia häiriöitä. Vakaviksi häiriöiksi luokitellaan viat, jotka vaikuttavat vähintään 100 000:aan puhelin- ja internetpalvelujen käyttäjään tai 300 000:aan tv- ja radiopalvelujen käyttäjään vähintään puolen tunnin ajan.

Elokuun lopulla Rauli-kesämyrsky katkoi sähkö- ja ja aiheutti häiriöitä matkaviestinverkossa Keski- ja Itä-Suomesta Etelä-Suomeen ulottuvalla alueella. Puhelu- ja datapalvelut pätkivät lähes kaksi vuorokautta, mutta vakavilta vioilta vältyttiin. Häiriöt vaikuttivat pienehköillä alueilla ja koskivat enintään 10 000 henkilöä yhtäaikaisesti.

Soneran häiriöille ei selvityksessä löytynyt yksittäistä tekijää

Vuonna 2015 ja 2016 Soneran verkoissa ja -palveluissa oli tavanomaista enemmän häiriöitä. Viestintävirasto selvitti niiden syitä yhdessä Soneran kanssa. Selvityksessä ei tullut ilmi teletoimintaa koskevien määräysten laiminlyöntejä. Sonera ja Viestintävirasto tunnistivat joitakin parannuskohteita, joiden kehittymistä seurataan.

Viestintäpalveluiden häiriöt

Tammikuu	19.1.2016	Soneran matkapuhelin- ja tekstiviestipalveluiden valtakunnallinen häiriö.
Helmikuu	10.2.2016	DNA:n matkapuhelinpalveluissa ja kiinteän verkon internetpalveluissa häiriöitä pääkaupunkiseudulla.
Maaliskuu	15.2.2016	Soneran matkapuhelin- ja tekstiviestipalveluiden valtakunnallinen häiriö.
Huhtikuu	22.3.2016	Soneran tekstiviestipalveluissa ja tietyissä kiinteän puhelinverkon palveluissa valtakunnallisia häiriöitä.
Toukokuu	28.4.2016	Digitalla häiriö antenni-TV-lähetyksissä Lahden seudulla.
Kesäkuu	27.8.2016	Rauli-myrsky katkoi viestintäyhteyksiä.
	10.9.2016	Soneralla häiriöitä matkapuhelinpalveluissa Etelä- ja Kaakkois-Suomessa.
Heinäkuu	7.11.2016	Soneran matkapuhelin- ja tekstiviestipalveluiden valtakunnallinen häiriö.
Elokuu	9.11.2016	Digitalla kaksi samanaikaista radion ja antenni-TV:n lähetyshäiriötä Itä-Suomessa sekä Pohjois-Suomessa ja Lapissa.
Syyskuu	17.11.2016	Digitalla häiriö antenni-TV-lähetyksissä Turun seudulla.
Lokakuu	21.11.2016	Digitalla häiriö antenni-TV-lähetyksissä Länsi-, Keski-, Itä- ja Pohjois-Suomessa ja Lapissa.
Marraskuu	28.11.2016	Soneran GSM-verkon palveluiden häiriö Pohjois-Pohjanmaalla, Pohjanmaalla, Satakunnassa, Pirkanmaalla ja Jyväskylän seudulla.
Joulukuu	30.12.2016	Soneran GSM-verkon palveluiden häiriö Pohjois-Pohjanmaalla, Pohjanmaalla, Satakunnassa, Varsinais-Suomessa, Pirkanmaalla, Etelä-Savossa ja Kymenlaaksossa.

Uhka-arvio: **Verkkojen häiriöt**

	Kansalaiset	**Yritykset**	**Valtio**
Huomio/Häirintä	Oma tavoitettavuus	Organisaation sisäinen viestintä	Palvelujen saatavuus, oma tavoitettavuus
Raha	Palvelujen saatavuus	Palvelujen saatavuus, oma tavoitettavuus	Palvelujen saatavuus, oma tavoitettavuus
Tieto	Hätäpuhelut, estää viestintää	Estää viestintää	Hätäpuhelut, estää viestintää
Väliresurssi			

Ei uhkaa · Lievä uhka · Haittaava uhka · Vakava uhka

Oikean alakulman väri kertoo vuoden 2015 tilanteen.

Uhka-arvion muutokset viime vuodesta: Suurhäiriötilanteita on ollut entistä vähemmän, ja ihmiset ja organisaatiot ovat oppineet tulemaan paremmin toimeen toimivuushäiriötilanteissa.

Esineiden internet (IoT)

Kun internetverkko laajentuu laitteisiin ja koneisiin, joita voidaan ohjata, mitata ja sensoroida internetin yli, puhutaan esineiden internetistä (Internet of Things, IoT). Vuotta 2016 voidaan pitää IoT:n läpimurtona hyvässä ja pahassa.

Tietoturvan laiminlyönti ei herätä luottamusta

IoT esiintyi otsikoissa niin uusien käyttötarkoitustensa kuin myös tietoturvaongelmiensa vuoksi. Tietoturva on huomioitava, jos halutaan saavuttaa IoT:n monipuoliset mahdollisuudet, sillä suojaamattomat laitteet ja ratkaisut vähentävät käyttäjien luottamusta digitaalisiin hyödykkeisiin.

IoT-laitteiden tietoturvassa olennaista on laitteiden fyysinen ja niiden tietoliikennekomponenttien turvallisuus sekä niissä käytettävien ohjelmistojen turvallisuus. Puutteellinen tietoturva altistaa internetiin kytketyt laitteet rikolliselle hyödyntämiselle, esimerkiksi palvelunestohyökkäyksissä valvontakameroiden ja automaatiolaitteiden avulla.

Käyttäjät tietämättään laitteen tietoturvasta vastuussa

IoT-laitteiden käyttäjät harvoin tietävät laitteensa haittaohjelmatartunnasta. Usein tartunta ei näy laitteen toiminnassa, vaikka se olisi osa hyökkäykseen valjastettua laiteverkostoa. Toisinaan IoT-laite ei kuitenkaan toimi sille tarkoitetulla tavalla, koska se kuormittuu liikaa.

Merkittävä haaste on nk. ”minimum viable product/service” -ajattelu. Tämä tarkoittaa sitä, että markkinoille tuodaan mahdollisimman edullisia ratkaisuita, joiden tietoturvaominaisuudet ovat puutteelliset. Ongelma koskettaa erityisesti kuluttajia, koska heille suunnatuissa laitteissa tietoturva on usein erittäin kehno, eivätkä kuluttajat usein osaa tai haluakaan varmistua laitteen tai ratkaisun tietoturvasta tai sen varmistavista toimenpiteistä, kuten ohjelmistopäivityksistä.

Yksittäisiä IoT-laitteita, joissa oli heikko tietoturva, murrettiin ja valjastettiin osallistumaan palvelunestohyökkäyksiin ja roskapostituksiin. Vuonna 2016 tuli esiin tapauksia, joissa laitteiden omistajille aiheutettiin kustannuksia lähettämällä laitteista viestejä maksullisiin ulkomaisiin numeroihin. Näissä tapauksissa aiheutuneet kustannukset nousivat jopa kymmeneen tuhanteen euroon.

Uhka-arvio: **Esineiden internet**

	Kansalaiset	**Yritykset**	**Valtio**
Huomio/Häirintä	Suojaamattomien kuluttajalaitteiden häiriintyminen haittaohjelmien ja/tai haitallisen liikenteen vaikutuksesta. Kuluttajille suunnattujen palvelujen häiriintyminen palvelunestohyökkäysten seurauksena.	Organisaatioiden liiketoiminnan häirintä palvelunestohyökkäyksillä. Työntekijöiden omien IoT-laitteiden liittäminen yrityksen verkkoon.	Suuret palvelunestohyökkäykset uhkaavat yhteiskunnan elintärkeitä toimintoja. Suomeen vaikuttavat hyökkäykset voivat tapahtua myös Suomen ulkopuolella.
Raha	Kiristyshaittaohjelmien levittäminen kotitalouksien IoT-laitteisiin.	Kiristys- ja muiden haittaohjelmien levittäminen organisaation hallussa oleviin IoT-laitteisiin.	Kiristys- ja muiden haittaohjelmien levittäminen organisaation hallussa oleviin IoT-laitteisiin.
Tieto	Kuluttajien näkyvyys IoT-laitteiden keräämään tietoon ja sen säilytykseen vähenee. Kuluttajien terveystiedot rikollisten mielenkiinnon kohteena.	IoT-laitteiden keräämät tietovarannot tietomurtojen kohteena.	IoT-laitteiden keräämät tietovarannot tietomurtojen kohteena.
Väliresurssi	Suojaamattomien kuluttajalaitteiden käyttö palveluihin ja organisaatioihin kohdistettuihin palvelunestohyökkäyksiin.	Suojaamattomien laitteiden käyttö palveluihin ja muihin organisaatioihin kohdistettuihin palvelunestohyökkäyksiin. Suojaamattomat IoT-laitteet voivat muodostaa hyökkääjälle pääsyn yrityksen sisäverkkoon.	Suojaamattomien laitteiden käyttö palveluihin ja muihin organisaatioihin kohdistettuihin palvelunestohyökkäyksiin. Suojaamattomat IoT-laitteet voivat muodostaa hyökkääjälle pääsyn yrityksen sisäverkkoon.

Ei uhkaa | Lievä uhka | Haittaava uhka | Vakava uhka

Oikean alakulman väri kertoo vuoden 2015 tilanteen.

Tietoturvakehitystä 2016

NIS-direktiivi nostaa yhteiskunnan kriittiset toimijat esiin

Euroopan unionin verkko- ja tietoturvadirektiivi tuli voimaan elokuussa 2016. EU:n jäsenvaltioiden on saatettava säännökset osaksi kansallista lainsäädäntöä 9. toukokuuta 2018 mennessä. Direktiivi velvoittaa jäsenvaltiot määrittämään keskeiset palvelun tarjoajat niiltä aloilta, jotka ovat kriittisiä yhteiskunnan toiminnan kannalta. Näitä ovat energia, liikenne, pankkiala, finanssimarkkinoiden infrastruktuurit, terveydenhuoltoala, juomaveden toimittaminen ja jakelu sekä digitaalinen infrastruktuuri.

Jäsenvaltioiden on velvoitettava keskeiset palvelun tarjoajat sekä tietyt digitaalisten palvelujen tarjoajat varautumaan verkko- ja tietoturvallisuusriskeihin kattavasti. Lisäksi niiden on raportoitava palveluitaan vaarantavista turvallisuuspoikkeamista kansallisille viranomaisille.

Liikenne- ja viestintäministeriö asetti direktiivin kansallisen täytäntöönpanon tueksi työryhmän, jossa on edustettuna direktiivin soveltamisen kannalta keskeiset valtionhallinnon toimijat ja sidosryhmät. Työryhmän työn on tarkoitus valmistua helmikuun 2017 loppuun mennessä.

Tunnistuslakihanke tähtää kohti toimivaa luottamusverkostoa

Viestintävirasto on jatkanut ponnistuksiaan vahvan sähköisen tunnistamisen ja uusien sähköisten luottamuspalveluiden tarjonnan edistämiseksi. EU:n eIDAS-asetuksen (EU(910/2014) ja kansallisen tunnistus- ja luottamuspalvelulain (617/2009) muutosten täytäntöönpanoa on työstetty yhteistyössä toimialan yritysten ja muiden viranomaisten kanssa. Työ tähtää kansallisen luottamusverkoston käynnistymiseen 1.5.2017.

Luottamusverkoston tarkoitus on tehdä tunnistusvälitys jäseniensä välillä mahdolliseksi niin, että asiointipalvelut voisivat hankkia tunnistuspalveluita keskitetysti välityspalveluilta. Teknistä ja sopimuksellista yhteistoimintaa tukevat uusittu Viestintäviraston tunnistus- ja luottamuspalvelumääräys 72/2016 M, suositukset rajapintamäärittelyistä ja suositus sopimusehtoja ohjaavista käytännesäännöistä.

Asetuksen täytäntöönpano edistyy EU:n jäsenvaltioiden ja komission asiantuntijayhteistyössä. Vuoden 2016 aikana kansallisessa laissa ja Viestintäviraston määräyksessä on luotu raamit kiinnostuneille toimijoille, jotta ne voisivat toimia sähköisten asiointipalvelujen tarjoajina eIDAS-asetuksen mukaisesti hyväksyttyinä.

Radioviestinnän luottamuksellisuuden rajoja lievennetään

Tietoyhteiskuntakaaren 136 §:ää muutettiin lisäämällä siihen uusi 5 momentti, joka on väliaikaisesti voimassa 20.6.2016–20.6.2021. Momentin mukaan radioviestintää ja sen välitystietoja voi käsitellä tilastollisesti automaattisen tietojenkäsittelyn avulla niin, ettei yksittäistä luonnollista henkilöä voi tunnistaa tietoja käsiteltäessä tai käsittelyn tuloksesta.

Käsittelyoikeus koskee pienoismallin tai miehittämättömän aluksen kauko-ohjaukseen liittyvää radioviestintää sekä päätelaitteen ja langattoman lähiverkon tai matkaviestinverkon välistä radioviestintää yhteyden muodostamista tai ylläpitoa varten.

Lisäksi tietoyhteiskuntakaaren 3 §:n 40 kohdan välitystiedon määritelmää muutettiin siten, että radiolähettimen laji ei enää ole laissa tarkoitettu välitystieto, jonka luottamuksellisuutta 136 § säntelee.

Lievennysten avulla halutaan kokeilla, voidaanko näin kehittää uudenlaisia palveluja ja liiketoimintamalleja. Tarkoitus ei ole vaarantaa luottamuksellisuuden suojaa, joka koskee henkilöiden yksityisyyttä tai heidän viestintäänsä.

Suomen kanta muodostumassa sähköisen viestinnän tietosuojaan

Komissio on uudistamassa sähköisen viestinnän tietosuojalainsäädäntöä, E-privacy-direktiiviä, EU:n tietosuojauudistuksen mukaisesti. Se antoi uuden lainsäädäntöehdotuksen loppuvuodesta 2016. Viestintävirasto on ollut luomassa Suomen kantaa yhteistyössä Liikenne- ja viestintäministeriön kanssa. Viestintäviraston kannalta direktiivin keskeisintä sisältöä on, että viestinnän luottamuksellisuus on turvattava jatkossakin erityislainsäädännöllä. Sääntelyn halutaan olevan myös mahdollisimman teknologianeutraalia ja kilpailua edistävää.

Tietosuoja-asetus muuttaa kansallista lainsäädäntöä

EU:n yleinen tietosuoja-asetus hyväksyttiin huhtikuussa Euroopan parlamentin ja neuvoston päätöksillä. Asetus koskee henkilötietojen käsittelyä ja sisältää säännökset muun muassa rekisteröidyn oikeuksista sekä rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista.

Oikeusministeriö on käynnisti jo alkuvuodesta mittavan hankkeen toteuttaakseen asetuksen mukaiset kansalliset toimet. Muun muassa erillinen työryhmä selvittää, edellyttääkö tietosuoja-asetus kansallisen lainsäädännön muutoksia. Tarvittaessa muutostarpeista laaditaan ehdotus.

EU:n tietosuoja-asetusta ryhdytään soveltamaan jäsenvaltioissa toukokuussa 2018.

Viestintäviraston PRS-tehtävät laajenivat ja saivat lain voiman

Viestintäviraston tehtävä PRS-vastuuviranomaisena on nyt todettu laintasoisesti tietoyhteiskuntakaaressa, kun lain muutokset tulivat voimaan 20.6.2016.

Yhteiskuntakaareen lisättiin muun muassa PRS-toimintaan liittyviä säännöksiä, joissa määritellään julkisesti säännelty satelliittipalvelu, kenelle sitä voidaan tarjota ja valtuutetaan Viestintävirasto antamaan määräyksiä. Lisäksi säädetään satelliittipalveluteknologian valmistuksesta hyväksyntälautakunnan luvalla, Viestintäviraston kautta.

Omat säännöksensä ovat saaneet myös satelliittipalvelun käyttö, kehittäminen ja valmistukseen liittyvä teknologiavienti EU:hun ja sen ulkopuolelle. Viestintävirastolla on tarkastusoikeus nyt myös PRS-valmistajiin ja -käyttäjiin.

PRS-viranomaistyöryhmä on jatkanut toimintaansa kuluneena vuonna. Lisäksi sille on perustettu teknінen alatyöryhmä, joka aloittelee toimintaansa vuoden 2017 lopulla.

Hyväksyttyjä arviointilaitoksia on nyt kaksi

Viestintävirasto hyväksyi tietoturvallisuuden arviointilaitokseksi Nixu Certification Oy:n 2.9.2016. Nyt Viestintäviraston hyväksymiä tietoturvallisuuden arviointilaitoksia on kaksi, sillä KPMG IT Sertifiointi Oy hyväksyttiin jo vuonna 2014. Vuonna 2016 on myös päivitetty valvontaa koskevia osioita Viestintäviraston tietoturvallisuuden arviointilaitoksille tarkoitetussa ohjeessa.

Viranomaisen tuotehyväksynnät kiinnostavat edelleen

Viestintävirasto tutkii ja hyväksyy salaustuotteet, joita käytetään turvallisuusluokitellun ja salassa pidettävän tiedon käsittelyyn kansainvälisten sopimusten mukaisesti. Kansallisen viranomaisen hyväksyntä avaa salaustuotteita valmistaville yrityksille ovia kansainvälisille markkinoille.

Vuonna 2016 hyväksynnän saivat seuraavat salaustuotteiden uudet versiot:

- Insta SafeLink, VPN-tuote
- Forcepoint Stonesoft NGFW, VPN-tuote
- Deltagon Sec@GW, sähköpostin salausjärjestelmä

Tällä hetkellä Viestintävirastossa on useita käynnissä olevia arviointeja, mikä kertoo suomalaisten yritysten kiinnostuksesta hyväksyttää tuotteitaan viranomaisella. Hyväksynnöistä tiedotetaan niiden valmistumisien jälkeen.

Yhteystietojen luovutuspyynnöt ja maksuvaatimukset lisäsivät yhteydenottoja

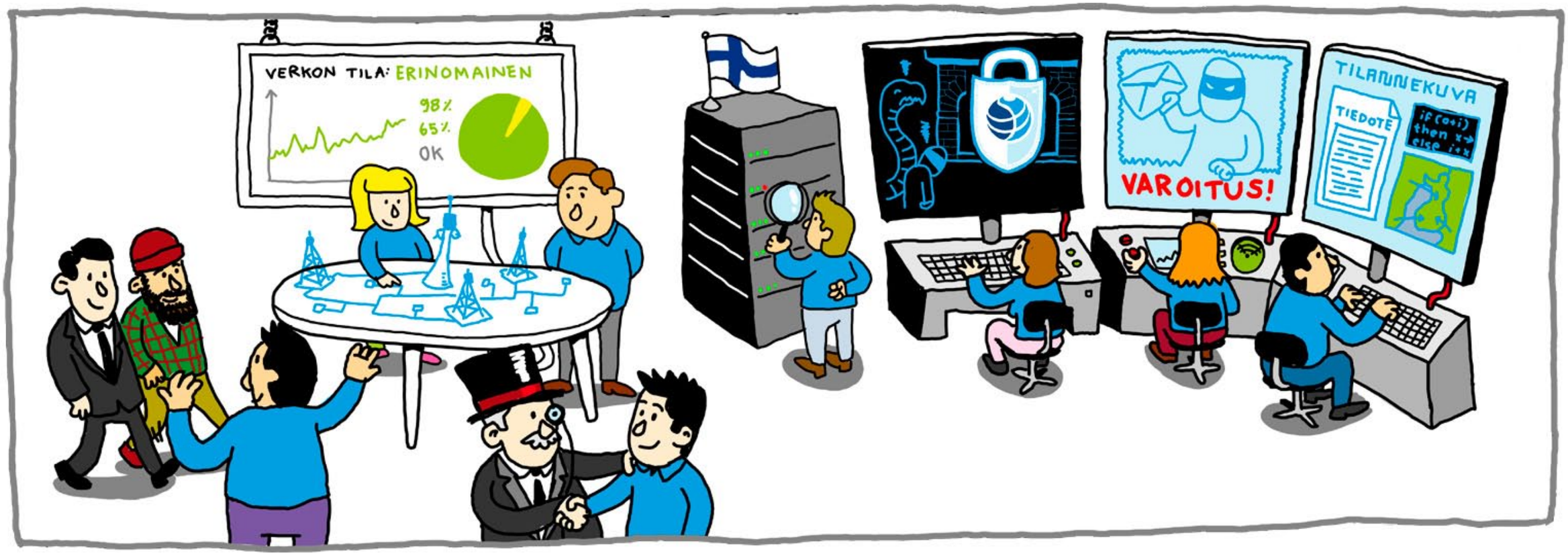
Hakemukset markkinaoikeudelle teleliittymän yhteystietojen saamiseksi kasvoivat merkittävästi.

Tietopyyntöjä teleyrityksille on tehty kuluneena vuonna kymmeniä tuhansia kappaleita. Hakemusten ja tietopyyntöjen taustalla on tekijänoikeuslailla suojatun materiaalin, esimerkiksi elokuvan, laiton jakaminen vertaisverkossa.

Viestintävirastokin sai lukuisia yhteydenottoja, joissa kirjeen ja maksuvaatimuksen saaneet ovat kyselleet syytä vastaanottamaansa postiin.

Teleyritykset puolestaan ovat ottaneet yhteyttä Viestintävirastoon selvittääkseen asiakkaidensa mahdollisuuden tarkistaa IP-osoitteen ja aikaleiman oikeellisuuden, jotka ovat markkinaoikeudenpäätöksen perusteena.

10 tietoturvanäkymää vuodelle 2017



1 Teknologian kehitys jatkuu räjähdysmäisesti

Teknologian räjähdysmäinen kehitys synnyttää uusia tuotteita palveluita ja toimintamalleja kiihtyvää tahtia. Uudet mallit tuovat mukanaan myös uhkia, joita vastaan ei vielä osata suojautua.

2 Häiriöt osoittavat riippuvuutemme tietoverkoista

Riippuvuutemme toimivista tietoverkoista ja -järjestelmistä kasvaa edelleen. Verkottuneessa yhteiskunnassa tietoverkkohäiriöiden vaikutukset ketjuuntuvat ja ulottuvat ennakoimattomiin paikkoihin yli verkko- ja organisaatiorajojen. Häiriöt vaikuttavat vakavasti yhteiskunnan toimintaan, turvallisuuteen ja talouteen.

3 Uhkat omissa järjestelmissä tunnistetaan heikosti

Suomalaisilla organisaatioilla on edelleen vaikeuksia havainnoida kyberuhkia riittävän hyvin. Moni suomalainen julkishallinnon organisaatio ja yksityinen yritys tulee olemaan tietämättään vakavan tietoturvaloukkauksen kohteena. Organisaatiot eivät tunne riittävästi omia tietojärjestelmiään, jotta voisivat suojella niitä tehokkaasti. Kaikkia tarvittavia lokitietojakaan ei kerätä ja seurata.

4 Tietoturvaosaamisesta on pulaa

Tietoturvan merkitys liiketoiminnalle ymmärretään entistä paremmin ja siihen liittyvän osaamisen kysyntä lisääntyy. Tietoturvaosaamisen tarjonta ei todennäköisesti ennätä kasvaa kysynnän mukaan ja osaamista ei ole välttämättä tarjolla riittävästi kaikille tarvitsijoille.

5 Kyberrikollisuus jatkaa ammattimaistumista

Rikollisten operaatiot, esimerkiksi kiristyshaittaohjelmakampanjat ja erilaiset huijaukset, ovat yhä pitkäkestoisempia ja korkeatasoisempia. Kohteena ovat kansalaiset, yritykset ja valtionhallinnon organisaatiot. Rikollisen toiminnan kaupallistuminen jatkuu; rikolliset myyvät palveluina muun muassa palvelunestohyökkäyksiä, tietomurtoja ja haittaohjelmia. Näin saatuja tietoja voidaan myydä tai käyttää uhrin kiristykseen.

6 Verkkovakoilu lisääntyy

Verkkovakoilulla vaikutetaan ja hankitaan tietoa poliittiseen päätöksentekoon, kaupalliseen kilpailutukseen ja tuotekehitykseen. Organisaatioiden kyky havaita itseensä kohdistuvaa verkkovakoilua on huono.

7 IoT palvelunestohyökkäysten käyttövoimana

IoT-laitteiden yleistyminen voimistaa palvelunestohyökkäyksiä. Voimakkailla hyökkäyksillä estetään tai häiritään suosittujen kansainvälisten verkkopalvelujen käyttöä. Hyökkäysten vaikutukset näkyvät myös yllättävinä sivuvaikutuksina palvelunestohyökkäysten resursseiksi valjastettujen laitteiden käyttäjille.

8 Kiristyshaittaohjelmat monipuolistuvat

Rikolliset kohdentavat kiristyshaittaohjelmiaan toimiala- ja yrityskohtaisesti yhä enemmän. Haitakkeilla pyritään salaamaan myös varmuuskopiot. Hinta asetetaan organisaation maksukyvyn mukaan. Kiristyshaittaohjelmia levitetään perinteisten menetelmien (sähköpostin liitetiedostot ja murretut verkkosivut) lisäksi hyökkäämällä suoraan järjestelmiin tietomurtojen ja haavoittuvuuksien avulla.

9 Kohdistetuilla hyökkäyksillä halutaan rahaa

Aiemmin kohdistetuilla haittaohjelmahyökkäyksillä tavoiteltiin pääasiallisesti tietoa. Kohteena on jatkossa myös raha, koska maksuliikenteen ja valuuttavirtojen hallinta on siirtynyt lähes täysin verkkoon. Uusilla kohdistetuilla haittaohjelmilla tavoitellaan suurta taloudellista voittoa.

10 Mobiililaitteiden tietoturvaa koetellaan

Tietoa käsitellään pääasiassa mobiililaitteilla, joista tulee yhä kiinnostavampi kohde rikollisille. Vuoden 2017 aikana tullaan näkemään yhä laajempia ja kehittyneempiä mobiililaitteille suunnattuja haittaohjelmakampanjoita.

Viestintävirasto

Tavoitat meidät
sähköpostitse: cert@ficora.fi
asiakaspalvelu: 0295 390 230

Seuraa uutisia ja liity postituslistalle:
www.viestintavirasto.fi/kyberturvallisuus

Seuraa meitä:
www.facebook.com/NCSC.fi
twitter.com/certfi

Ilmoita meille:
cert@ficora.fi

Yhteystiedot:

Viestintävirasto
PL 313
Itämerenkatu 3 A
00181 Helsinki

Puh: 0295 390 100 (vaihde)

kyberturvallisuuskeskus.fi
viestintävirasto.fi