



Kyberturvallisuuskeskuksen vuosikatsaus

Vuosi 2014

Sisällys

Johdanto	4
Tietoturvavuoden keskeiset havainnot ja toimet	5
Vuoden 2014 merkittävimmät tietoturvailmiöt	6
Verkkopankkitietojen kalastelu oli aktiivista ja taitavasti toteutettua.....	6
Tietoja varastavat haittaohjelmat.....	7
Windows XP:n tuki loppui.....	8
Pankkeihin kohdistuneet palvelunestohyökkäykset	8
Internetin perusrakenteet horjuivat	10
Heartbleed	10
Shellshock.....	12
WordPress.....	13
Kohdistettujen hyökkäysten uhka otettava vakavasti	14
Havainnot vakoiluhaittaohjelmista lisääntyneet	14
Energiasectoriin kohdistunut Energetic Bear/Havex	15
Valtioilta tietoja varastava Snake	15
Sandworm ja Windowsin nollapäivähaavoittuvuus	16
Kohdistettujen haittaohjelmahyökkäysten torjunta	16
HAVARO on osa kyberturvallisuuden tilannekuvaa	18
Keskeiset kumppanit ja asiakkaat	18
HAVARO:n toteutuksesta	18
Robotin jälki on harmaata, ihminen lisää värin.....	19
HAVARO ja vuoden isot tietoturvatapaukset	19

Suomalaiset tietoverkot edelleen maailman puhtaimpien joukossa	21
Työjuhta Autoreporter	22
Haittaohjelmahavainnoista 85 % peräisin yhden teleyrityksen verkosta	24
Viestintäverkkojen häiriöiden määrä väheni	25
Elisan häiriö johtui virheistä - Soneran ohjelmistoviasta	25
Tarkastustoiminta	26
Teknisissä tarkastuksissa havaittiin puutteita	26
Häiriöiden käyttäjätiedotuksen valvonta	27
Tuotehyväksynät	27
Viranomaisten järjestelmien tarkastukset	27
Tietoyhteiskuntakaari ohjasi parantamaan määräyksiä	29
Tietoturvamääräys	29
Häiriötilannemääräys	29
Varautumisen ohjaus	30
SOPIVA-suositukset	31
Kansallisen tietoturvallisuuden kehittäminen	32
Neuvontaa tunnistamistietojen käsittelyoikeuksista ja yksityisyyden suojasta	32
Suositus kansainvälisesti toteutetun palvelun tietoturvasta tiedottamiseen	32
Kyberturvallisuuskeskuksen teemakuukaudet	32
Kansainvälinen yhteistyö	33
CERT-yhteistyö	33
NCSA-yhteistyö	34
Säätelyyn liittyvä kansainvälinen yhteistyö	34

Johdanto

Vuoden 2014 tietoturvaongelmat koskivat laajasti verkon käyttäjiä ja koostuivat monitasoista kybermaailman uhkista

Keväällä alkanut pankkitunnusten huijauskampanja kiusasi kuluttajia kuukausien ajan. Onnistuimme tiiviillä viranomaisten ja yritysten yhteistyöllä vähentämään merkittävästi taloudellista haittaa, kun huijaussivustot saatiin ripeästi tietoon ja irrotettua verkosta.

Huhtikuussa löytyi internetin vuosikymmeniin merkittävin haavoittuvuus, Heartbleed. Kyberturvallisuuskeskus seurasi hyväksikäyttöyrityksiä Suomessa ja muualla maailmassa.

Maailmalla paljon julkisuutta saaneiden kohdistettujen hyökkäysten vaikutukset heijastuivat myös Suomeen. Välitimme kuluneen vuoden aikana kohdistettuihin hyökkäyksiin liittyen tietoja vähintään tuplamäärän edellisvuoteen nähden. Suuntaus vaikuttaa olevan pysyvä ja laajenemassa entistä moninaisimpiin toimijoihin.

Kuluneen vuoden aikana Viestintävirasto sai teleyrityksiltä noin 150 ilmoitusta merkittävästä yleisen viestintäverkon häiriöistä. Näistä 14 luokiteltiin vakaviksi. Häiriöt jakaantuivat melko tasan TV- ja radiopalvelujen katkoksien sekä matkaviestinverkon häiriöiden kesken.

Tietojärjestelmiä tai tietoliikennejärjestelmiä, joissa käsitellään viranomaisen turvaluokiteltua tietoa, tuli vuoden aikana 2014 Kyberturvallisuuskeskuksen arvioitavaksi tai hyväksyttäväksi 13 kappaletta. Salaustotehyväksyntäprosessin hyväksytysti läpäisi kaksi tuotetta ja kaksi tuotetta läpäisi tuoteturvallisuusarvioinnin.

Kyberturvallisuuskeskus antoi lokakuussa 2014 KPMG IT Sertifiointi Oy:lle hyväksynnän toimia tietoturvallisuuden arviointilaitoksista annetun lain mukaisena arviointilaitoksena.

Tietoturvallisuuteen liittyviä määräyksiä selkeytettiin ja ryhmiteltiin uudelleen. Lähtötilanteessa Kyberturvallisuuskeskuksen toimialalle kuuluvia määräyksiä oli yhteensä 13 kappaletta. Ne korvautuivat seitsemällä uudella tai päivitetyllä määräyksellä.

Kansallista havainnointikykyä vahvistettiin kehittämällä valtionhallinnolle tuotettavia GovCERT- ja GovHAVARO-palveluja. Vuonna 2015 palvelut kattavat jo lähes koko valtionhallinnon. Lisäksi Viestintävirasto osallistuu valtionhallinnon häiriönhallintatoimintaan (VIRT) tuottamalla kyberturvallisuuden tilannekuvaa.

Kyberturvallisuuskeskus vastasi asiantunteumuksella useisiin satoihin mediahaastatteluihin ja julkaisi yli kolmesataa tietoturvaan liittyvää tuotetta erilaisiin tarpeisiin.

Antoisia lukuhetkiä vuosikertomuksen parissa.

Helsingissä 2.2.2015

Kirsi Karlamaa

Johtaja
Kyberturvallisuuskeskus
Viestintävirasto



Tietoturvuuden keskeiset havainnot ja toimet

1. Tietojen kalastelu yleistyy

Verkkohuijarien toiminta on entistä ammattimaisempaa. Uhreja voidaan lähestyä sähköpostin ja verkkosivun lisäksi myös tekstiviestein ja puheluin. Ihmisten hyväuskoisuus, viestien hyvä kieliasu tekee tietojen kalastelusta entistä tehokkaampaa. Yleistä tietoa henkilökohtaisten tietojen kalastelusta on pidettävä jatkuvasti yllä.

2. Havainnot vakoiluhaittaohjelmista lisääntyvät

Suomalaisissa organisaatioissa on puutteellinen havainnointikyky kohdistettujen haittaohjelmien havaitsemiseksi. Suomen teknologiayritysten korkea innovatiivisuus ja valtionhallinnon toimivuus ovat vakoilulle mielenkiintoisia kohteita. Havainnointikyvyn kasvattaminen ja yhteistyön lisääminen ovat oleellinen osa suojautumista.

3. Palvelunestohyökkäyksien voima kasvaa

Palvelunestohyökkäyksien voima on kasvanut merkittävästi viime vuosina. Globaalilla tasolla raportoidaan kuukausittain yli 100 Gbit/s hyökkäyksistä. Yli 50 Gbit/s hyökkäykset voivat aiheuttaa runkoverkkotason ongelmia internetpalvelujentarjoajille Suomessa. Torjunnassa on merkittävässä asemassa organisaatioiden kriittisten verkkopalveluiden ja tietoliikennejärjestelyiden selvittäminen. Selvityksen perusteella tulisi tehdä riskikartoitus, jonka jälkeen voidaan toteuttaa toiminnan kannalta oikein mitoitettut tietoturvatoinenpiteet.

4. Kansallinen havainnointikyky paranee

Viestintävirasto on laajentanut sekä kehittänyt vakavien tietoturvaloukkausten havainnointija varoituspalvelua (HAVARO) vuoden 2014 aikana. Huoltovarmuuskriittisten toimijoiden määrä kasvaa ja palvelu kattaa vuoden 2015 lopussa koko valtiohallinnon. Järjestelmä tuotti vuonna 2014 vakavia punaisia hälytyksiä 1930 kpl.

5. Teleoperaattorien toimilla on merkitystä

Teleoperaattorit pystyvät reagoimaan asiakkaiden haittaohjelmatartuntoihin. Kyberturvallisuuskeskuksen Autoreporter-työkalu keräsi yli 200 000 haittaohjelmiin ja tietoturvaloukkauksiin liittyvää havaintoa. Näiden tietojen perusteella verkkojen vastuuhenkilöt voivat toimia havaitun tietoturvuhan torjumiseksi. Microsoftin raportin mukaan Suomessa on vähiten saastuneita Windows-koneita maailmassa.

6. Suomalaisia salaustuotteita edelleen vähän

Helpoin tapa suojata yksityinen viestintä tietoverkoissa on tiedon salaaminen. Luotettavia ja helppokäyttöisiä salaustuotteita on käytössä vähänlaisesti ja kotimaisia tuotteita ei juuri lainkaan. Viranomaisilla on myös omat tarpeensa salassa pidettävän tiedon suojaamiselle kotimaisilla, viranomaiskriteerit täyttävillä, salaustuotteilla. Viranomaiskriteerit täyttävä tuote olisi myös mahdollisuus päästä EU:n markkinoille EU:n salassa pidettävän tiedon suojaamiseksi.

7. Yhteistoiminta on elinehto

Kyberturvallisuuskeskuksen vuoden aikana käsittelemien tapauksien aikana syntynyt hyvä yhteistyö sidosryhmien kanssa kannustaa entistä parempaan verkostoitumiseen. Yhteisen tilannekuvan luomiseksi jokainen tiedonjyvä on tärkeä. Kyberturvallisuuskeskus käsittelee tietoturvaloukkaukset luottamuksellisina.

Vuoden 2014 merkittävimmät tietoturvailmiöt

Tietoturvaluvuosi 2014 muistetaan Suomessa etenkin toisia haittaohjelmia lataavien haittaohjelmien, vakavien haavoittuvuuksien ja tehokkaiden huijauskampanjoiden vuotena. Merkittävistä tietoturvauhista huolimatta Suomi loisti maana, jossa on maailman vähiten haittaohjelmien saastuttamia tietokoneita - vain 0,21 % kaikista Windows-tietokoneista.

Haittaohjelmahavainnoissa erot vuosien 2013 ja 2014 välillä olivat selvät. Vuonna 2014 toisia haittaohjelmia lataavien haittaohjelmien määrä kasvoi huomattavasti, mutta roskapostia lähettävien haittaohjelmien määrä väheni murto-osaan vuoteen 2013 verrattuna.

Verkkopankkitietojen kalastelu oli aktiivista ja taitavasti toteutettua

Internetin käyttäjiin kohdistui keväästä loppukesään 2014 taidokkaasti suomeksi ja suomalaisille netinkäyttäjille laadittuja huijauksia, joilla kalasteltiin verkkopankkitunnuksia. Rikosvyyhdellä on yli 400 asianomistajaa, jotka olivat syöttäneet tunnuksensa huijaussivulle. Huijatuksi tulleet menettivät yhteensä yli puoli miljoonaa euroa.

Viestintäviraston Kyberturvallisuuskeskuksen yhteistyöverkoston ansiosta huijaussivut saatiin nopeasti suljettua. Huijauskampanja saatiin loppumaan laaja-alaisella viranomaisyhteistyöllä elokuussa. Huijaustapauksia tutkii Helsingin poliisilaitos.

Huijarit lähestyivät uhrejaan sähköpostin ja verkkosivun lisäksi poikkeuksellisesti myös tekstiviestein ja puheluin, joilla varoitettiin erääntyvästä tekaistusta laskusta ja siitä seuraavasta maksuhäiriömerkinnästä. Ihmistien hyväuskoisuus, viestien hyvä kieliasu sekä tekstiviestien ja puheluiden hyödyntäminen tekivät kalastelusta entistä tehokkaampaa. Reaaliaikaisesti tapahtuvan huijauksen aikana uhrin tiedoilla otettiin pika- vippejä tai siirrettiin rahaa heidän tileiltään rahamuulien tileille.

Viron poliisi pidätti loppukesästä huijauskampanjan pääepäilyn Tallinnassa Suomen poliisin pyynnöstä ja avustuksella. Tämän

jälkeen huijaussivustoja pystytti vielä toinen henkilö, joka otettiin kiinni muutama viikko sen jälkeen. Molemmat epäillyt on vangittu oikeuskäsittelyn ajaksi. Lisäksi tapaukseen liittyen epäillään 40 henkilöä rahanpesusta. Pidätysten jälkeen ei uusia samalla tavalla toteutettuja tietojenkalastelusivuja ole ilmennyt.

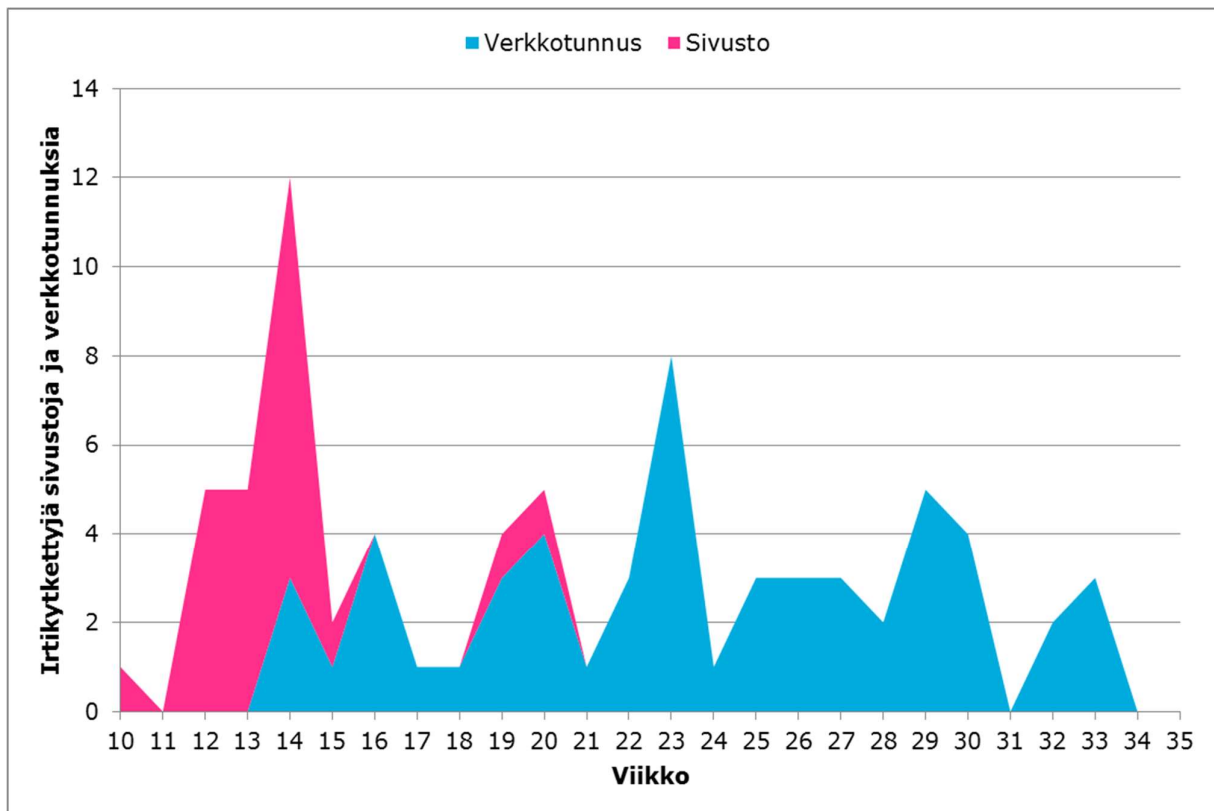
Kampanjan takana epäillään olleen suomalainen tekijä, jonka avulla huijaussivustot oli laadittu uskottaviksi.

Kyberturvallisuuskeskus osallistui kampanjan torjuntaan tuottamalla ajantasaisista tietoa, tiedottamalla asiasta sekä tekemällä aktiivisesti irtikykentäpyyntöjä tunnistetuista huijaussivustoista.

Sivustojen poistaminen verkosta hidasti huijareiden toimintaa ja pakotti heidät lähettämään yhä uusia tietojenkalasteluviestejä uusilla osoitteilla. Kyberturvallisuuskeskuksen lähettämiin irtikykentäpyyntöihin reagoitiin hyvin, sillä viive pyynnön lähettämisestä sivuston poistumiseen vaihteli minuuteista enintään muutamiin tunteihin. Kampanjaan liittyen irtikykettiin 23 huijaussivustoa ja 55 verkkotunnusta (Kuva 1).

Nettihuujaukset ovat maailmalla vanha ja vakiintunut ilmiö. Suomalaisten on aiemmin ollut usein helppo tunnistaa huujaukset, koska niiden kieli on ollut muu kuin suomi, teksti on ollut huonosti käännettyä tai huujauksessa käytetyt tuotemerkit eivät ole olleet suomalaisille tuttuja.

Suurin osa suomalaisten jatkossakin kohtaa mista nettihuujauksista tulee olemaan ulkomaista alkuperää ja toteutettu vieraalla kielellä tai koneellisesti käännetty suomenkielelle. Konekäännösten laatu on viime vuosina parantunut huomattavasti ja huujaukset ovatkin entistä uskottavamman näköisiä.



Kuva 1 Kyberturvallisuuskeskuksen pyynnöstä irti kytkettyjen suomalaisen verkkohuijauksen kampanjaan liittyneiden sivustojen ja verkkotunnusten määrät

Suomalaiset myös käyttävät entistä enemmän kansainvälisiä nettikauppoja, joiden tavaramerkkejä ulkomaiset rikolliset osaavat käyttää taitavasti hyväkseen. Nopeasti kasvavan kansainvälisen nettikaupan ja huijausten entistä paremman kielen ansiosta huijausten odotetaan muodostuvan entistä vakavammaksi uhkaksi suomalaisille.

Huijauksia ja niiltä suojautumista on käsitelty heinä-elokuun teemana Tietoturva nyt! -palstalla ¹.

Tietoja varastavat haittaohjelmat

Satunnaisten käyttäjien tietoja varastamaan pyrkivät haittaohjelmat muodostivat vuoden aikana suurimman yksittäisen uhan tavallisten käyttäjien tietoturvallisuudelle. Kyberturvallisuuskeskus välitti yli 33 000 havaintoa suomalaisissa verkoissa olevista tietoja

varastavista haittaohjelmista (noin seitsemäsosa kaikista havainnoista).

Tietoja varastavat haittaohjelmat tarttuvat samoin kuin muutkin haittaohjelmat. Käyttäjä voidaan houkutella asentamaan sähköpostin liitetiedostona tai verkosta ladattu haittaohjelma itse. Haittaohjelma saattaa päätyä käyttäjän työasemaan myös siirrettävien muistilaitteiden välityksellä. Haittaohjelmat tarttuvat myös hyväksikäyttämällä käyttöjärjestelmän ja varusohjelmien haavoittuvuuksia. Tällöin käyttäjän on tyypillisesti vierailtava haitallisella www-sivulla tai murretulla www-sivulla, jolle on sivuston ylläpitäjän tietämättä lisätty haitallista sisältöä.

Tietoja varastavat haittaohjelmat pyrkivät varastamaan muun muassa henkilötietoja ja kirjautumistietoja erilaisiin palveluihin. Va-

¹ Katso <https://www.viestintavirasto.fi/tietoturva/tietoturva-nyt/2014/07/ttn201407231408.html>

rastettuja tietoja voidaan hyödyntää jatkorkosten tekemisessä esimerkiksi ostamalla tavaroita uhrin laskuun.

Windows XP:n tuki loppui

Suosituksen Windows XP -käyttöjärjestelmän tuen päättymisen huhtikuussa 2014 vaati sitä käyttäviltä organisaatioilta ja kuluttajilta valppautta ja aktiivisia toimia tuettuun käyttöjärjestelmään siirtymiseksi. Viestintävirasto seurasi XP-päivitysten etenemistä vuoden 2014 aikana. Marraskuun lopussa XP:n osuus kaikista Windows-käyttöjärjestelmistä oli laskenut 5,2 %:iin vuoden alun 16,5 %:sta.

Microsoft Windows XP on hyvin laajalle ja pitkän aikaa käyttöön levinnyt PC-tietokoneiden käyttöjärjestelmä. Microsoftin lopetettua suunnitellusti käyttöjärjestelmän tukemisen 8.4.2014 siitä löytyneisiin haavoittuvuuksiin ei ole enää saanut korjauksia muuten kuin maksamalla niistä erikseen. Maksullisia päivityksiä ei tarjota kuluttajasiakkaille. Korjausten puuttuminen voi altistaa Windows XP:tä käyttävät tietokoneet jatkuville vakaville tietoturvaloukkauksille.

Vaikka tuen päättymisen oli julkisesti tiedossa hyvän aikaa ennakkoon, on käyttöjärjestelmän vaihtaminen kaikista Windows XP:tä käyttäneistä tietokoneista ollut suuri urakka. Haasteita vaihtoon on tuonut tietokoneiden suuren määrän lisäksi uudempien käyttöjärjestelmien entistä korkeammat vaatimukset tietokoneen suorituskyvylle, Windows XP:stä riippuvien tärkeiden sovellusten korvaaminen uusilla ja tietysti myös vaihdosta syntyvät kustannukset.

Reilut 18 % maailman kaikista PC-tietokoneista toimi Windows XP:llä joulukuussa 2013. Lokakuussa 2014 osuus oli vielä reilut 13 % eikä lasku ole nopeaa (<http://gs.statcounter.com>). Windows XP:tä käyttävissä tietokoneissa on siis edelleen haittaohjelmaepidemian ainekset.

Kaikista käyttöjärjestelmistä on vuosittain löytynyt kymmeniä haavoittuvuuksia. Windows XP julkaistiin vuonna 2001, minkä jälkeen siitä on löytynyt vuosittain keskimäärin 55 haavoittuvuutta.

Windows XP:n tietoturvapäivitysten loppumisen jälkeen julkiseen tietoon on tullut kaksi sitä koskevaa haavoittuvuutta. Teoriassa yksikin ennen tuntematon vakava haavoittuvuus Windows XP:ssä voi nyt saada aikaan laajoja haittaohjelmatartuntoja, koska samaa haavoittuvuutta voi käyttää Windows XP:llä toimivia tietokoneita vastaan loputtomasti uudelleen.

Laajoja Windows XP:n haavoittuvuuksien hyväksikäyttökampanjoita ei kuluneena vuonna todettu. Windows XP:n käyttö tietyissä organisaatioissa ja rajallisella yksityiskäyttäjien joukolla kuitenkin jatkuu yhä, joten vaikutukset voivat ulottua tulevillekin vuosille. Viestintäviraston Kyberturvallisuuskeskus suosittelee Windows XP -käyttöjärjestelmästä luopumista.

Windows Server 2003:n tuki loppuu heinäkuussa 2015

Seuraava Microsoftin valmistama käyttöjärjestelmä, jonka tuki loppuu, on Windows Server 2003. Windows Server 2003:llä toimii maailmanlaajuisesti 11 miljoonaa tietokonetta (Hewlett-Packard-yhtiön arvio toukuussa 2014).

Kyberturvallisuuskeskuksen valtiovarainministeriöltä ja Valtorilta saamien tietojen mukaan valtionhallinto ja virastot ovat varautuneet hyvin Windows Server 2003 -käyttöjärjestelmän tuen loppumiseen. Monista järjestelmistä Windows Server 2003 on jo vuoden 2014 loppuun mennessä vaihdettu muuhun käyttöjärjestelmään ja vaihdokset jatkuvat ripeään tahtiin vuoden 2015 puolella.

Pankkeihin kohdistuneet palvelunestohyökkäykset

Uudenvuodenaattona 2014 alkoi muutamia päiviä kestänyt suomalaisiin pankkeihin kohdistunut merkittävä palvelunestohyökkäyskampanja. Vaikutukset näkyivät voimakkaimpina OP-ryhmän ja Nordean verkkopankkipalveluissa.

Vaikutukset ulottuivat OP:n tapauksessa myös korttimaksuihin ja pankkiautomaattipalvelujen saatavuuteen. Kyberturvallisuuskeskus osallistui aktiivisesti hyökkäysten tekniseen selvittelyyn sekä kokonaistilannekuvan muodostamiseen.

Palvelunestohyökkäyksien voima on kasvanut merkittävästi viime vuosina. Globaalilla

tasolla raportoidaan kuukausittain yli 100 Gbit/s hyökkäyksistä. Yli 50 Gbit/s hyökkäykset voivat aiheuttaa runkoverkkotason

ongelmia internet-palveluntarjoajille Suomessa.

Internetin perusrakenteet horjuivat

Vuosikymmenen keskeisimmät haavoittuvuudet olivat Bash-komentotulkin Shellshock-haavoittuvuus sekä OpenSSL-salauskirjaston Heartbleed-haavoittuvuus. Bash ja OpenSSL ovat loppukäyttäjille yleisesti varsin tuntemattomia ohjelmistoja, mutta ne ovat osa sitä koodipohjaa, josta koko internetin selkäranka muodostuu.

OpenSSL:n, Bashin ja joukon muita ohjelmistoja päälle on rakennettu valtaosa nykyisestä tiedonsiirtoteknologiasta. Niiden ohjelmistovirheet muodostuivat vuoden 2014 aikana sellaisiksi ilmiöiksi, että niistä tullaan kuulemaan myös vuoden 2014 jälkeen. Esimerkiksi Heartbleed koski Googlea, Amazonia ja montaa muuta palveluntarjoajaa. Virheet suosituissa palveluissa vaarantavat kerralla suuren käyttäjämäärän tietoturvallisuuden.

Muitakin ohjelmistovirheitä, joita voidaan käyttää tietoturvallisuuden loukkauksiin, havaittiin vuonna 2014 runsaasti. Etenkin tietoliikenteen salausohjelmistoihin liittyneet virheet koskettivat kaikkia internetin käyttäjiä. Viestintävirasto julkaisi vuoden aikana kolme varoitusta erityisen vakavista ohjelmistohaavoittuvuuksista (Heartbleed, Shellshock ja WordPresin haavoittuvuus).

Kyberturvallisuuskeskus arvioi, että aiemmin vähälle huomiolle jääneiden keskeisten ohjelmakirjastojen ja ohjelmien tietoturvatkumukseen kiinnitetään jatkossa tarkempaa huomiota. Tällaisten haavoittuvuuksien löytäminen käynnistää tulevaisuudessakin laajoja päivityskierroksia.

Tietokoneohjelmien käyttäjien kannalta yleisesti ainoa lääke ohjelmistohaavoittuvuuksiin on ohjelmistojen päivittäminen. Keskeiset kotitietokoneiden käyttöjärjestelmät ja iso osa sovelluksista osaavat hakea itselleen päivitykset internetistä automaattisesti. Käyttäjän huoleksi jää vahtia, että tietokoneen automaattipäivitystoiminto on käytössä, ja päivitykset asennetaan, kun käyttöjärjestelmä niitä tarjoaa.

OpenSSL-kirjastossa ja Bash-komentotulkitissa ei ole tällaista sisäänrakennettua automaattista päivitysmekanismia, eikä niiden päivittämistä ole monessa paikassa automa-

tisoitu muilla keinoin. Lisäksi ne ovat käytössä suurten ihmisjoukkojen käyttämissä internetin palveluissa. Tämä nosti osaltaan Heartbleed- ja Shellshock-haavoittuvuuk-sien vakavuutta.

Heartbleed

Heartbleed tuli julki 7.4.2014. Kyseessä on haavoittuvuus eräässä versiossa avoimen lähdekoodin OpenSSL-ohjelmistokirjastosta. OpenSSL:ä käytetään hyvin yleisesti tietoliikenteen salakirjoitukseen internetissä. Kyberturvallisuuskeskus koordinoi haavoittuvuudesta tiedottamista ja tutki sen hyväksikäyttömenetelmiä.

Haavoittuvuuden löysivät toisistaan riippumatta suomalainen Codenominon sekä Googlelle työkennellyt tietoturvatutkija. Codenominon nimesi tämän OpenSSL:n "sydämenlyönti"-toimintoon (engl. "heartbeat") liittyvän haavoittuvuuden Heartbleediksi.

Haavoittuvuuden oivaltava nimi ja vetävä logo toivat runsaasti maailmanlaajuisista näkyvyyttä haavoittuvuudelle sekä suomalaiselle tietoturvaosaamiselle. Runsa julkisuus kuitenkin ruokki tässäkin tapauksessa spekulatioita julkistuksen tehneiden tahojen salatuista tarkoituseristä. Epäluulo johti poikkeukselliseen julkiseen väittelyyn haavoittuvuuden hyväksikäytön oletetusta helpoudesta ja sen myötä haavoittuvuuden todellisesta vakavuudesta.

Cloudflare esitti julkisen hakkerointihaasteen, johon Kyberturvallisuuskeskuksen tietoturva-asiantuntija osallistui. Hänen onnistui pienellä vaivannäöllä ratkaista haaste. Näin hän osoitti, että haavoittuvuuden avulla hyökkääjän on mahdollista varastaa palvelimen muistista muun muassa salausavaimia. Väittely haavoittuvuuden vakavuudesta päättyi siihen.

**Ohjelmisto-
virheet mah-
dollistavat in-
ternetin vää-
rinkäytön**

Kolme seikkaa tekee Heartbleed-haavoittuvuudesta erityisen vaarallisen:

1. Haavoittuvuutta hyväksikäyttäen salakirjoitusta tiedonsiirtoon käyttävältä palvelimelta voidaan varastaa tietoja, jotka saattavat sisältää palvelimen salaisen digitaalisen salakirjoitusavaimen. Avaimen tietävät tahot pystyvät vaivatta avaamaan kaiken kyseisen palvelimen saaman ja lähettämän liikenteen.
2. Haavoittuvuuden hyväksikäytöstä ei jää mitään jälkiä palvelimelle. Ei voida siis tietää, millä haavoittuvilla palvelimilla haavoittuvuutta on oikeasti käytetty hyväksi.
3. Haavoittuvuuden hyväksikäyttö on erittäin helppoa.

Kuluttajille vaarana oli, että heidän salaisia tietojaan, kuten terveystietoja ja salasanoja, oli mahdollista paljastaa salakirjoitetusta liikenteestä ja liikennettään salakirjoitavilta palvelimilta.

Haavoittuvuuden vaikutukset Suomessa

Kyberturvallisuuskeskus koordinoi tilannetta Suomessa kokoamalla, analysoimalla ja jakamalla tietoja haavoittuvuudesta ja sen hyväksikäytöstä. Tietoja jaettiin sekä suurelle yleisölle että kohdistetusti valtionhallinnolle ja huoltovarmuuskriittisille organisaatioille. Lisäksi Kyberturvallisuuskeskus kartoitti, mitkä .fi-verkkoalueella olevat palvelimet olivat haavoittuvia, ja otti niiden ylläpitäjiin yhteyttä korjauksen tärkeyden korostamiseksi.

Heartbleedistä uutisoitiin runsaasti muuallakin kuin tietotekniikkaan keskittyvissä tiedotusvälineissä. Haavoittuvuudesta on tullut tietoturvamailmassa nopeasti käsite: muiden ongelmien mahdollisia seurauksia verratetaan tämän tästä Heartbleedin vakavuuteen.

Oletettavasti Heartbleedin paljastumisen myötä myös muiden salauskirjastojen haavoittuvuustutkinta lisääntyi, sillä vuoden aikana kaikista yleisessä käytössä olevista salauskirjastoista löytyi huolestuttavia vikoja. Suuri haavoittuvuuksien määrä voi saada epäilemään salakirjoituksen ja tietoturvan uskottavuutta. Ilmiö osoittaa tietoturvan herkkyyden, mutta toisaalta systemaattinen testaaminen mahdollistaa ongelmien pai-

kantamisen ja korjaamisen. Vuoden seuraamusten vaikutus voikin olla päinvastainen ja tuloksena ovat todennäköisesti entistä tietoturvaisemmat ja varmemmat salausratkaisut.

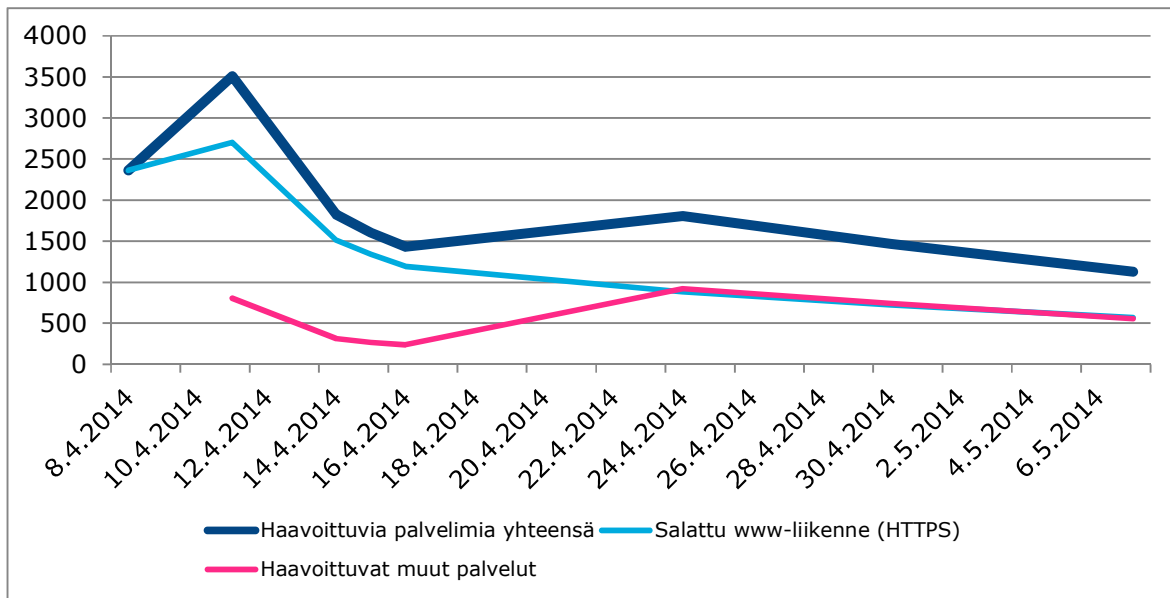
Lukuisat laitteet ja palvelimet Suomessa ja maailmalla ovat olleet haavoittuvia. Esimerkiksi suosituissa www-palvelinohjelmistoissa Apachessa ja nginx:ssä käytetään yleisesti OpenSSL-kirjastoa. Netcraft-yhtiön mukaan huhtikuussa 2014 kyseisiä ohjelmistoja käytti 66 % verkkosivustoista. Heartbleedille haavoittuvia palvelimia arvioidaan olevan internetissä vielä pitkään, sillä tavallisesti ensi kohun laannuttua ylläpitäjien mielenkiinto päivittää haavoittuvia ohjelmistoja laantuu. Haavoittuvina olleiden palvelinten varmenneavainten vaihtamisessa arvioidaan kestävän vielä pidempään, sillä niiden vaihtaminen vaatii enemmän käsityötä kuin ohjelmiston päivittäminen.

Haavoittuvuuden vaikutukset maailmalla

Joitakin merkittäviä onnistuneita hyväksikäyttötapauksia on tullut julki. Heti tuoreeltaan Kanadan veroviranomaisen verkkosivujen kautta varastettiin tieto noin 900 kanadalaisen sosiaaliturvatunnukset, internetyhtiö Yahoo!:n web-sähköpostipalvelusta varastettiin useiden sähköpostitilien salasanat ja amerikkalainen Community Health Systems Inc. (CHS) tiedotti 18.8.2014, että siihen oli huhti- ja heinäkuussa 2014 kohdistunut tietovuotoon johtaneita kyberhyökkäyksiä. Toisesta lähteestä kävi ilmi, että hyökkäykset CHS:ä vastaan oli tehty Heartbleediä hyväksikäyttäen. Suomessa vastaavia ei ole havaittu.

Heartbleed antoi hyvän näkymän palvelinten ylläpitoon. Sen korjaavan päivityksen asentaminen oli yksinkertaista, mutta edellytti ylläpitäjältä aktiivisia toimia. Valtaosa Suomen sähköisistä palveluista päivitettiin nopeasti, mutta verkossa on edelleen haavoittuvia järjestelmiä. Suomesta kerätystä tilastosta (Kuva 2) näkyy, että jäljellä olevien korjaamattomien palvelinten määrä vähenee hitaasti ensimmäisen korjausaallon jälkeen.

Nousu haavoittuvien palvelinten määrässä 24.4.2014 johtui siitä, että suomalaisten verkkojen tarkastelussa löytyi palvelimia, joita ei alkutilanteessa ollut huomattu.



Kuva 2 Suomessa havaittujen Heartbleed-haavoittuvien palvelinten määrä

OpenSSL-ohjelmistokirjastoja hyödyntäviä ohjelmistoja käyttävien palvelinten ylläpitäjiä kehoitetaan asentamaan korjaava ohjelmistopäivitys ensi tilassa sekä vaihtamaan niiden palvelinten varmenneavaimet, joissa on ollut asennettuna haavoittuva OpenSSL:n versio. Internetin palveluiden käyttäjiä kehoitetaan olemaan käyttämättä haavoittuvia palveluita. Palvelun haavoittuvuutta voi testata esimerkiksi verkkosivulla <https://filiippo.io/Heartbleed/> olevalla skannauspalvelulla.

Kyberturvallisuuskeskus on laatinut julkisen raportin haavoittuvuudesta². Haavoittuvuuden löytänyt Codenomicon on laatinut haavoittuvuudesta ja sen seurauksista sekä korjauksesta tiedottavan heartbleed.com -sivuston.

Shellshock

Bash-komentotulkki on Linux/Unix-järjestelmissä käytetty, käyttöjärjestelmän ohjaamiseen tarkoitettu ohjelmisto, joka ottaa vastaan ja suorittaa tekstikomentoja. Se on ollut osa Linux/Unix-järjestelmiä jo vuosikymmeniä. Myös Unixiin pohjautuva Apple OS X-käyttöjärjestelmä sisältää Bash-komentotulkin.

Bash-komentotulkista löytyi useita haavoittuvuuksia 24.9.–1.10.2014. Vakavin haavoittuvuus on ollut Bash-komentotulkissa vuodesta 1989. Haavoittuvuus mahdollisti hyökkääjän komentojen suorittamisen kohdejärjestelmässä. Haavoittuvuuden onnistunut hyödyntäminen vaati haavoittuvan Bash-komentotulkin lisäksi järjestelmän, jossa Bash-komentotulkille syötetään käyttäjän määriteltävissä olevaa sisältöä. Tällaisia ovat esimerkiksi HTTP- ja sähköpostiosakkeet, joita palvelin käsittelee. Haavoittuvuus nimettiin Heartbleedin mallin mukaan näyttävästi Shellshockiksi.

Haavoittuvuudelle julkaistiin nopeasti erilaisia hyväksikäyttömenetelmiä. Hyökkäysyritysten tavoitteena oli saada asennettua palvelimelle takaovi tai liittää palvelin osaksi bottiverkkoa haittaohjelman avulla. Haavoittuvuuden skannausta eri tahojen toimesta esiintyi runsaasti.

Myös Kyberturvallisuuskeskuksen HAVARO-järjestelmässä havaittiin hyökkäysyrityksiä. Kyberturvallisuuskeskukseen ei ole tullut tietoa yhdestäkään onnistuneesta hyväksikäytöstä Suomessa.

Shellshockille haavoittuvien tietokoneiden määrää ei pystytty arvioimaan niin kuin Heartbleedille haavoittuvien määrää pystyt-

² <https://www.viestintavirasto.fi/tietoturva/tietoturvanvnt/2014/04/ttn201404301533.html>

tiin, sillä Shellshock-haavoittuvuuden toteaminen edellyttäisi murtautumisen yrittämistä tutkittaville tietokoneille. Ilman tietokoneiden omistajien lupaa tehty murtautumisyritys on Suomen rikoslain nojalla rangaistava teko.

Lisävaikeutta uhan poistamiselle tuo se, että useissa sulautetuissa järjestelmissä, kuten ADSL-modeemeissa ja kotireitittimissä on jokin Linux-käyttöjärjestelmä ja joissakin niistä saattaa olla käytössä Bash-komentotulkki. Haavoittuvuuden toteaminen niistä voi olla vaikeaa niiden omistajillekin ja niiden päivittäminen voi olla ylivoimainen tehtävä useille kotikäyttäjille.

Shellshock on osoitus siitä, että kymmeniä vuosia aiemmin tehty ohjelmistovirhe ei luontihetkellään ole edes ollut virhe, vaan ajalleen tyypillinen tapa ratkaista senhetkisiä ongelmia. Vakavat ja kriittiset haavoittuvuudet löytyvät monesti vuosien pölykerrosten alta odottamasta hyväksikäyttöä.

WordPress

Laajalti käytössä olevasta WordPress-julkaisualustasta paljastettiin 20.11.2014 useita haavoittuvuuksia. WordPress-ohjelmistoa käytetään esimerkiksi yhdistysten ja yritysten kotisivujen sekä blogien julkaisussa. Haavoittuvuuksista kriittisin on suomalaisen Klikki Oy:n löytämä haavoittuvuus, joka liittyy sivuston kommentointiominaisuuden kautta jätettävän tekstin käsittelyyn julkaisualustassa. Sopivalla tavalla muodostetun

kommenttitekstin avulla hyökkääjä voi ottaa haltuunsa julkaisualustan ja sitä kautta myös palvelimen, jolla se toimii. Kyberturvallisuuskeskus antoi WordPress-haavoittuvuuksista vuoden 2014 kolmannen varoituksen 21.11.

Julkaisualustan haltuunoton avulla hyökkääjä voi esimerkiksi muuttaa tai poistaa sen sisältöä, lisätä sivustolle haitallista sisältöä tai hyödyntää palvelinta palvelunestohyökkäyksessä tai komentopalvelimena.

Kyberturvallisuuskeskus seurasi aktiivisesti WordPress-päivitysten etenemistä. Muutama päivä päivitysten julkaisun jälkeen, 23.11., haavoittuvuuksille alttiita julkaisujärjestelmiä oli Suomessa 60,7 % kaikista WordPress-alustoista, eli noin 23 000 kappaletta. Päivitykset etenivät alkusysäyksen jälkeen hitaahkosti, ja kolme viikkoa päivitysten julkaisun jälkeen päivittämättömiä julkaisualustoja oli edelleen 38,4 % eli noin 14 tuhatta kappaletta.

WordPress-haavoittuvuuden tehoseurannassa kävi ilmi, että päivittämättä jääneiden julkaisualustojen lukumäärä ja prosenttiosuus on hälyttävän suuri. Yli kolmannes ylläpitäjistä ei hoida palvelimiaan aktiivisesti.

Tällaiset internetiin avoimena olevat, vanhaa ja haavoittuvaa julkaisualustaa ajavat palvelimet muodostavat kyberrikollisille, haktivisteille ja muille pahantahtoïsille toimijoille oivan reservin potentiaalisia hyökkäyksissä hyödynnettäviä apuvälineitä.

Kohdistettujen hyökkäysten uhka otettava vakavasti

Tietoverkoissa tapahtuva vakoilu on tullut maailmalla entistä enemmän julkisuuteen. Eriyisen suurta huomiota ovat saaneet kampanjat nimiltään Snake, Energetic Bear, Sandworm ja Regin. Suomalaisiin organisaatioihin kohdistettuja haittaohjelmahyökkäyksiä on havaittu kymmenkunta ja yleensä tekojen motiiviksi on voitu nimetä ainakin luottamuksellisten tietojen varastaminen.

Kyberturvallisuuskeskus reagoi vakavaan ilmiöön paitsi tukemalla hyökkäysten kohteiksi joutuneita organisaatioita ja tapauksia tutkivia viranomaisia sekä laatimalla raportin kohdistettujen haittaohjelmahyökkäysten torjunnasta. Kyberturvallisuuskeskus on myös välittänyt suomalaisille viranomaisille ja kriittisen infrastruktuurin tahoille aikaisempaan verrattuna ennätyksellisen paljon teknisiä tietoja kybervakoilusta.

Suomalaiset organisaatiot eivät ole suojassa kohdistetuilta hyökkäyksiltä

Havainnot vakoilu- haittaohjelmista lisääntyneet

Kohdistettujen haittaohjelmahyökkäyksien havaintomäärät lisääntyivät Kyberturvallisuuskeskuksen seuraamien lähteiden mukaan vuonna 2014 sekä maailmanlaajuisesti että Suomessa. Kyberturvallisuuskeskus on pyrkinyt lisäämään ilmiön tunnettavuutta julkaisemalla organisaatioiden käyttöön aihetta taustoittavan raportin "Kohdistettujen hyökkäysten uhka on otettava vakavasti". Se on saatavilla Viestintäviraston verkkosivuilla.

Vakoiluhaittaohjelmista ja niiden leviämisestä on puhuttu vuosien ajan. Kuluneena vuonna ilmiö on tietoturvapiireissä lähes arkipäiväistynyt. Kansainväliset tietoturvayhtiöt julkaisivat raportteja tiheämmin ja enemmän kuin edeltävinä vuosina. Myös Kyberturvallisuuskeskus on saanut entistä enemmän tunnistus- ja havainnointitietoja sidosryhmiltä ja HAVARO-järjestelmästä. Kyberturvallisuuskeskus on välittänyt ilmiöön liittyen tietoja vähintään tuplamäärän edellisvuoteen nähden.

Suuntaus vaikuttaa olevan pysyvä ja kybervakoilu on laajenemassa entistä moninai-
sempiin toimijoihin. Ongelmana on yhä uhan ja sen vaikutusten laajuuden tiedostaminen organisaatioissa, sillä sekä havainnointi että

reagointi eroavat tavanomaisiin haittaohjelmiin purevista periaatteista. Kokemukset osoittavat, että päteväkin järjestelmä- tai tietoturva-asiantuntija voi olla avuton kohdatessaan vakoiluhaittaohjelman.

Pahimmassa tapauksessa hyökkääjä voi saada organisaation verkon haltuunsa kenenkään huomaamatta. Näin hyökkääjän on mahdollista päästä kiinni organisaation salassa pidettäviin tietoihin ja hyökkääjä voi lymyillä verkossa vuosikausiakin.

Haittaohjelmia hyödyntäneistä vakoiluoperaatioista merkittävimiksi nousevat laajuuden ja kehittyneisyyden vuoksi Snake ja Energetic Bear.

Havaintomäärällisesti laajimmalle levinneeksi vakoiluohjelmaksi nousee PlugX ja mielenkiintoa herättää myös loppuvuonna julkitullut Sandworm, jossa oli todennetusti kyetty osoittamaan tuoreen nollapäivähaavoittuvuuden hyödyntäminen. On myös havaittavissa, että tavanomaisten ja kohdistettujen haittaohjelmien ero on hälvenemässä, esimerkiksi PlugX:ää käytetään hyvin monenlaisiin kohteisiin ja tarkoituksiin.

Huomionarvoista vuoden aikana julkaisuista raporteissa on, että eri tietoturvayhtiöt ovat saaneet havaintoja ja näyttöjä samoista haittaohjelmaperheistä todennäköisesti eri lähteistä. Tämä viittaa sekä ongelman laajuuteen että tietoturvatoimijoiden kehittyneeseen havainnointikykyyn. Vaikka aiheeltaan päällekkäisten raporttien syy on kilpailu, täydentävät ja täsmentävät ne hyvin toisiaan.

Tietoturvayhtiöiden havainnot ja julkistamat tiedot lienevät kuitenkin yhä vain jäävuoren huippu vakoiluoperaatioiden todellisesta mittakaavasta. Tyypillistä raporttien ja ko-

kemusten mukaan on, että havainto vakoi-luhahttaohjelmasta tehdään pitkän ajan ku-luttua hyökkäysoperaation alkamisesta ja varsin usein havainnot jäävät vain epäilyiksi, kun riittäviä todisteita ei saada kerätyksi en-nen kuin vakoilijat häivyttävät jälkensä. Vuoden 2014 todellinen kybervakoilutilanne on oikeastaan arvioitavissa vasta vuosien kuluttua, jos täsmällisesti silloinkaan.

Suomalaiset organisaatiot eivät ole suojassa kohdistetuilta hyökkäyksiltä. Suomessa koh-distettuihin haittaohjelmiin liittyviä eritasoi-sia havaintoja on tehty niin sidosryhmiltä saatujen tunnistetietojen, HAVARO-järjes-telmän, kuin itsenäisten havaintojenkin pe-rusteella. Tapaukset käsitellään luottamuk-sellisesti asianosaisten tahojen kesken. Ky-berturvallisuuskeskuksen tiedossa on myös suomalaisia tapauksia, joissa on viitteitä maailmalla julkaistuissa raporteissa mainit-tujen haittaohjelmien käytöstä.

Kokemusten perusteella oleellista organisaa-tioissa on kiinnittää huomiota lokitietojen seuraamisen ja tallentamiseen jälkianaly-soinnin helpottamiseksi. Kyberturvallisuus-keskus tekee aktiivisesti työtä organisaatioi-den tukemiseksi havainnointikyvyn paranta-misessa ja ajantasaisten tietojen välittämi-sessä soveltuvien sidosryhmien kesken.

Energiasektoriin kohdistunut Energetic Bear/Havex

Energetic Bear on nimitys kybervakoilukam-panjalle, joka on ollut käynnissä ainakin jo vuodesta 2010. Haittaohjelma, jota kam-panjassa on erityisesti käytetty, on nimel-tään Havex. Kampanja ja sen takana oleva ryhmä on vuoden 2013 jälkeen tähdännyt erityisesti energia-alan toimijoita ja näiden yhteistyökumppaneita kohtaan. Kybertur-vallisuuskeskus on välittänyt saamansa hait-taohjelmaan liittyvät tunnistetiedot energia-alan toimijoille Suomessa.

Energetic Bear -ryhmän tiedetään myös saastuttaneen teollisuusautomaatiojärjes-telmiä valmistavien yritysten ohjelmistojen

päivityksiä haittaohjelmilla. On myös viit-teitä siitä, että ryhmän tähtäimessä on ollut lisäksi lääketieteellisuuden yrityksiä.

Tietoturveyshtiöiden analysoimat haittaohjel-manäytteet viittaavat siihen, että saastuneiden tietokoneiden käyttäjistä on mahdollista saada hyvin yksityiskohtaisia tietoja, kuten käyttäjätunnuksia ja salasanoja, yhteystie-toja osoitekirjoista ja salattujen VPN-yhteyk-sien asetustiedostoja. Kampanjaa kutsutaan myös nimillä Dragonfly ja Crouching Yeti. Useat nimet johtuvat eri tietoturveyshtyrysten omista tavoista nimetä haittaohjelmakam-panjoita.

Valtioilta tietoja varastava Snake

Keväällä 2014 tietoturveyshtiö G DATA kertoi raportissaan erittäin kehittyneestä kohdiste-tuissa hyökkäyksissä hyödynnetystä haitta-ohjelmasta nimeltä Uroburos. Eri tietotur-vayhtiöt ovat antaneet sille omat nimet, ja se tunnetaan muun muassa myös nimillä Snake ja Turla.

Snake on modulaarinen, helposti muokatta-vissa oleva vakoiluohjelma. Se on luotu va-rastamaan kohteen tiedostoja ja kuuntele-maan verkkoliikennettä. Tietoturveyshtiö G DATA:n julkaiseman raportin mukaan Sna-ken monimutkaisuus viittaa siihen, että sen takana on valtiollinen toimija³.

Snaken tekee merkittäväksi sen laaja levin-neisyys ja kohteena olevat valtiolliset tahot, kuten sisä- ja ulkoministeriöt sekä suurlähe-tystöt. Tietoturveyshtiö Symantecin mukaan vakoiluohjelmaa on löydetty Belgiasta, Uk-rainasta, Kiinasta, Jordaniasta, Kreikasta, Kazakstanista, Armeniasta, Puolasta, Sak-sasta ja useasta muusta Euroopan maasta⁴. Tietoturveyshtiö BAE Systemsin mukaan tar-tuntoja on myös Liettuassa, Yhdistyneessä kuningaskunnassa, Georgiassa, Yhdysval-loissa, Romaniassa, Unkarissa ja Italiassa⁵. Lisäksi Luxemburgin CERT-viranomainen on julkaissut analyysin ja tunnistetietoja van-hemmasta Uroburos-perheen haittaohjel-masta⁶.

³ https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf

⁴ <http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats>

⁵ http://info.baesystemsdetica.com/rs/baesys-tems/images/snake_whitepaper.pdf

⁶ <http://www.circl.lu/pub/tr-25/>

Vakoiluohjelmaa on levitetty kohdistetuilla sähköposteilla (spear phishing) ja valikoitujen saastutettujen verkkosivujen (watering hole) avulla. Snakelle riittää yksi saastunut kone, jonka kautta muut samassa kohteessa olevat tietokoneet voivat viestiä komento-palvelimelle. Vanhimmat Snake-haittaohjelmanäytteet ovat tammikuulta 2006.

Sandworm ja Windowsin nollapäivähaavoittuvuus

Ainakin puolustusliitto NATO, Ukraina ja Puola sekä useita suuryrityksiä ja muita organisaatioita on joutunut ammattimaisesti toteutetun vuosia jatkuneen kybervakoilu-kampanjan kohteeksi. Kampanjalla pyritään hankkimaan salassa pidettäviä tietoja. Kampanjan 14.10.2014 paljastanut tietoturvayhtiö iSIGHT Partners nimesi kampanjan ja oletetun ryhmän sen takana Sandwormiksi (suomeksi "hiekkamato"). Myös tietoturvayhtiö F-Secure on itsenäisesti löytänyt viitteitä kampanjasta ja antanut sille nimen Quedagh.

Kampanjassa on hyödynnetty muiden hyökkäystekniikoiden muassa ennestään tuntematonta ohjelmistovirhettä (niin sanottu nollapäivähaavoittuvuus) useissa Microsoftin Windows-käyttöjärjestelmissä. Microsoft julkaisi sen korjaavan päivityksen samana päivänä iSIGHT Partnersin paljastuksen kanssa.

Kuten nollapäivähaavoittuvuuksien julkaisemisessa usein käy, muutkin rikolliset ryhtyivät hyödyntämään Sandworm-ryhmän hyväksikäyttämää ohjelmistovirhettä. Moniin suomalaisiin organisaatioihin kohdistui pian julkaisun jälkeen haittaohjelmahyökkäyksiä, joissa käytettiin kyseistä ohjelmistovirhettä. Sandworm-kampanjan tutkiminen jatkuu edelleen. Kyberturvallisuuskeskus on välittänyt mahdollisten hyökkäysten havaitsemiseksi tarpeellisia teknisiä tunnistetietoja Suomessa.

Kohdistettujen haittaohjelmahyökkäysten torjunta

Kyberturvallisuuskeskus julkaisi elokuussa 2014 raportin, jossa kuvataan kohdistettujen haittaohjelmahyökkäysten toteutusta, ilmiön nykytilaa ja uhkaan varautumista. Raportin tarkoituksena on lisätä tietoisuutta ongelmasta, parantaa organisaatioiden suojaus- ja reagointikykyä uhkaa vastaan ja lisätä kansallista yhteistyötä kohdistettujen haittaohjelmahyökkäysten havainnoinnissa ja torjunnassa.

Suomalaisissa organisaatioissa on oletettavasti osin puutteellinen havainnointikyky. Suomessa tunnistetaan vuosittain vain muutamia kohdistettuja haittaohjelmatautuntoja, kun järjestelmällisesti ilmiötä seuraavissa länsimaissa kerrotaan tunnistettavan kymmeniä tapauksia. Kuitenkin Suomen teknologiayritysten korkea innovatiivisuus ja valtionhallinnon toimivuus koetaan yleisesti vakoilulle mielenkiintoisiksi tekijöiksi, joten havainnointikyvyn kasvattaminen ja yhteistyön lisääntyminen on toivottavaa tilanteen näkyyden korjaamiseksi kansallisesti.

Raportti perustuu suomalaisten viranomaisien kokemuksiin, yhteistyöverkostojen kautta saatuihin tietoihin ja näkemyksiin, sekä julkisiin raportteihin. Se on laadittu yhteistyössä Suojelupoliisin ja Puolustusvoimain kanssa. Lisäksi raporttia varten on haastateltu tietoturvayhtiöitä F-Securea, Nixia ja nSenseä.

Kyberturvallisuuskeskuksen raportti kohdistetuista haittaohjelmista⁷ on luettavissa ja ladattavissa Viestintäviraston verkkosivuilta. Sen tavoitteena on lisätä tietoisuutta, parantaa organisaatioiden suojaus- ja reagointikykyä sekä lisätä kansallista yhteistyötä kohdistettujen haittaohjelmahyökkäysten havainnoinnissa ja torjunnassa. Raportissa on neuvoja muun muassa uhan arviointia varten (ks. kuva 3).

⁷ https://www.viestintavirasto.fi/tietoatoimialasta/katsaukset/taartikkelit/tietoturva-artikkelit/kohdistetut_haittaohjelmatovatnykyvakoilunarkipivaa.html



Kuva 4 Mahdollinen hyökkääjä arvioi hyökkäyksen kannattavuutta kohteensa kiinnostavuuden, yhteistyöverkoston sekä teknisten ja toimintakyvyllisten puolustusmahdollisuuksien kautta

HAVARO on osa kyberturvallisuuden tilannekuvaa

Tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä HAVARO on Viestintäviraston tuottama palvelu, jolla valikoitujen asiakasorganisaatioiden verkkoliikenteestä etsitään jälkiä tietoturvallisuutta vaarantavasta toiminnasta.

Keskeiset kumppanit ja asiakkaat

Vuonna 2011 käyttöönotetun palvelun keskeisenä yhteistyökumppanina Viestintävirastolle on alusta alkaen ollut Huoltovarmuuskeskus ja vuodesta 2013 alkaen myös valtiovaraministeriö.

Palvelu on suunnattu Suomeen sijoittuneille huoltovarmuuskriittisille elinkeinoelämän toimijoille ja julkisen hallinnon organisaatioille, joihin voidaan perustellusti olettaa kohdistuvan korostunut kyberhyökkäysten uhka. Vuoden 2014 lopussa HAVARO:a käytti noin kolmekymmentä asiakasorganisaatiota. Vuonna 2013 käyttäjiä oli noin 15.

HAVARO-palveluun liittyminen perustuu vapaaehtoisuuteen ja edellyttää osallistumista järjestelmän rakennus- ja ylläpitokustannusten kattamiseen. Viestintävirasto tavoittelee HAVARO:n asiakaskunnan osalta hyvää edustavuutta täyden valtakunnallisen kattavuuden sijaan.

Ennen palveluun liittämistä organisaation tekninen yhteensopivuus ja tietoturvakontrollien kattavuus selvitetään sekä arvioidaan asiakkaan liittämistä koituva hyöty Kyberturvallisuuskeskuksen muulle tilannekuva-toiminnalle.

HAVARO:n tehtävänä ei ole estää tietoturvaloukkauksia, vaan ainoastaan tehdä muut suojaukset läpäisseistä edistyneistä hyökkäyksistä näkyviä. Näin ollen HAVARO ei myöskään saa koskaan olla asiakkaan ainoa tai ensisijainen tietoturvakontrolli.

Viestintävirasto kannustaa myös HAVARO:n piiriin päässeitä asiakkaitaan jatkamaan panostuksia tietoturvallisuuden perusasioihin kuten ohjelmistojen tietoturvapäivityksiin,

tietoliikenteen suodattamiseen, käyttövaltuuksien hallintaan, virustorjuntaan ja tunkeutumisen havaitsemisjärjestelmien valvontaan.

Huonosti suojatun verkon tietoturvan valvonta olisikin HAVARO:n keinoin hyödyntöä. HAVARO:lla tehdyistä havainnoista syntyy hyödyllistä tietoa myös julkiseen käyttöön⁸.

HAVARO:n toteutuksesta

HAVARO etsii organisaation verkkoon saapuvasta ja sieltä lähtevästä liikenteestä jälkiä tietoturvaa vaarantavasta liikenteestä. Havainnointijärjestelmä perustuu avoimiin ja kaupallisesti saatavilla oleviin tunkeutumisen havaitsemisjärjestelmiin ja liikennevoimien analysointiin kehitettyyn tekniikkaan. HAVARO toteuttaa tietyllä tavalla ensimmäisenä Suomessa niin kutsutun passiivnimipalvelun, jonka avulla esimerkiksi haittaohjelmien komentopalvelinten tai muiden tietoturvallisuutta vaarantavien osoitekeskittymien tunnistaminen on aiempaa helpompaa.

Viestintävirasto hyödyntää HAVARO:n havaintoja yhdistelemällä niitä muuhun kyberturvallisuustietoon. Näin kertynyt ymmärrys tietoturvaloukkausten toteutustavoista puolestaan mahdollistaa entisestään parempien tunnusmerkistöjen tuottamisen HAVARO:n käyttöön. Viestintäviraston omaan tiedonhankintaan pohjautuva osuus säännöstöstä on salassa pidettävää eikä vastaavaa materiaalia ole saatavilla kaupallisista lähteistä.

HAVARO toteutetaan tietoyhteiskuntakaaren 272 §:n perusteella. Pykälä antaa organisaatioille oikeuden käsitellä tietoliikennettä viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitse-

⁸ Katso esimerkiksi <https://www.viestintavirasto.fi/tietoturva/tietoturva-nyt/2014/07/ttn201407091103.html>

miseksi, estämiseksi ja selvittämiseksi. Viestintävirasto käsittelee tietoja sopimusperusteisesti asiakasorganisaation lukuun.

Robotin jälki on harmaata, ihminen lisää värin

HAVARO:ssa hyödynnetään edistyneitä päättelymekanismeja, joilla järjestelmän tuottama tekninen havaintomateriaali yhdistellään ja sen paikkansapitävyys arvioidaan automaattisesti ennen ihmisvoimin tehtävää lopullista analyysiä.

Automatiikan ansiosta järjestelmän vuosittain tuottamien kymmenien miljoonien havaintojen sijasta asiantuntijavoimin joudutaan käsittelemään ainoastaan joitakin kymmeniä tuhansia havaintoja.

Ennen kuin HAVARO:n tuottamat hälytykset lähetetään asiakkaille toimenpiteitä varten, Viestintäviraston asiantuntijat arvioivat niiden paikkansapitävyyden ja määrittelevät tapausten vakavuuden. Tämän tuloksena hälytykset ryhmitellään eri vakavuusluokkiin ja niille annetaan erityiset värikoodit. Automaatilta "harmaina" saapuneet hälytyksiin "väritetään" tässä yhteydessä punaisiksi, keltaisiksi tai vihreiksi.

Vakavimmat ja kiireellisiä toimenpiteitä edellyttävät hälytykset merkitään punaisella. Tällaisia ovat muun muassa tapaukset, joissa Viestintäviraston arvion mukaan asiakkaan tietojärjestelmiin on onnistuneesti tunkeuduttu ilman, että mikään tietoturvakontrolli olisi pystynyt estämään tai rajaamaan vahinkoja. Punaiset hälytykset raportoidaan välittömästi. Vuonna 2014 HAVARO tuotti 1 930 punaista hälytystä.

Väärät hälytykset tai sellaiset tapaukset, joilla ei ole välitöntä vaikutusta tietoturvasuuteen, merkitään vihreiksi. Vihreitä hälytyksiä ovat tyypillisesti tapaukset, joissa tietokoneelle on ladattu haittaohjelma, mutta se ei ole jostakin syystä aktivoitunut — yleensä toimivan virustorjunnan tai tietoliikennesuodatuksen ansiosta.

HAVARO-asiakkaat hyödyntävät vihreitä raportteja todisteena omien tietoturvakontrolliensä tehosta. Niiden avulla on myös löydetty verkkoon "unohtuneita" tietojärjestelmiä ja tietoturvasuutta potentiaalisesti vaarantavia konfiguraatiovirheitä. Vuonna 2014 vihreitä hälytyksiä kirjattiin 18 014 kappaletta.

Keltaiset hälytykset ovat tapauksia, joissa tietoturvakontrollien teho on jäänyt kyseenalaiseksi. HAVARO:n tietojen perusteella tietoturvasuus on saattanut vaarantua, mutta lopullinen selvitys asiaan saataisiin vasta asiakkaan omien selvitysten perusteella. Keltaisia hälytyksiä annettiin 4 757 kappaletta.

HAVARO ja vuoden isot tietoturvatapaukset

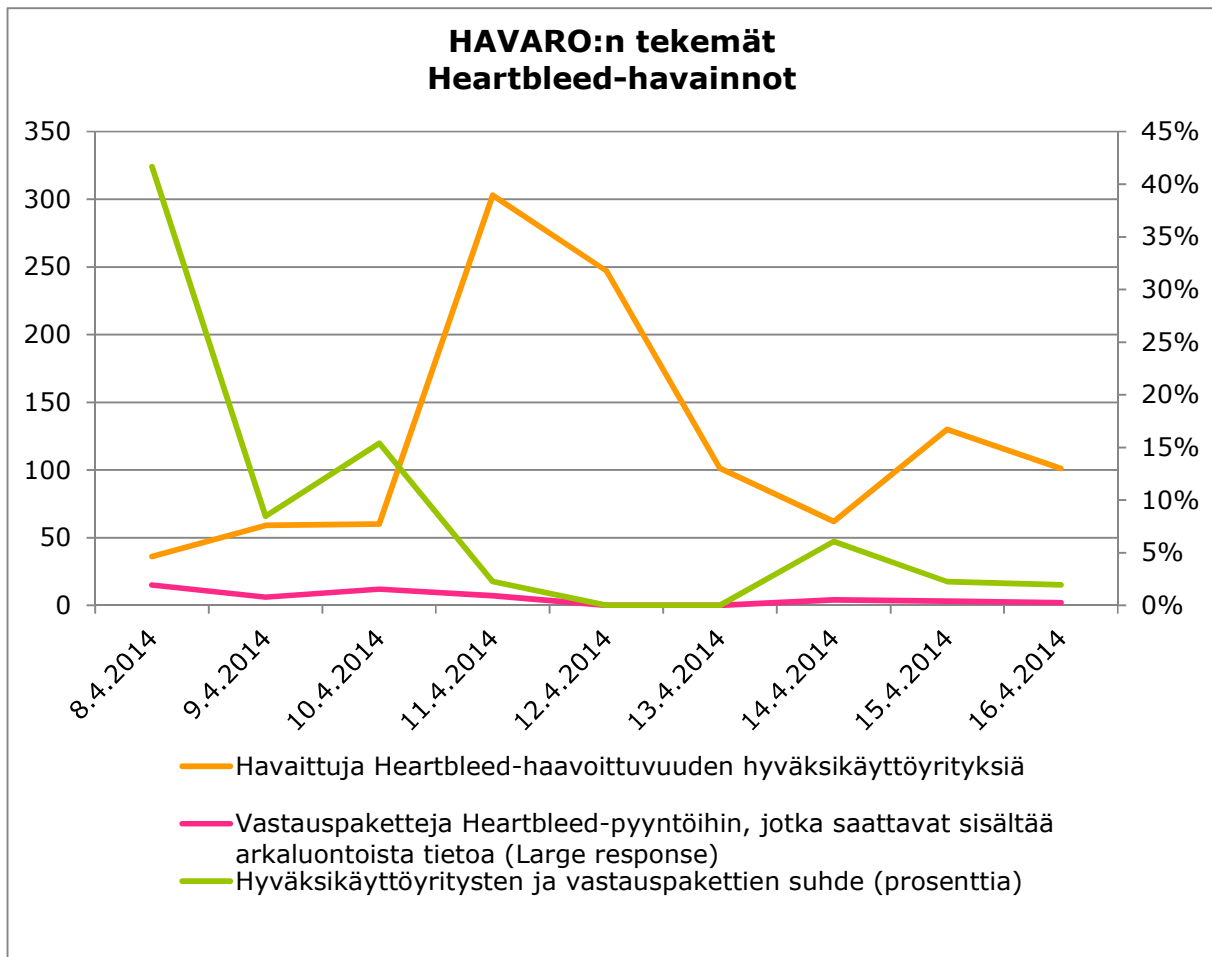
HAVARO:n avulla on saatu arvokasta täydentävää tietoa useista vuonna 2014 tietoon tulleista tietoturvaloukkaustapauksista.

Heartbleed-haavoittuvuuden tarkoista hyväksikäyttömenetelmistä, haavoittuvien järjestelmien yleisyydestä ja hyväksikäyttöyritysten määrästä oli alkupäivinä julkisissa lähteissä ainoastaan arvailuja.

Viestintäviraston Kyberturvallisuuskeskuksella oli alusta alkaen käytössään HAVARO-tunnisteet, joilla kyettiin reaaliaikaisesti seuraamaan (vrt. Kuva 5) haavoittuviin järjestelmiin kohdistuvia hyökkäysyrityksiä sekä päättämään, milloin hyökkääjät saattoivat onnistua yrityksessään varastaa palvelimilta tietoja.

Myös Shellshock-haavoittuvuuden hyväksikäyttöyritykset näkyivät HAVARO:ssa. Heti haavoittuvuuden tultua julki hyväksikäyttöyrityksiä havaittiin useita tuhansia saman päivän aikana. Yritysten määrä laski kuitenkin nopeasti.

Kyberturvallisuuskeskus kerää aktiivisesti tietoja kohdistetuista haittaohjelmista. Rutinotoimenpiteisiin kuuluu, että uudet tunnisteet lisätään HAVARO:on, jolloin mahdolliset hyökkäykset kyetään jatkossa havaitsemaan.



Kuva 5 Suomeen kohdistuneita Heartbleed-haavoittuvuuden hyväksikäyttöyrityksiä ja tilastoja hyökkäysten vaikutuksista.

Suomalaiset tietoverkot edelleen maailman puhtaimpien joukossa

Viestintävirasto vahvistaa toiminnallaan kansallista tietoturvaa ja viestintäverkkojen toimintavarmuutta.

Suomalaiset tietoverkot arvioitiin tuoreimmassa Microsoft Security Intelligence Report (SIR) 17 -raportissa jälleen puhtaimmiksi maailmassa. Raportti kattoi ajanjakson heinäkuusta 2013 kesäkuuhun 2014. Sen mukaan puhtaimmat tietoverkot kyseisellä ajanjaksolla olivat Suomessa ja Japanissa. Suomen lisäksi myös muut Pohjoismaat pärjäsivät vertailussa hyvin.

Microsoftin Windows-käyttöjärjestelmät ovat selvästi maailman yleisimpiä henkilökohtaisissa tietokoneissa (PC). Myös selvästi suurin osa henkilökohtaisista tietokoneista saastuttavista haittaohjelmista toimii Windowsissa. Microsoft saa kaukomittauksillaan hyvän kuvan haittaohjelmatilanteesta maailmalla ja sen tietoturvaraportteja pidetään korkealaatuisina.

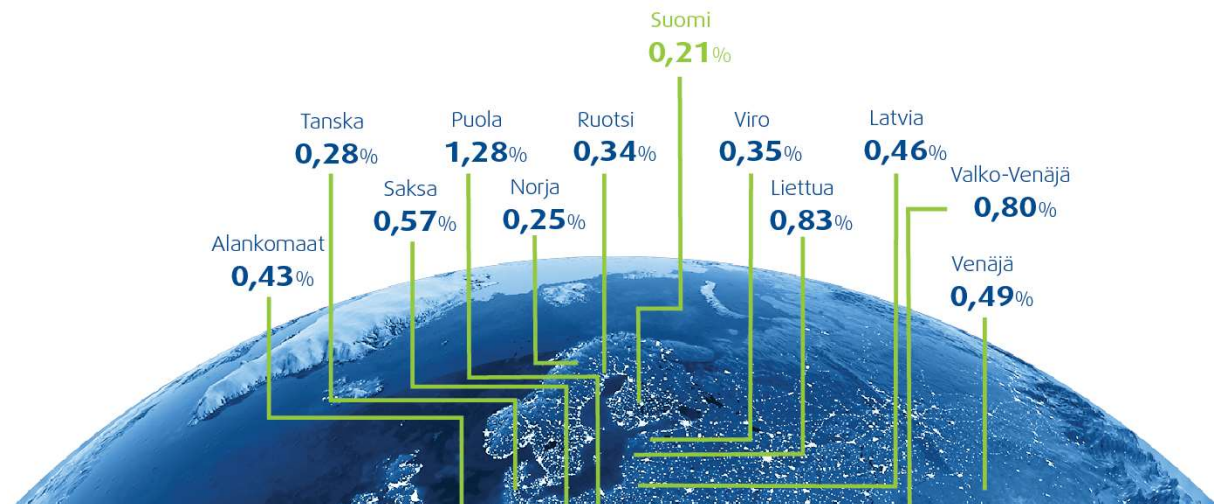
Raportin viimeisellä mittausjaksolla Q2 2014 Suomen osalta noin 0,21 % koneista on luokiteltu saastuneiksi (Kuva 6), kun keskiarvo

maailmalla on noin 0,72 % (Microsoftin termien "Cleaned computers per mille, CCM"). Lukema saadaan Microsoftin Malicious Software Removal Tool -ohjelman lähettämistä tiedoista. Ohjelma suoritetaan Windows-koneissa ajoittain esimerkiksi käyttöjärjestelmän kuukausittaisten päivitysten yhteydessä.

CCM-lukema kuvaa, kuinka hyvin tietokoneiden omistajat ja ylläpitäjät pitävät huolta koneidensa tietoturvasta. Alhainen lukema tarkoittaa muun muassa, että harva haittaohjelma pystyy tarttumaan tietokoneeseen, koska koneen ohjelmistot päivitetään ripeästi haa-voittuvuuksien paikkaamiseksi ja koska koneessa on ajantasainen tietoturvaohjelmisto.

Toinen verkkojen puhtauden mitta on se, kuinka usein verkkoon liitetty tieto-

Kyberturvallisuuden kärkeksi pääsee vain jatkuvalla ponnistelulla



Kuva 6 Microsoftin toimenpitein haittaohjelmista puhdistettujen tietokoneiden osuudet (lähde: SIR 17)

koneet saavat haittaohjelmia sisältävää liikennettä ("Encounter rate"). Raportin viimeisellä mittausjaksolla Suomessa vain 5,9 % tietokoneista kohtasi haittaohjelmia. Kansainvälinen keskiarvo on 19,1 %.

Encounter rate -lukema kuvaa, kuinka hyvin maan ekosysteemi toimii tietoturvamielessä. Alhainen lukema tarkoittaa muun muassa, että tietokoneiden käyttäjät ovat valveutuneita ja harvoin lataavat haittaohjelmia sisältävää materiaalia netistä, ja että saastuneita tietokoneita estetään aktiivisesti levittämästä haittaohjelmaa edelleen.

Suomalaisten tietoverkkojen puhtautta selittää muun muassa teleoperaattoreiden hyvä reagointikyky asiakkaiden haittaohjelmataruntoihin sekä suomalaisten käyttäjien hyvä tietoturvatietämys.

Toimiva julkisen ja yksityisen sektorin yhteistyö edesauttaa ongelmien havainnointia sekä ratkaisemista. Myös lainasäädännöllä on oma osuutensa tietoverkkojen turvallisuudesta huolehtimisessa. Suomen Tietoyhteiskuntakaari muun muassa velvoittaa teleoperaattoreita välittömiin toimenpiteisiin viestintäverkolle merkittävää häiriötä aiheuttavien laitteiden korjaamiseksi tai irrottamiseksi yleisestä verkosta. Operaattorien suorittamaa puhdistustyötä tuetaan Kyber-

turvallisuuskeskuksen Autoreporter-palvelun päivittäisillä yhteenvedoilla operaattorien verkoissa havaituista haitallisista ilmiöistä.

Työjuhta Autoreporter

Yksi tärkeimmistä Kyberturvallisuuskeskuksen työkaluista on keskuksen kehittämä palokittu Autoreporter-järjestelmä. Autoreporter on ollut käytössä vuodesta 2006 lähtien ja se kerää jatkuvasti ja automaattisesti suomalaisia verkkoja koskevia haittaohjelma- ja tietoturvaloukkaushavaintoja. Tiedot Autoreporter saa koti- ja ulkomaisilta Kyberturvallisuuskeskuksen luotetuilta kumppaneilta. Autoreporterin lähettämien tietojen perusteella verkkojen vastuuhenkilöt voivat toimia havaitun tietoturvauhan torjumiseksi.

Autoreporter-järjestelmän kokoamista tiedoista saadaan myös hyvä kuva suomalaisissa tietoverkoissa esiintyvistä tietoturvauhista. Vuonna 2014 Autoreporter-järjestelmä välitti 204 139 havaintoa eri haittaohjelmista teleyrityksille. Vuonna 2013 havaintoja oli 492 426 kpl. Havaintojen absoluuttisia määriä ei kannata vertailla tarkasti, sillä lukumääriin vaikuttavat myös alati vaihtuvat tietolähteet, joista Autoreporter kerää tietonsa.

Vuonna 2014 yleisimpien haittaohjelmien tyypillisiä rahantekomenetelmiä olivat muun muassa:

- Bitcoin-virtuaalivaluutan louhiminen
- Verkkosivuilla olevien mainosten automaattinen avaaminen
- Verkkopankki-istunnon tietojen kaappaaminen ja sen kautta tapahtuvat rahavarkaudet
- Kiristyshaittaohjelmien asennus uhrin koneelle ja lunnaiden vaatiminen koneen avaamiseksi
- Peloteohjelmien asennus, jotka väittävät esimerkiksi löytäneensä uhrin koneelta haittaohjelman, joka poistetaan jos uhri ostaa ohjelman täyden version

Ryhmittely

Kuva 7) on karkea, sillä liki kaikissa nykyisissä haittaohjelmissä on useita eri toimintoja, joiden perusteella ne voitaisiin sijoittaa eri ryhmiin. Haittaohjelma-ryhmille on tässä määrätty ryhmä sen mukaan, mihin tarkoitukseen ohjelmia pääasiassa käytetään.

Lataajien suurta osuutta vuonna 2014 selittää alkuvuodesta Suomessa esiintynyt pieni Zeroaccess-epidemia. Vuoden 2013 osalta roskapostittajien suuri määrä johtui yksittäisestä piikistä spambot-haittaohjelmien määrässä.

Havainnot jakautuvat seuraaviin ryhmiin:

Lataaja = toisia haittaohjelmia tietokoneelle hakeva ja lataava haittaohjelma
Yleensä hyökkääjä pystyy ohjaamaan lataajaa etänä. Esimerkkejä yleisimmistä lataaja-haittaohjelmista: Zeroaccess, Sality, Dofail, Virut.

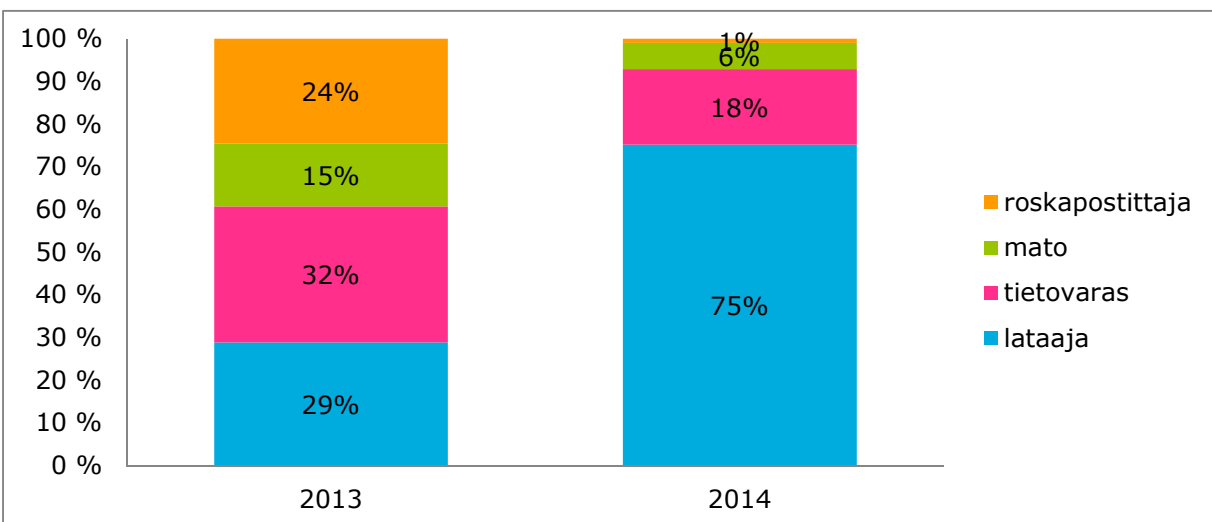
Tietovaras = käyttäjän tietoja, erityisesti käyttäjätunnuksia ja salasanoja, varastava haittaohjelma. Varastamallaan salaisuuksilla hyökkääjät voivat esiintyä uhrin identiteet-

tillä. Erityisen vakavaa tämä on, jos hyökkääjät varastavat verkkopankin tai sähköpostitilin salasanat. Yleisimmät tietoja varastavat haittaohjelmat ovat Zeus eli Citadel eri versioineen, Torpig, Tiny banker eli Tinba, ja KINS.

Mato = haittaohjelma, joka leviää omatoimisesti tietokoneesta toiseen. Madot kuluttavat saastuttamiensa tietokoneiden ja verkkojen resursseja, saattavat estää tietoturvaohjelmia toimimasta ja voivat ladata tietokoneeseen muita haittaohjelmia. Esimerkkejä madoista ovat Conficker eli Downadup, Palevo ja erilaiset Ircbot-perheen ohjelmat.

Roskapostittaja = roskapostia lähettävät useimmiten haittaohjelmalla saastuneet tietokoneet. Tavallisimpia Suomessa havaittuja roskapostia lähettäviä haittaohjelmia ovat StealRAT, Pushdo ja Pony.

Kuvaajassa ei näytetä muiden haittaohjelmaryhmien, sillä niiden osuus kokonaisuudesta on alle 1 %. Muita haittaohjelmaryhmiä ovat esimerkiksi kiristys-, vakoilu- ja klikkauspetoshaittaohjelmat sekä tilisiirtoja muokkaavat haittaohjelmat.



Kuva 7 Suomessa havaittujen haittaohjelmaryhmien suhteelliset osuudet vuosina 2013 ja 2014

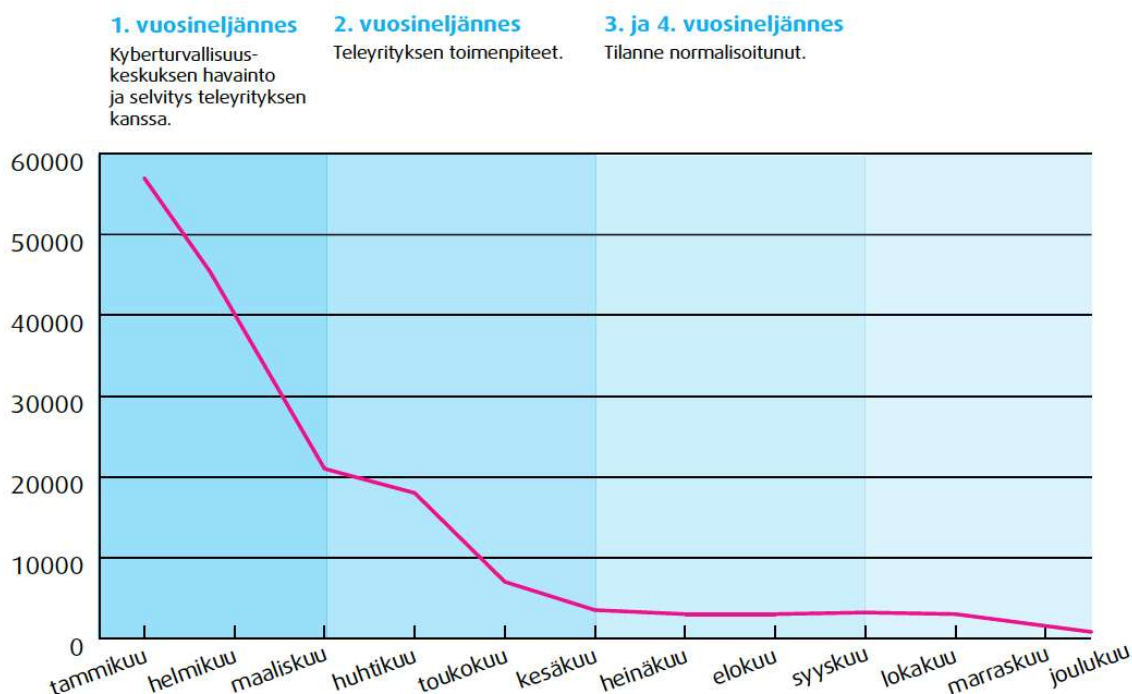
Haaitaohjelmahavainnoista 85 % peräisin yhden teleyrityksen verkosta

Suomalaisen teleyrityksen verkosta ulos suuntautuvan haaitaohjelmaliikenteen määrän kasvu huomattiin Kyberturvallisuuskeskuksen Autoreporter-palvelun avulla. Raportoitujen haaitaohjelmataartuntojen määrä oli moninkertainen normaalitilanteeseen verrattuna.

Kyseisen teleyrityksen ryhdyttyä tarvittaviin toimenpiteisiin asiakkaiden saastuneiden koneiden osuus kokonaismäärästä palautui

vastaamaan sen markkinaosuutta. Tapaus on esimerkki siitä, että aktiivisilla toimilla on merkitystä asiakkaiden päätelaitteiden tietoturvalle.

Alla olevasta kuvaajasta (Kuva 8) nähdään haaitaohjelmahavaintojen määrän kehitys kyseisen teleyrityksen verkossa. Tammi-maaliskuun aikana Kyberturvallisuuskeskus havaitsi ongelman ja otti yhteyttä teleyritykseen. Teleyritys suoritti korjaavia toimenpiteitä huhti-kesäkuun aikana. Loppuvuodeksi tilanne normalisoitui vastaamaan teleyrityksen markkinaosuutta Suomessa.



Kuva 8 Autoreporterin haaitaohjelmahavainnot erään teleyrityksen osalta vuonna 2014

Viestintäverkkojen häiriöiden määrä väheni

Vuoden 2014 aikana Viestintävirasto sai teleyrityksiltä noin 150 ilmoitusta merkittävästä yleisen viestintäverkon häiriöistä. Näistä 14 luokiteltiin vakaviksi, jotka koskivat vähintään 100 000 puhelin- ja internetyhteyspalveluiden käyttäjää, 300 000 TV- ja radiopalvelujen käyttäjää tai vaikuttivat laajalla maantieteellisellä alueella vähintään puolen tunnin ajan.

Vuonna 2013 häiriöiden kokonaisluku oli noin 200, ja vakavia häiriöitä ilmoitettiin hieman alle 20. Kaikkiaan vakavaksi luokiteltavien laajojen häiriöiden määrä väheni vuonna 2014 edellisestä vuodesta.

Häiriöt jakaantuivat melko tasan TV- ja radiopalvelujen katkoksien sekä matkaviestinverkon häiriöiden kesken. Suurin osa häiriöstä saatiin korjattua 1–3 tunnissa. Pitkäkestoisia yli 6 tunnin häiriöitä esiintyi vain kaksi, joista molemmat johtuivat maanrakennustöiden aiheuttamista kaapelikatkoista.

Luonnonilmiöiden aiheuttamat sähkökatkokset aiheuttavat viestintäverkkokatkoksia edelleen, mutta niiden pitkäkestoiset vaikutukset palvelujen toimivuuteen ovat vähentyneet. Tästä kiitokset menevät sähkö- ja teleyritysten yhteistyön parantumiselle. Suurin osa vuoden 2014 häiriöistä olikin maanrakennustöiden, ohjelmisto- tai ohjelmointivirheiden seurausta.

Yksittäisistä häiriötapauksista eniten huomiota saivat Elisan ja Soneran verkossa tapahtuneet laajavaikutteiset häiriötilanteet, joihin johtaneita syitä Viestintävirasto on selvittänyt teleyritysten kanssa vastaavien tapahtumien välttämiseksi ja arvioidakseen, onko teleyrityksissä noudatettu määräyksiä.

Elisan häiriö johtui virheistä - Soneran ohjelmistoviasta

Elisan viestintäyhteyksissä oli 26.11.2014 vakava häiriö, jonka vaikutukset näkyivät noin kahdeksan tunnin ajan ulkomaanyh-

teyksiä hyödyntävissä palveluissa. Häiriö alkoi, kun kaivinkone katkaisi ulkomaanliikenteessä käytetyn runkokaapelin. Elisan toiselle ulkomaanyhteydelle oli tehty samalla viikolla muutostöitä, mutta yhteys oli unohdettu ottaa takaisin käyttöön.

Soneran matkaviestinverkoissa ilmeni 16.12.2014 lähes kaikkiin sen matkaviestinverkon asiakkaisiin vaikuttanut häiriö, joka kesti noin 1,5 tuntia. Häiriön syynä oli ohjelmistovirhe, joka vaikutti useisiin verkon laitteisiin samanaikaisesti.

Viestintäviraston selvitysten mukaan molempien teleyritysten verkkojen rakenteet ja ylläpitoikätytännöt ovat vastanneet Viestintäviraston valvomaa säädäntöä. Yleisesti merkittävä osa verkkojen vikatilanteista jää käyttäjiltä havaitsematta, koska operaattoreiden varmistusjärjestelmät ehkäisevät asiakkaille näkyvät vaikutukset.

Elisan häiriö aiheutui kahdesta täysin erillisestä, mutta samanaikaisesta tapahtumasta, ja TeliaSoneran useassa laitteessa käytetyssä ohjelmistosta. Tällaiset tapaukset ovat harvinaisia ja niiden ennakoiminen hankalaa. Ennaltaehkäisemisen lisäksi tärkeää on, että teleyrityksillä on valmiudet reagoida nopeasti tilanteiden korjaamiseksi.

TeliaSoneran tiedottamisessa kyseisestä häiriöstä Viestintävirastolle ja käyttäjille oli puutteita vaatimuksiin nähden. TeliaSonera on ilmoittanut uudistavansa Viestintävirastolle tiedottamista vuoden 2015 alusta alkaen ja myös asiakastiedottamisen kehittämisen on Sonerassa otettu tapahtuman seurauksena lisäselvitykseen.

**Viestintä-verkoissa
14 vakavaa
häiriötä**

Tarkastustoiminta

Viestintäviraston Kyberturvallisuuskeskus tarkasti televerkkojen ja -yritysten toimintaa niiden tietoturvallisuutta ja häiriön sietokykyä koskevien määräysten valossa. Viranomaisten tietojärjestelmien tietoturvallisuuden tarkastustoimintaan saatiin Kyberturvallisuuskeskuksen lisäksi mukaan ensimmäinen kaupallinen yritys.

Teknisissä tarkastuksissa havaittiin puutteita

Viestintäviraston teknisten määräysten tarkoituksena vähentää häiriöiden vaikutuksia palvelujen käyttöön ja taata, että viestintäverkot toimivat mahdollisimman laadukkaasti. Teleyritystarkastukset ovat tehokas tapa valvoa, että tekniset vaatimukset, toimintatavat ja dokumentointi on Viestintäviraston valvomien määräysten mukaista. Vuonna 2014 on arvioitu vuosina 2012 ja 2013 toteutettujen laajamittaisten tarkastuskäyntien tuloksia ja seurattu annettujen korjauskehotusten toteutusta teleyrityksissä.

Tulokset vaihtelivat teleyrityskohtaisesti. Osalla toteutukset vastasivat varsin hyvin määräyksiä, kuin toisilla todettiin enemmän epäkohtia. Kokonaismäärällisesti merkittävimmät puutteet todettiin akkujen varmistusajoissa, laitetilojen varavoimakoneiden liitännöissä, laadunvalvonnassa sekä tehonsyöttö- ja olosuhdehäilytyksissä. Yksittäisiä puutteita havaittiin lukuisten vaatimusten osalta. Kaikista havaituista ongelmista on teleyrityksille annettu korjauskehoitteet, joiden toteutusta on vuonna 2014 seurattu.

Tyypillisimmät puutteet aiheuttavat käyttäjille ongelmia erityisesti sähkökatkojen aikaan. Akkuvarmistusten riittämättömyys aiheuttaa matkaviestinverkon palveluihin katkoksia lyhyiden sähkökatkojen aikaan, jolloin akut pitävät huolta tukiaseman toiminnasta. Sähkökatkon pitkittyessä puolestaan siirrettävä varavoima on tarpeen, mutta liitännämahdollisuus on oltava ennalta tunnossa. Olosuhdehäilytykset taas auttavat teleyrityksiä reagoimaan laitetilä

ongelmiin, esimerkiksi vesivahinkojen yhteydessä. Korjaavien toimenpiteiden käynnistäminen on mahdotonta, mikäli teleyritys ei saa tietoa ongelmasta laitteen sijaitessa vuokratussa tilassa.

Tarkastusten kohteina olivat muun muassa DNA Oy, Elisa Oyj, TeliaSonera Finland Oyj ja merkittävimmät Finnet-yhtiöt. Tarkastuskäynti toteutettiin yhteensä 26 teleyritykseen.

Tarkastustoiminnan avulla voidaan arvioida, kuinka hyvin teleyritysten palvelujen käytännön toteutukset ja toimintatavat vastaavat annettuja määräyksiä. Tuloksia voidaan myös hyödyntää määräysten kehittämisessä ja Viestintäviraston valvonnan kohdentamisessa. Lisäksi vierailut toimivat hyvänä olemmanpuoleisena palautekeskusteluna. Kokonaisuutena tarkastuskäyntien tulokset osoittavat niiden tarpeellisuuden erityisesti parantaessa teleyritysten varautumista vakaviin häiriötilanteisiin.

Tarkastuksissa havaitut tyypillisimmät puutteet teleyritysten toiminnassa

Varmistamisessa havaitut puutteet (M54)

- Liian lyhyitä varateholähteiden (akkujen) varmistusajoja oli 22 teleyrityksellä.
- Siirrettävän varavoimakoneen liitäntöjä puuttui 20 teleyritykseltä.
- Tasasuuntaajien N+1 -varmistuksissa oli puutteita 13 teleyrityksellä.

Verkkojen ylläpidossa ja tiedottamismenettelyissä havaitut puutteet (M57)

- Tehonsyöttö- ja olosuhdehäilytysten siirtoa vuokralaitetoista vuokralaiselle ei ollut järjestetty 18 teleyrityksessä.
- Häiriökarttatoteutuksissa oli puutteita 9 teleyrityksellä (huomio: toteutuksen siirtymäaika ei ollut tarkastusajankohtana vielä päättynyt).
- Käyttäjille tiedottamisessa oli puutteita muun muassa menettelyjen ja tiedotteiden sisällön osalta 7 teleyrityksellä.

Palvelun laadun seurannassa havaitut puutteet (M58)

- Laadunvalvontatoimenpiteiden toteutuksessa ja dokumentoinnissa oli puutteita 20 teleyrityksellä.
- Televisiotoiminnan laadunvalvontamenettelyt olivat puutteellisia 12 kaapelitelevisiopalveluja tarjoavalla teleyrityksellä.
- Puhelin- ja laajakaistaliittymien toimitusvarmuutta ei ollut mitattu eikä tilastoitu 6 teleyrityksessä.

Häiriöiden käyttäjätiedotuksen valvonta

Teleyrityksillä on velvoite ilmoittaa käyttäjille viestintäpalvelujen häiriötilanteista mm. verkkosivuilla. Velvoitteen käytännöntöteutusta seurattiin normaalia laajemmassa valvonnassa vuonna 2014. Syynä laajalle valvonnalle oli useat Viestintäviraston tietoon tulleet tapaukset, joiden yhteydessä oli syytä epäillä tiedotuksessa olevia yleisiä puutteita.

Valvonnan tulokset paljastivat puutteita teleyritysten käyttäjille tiedottamisessa - puolella valvotuista teleyrityksistä ei ollut paikkaa karttamuotoiselle tiedottamiselle ja käyttäjille tärkeä arvio siitä, milloin vika tai häiriö on poistunut, puuttui melko usein. Toisaalta tekstimuotoinen tiedottaminen oli useimmilla teleyrityksillä melko hyvällä tasolla. Viestintävirasto on yhteydessä tuloksista teleyrityksiin ja arvioi tarpeita jatkotoimenpiteille.

Tuotehyväksynnot

Viestintäviraston National Communication Security Authority (NCSA) -toiminnon vastuulla on muun muassa arvioida ja hyväksyä salaustuotteita viranomaiskäyttöön. Monet salaustuotteille asetettavista vaatimuksista liittyvät valtioiden väliseen luottamuksellisten tietojen vaihtoon. Suomalaisten salaustuotteiden hyväksynnällä edistetään suomalaisten yritysten liiketoimintamahdollisuuksia.

Salaustuotearviointit edellyttävät erikoisosaamista. Arviointiprojektit ovat usein pitkäkestoisia ja vaativat jatkuvaa kommunikointia valmistajan tuotekehityksen kanssa. Viestintävirasto esimerkiksi tarkastaa tuotteen ohjelmiston lähdekoodista, että tuote

tekee täsmälleen sitä, mitä valmistaja lupaa ja mitä asiaankuuluvat määräykset vaativat. Lähdekoodista tarkastetaan myös, ettei ohjelmistossa ole sitä heikentäviä haavoittuvuuksia.

Vuonna 2014 salaustuotehyväksyntäprosessin hyväksytysti läpäisi kaksi tuotetta. Lisäksi NCSA-toiminto arvioi myös muiden kuin salaustuotteiden tuoteturvallisuutta. Vuoden 2014 aikana tuoteturvallisuusarvioinnin läpäisi kaksi tuotetta joista esimerkiksi voidaan mainita Blancco Oy:n Blancco 5-tiedonhävitystuote.

Viranomaisten järjestelmien tarkastukset

Valtioneuvoston asetuksen ja päätöksen mukaisesti tiedonkäsittely on järjestettävä ja tehtävä valtionhallinnossa tietoturvallisesti. Tietoturvallisuuden toteutumista on myös arvioitava. Tietoturvallisuuteen vaikuttavat hyvin monet asiat eikä se kosketa pelkästään tietotekniikkaa.

Laadukas tietoturvallisuuden arviointi, joka todella paljastaa mahdolliset piilevät virheet järjestelmien ja organisaation toiminnassa, tai luotettavasti osoittaa, ettei merkittäviä virheitä ole, on erityistä ammattitaitoa vaativaa työtä. Siksi organisaatiot mielellään antavat tietoturvallisuutensa arvioinnin siihen erikoistuneen organisaation tehtäväksi.

Arvioinnissa on perehdyttävä syvällisesti organisaation tietojenkäsittelyyn, mikä voi paljastaa arvioijalle luottamuksellisia tietoja. Salassapitosäädökset ovat käytännössä rajanneet muut kuin viranomaiset pois valtionhallinnon tietoturvallisuuden arviointiin soveltuvien organisaatioiden joukosta.

Tietojärjestelmiä tai tietoliikennejärjestelmiä, joissa käsitellään viranomaisen turvallukiteltua tietoa (ST IV-II), tuli vuoden aikana 2014 Viestintäviraston Kyberturvallisuuskeskuksen arvioitavaksi tai hyväksyttäväksi 13 kappaletta. Järjestelmäkohtaiset arviointi- tai hyväksyntäprosessit voivat ajallisesti kestää useita kuukausia, järjestelmän tilanteesta sekä laajuudesta riippuen.

Kysyntä tietoturvallisuuden arvioinneille on paljon suurempi kuin mihin Viestintäviraston resurssit riittävät. Suurin osa valtionhallinnon tietojärjestelmistä on tarkoitettu sellaisen luottamuksellisen tiedon käsittelyyn,

jonka paljastuminen ei aiheuttaisi merkittävää uhkaa yhteiskunnan turvallisuudelle, vaan seuraukset olisivat paljon rajatumpia (ST IV). Sellaiset järjestelmät vastaavat pitkälti tavallisten yritysten tietojärjestelmiä. Niiden tietoturvallisuuden tarkastaminen on jo pitkään ollut vakiintunutta liiketoimintaa, joten sitä on tarkoituksenmukaista hyödyntää myös valtionhallinnossa.

Hyväksytyllä tietoturvallisuuden arviointilaitoksella tarkoitetaan toimijaa, joka on Viestintäviraston hyväksymä ja toimii viranomaisvalvonnassa. Hyväksytty laitos voi toimeksiannosta suorittaa esimerkiksi viranomaisten tietojärjestelmien arviointeja sekä viranomaisen salassa pidettävää tietoa käsittelevien yritysten tietoturvaluustason arviointeja. Valtionhallinnon viranomaiset voivat 1.6.2015 alkaen käyttää tietojärjestelmiensä tietoturvallisuuden arvioinnissa ai-noastaan Viestintäviraston tai sen hyväksymän arviointilaitoksen palveluja.

Kyberturvallisuuskeskus antoi lokakuussa 2014 KPMG IT Sertifiointi Oy:lle määräaikaisen hyväksynnän toimia tietoturvallisuuden arviointilaitoksista annetun lain mukaisena arviointilaitoksena. Hyväksynnän perusteella KPMG IT Sertifiointi voi tehdä virallisia kansalliseen turvallisuusauditoinnin KATA-KRI-kriteeristöön ja valtionhallinnon tietoturvaohjeen VAHTI-kriteeristöön perustuvia suojaustason IV mukaisia tietoturvaluustason arviointeja. Hyväksyntä on voimassa 1.2.2015 asti, johon mennessä yrityksen tavoitteena on täydentää pätevyysaluetta kattamaan ISO 27001-standardin mukaiset sertifiointit sekä VAHTI-toimitilaturvaluustousarvioinnit.

Useat muutkin tietoturvaluustouden arviointiin erikoistuneet yritykset ovat osoittaneet kiinnostusta arviointilaitostoimintaa kohtaan.

Tietoyhteiskuntakaari ohjasi parantamaan määräyksiä

Viestintäviraston määräysten uudistamistyö käynnistyi vuonna 2013, jolloin laadittiin suunnitelmat määräysten päivittämisestä ja mahdollisten uusien määräysten laatimisesta tietoyhteiskuntakaaren (TYK) ja muiden määräyksiin vaikuttavien säädösten pohjalta.

Uudistamistyön tavoitteena oli selkeyttää määräyskokonaisuutta ryhmittelemällä määräysten sisältöä uudestaan sekä samalla vähentää määräysten kokonaismäärää. Merkittävimmät muutokset kohdistuivat tietoturva- ja häiriötilannemääräyksiin.

Lähtötilanteessa Kyberturvallisuuskeskuksen toimialalle kuuluvia määräyksiä oli yhteensä 13 kappaletta. Ne korvautuivat seitsemällä uudella tai päivitettyllä määräyksellä. Kaikki määräykset tulivat voimaan 1.1.2015. Niistä tunnistuspalveluita ja laatuvarmenteita koskeva määräys pohjautuu muuhun lainsäädäntöön kuin tietoyhteiskuntakaareen ja sen valmistelu tapahtuu aikaisintaan vuonna 2015.

Tietoyhteiskuntakaaren määräysvaltuuksien pohjalta on todettu neljä sellaista aluetta, joilla toistaiseksi ei ole Viestintäviraston määräystä, mutta määräyksen laatiminen voi olla tarpeellista. Niiden tarpeellisuutta on selvitetty, mutta lopullisia päätöksiä määräysten laadinnasta ei tehty vuonna 2014.

Tietoturvamääräys

Teleyrityksiä velvoittavat, aiemmin neljässä eri määräyksessä asetetut tietoturvan suunnittelua ja toteuttamista koskevat vaatimukset kerättiin vuoden 2014 aikana yhdeksi uudeksi määräykseksi: määräys 67/2014 M *teletoiminnan tietoturvasta*.

Määräyksessä 67 määritellään teletoiminnan tietoturvaa koskevat vähimmäisvaatimukset. Määräyksellä pyritään varmistamaan, että tietoturvatekijät huomioidaan rutiininaisesti ja tehokkailla prosesseilla osana viestintäverkkojen ja -palvelujen toteutusta.

Suhteessa aiemmin voimassa olleisiin velvoitteisiin, valtaosa uudessa määräyksessä asetetuista vaatimuksista säilytettiin sisällöllisesti ennallaan. Muutoksia tehtiin siten,

että määräykseen lisättiin uutena velvoitteena vaatimus viestintäverkon tai -palvelun komponenttien hallintaliikenteen suojaamisesta. Dokumentointivaatimukset taas pyrittiin osoittamaan aiempaa selkeämmin.

Häiriötilannemääräys

Teleyrityksiä velvoittavat, aiemmin neljässä eri määräyksessä asetetut erilaisten häiriöiden havainnointia, hallintaa, niistä viranomaisille ja käyttäjille ilmoittamista sekä häiriöiden tilastointia koskevat vaatimukset kerättiin vuoden 2014 aikana yhteen määräykseen: määräys 66/2014 M *teletoiminnan häiriötilanteista*.

Määräyksessä käsitellään erilaisia teletoiminnan häiriötilanteita jaettuna kahteen eri tyyppiin:

- tilanteet, joissa teleyrityksen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus (*tietoturvahäiriö*) ja
- tapahtumat, jotka estävät viestintäpalvelun toimivuuden tai häiritsevät sitä olennaisesti (*toimivuushäiriö*).

Määräyksellä 66 pyritään varmistamaan, että kaikilla teleyrityksillä on niiden omaan toimintaan soveltuvat, riittävät ja muutoinkin asianmukaiset keinot havaita sekä tietoturva- että toimivuushäiriöitä ja että teleyrityksillä on menettelyvalmiudet tällaisten tilanteiden ratkomiseen. Tarkoitus on myös luoda mahdollisimman selkeät ohjeet niin Viestintävirastolle kuin käyttäjillekin ilmoitusvelvollisuuden menettelyistä ja sisällöistä, jotta tarpeellinen tieto pystytään itse häiriötilanteessa tuottamaan ja toimittamaan rutiininomaisesti.

Suhteessa aiemmin voimassa olleisiin velvoitteisiin, merkittävimpiä muutoksia tehtiin lähinnä häiriöistä ilmoittamista ja tilastointia koskeviin vaatimuksiin. Koska henkilötietojen tietoturvaloukkauksista ilmoittamisen

Viestintävirasto
terävöittää
tekniistä
ohjausta ja
valvontaa

menettelyt on harmonisoitu Euroopan komission asetuksella 611/2013, määräyksessä 66 päädyttiin useiden rinnakkaisten ilmoitusmenettelyjen välttämiseksi siihen, että kaikki tietoturvahäiriöt ilmoitetaan mainitun asetuksen mukaisesti.

Varautumisen ohjaus

Häiriötilanteiden yhteistoimintaryhmä HÄTY:n toiminnan pääpaino vuonna 2014 oli voimakkaisiin ja laajoihin myrskyihin varautumisessa ja myrskyjen viestintä- ja sähkönjakeluverkoille aiheuttamista ongelmista toimimisessa.

HÄTY-ryhmä laati teleyrityksille sähkönkäyttöpaikkojen priorisointikriteerit, joiden perusteella matkaviestinverkkoyritykset laativat omien sähkönkäyttöpaikkojen priorisointilistauksen. Listasta jaettiin kaikille sähkönjakeluuyhtiöille niiden jakelualueella olevien teleyritysten priorisoitujen sähkönkäyttöpaikkojen tiedot.

Tietojen avulla sähkönjakeluuyhtiöt voivat huomioida kyseiset sähkönkäyttöpaikat verkkojensa viankorjaustoiminnassa, esimerkiksi laajojen ja voimakkaiden myrskyjen yhteydessä ja sähkön toimitusvarmuutta parantavia toimenpiteitä suunnitellessaan ja toteuttaessaan.

Lisäksi koottiin matkaviestinverkkoyritysten ajantasaiset valvomoyhteystiedot ja jaettiin ne kaikille sähkönjakeluuyrityksille. Kerättiin myös kaikkien sähkönjakeluuyhtiöiden valvomoyhteystiedot ja jaettiin ne kaikille HÄTY:ssä mukana oleville teleyrityksille.

Ryhmässä sovittiin myös keskinäisestä tiedonvaihdon ja ennen kaikkea luottamuksellisen tiedonvaihdon periaatteista, jotka julkaistiin Viestintäviraston ohjeena.

Loppuvuoden 2014 aikana Viestintävirasto teki selvityksen teleyritysten varautumissuunnittelun määräys- tai muista ohjaustarpeista. Tietoyhteiskuntakaari antaa Viestintävirastolle valtuutuksen antaa teleyritysten varautumisvelvollisuutta koskevia tarkempia määräyksiä, jotka voivat koskea muun muassa varautumissuunnitteluun liittyviä asiakirjoja ja niiden tarkempaa sisältöä.

Selvitystä varten Viestintävirasto tutustui Anvia Oyj:n, Digita Oyj:n, DNA Oy:n, Elisa Oyj:n ja TeliaSonera Finland Oyj:n valmius-

suunnitteluun ja siitä laadittuun dokumentaatioon, minkä perusteella laaditaan arviomuistio kyseisten teleyritysten valmiussuunnittelun nykytilasta, kehittämistarpeista sekä tarkoituksenmukaisista Viestintäviraston ohjauskeinoista asiassa. Tämän jälkeen kuullaan muistion julkisesta versiosta myös muita teleyrityksiä, liikenne- ja viestintäministeriötä sekä valtiovarainministeriötä.

Arviomuistion ja siitä saatujen lausuntojen perusteella päätetään tarkoituksenmukaisista ohjauskeinoista ja ohjauksen pääpiirteisestä sisällöstä sekä laaditaan toimintasuunnitelma vuodelle 2015.

Viestintävirasto osallistui vuonna 2014 seuraavien huoltovarmuusorganisaation (HVO) poolien työhön:

- aluepooli,
- ICT-pooli ja
- joukkoviestintä-/mediapooli.

Aluepoolissa tehtävä työ oli lähinnä ns. alueellisen varautumisen toimikuntien (ALVAR) toiminnan käynnistäminen ja vakiinnuttaminen vuoden 2014 alusta. ALVAR-toimikuntia on yhteensä viisi ja ne sijaitsevat eri puolilla Suomea ELY-keskusten yhteydessä. ALVAR-toimikunnissa käynnistyi mm. Sähkö/Teleharjoitusten valmistelut, jotka kukin ALVAR-toimikunta järjestää omalla toimialueellaan. Ensimmäinen harjoitus pidettiin marraskuussa Itä-Suomessa.

ALVAR-toimikunnissa, samoin kun HÄTY:ssä mietittiin näiden keskinäisen yhteistyön tarpeita ja muotoja.

ICT-poolissa vuoden 2014 painopisteinä oli kyberturvallisuus ja ennen kaikkea kolme käytännön projektia:

- Projekti 1/2014: Kriittisten informaatioekosysteemien tunnistaminen ja niiden varmistaminen
- Projekti 2/2014: Kyberturvallisuuden edistäminen verkostoitumalla
- Projekti 4/2014: Vaatimustenhallinnan perusteet

Viestintävirasto osallistuu näiden projektien työhön, jonka arvioidaan valmistuvan vuoden 2015 alussa.

Joukkoviestintä-/mediapoolia koskeva vuoden 2014 merkittävin tapahtuma oli, että HVO:ssa alettiin selvittää ja suunnitella joukkoviestintäpoolin ja graafisen poolin yhdistämistä mediapooliksi. HVO päätti toteuttaa yhdistämisen ja mediapoolin perustamiskokous pidettiin 5.9.2014. Viestintäviraston joukkoviestintäpoolissa ollut edustaja jatkaa mediapoolissa.

SOPIVA-suositukset

Yhteiskunnan verkottuessa ja eri organisaatioiden välisten riippuvuuksien kasvaessa yhä suurempi osuus organisaation kriittisestä toiminnasta tapahtuu sen itsensä suoran vaikuttamisen ulkopuolella. Tällöin yksittäisen toimijan (yrityksen tai muun organisaation) omassa hallinnassa olevien riskien hallintakeinojen vaikuttavuus vähenee. Siksi on tärkeää, että toimijat voivat sopimuksilla, vaatimuksilla, ohjeilla ja auditoinneilla vaikuttaa siihen, miten niiden yhteistyökumppanit ovat varautuneet oman toimintansa häiriöihin.

Elinkeinoelämän, Huoltovarmuuskeskuksen ja muun julkishallinnon yhteistyönä on laadittu joukko suosituksia ja sopimusten mallilauseita toimijoiden yhteistyöverkostojen jatkuvuudenhallintaa varten.

SOPIVA-suositusten ja -mallilauseiden tarkoituksena on levittää hyviä jatkuvuudenhallinnan käytäntöjä yhteistyöverkostoissa sekä osaltaan varmistaa, että organisaation oma toiminta voi jatkua ilman häiriöitä. SOPIVA-suosituksissa on kehitetty yrityksille ja organisaatioille työkaluja, joilla parannetaan organisaation toimintavarmuutta erilaisten toimintaa uhkaavien tilanteiden varalta. Samalla huolehditaan koko yhteiskunnan häiriöttömän toiminnan jatkumisesta. Suositusten hallinnointi ja käytön edistäminen siirtyi osittain Viestintäviraston vastuulle vuonna 2014.

Vuoden 2014 jälkimmäisen puoliskon aikana Kyberturvallisuuskeskus kävi yritysten ja organisaatioiden kanssa SOPIVA-suositusten käytöstä, kehitystoiveista ja tarvittavasta tuesta suositusten käyttöönottoa varten. Lisäksi Kyberturvallisuuskeskuksessa on kehitetty soveltuvia työvälineitä SOPIVA-suositusten käyttöönoton tueksi.

Kansallisen tietoturvallisuuden kehittäminen

Viestintävirasto edistää internetpalvelujen käyttöä kehittämällä kansallista tietoturvallisuutta. Kyberturvallisuuskeskuksessa käsitellään yksittäisten kansalaisten, yritysten ja yhteisöjen sekä teleyritysten asiakasyhteydenottoja.

Neuvontaa tunnistamistietojen käsittelyoikeuksista ja yksityisyyden suojasta

Neuvontatapausten joukosta ei ole selkeästi hahmotettavissa tyyppitapauksia, sillä jokainen yksittäinen kysymyksensä on aina oma asiakokonaisuutensa, johon liittyy omia erityisiä piirteitä. Joitain trendejä neuvontatapauksissa on kuitenkin havaittavissa.

Yksityisyyden suojaan liittyen Viestintäviraston Kyberturvallisuuskeskus on syksyllä 2014 laatinut käyttäjille ohjeistuksen *Yksityisyyden suoja sopimuksissa*. Ohjeistuksessa pyritään kiinnittämään käyttäjän huomio siihen, mistä erilaisista yksityisyyden suojaan liittyvistä asioista internetpalveluiden sopimuksissa voidaan sopia. Ohjeessa esitellään muun muassa käyttäjälle lista, jonka avulla voidaan tarkastella sopimukseen liittyviä yksityisyyden suojaan vaikuttavia ehtoja. Suostumus on yksi tietojenkäsittelyperuste ja tällainen suostumus voidaan saada myös internetpalvelusopimuksessa.

Suositus kansainvälisesti toteutetun palvelun tietoturvasta tiedottamiseen

Kesän 2013 jälkeen keskusteltiin yleisesti ulkomaisten viranomaisten kansainvälisen massatiedustelun vaikutuksista luottamuksellisen viestinnän suojaan. Viestintäviraston vuonna 2013 tekemien selvitysten perusteella suomalaiset teleyritykset eivät ole havainneet tiedustelutoiminnalla olleen vaikutuksia yleisten viestintäpalvelujen tietoturvaluuteen.

Koska osa viestintäpalveluista toteutetaan osin tai kokonaan Suomen ulkopuolella tai hyödyntäen ulkomaisten yritysten tarjoamia palveluja ja näin ollen palvelutoteutukseen saattaa kohdistua Suomen lainsäädännöstä poikkeavaa sääntelyä, on perusteltua, että palvelujen käyttäjillä on saatavilla tietoa asiasta. Tällaisen tiedon avulla käyttäjä voi itse

arvioida, millaisia mahdollisia uhkia hänen viestintäänsä ja tunnistamistietoihin kohdistuu.

Viestintävirasto valmisteli keväällä 2014 yhteistyössä teleyritysten kanssa suosituksen (205/2014 S) siitä, missä tilanteissa, miten ja millaista tietoa teleyritysten tulisi tarjota käyttäjille kansainvälisen kytköksen sisältävistä palvelutoteutuksista. Viestintävirasto aikoo vuoden 2015 aikana valvoa, että suosituksen mukaista tietoa tosiasiallisesti on käyttäjien saatavilla.

Kyberturvallisuuskeskuksen teemakuukaudet

Kesän lopulla Kyberturvallisuuskeskus alkoi julkaista Tietoturva nyt! -artikkeleita ajankohtaisista ja ajattomista tietoturva-aiheista. Tietoturva nyt! on vuosia ollut Kyberturvallisuuskeskuksen ja sen edeltäjän CERT-FI:n julkaisukanava ajankohtaisia ilmiöitä taustoittaville kirjoituksille.

Ensimmäinen teema oli nettihuijaukset, joita käsiteltiin heinä- ja elokuun ajan. Teema liittyi keväällä alkaneisiin suomalaisiin kohdistettuihin huijauksen kampanjoihin, joissa kalasteltiin verkkopankkitunnuksia. Syyskuun teema oli langattomien lähiverkkojen tietoturva, lokakuussa käsiteltiin päätelaitteiden tietoturvalista käyttöä ja yksityisyyden suoja. Pilvipalveluiden tietoturva oli vuorossa marraskuussa ja joulukuussa kerrottiin salasanojen muodostamisen, käytön ja hallinnan hyvistä käytännöistä. Lokakuun teema oli sovitettu yhteen Euroopan Unionin kyberturvallisuuskuukauden teemojen kanssa.

Teemakirjoitukset on kirjoitettu mahdollisimman yleistajuiseen muotoon, jotta ne olisivat hyödyllisiä suurelle yleisölle. Joukossa on myös yksityiskohtaisempia osuuksia järjestelmien ylläpitäjille. Kyberturvallisuuskeskus jatkaa teemakuukausia myös vuonna 2015.

Kansainvälinen yhteistyö

Kyberturvallisuuskeskuksen toiminnan perusedellytyksiä on laajamittainen kansainvälinen yhteistyöverkosto. Toimivia yhteistyösuhteita tarvitaan sekä tietoturvaloukkaustapausten selvittelyssä että kansainvälisten tietoturvavelvoitteiden koordinointiin liittyvissä kysymyksissä.

CERT-yhteistyö

Aktiivinen tiedonvaihto CERT-toimijoiden kesken selvittelyn kohteena olevista tietoturvaloukkaustapauksista on oleellinen osa CERT-toimintaa. Kyberturvallisuuskeskuksella on toimivat yhteistyökontaktit käytännössä kaikkiin kansallisiin CERT-toimijoihin maailmassa. Yksi tärkeistä yhteistyöjärjestöistä on Forum of Incident Response and Security Teams (FIRST).

Tietoturvaloukkaustapausten yhteydessä tiedotetaan ulkomaisia CERT-toimijoita kyseisessä maassa havaitusta tietoturvallisuutta vaarantavasta toiminnasta, esimerkiksi haittaohjelmien levitykseen käytetyistä www-palveluista ja haittaohjelmien komentopalvelimista. Yhteydenottoja valmisteltaessa huomioidaan tapauskohtainen turvallisuustilanne ja tarpeet tiedonvaihtoon. Kansainvälisten kontaktien kautta saadaan myös esimerkiksi ennakkotietoja julkaistaviksi aiotuista ohjelmistohaavoittuvuuksista.

Vakiintunut englanninkielinen yleisnimitys teknisen tietoturvan parantamiseksi toimiville ryhmille on Computer Emergency Response Team (CERT).

EGC-ryhmä

Teknisen yhteistyön kannalta keskeisin kansainvälinen yhteistyöryhmä on EGC (European Government CERTs group). Ryhmän jäsenenä on kansallisia tai valtiollisia CERT-toimijoita 14 eri organisaatiosta. Ryhmän operatiivinen yhteistyö tietoturvauhkien ja -loukkausten selvittelyssä on päivittäistä. Varsinaisia tapaamisia järjestettiin kolme kertaa viime vuoden aikana.

Nordic CERT Cooperation (NCC)

Pohjoismaisten kansallisten CERT-toimijoiden yhteistyö on järjestäytynyt Nordic CERT Cooperation (NCC) -nimikkeen alle. Yhteistyössä ovat mukana Viestintäviraston Kyber-

turvallisuuskeskus, CERT-SE (Ruotsi), NorCERT (Norja), Center for Cybersikkerhed (Tanska) ja CERT-IS (Islanti).

NCC-ryhmä otti vuoden 2014 aikana käyttöön turvaluokitellun tiedon siirtoon hyväksytyn tietoliikenneverkon (NCIS, Nordic National CERT Information Sharing Network) ryhmän jäsenten välistä luottamuksellista tiedonvaihtoa varten. Ryhmä järjestää jäsenilleen yhteisiä harjoituksia ja koulutustilaisuuksia. Vuoden 2014 aikana Kyberturvallisuuskeskus osallistui teollisuusautomaatiojärjestelmien tietoturvaan liittyvään koulutustilaisuuteen Ruotsissa. Teemaan liittyvä harjoitus toteutetaan vuoden 2015 alkupuolella.

ENISA

Kyberturvallisuuskeskus osallistui kahteen ENISA:n CERTs in Europe workshop -tapamiseen sekä vuoden 2014 aikana useassa osassa järjestettyyn Cyber Europe 2014 -harjoitukseen. Lisäksi osallistuttiin tietoturvaloukkausten ilmoitusvelvollisuutta harmonisoivan Article 13a -työryhmän työhön. ENISA on Euroopan Unionin tietoturvallisuusvirasto.

Terena TF-CSIRT

TF-CSIRT on eurooppalaisen tutkimusverkko-organisaatio TERENA:n yhteistyöryhmä eurooppalaisille CERT-toimijoille. Mukana on kansallisia, akateemisia ja kaupallisia CERT-ryhmiä. TF-CSIRT ylläpitää Trusted Introducer -palvelua joka ylläpitää luetteloa eurooppalaisista CERT-toimijoista sekä sertifioi CERT-ryhmien toimintaa. Viestintäviraston Kyberturvallisuuskeskuksen CERT-toiminta auditointiin ja sertifioitiin Trusted Introducer -palvelun kautta vuoden 2014 aikana.

NCSA-yhteistyö

NCSA-toiminto yhtenä nimettynä turvallisuusviranomaisena osallistuu aktiivisesti kansainväliseen yhteistyöhön.

EC/ESA

Euroopan komission alaisissa maailmanlaajuisissa satelliittihankkeissa toimii useita turvallisuuteen liittyviä alatyöryhmiä, joissa valmistellaan, käsitellään ja hyväksytään satelliittihankkeita koskevia turvallisuusvaatimuksia ja ohjataan niiden toteutumista.

Liikenne- ja viestintäministeriö nimesi 11.11.2014 Viestintäviraston kansalliseksi PRS-viranomaiseksi (Public Regulated Service). PRS-viranomainen vastaa Suomen osalta eurooppalaisten satelliittihankkeen tarjoamien palveluiden turvallisuudesta. Näiden palveluiden kansallinen hallinta on edellytys sille, että Suomen viranomaiset ja eräät muut infrastruktuurin kriittiset toimijat saavat käyttöönsä erityisesti Galileo-järjestelmän viranomaispalvelujen kautta jatkossa tarjottavan salatun ja häiriösietoisien paikka- ja aikasignaalin. Näiden signaaleiden vastaanottokyky on tärkeä osa nyky-yhteiskunnan, esimerkiksi pankkijärjestelmien, toimivuutta.

Uusi viranomaistoiminto antaa myös suomalaiselle elinkeinoelämälle mahdollisuuden osallistua kansainvälisessä yhteistyössä tarvittavien teknologioiden kehittämiseen ja kaupallistamiseen. Galileon viranomaispalveluiden testikäytön ennakoidaan alkavan vuoden 2016 alussa.

Common Criteria Recognition Arrangement

Viestintävirasto on Suomen edustajana maailmanlaajuisessa Common Criteria -tuotehyväksyntäjärjestelyssä. Järjestelmä perustuu tietotekniikkatuotteiden hyväksyntö-

jen vastavuoroiseen tunnustamiseen. Kansainväliset tuotehyväksynnät voivat auttaa suomalaisten tietotekniikkatuotteiden markkinoille pääsyä tietyillä alueilla.

Säätelyyn liittyvä kansainvälinen yhteistyö

Kyberturvallisuuskeskus osallistuu aktiivisesti eurooppalaisten säätelyviranomaisten väliseen yhteistyöhön sekä pohjoismaisella että eurooppalaisella tasolla. Yhteistyötä tehdään muun muassa varautumisessa (NORDIC NIS-, IRG NIS- ja Artikla 13 -työryhmät). Yhteistyön tavoitteena on vaihtaa tietoa ajankohtaisista ilmiöistä, jakaa kokemuksia erilaisten ratkaisujen ja toimintamallien toimivuudesta sekä tukea säätelyviranomaisten säädösvalmistelua.

eIDAS (electronic identification and trust services) -asetuksen artikla 19 asettaa tietoturva vaatimukset luottamuspalveluiden tarjoajille. ENISA on komission toivomuksesta perustanut asiantuntijaryhmän, jonka tavoitteena on muun muassa varmistaa artiklan 19 tehokas ja mahdollisuuksien mukaan harmonisoitu toimeenpano jäsenmaissa. Ryhmän ensimmäinen kokous oli marraskuussa 2014.

ETSI (European Telecommunications Standards Institute) vastaa televiestinnän eurooppalaisesta standardoinnista. Kyberturvallisuuskeskus on mukana ETSI:n komiteoiden EMTEL (Emergency Telecommunications) ja ESI (Electronic Signatures and Infrastructure) työssä. EMTEL kokoaa hätäliikenteen toteutusta koskevia vaatimuksia hallinnoilta, teleyrityksiltä ja teollisuudelta ja laati niiden pohjalta dokumentteja muissa ETSI:n komiteoissa tehtävän työn pohjaksi. ESI laatii sähköistä allekirjoitusta koskevia standardeja. Tällä hetkellä pääosa työstä liittyy eIDAS -asetuksen ja sen toimeenpanosäädösten pohjana toimivien standardien laadintaan.

Yhteystiedot

Viestintävirasto

PL 313

Itämerenkatu 3 A

00181 Helsinki

Puh: 0295 390 100 (vaihde)

kyberturvallisuuskeskus.fi

viestintävirasto.fi