Nixu Oyj 6.4.2015

Petri Kairinen

**NIXU OYJ:N LAUSUNTO “SUOMALAISEN TIEDUSTELULAINSÄÄDÄNNÖN SUUNTAVIIVOJA” -MIETINTÖÖN**

**Taustaa:**

Nixu Oyj kiittää mahdollisuudesta antaa lausunto työryhmän mietintöön. Lausuntomme taustalla on Nixun rooli suomalaisia yrityksiä ja julkishallintoa palvelevana kyberturvallisuuden palveluyrityksenä. Tuemme tietoturvatyössä erittäin laajaa joukkoa isoja ja keskisuuria suomalaisia yrityksiä, jota kautta meille on kertynyt varsin hyvä kollektiivinen ymmärrys yritysten tietoturvan ja niiden kuluttaja-asiakkaiden tietosuojan tilanteesta ja tahtotiloista. Lisäksi tarkastelemme asiaa Nixun palveluksessa olevien yli 150 tietoturva-asiantuntijan näkemysten kautta. Heidän näkemyksensä peilaavat ymmärrystä kyseisten järjestelmien teknisistä toteutusmahdollisuuksista ja toisaalta laajaa tietoa ja ymmärrystä tällaisten järjestelmien mahdollisuuksista väärinkäytöksiin.

**Lausunto:**

Nykyaikainen digitaalinen yhteiskunta on haavoittuva. Valtiovallalla tulee olla mahdollisuus varautua poikkeusoloihin ja pitää yllä tilannetietoisuutta yhteiskuntaa uhkaavista mahdollisista kyberhyökkäyksistä. Kyberhyökkäyksen kohteeksi jouduttaessa yhteiskunnan täytyy pystyä vastaamaan puolustautuen tai vaikuttamalla hyökkäyksen lähteeseen. Tätä taustaa vasten näemme ehdottoman tarpeelliseksi saada Puolustusvoimille toimivaltuudet **tietojärjestelmätiedusteluun** ja myös laajemmin kybervaikuttamiseen poikkeustilanteessa, jolloin yhteiskuntaa vastaan kohdistuu valtiollisen tason uhkia.

**Tietoliikennetiedusteluun** liittyy merkittävä määrä muita näkökohtia. Lähtökohtaisesti mitä enemmän tietoa kerätään ja mitä laajempi järjestelmä on, sitä todennäköisempiä ovat väärinkäytökset. Tietoliikennetiedustelulla pystyttäisiin luomaan yksi tilannekuvakerros Suomen runkoverkkorakenteeseen. Tämä kerros pystyisi mahdollisesti tunnistamaan ja suodattamaan haluttua liikennettä. Poikkeusoloissa ja nykyaikaisen hybridisodankäynnin vallitessa Puolustusvoimilla tulisi näkemyksemme mukaan olla toimivaltuudet tunnistaa, tiedustella ja tarvittaessa estää vieraiden valtioiden ja asevoimien suorittama viestiliikenne suomalaisissa tietoverkoissa.

Suurimmat haasteet tietoliikennetiedustelun osalta liittyvät toteutustapaan, mielikuviin siitä ja siviililiikenteen osalta kansalaisten tietosuojaan. Käsittelemme näitä haasteita alla lyhyesti:

Kuvatulla tavalla toteutettuna tietoliikennetiedustelu ei tule estämään kehittyneitä vakoiluohjelmia kuin korkeintaan siinä tapauksessa, että niistä saadaan muilta tiedustelutahoilta tunnistetietoja. Jos tunnistetietoja taas olisi käytettävissä, pystyttäisiin näitä uhkia torjumaan jo monessa muussakin suojauskerroksessa. Oletettavaa on siis, että tiedusteluviranomaisilla ei ole mahdollisuutta jakaa näitä muualta saatuja tietoja laajemmin, joka olisi toimivan kyberturvan kannalta paras ratkaisu. Digitaalisen yhteiskunnan toimivan suojautumisen kannalta on siis olennaisen tärkeää, että yhteiskunnan muille toimijoille ei synny vaikutelmaa, että kuvattu lainsäädäntö ja sen myötä luotavat järjestelmät ja turvallisuusviranomaiset riittävät suojaamaan yhteiskunnan kyberhyökkäyksiltä. Tämä on erityisen tärkeää kansainvälisesti toimivien yritysten osalta.

Siviileihin kohdistuvan tiedustelun osalta on äärimmäisen tärkeää rajoittaa varsinaisen järjestelmän käyttö taholle, jolla on riittävä turvallisuuskulttuuri. Tämän tahon tulisi toimia kuvatulla tavalla portinvartijana ja valvontatoimien tulisi perustua erillisiin yksilöityihin ja oikeutettuihin toimeksiantoihin. Järjestelmän ei tule tukea laajantietomäärän keräämistä varmuuden vuoksi. Järjestelmäkokonaisuudelle tulisi lisäksi järjestää lainmukainen valvonta riippumattoman tahon toimesta.

Tulevaisuudessa liikenteen siirtyminen enenevissä määrin salattuihin verkkopalveluekosysteemeihin (kuten Facebook, Google, WhatsApp) tulee muodostamaan kasvavan haasteen tietoliikennetiedustelun toimivuudelle ylipäätään.

Asiakasyritystemme näkökulmasta näemme kuvatun tyyppisen lainsäädännön melko ongelmattomana. Suojatakseen omia tietojaan, yritysten pitää huolehtia tiedon riittävästä salaamisesta, joka on ollut tarpeellista kansainvälisesti toimiville yrityksille tähänkin asti. Palvelinkeskustoimijoille ja muille vastaaville toimijoille oleellista on kyky pitää takaportit poissa keskuksistaan ja toisaalta mahdollisuus salata tuleva ja lähtevä liikenne luotettavasti. Tietojensa luottamuksellisuudesta huolestuneille yrityksille oleellista on ymmärtää ja ennakoida mahdollisen tiedustelun laajuus ja lainmukaisuus. Tätä taustaa vasten näemme Suomen edelleen voivan lainmukaisen ja valvotun toteutuksen ansiosta korostaa asemaansa neutraalina tiedon suojapaikkana.

Yritysten omaa tietoturvasuojautumista ei kuvattu lainsäädäntö auta oletettavasti muuten kuin korkeintaan valtiollisia kyberhyökkäystä torjuttaessa.

**Yhteenveto:**

Kokonaisuudessaan näemme esitetyt suuntaviivat perustelluiksi huomioiden taustalla olevien turvallisuusviranomaisten tarpeet kyberulottuvuudessa. Huolemme liittyvät tietoliikennetiedustelun järjestelmän lainmukaiseen ja valvottuun toteutukseen ja käyttöön etenkin kansalaisiin kohdistuvan tiedustelun osalta. Tämän ei tulisi olennaisesti erota muissa ulottuvuuksissa käytössä olevissa menetelmistä kuten puhelinkuuntelusta.

Kaikkien tahojen on hyvä myös tiedostaa, että tulevalla lainsäädännöllä ja siihen liittyvillä järjestelmillä ei ole teknisesti mahdolista luoda “kyberrajavalvontaa” joka estäisi kyberrikollisuuden pääsyn suomalaisiin verkkoihin ja yrityksiin. Digitaalinen yhteiskunta tulee tulevasta lainsäädännöstä riippumatta olemaan haavoittuva niin kauan kuin kukin itsenäinen toimija ei kanna itse vastuuta riittävistä toimista omien prosessiensa, tuotteidensa tai tietojärjestelmiensä turvaamiseksi.

**Lisätietoja:**

Petri Kairinen, toimitusjohtaja, Nixu Oyj

petri.kairinen@nixu.com, 040 832 1832, @kairinen