FICIX

Finnish Internet Exchange Point

Puolustusministeriö
Tiedonhankintalakityöryhmä

Lausunto tiedonhankintalakityöryhmälle

FICIX ry kiittää mahdollisuudesta lausua Puolustusministeriön tiedonhankintalakityöryhmälle kyberturvallisuusstrategian toimeenpano-ohjelmaan liittyvistä tiedonhankinnan aloitteista ja tietoturvauhkien torjumisesta.

Yleistä

Tiedustelutiedon hankkimisen ja käyttämisen pelisäännöt ovat nousseet kansainväliseen keskusteluun kesän 2013 jälkeen. Suomenkin tulee käydä tämä keskustelu, avoimesti ja todenperäisin argumentein, jotta tasapaino tarpeen ja resurssien panostamisen kesken löydetään yhteiskunnan hyväksymällä tavalla. FICIX ry pitää kannatettavana, että oikeusvaltion periaatteita noudatetaan selvittämällä jo voimassaolevan lain ja sääntelyn antamat mahdollisuudet sekä niiden kehittämistarve. Oikeusvaltion periaatteita noudatetaan myös käyttämällä parlamentaarista harkintaa päätettäessä tiedustelun tasosta ja menetelmistä. Tätä harkintaa tulisi käydä asiapohjaisen keskustelun kautta perustuen riittävään ymmärrykseen tietoverkkojen rakenteesta ja ohjauksesta.

Suomen turvallisuuteen kohdistuvat uhat ja niiden vaikutukset

Suomalainen yhteiskunta on voimakkaasti digitalisoitunut ja verkottunut. Yhteiskuntamme polttoaineena toimii tietoverkot joista ovat riippuvaisia niin kansalaiset, elinkeinoelämä kuin viranomaisetkin. Järjestelmiä joita voitiin käyttää tietoverkoista riippumatta, ei nykyään juuri enää ole. Näin ollen Suomen voidaan katsoa olevan erittäin muttei poikkeuksellisen haavoittuvainen tietoverkkojen kautta syntyviin uhkakuviin. Useat valtiot maailmassa jakavat saman tilanteen.

Tietoverkkoturvallisuudessa keskiössä ovat suomessa toimivat teleyritykset, varsinkin ne toimijat jotka operoivat kansainvälisiä tietoliikennekaapeleita ja verkkoja. Suomen lainsäädäntö edellyttää teleyrityksiltä korkeaa tietoturvatason ylläpitoa, poikkeamien havainnointia ja niihin puuttumista. Myös viranomaisille lait antavat toimivaltuuksia sekä normaalioloissa että poikkeusolojen vallitessa. Viranomaisilla on myös laaja määräysvalta tietoturvan tekniseen järjestämiseen.
Käsityksemme mukaan viranomaiset eivät juuri ole käyttäneet tai nähneet tarpeelliseksi käyttää lain sallimia puuttumiskeinoja. Tietoturva-asiat televerkkojen palveluiden osalta ovat käytännössä hyvin järjestettyjä ja yhteistyö teleyritysten, Viestintäviraston ja Huoltovarmuuskeskuksen kesken on tiivistä ja rakentavaa.

Keskeisin televerkkojen ja yleensäkin kriittisten verkkojen käytettävyyden uhka ovat palvelunestohyökkäykset. Maailmalla rekisteröityjen isoimpien hyökkäysten intensiteetti ylittää kansallisten siirtoverkkojen välityskyvyn. On tosin hyvin epätodennäköistä kuitenkin, että tällainen hyökkäys pystyisi etenemään Suomen valtiorajojen sisäpuolelle. Hyökkäys kilpistyisi käytännössä jo Keski-Euroopassa tai viimeistään muissa pohjoismaissa yksinkertaisesti välityskapasiteetin täyttymiseen.
Palvelunestohyökkäys jonkin yhteiskunnallisesti kriittisen toimijan infrastruktuuriin on taas hyvinkin mahdollinen. Tällaisen seuraukset voivat myös hyvinkin olla vakavat. On huomioitava, että teleyrityksillä on kaupallisesti tarjolla palvelutuotteita joilla hyökkäyksiä voidaan estää tai heikentää. On tilaajan vastuulla huolehtia, että verkon suojaus on oikein mitoitettu uhkaa vastaan eli ko. palveluiden hankkimista on syytä harkita mikäli kriittinen toiminta on alttiina hyökkäyksille.

Suomen kauttakulkuliikenne on toteutettu pääosin valopoluin (DWDM) tai vuokrakaapelein (IRU). Näiden osalta kapasiteetti on pois kansallisesta välityskapasiteetista ja siten niissä kulkevan liikenteen määrä tai laatu ei uhkaa Suomen turvallisuutta millään tavoin.

Monikansallisilla teleyrityksillä on ollut jo vuosia tosiasiallinen mahdollisuus tunnistaa ja torjua uhkia lähes globaalisti. Yritykset seuraavat verkkoliikennettä ja voivat vaikuttaa sen ohjaukseen merkittävästi ilman erityisiä viranomaislupia tai määräyksiä, täysin omien toimintaprosessiensa mukaisesti. Näin myös toimitaan sekä kapasiteetinhallinnan vuoksi että myös tietoturvan varmistamisen vuoksi.

Järjestelmien tietoturvauhkista vakavimmat ovat kohdistettuja murtoja, APT-hyökkäyksiä. Murrot toteutetaan haittaohjelmien avulla joihin ei ole saatavissa teknistä tunnistetta ja/tai kohde saastutetaan sosiaalisen vaikuttamisen kautta. Näin käyttäjä itse on toimillaan osallinen murtoon.
APT-murtoja on haastavaa tietoliikenteen seuraamisen keinoin tunnistaa. Näiden uhkien torjumisessa organisaation tietoturvakäytänteiden, sovellusten ja käyttäjien valveutuneisuuden taso on oleellinen. APT-murto voidaan havaita epänormaalista tietoliikenteestä joissain tapauksissa mutta ollakseen tehokas se edellyttää toimijakohtaista liikenteen seurantaa ja profilointia.

Suomalaista tietoverkkoturvallisuutta kehitetään parhaiten edistämällä teleyritysten tuotekehitystä ja asiantuntemusta kyberturvallisuuden osa-alueista ja uhkamalleista. Tämä osaamisen kehittäminen edistää myös kansallista kilpailukykyä. Teleyritysten mahdollisuuksia reagoida muutostilanteisiin liikenteenohjauksella, tarvittaessa vaikka estotoimin, voidaan parantaa kehittämällä tiedonvaihtoa viranomaisiin ja toimialan keskeisiin organisaatioihin. Tässä kehittämisessä Viestintäviraston Kyberturvallisuuskeskus on keskeisessä asemassa.

Oikeudelliset näkökohdat

FICIX ry:llä ei ole oikeusopillista osaamista arvioida kokonaisvaltaisesti niitä vaatimuksia joita Suomen lailta edellytetään tiedustelun ulottamiseksi telekaapeleihin tai viestiliikenteeseen laajemminkin. Näkökohdat jäljempänä ovat yleisluonteisia elinkeinoelämän edustajan tulkintoja.
Suomella on suvereniteetti itsenäisenä valtiona määrätä alueellaan sijaitsevien viestintäkaapeleiden käytöstä. EU direktiivit ja regulaatio vaikuttavat kuitenkin käytännössä kansalliseen itsemääräämisoikeuteen. Suomen etu on sovittaa nämä yhteen.

Tiedustelun toteuttaminen kuuntelulla käytännössä tarkoittaa Suomen kansalaisiin ja elinkeinonharjoittajiin kohdistuvaa telekuuntelua ilman rikosepäilyä. Perusoikeuksien suoja suomalaisessa lainsäädännössä on vahva. Tiedonhankinnan toteuttaminen toimeenpano-ohjelmassa kuvatulla tavalla vaatii sekä perustuslain tarkastelua että viestinnän lakien tarkastelua. Perusoikeuksien kaventamisen edellytyksenä on linjata koskeeko se koko kansaa ml. viranomaiset ja edustuslaitokset (Eduskunta, Oikeuslaitos, Presidentti) vai pelkästään siviilioikeushenkilöitä. Ensimmäisessä vaihtoehdossa tiedustelun rajaaminen on erittäin monimutkaista, jälkimmäisissä tapauksissa perustuslain §6 tulee herkästi arvioitavaksi. Tiedustelutiedon käytössä vaihdannan välineenä ulkovaltojen tai muiden tahojen kanssa tulee arvioitavaksi oikeushenkilön oikeudet ja mahdollinen korvausvastuu. Luovutettava tieto saattaa sisältää sellaisia yrityssalaisuuksia, patentti- tai tekijänoikeuden suojaamia tietoja tai liiketoimiin liittyviä asioita joista saattaa viestinnän osapuolelle koitua haittaa, vahinkoa tai arvon menetystä.

Euroopan ihmisoikeussopimuksiin ja muihin kansainvälisiin sopimuksiin liittyviä oikeusnäkökohtia on syytä selvittää. Tiedustelutoimintaa on kuitenkin useissa Euroopan maissa toteutettu joten asiaa lienee jo selvitetty ja tulkintoja on olemassa. [lähde: http://en.wikipedia.org/wiki/List_of_government_surveillance_projects]

Yhteiskunnalliset näkökohdat

Internet –liikenteen järjestelyt Suomessa ovat hyvin monitahoiset. FICIX ry ylläpitää valtakunnallisesti yhteenliittämispisteitä kolmella paikkakunnalla: Espoossa, Helsingissä ja Oulussa. Kaikissa FICIX -pisteissä on Internetin juurinimipalvelin jotka palvelevat globaalisti kaikkia Internetin käyttäjiä. FICIX:n ylläpitämät yhdysliikennepisteet ovat tarkoitettu kansallisen liikenteen vaihtoon jäsenten välillä. Muita suomessa toimivia yhdysliikennepisteitä ovat TREX Tampereella ja DIX Helsingissä (VoIP-yhteenliittäminen).

FICIX ry ei puutu jäsentensä liikenteenvaihtosopimuksiin millään tavalla, asia on jäsenten keskenään sovittava. Sopimukset tai niiden puuttuminen määräävät liikenteen tosiasiallisen kulun ja reitin. Sopimukset voivat kattaa pelkän Suomeen ohjautuvan liikenteen, useimmiten kuitenkin mukana on lähialueiden reittejä kuten Baltian ja Venäjän liikennettä. Sopimusten puuttuminen usein tarkoittaa, että liikennettä ei vaihdeta FICIX ry:n laitteiden kautta lainkaan.
Suomessa on tarkat määräykset (Viestintävirasto M13 B/2011) tietoturvan varmistamiseksi miten yhteenkytkeminen tulee suorittaa jotta tietoturvariskit minimoidaan. Myös FICIX ry on ohjeistanut jäsenensä yleisimmistä tietoturvakäytännöistä. Määräyksessä ja ohjeessa ei eroteta kansallista ja kansainvälistä liikennettä toisistaan.

Liikenteen kulkeminen teleyrityksen verkosta toisen teleyrityksen verkkoon määräytyy sen mukaan mitä verkkonumeroita (prefix, NLRI) toiselle teleyritykselle mainostetaan. Liikenne seuraa näitä mainostuksia linjakurikäytäntöjen mukaan (protokollat). FICIX ry:n jäsenet mainostavat toisilleen reittejä oman reitityspolitiikkaansa mukaan ja kahdenvälisiin sopimuksiin perustuen. On yleisesti tiedossa, että kaikki suomessa sijaitsevat televerkot eivät vaihda liikennettä FICIX –pisteissä lainkaan. Käytännössä liikenne kulkee tällöin transit –operaattorin kautta tai ulkomaisen yhdysliikennepisteen kautta (esim. Netnod Ruotsissa).
Riippuen transit –operaattorien valinnoista ja niiden yhteyksistä toisiinsa liikenne kahden suomalaisen Internet –käyttäjän välillä voi hyvin kiertää ulkomaiden kautta. Mikäli yhteenliittäminen suomalaisten verkkojen kesken on toteutettu Ruotsissa niin liikenne kiertää vähintäin Ruotsin kautta, mahdollisesti jopa kauempaa.

Useat suomalaisilta näyttävät Internetin palvelut tuotetaan tosiasiallisesti ulkomailta. Esimerkiksi *www.google.fi* hakukone vastaa Tukholman alueelta suomalaisten käyttäjien hakuihin. Palvelussa käytetyt hakusanat, kuten myös käyttäjän saamat vastaukset ja niistä tehdyt valinnat, ovat Suomen ulkopuolella seurattavissa.

Suomen oma Internetin maatunnus .fi on globaalisti hajautettu Ruotsalaisen Netnod AB:n toimesta. Hajautus palvelee käytettävyyttä ja hyökkäyskestävyyttä mutta samalla mahdollistaa sen, että nimipalvelinkyselyt suomen maajuureen ovat yleisesti seurattavissa useammassakin eri valtiossa Suomen ulkopuolella.

FICIX ry haluaa saattaa selkeästi tietoon, että ehdotetunlaisen kuuntelun tekninen järjestäminen koskee myös Suomen sisäistä liikennettä eli Suomi alkaisi salakuunnella omia kansalaisiaan.

Työryhmälle harkittavaksi

Tiedustelutietoa voi hankkia sopimusperusteisesti tahoilta joilla sellaista on. Vaihdon välineenä voi harkita käytettäväksi vastaostoja puolustusvoimien materiaalihankintojen yhteydessä. Tiedustelutietoa voi myös hankkia verkoista ja sen palveluista kustannustehokkaasti ilman kuunteluakin.
Kyberturvallisuuskeskuksen Havaro –järjestelmä on toiminnassa ja osoittanut käyttökelpoisuutensa. Järjestelmää voitaneen kehittää tarkemmin tiedustelutiedon tarpeisiin sopivaksi. Järjestelmän käyttöönottoa laajasti julkishallinnossa tulisi edistää. Havaro –järjestelmän, tai kaupallisesti saatavilla olevien monitorointijärjestelmien, avulla ja kautta tiedustelu on mahdollista kohdistaa siten, että sen piiriin ei aiheettomasti päädy sellaista viestintää jolla ei ole itseisarvoa tai se on ristiriidassa yhteiskunnan yleisen oikeustajun kanssa. Tiedustelun kohdistaminen myös mahdollistaa kustannuskontrollin hyvinkin tarkasti ja optimaalisesti.

Tiedustelulla saadun arkaluontoisen ulkovaltoja koskevan tiedon säilytys ja salassapito kansallisesti sisältää poliittisen riskin. Tietovuoto, joko järjestelmään tunkeutumisella tai henkilövuodolla, voi aiheuttaa ulkopoliittisen kriisin johon Suomen kyky vastata on heikko. Uhkakuvana voi pitää tilannetta, jossa tietovuoto johtaa vaikkapa pakotteisiin kuten kauppasaartoon tai Suomi joutuu sotilaallisen painostuksen alle. Tällaisessa tapauksessa, joista siis on esimerkkejä maailmalta jo, Puolustusvoimien toimet tehtäviensä toteuttamiseksi kääntyisivät itseään vastaan – toiminta olisi saattanut Suomen väestön vaaraan tai ollut elinkeinoille haitallinen.

Helsingissä, 5.2.2014

FICIX ry hallitus
plsta: Jorma Mellin
Puheenjohtaja