25.10.2021

Puolustusvaliokunta

VNS 8/2021

Asiantuntijapyyntö: Puolustusvaliokunta 26.10.2021 / VNS 8/2021

F-Secure näkee kyberturvallisuuden edellyttävän vahvaa ja johdonmukaista viranomaisten ja teollisuuden välistä yhteistyötä. Kyberturvallisuus vaatii laajaa ja syvällistä teknologista tuntemusta, jolloin teollinen yhteistyö tuottaa tarvittavan osaamisen sekä säästöjä kustannuksissa.

Kysymykseen: "*Kuka puolustaa Suomen tietoverkkoja?*" ei Puolustusselonteko anna vastausta. Selonteossa tukeudutaan yhteistoiminnan käsitteeseen, joka hajauttaa vastuun useille julkishallinnon organisaatioille. Modernien strategisten kyberhyökkäysten keskeiset ominaisuudet ovat: näkymättömyys, harhautus ja kiistanalaisuus. Tällainen kyberuhka iskee suurella todennäköisyydellä Suomen viranomaisten toimivallan *harmaalle alueelle*. Tässä alueessa on F-Securen käsityksen mukaan epäselvää, kenen vastuulla on tilanteen haltuunotto ja kuka johtaa kyberhyökkäyksen torjuntaa.

Suomeen kohdistuvat strategiset kyberuhkat

F-Securen käsitys on että Suomi on jatkuvan kyberuhan alla. Osaksi tämä on yleinen trendi, ja osaksi se johtuu mm. Suomen turvallisuuspoliittisesta asemasta sekä kaupallisesta ja teollisesta profiilista. Valtionhallinnon, Puolustusvoimien, turvallisuusviranomaisten ja yksityissektorin kannalta strategisesti merkittävimmän uhkan muodostavat valtiolliset toimijat. Näillä uhkatoimijoilla on teknisesti edistyksellisimmät ja runsaimmat resurssit kehittää verkkohyökkäyksiä. Merkittävän uhkan muodostavat myös korkean profiilin järjestäytyneet verkkorikollisryhmät. Valtiollisten toimijoiden kehittämät kyberaseet myös "valuvat" näiden rikollisryhmien käyttöön valtiollisten toimijoiden kehittäessä uusia kyberaseita korvaamaan vanhentuneita kyvykkyyksiään.

Strategisten uhkatoimijoiden ensisijaiset tavoitteet ovat yhteiskunnallisen epävakauden aiheuttaminen, teollisuusvakoilu ja taistelukentän valmistelu kybertilassa. Useimmiten taustalla ovat geopoliittiset tavoitteet tai toimijan kyberkyvykkyyksien voiman näyttö.

Viime vuosilta tästä toiminnasta on useita esimerkkejä, joissa kybervaikuttamisen kohteena ovat olleet läntiset ja Itä-Euroopan maat. Esimerkkejä löytyy myös Suomesta (Ulkoministeriö 2013, Eduskunta 2020). Toisaalta myös länsimaat kehittävät ja ajoittain myös käyttävät operatiivisesti vastaavia kyvykkyyksiään. Länsimaat tuntuvat kokevan sen, että jäävät kiinni verkkovaikuttamisesta paljon kiusallisempana kuin Venäjä tai Kiina.

Vihamielisten ja muilla tavoin oikeudettomien edistyneiden kyberoperaatioiden yksi keskeinen ongelma on ns. *attribuutio* – hyökkääjän tunnistaminen. Autoritaariset aggressiiviset valtiotoimijat kiistävät osuutensa. Länsimaisia operaatioita havaittaessa puolestaan kohteeksi joutunut valtio paheksuu ja hämmästelee joutumistaan kohteeksi,

F-Secure, Tammasaarenkatu 7, 00181 Helsinki Finland

+358 9 2520 0700 www.f-secure.com

Business id 0705579-2 Registered office Helsinki

vaikka useissa tapauksissa kyseinen valtio edistää kansallisia tiedontarpeita ja muita etujaan vastaavilla menetelmillä.

Varautuminen näitä uhkia vastaan edellyttää pitkän aikavälin suunnittelua, ennakkoon tehtäviä investointeja ja kykyä varmistaa kansallinen suorituskyky uhkien havaitsemiseen ja toteutuneiden kyberhyökkäysten eri vaiheiden hallitsemiseen sekä vastatoimiin.

Länsimaissa kyberpuolustukseen käytettäviä kansallisia budjetteja on kasvatettu merkittävästi. Esimerkkinä mainittakoon Britannian puolustusministerin Ben Wallacen lokakuun alussa 2021 uutisoitu aloite kybertilassa toimivan kyberpuolustuksen organisaation perustamisesta. Kehitettävän organisaation 5 miljardin punnan budjetilla työllistetään tuhansia verkkohyökkääjiä ja tiedusteluanalyytikoita kyberpuolustuksen tarpeisiin vuoteen 2030 mennessä.

Suomessa käynnissä oleva *Kyberturvallisuuden kehittämisohjelma* (LVM julkaisuja 2021:7) tuottaa laajempaa ymmärrystä kehitystarpeisiin Suomessa. Ohjelman tulee kuitenkin jatkossa huomioida laajemmin kyberhyökkäysten vastaisen toiminnan vaiheiden hallintaan tarvittavat yhteistoimintamenettelyt, sekä niiden edellyttämät riittävät investointitasot.

Kansallisen kyberpuolustuksen johtaminen kyberhyökkäyksessä

Valtiollisten toimijoiden strategisen uhkan kyberhyökkäyksille on ominaista näkymättömissä pysyminen tehtävän aikana, toiminnan alkuperän kiistäminen (em. attribuutio-ongelma) ja hallinnollisten vastuualueiden *harmaan alueen* hyödyntäminen toiminnan mahdollistamiseksi.

Tämä asettaa paineita yhteiskuntamme kyberturvallisuudesta vastaavan johtamisrakenteen tehokkaalle toiminnalle. Julkishallinnon kyberturvallisuutta tuottavat Kyberturvallisuuskeskus, Poliisi ja Puolustusvoimat. Kyberhyökkäyksen ensivaiheen havaitsemisen jälkeen ei ole selvää, kuka on hyökkäävä toimija – toimijan selvittäminen voi viedä vuosikausia. Tämä vaikeuttaa sen päättämistä, minkä viranomaisen toimivaltaan tilanteen haltuun ottaminen ja johtaminen kuuluu.

Tämä epäselvyys osaltaan hidastaa tarpeellisten toimenpiteiden, kuten hyökkäyksestä toipumisen sekä tarvittavien vastatoimenpiteiden toimeenpanoa.

Kansallisen kyberturvallisuuden kokonaisuuden ja sen osana kyberpuolustuksen tulisi käsittää keskitetty johtamisrakenne, minkä kautta pystytään aktivoimaan eri osapuolten yhteistyö – joka käsittää niin julkisen kuin yksityisen sektorin – ennalta määritetyin toimintaperiaattein. Näin toteutettuna kansallinen vaste kyberhyökkäyksen alla toimiseksi saadaan toimimaan tehokkaasti ja saadaan aktivoitua tarvittavat resurssit oikea-aikaisesti.

25.10.2021

Puolustusvaliokunta

VNS 8/2021

Kyberpuolustuksen tarpeiden huomioiminen puolustuspoliittisissa perusteissa ja kansallisessa kyberturvallisuusstrategian kehittämisohjelmassa

Teknisellä valvonnalla ja torjunnalla ei kyetä puolustautumaan kaikkia kyberhyökkäyksiä vastaan. Edistyneimpiä hyökkäysmenetelmiä hyödyntävät valtiolliset toimijat löytävät heikkoudet järjestelmissä tai materiaalien toimitusketjuissa (laitteistot ja ohjelmistot) päästäkseen tavoiteltaviin hyökkäyskohteisiin. Kyberpuolustuksen kannalta on tunnistettava, että nämä hyökkäykset havaitaan aina *liian myöhään* – kun hyökkääjä on jo saanut pääsyn suojattavaan kohteeseen.

Hyökkääjän päästyä kohteeseen puolustajan haasteena on eristää ja hävittää hyökkääjä murretuista järjestelmistä, sekä toipua ja oppia hyökkäyksestä toiminnan jatkumiseksi. Viranomaistyössä on myös oleellista hyökkääjän toimien tunnistaminen suorittamalla tarvittavia vastatoimenpiteitä.

Seuraavalla sivulla esitettävässä kaaviossa kuvataan kyberhyökkäyksen käsittelyn eri vaiheita ja niiden keskeisiä ominaisuuksia. Kansallisessa kyberstrategiassa alla esitetyn kaavion kyberpuolustuksen neljä jälkimmäistä osa-aluetta ovat toistaiseksi jääneet vaille huomiota – vaikka niihin löyhästi puolustusselonteossa viitataan.

F-Secure

F-Secure, Tammasaarenkatu 7, 00181 Helsinki Finland

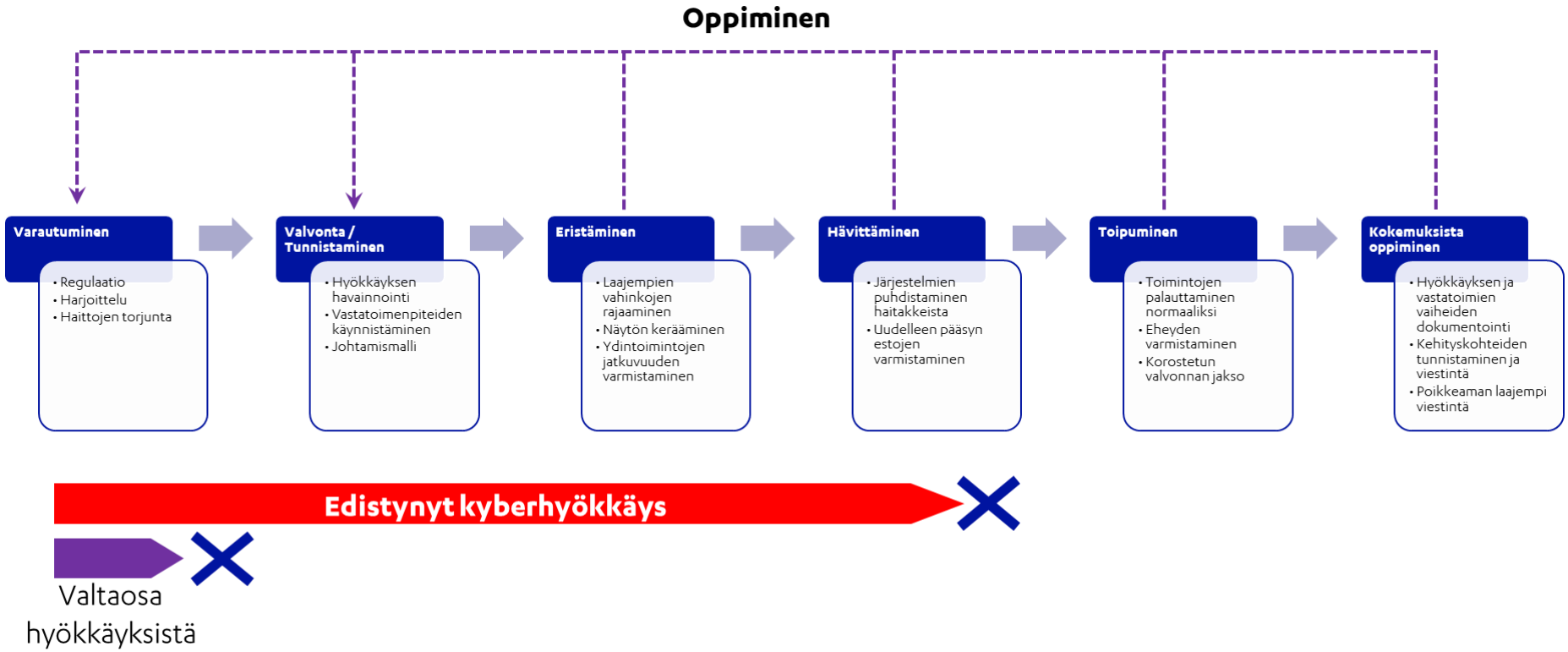
+358 9 2520 0700 www.f-secure.com

Business id 0705579-2 Registered office Helsinki

25.10.2021

Puolustusvaliokunta

VNS 8/2021



F-Secure, Tammasaarenkatu 7, 00181 Helsinki Finland

+358 9 2520 0700 www.f-secure.com

Business id 0705579-2 Registered office Helsinki

25.10.2021

Puolustusvaliokunta

VNS 8/2021

Puolustusselonteossa todetaan (luku 4.2.4): "*Kybervaikuttamisen ja kybervastatoimien kehittämiselle luodaan parempi kansallinen perusta.*" Selonteon puolustuspoliittisissa perusteissa (luku 4.1) viitataan kyberturvallisuusstrategian kehittämisohjelmaan, minkä tuotoksena on syntynyt dokumentti *Liikenne- ja Viestintäministeriö* julkaisu 2021:7 – *Kyberturvallisuuden kehittämisohjelma*.

Näitä kahta dokumenttia tarkasteltaessa F-Securen näkemys on, että puolustusselonteko ja kyberturvallisuuden kehittämisohjelma eivät nykyisellään huomioi kyberhyökkäyksen vahinkojen rajaamisen ja hyökkäyksestä toipumisen edellytyksiä (edellä esitetyn kaavion neljä jälkimmäistä vaihetta).

Hyökkäys- ja haittaohjelmistojen eristäminen sekä hävittäminen kybertilassa - kun organisaatio on aktiivisen kyberhyökkäyksen kohteena - on erityisen vaativaa osaamista edellyttävä toimenpide. Tämän osaamisen varmistaminen edellyttää julkisen ja yksityisen sektorin saumatonta yhteistyötä.

Kyberturvallisuuden kehittämisohjelmassa todetaan myös: "*Kyberturvallisuuden huippuosaajista käydään jatkuvasti kovaa kansainvälistä kilpailua.*" (luku 3).

F-Secure tukee tätä väittämää toteamalla lisäksi, että kyberhyökkäysten hallinnan ja toipumisen edistynein osaaminen keskittyy kansainvälisiin yrityksiin – joiden palkkatason ja työetujen kanssa julkinen sektori ei nykyisellään voi kilpailla. Nämä yritykset työskentelevät päivittäin globaalilla toimikentällä auttamassa kyberhyökkäysten kohteena olevia organisaatioita. Yritykset ja niiden työntekijät oppivat jatkuvasti hyökkääjien työkaluista ja menetelmistä, jotka edelleen auttavat teknologista kehitystä torjuntamenetelmien parantamiseksi.

Puolustusselonteon ja kyberturvallisuusstrategian tulee tunnistaa ja korostaa niitä puitteita, millä varmistetaan julkisen ja yksityissektorin kiinteä yhteistoiminta nopeasti kehittyvien kyberhyökkäysten alla. Kansallisessa regulaatiossa tulee huomioida myös kansainvälisten yritysten ulkomaisen osaamisvarannon hyödyntämisen tärkeys ja mahdollistaminen – esimerkiksi kansallisesti turvallisuusluokitelluiden järjestelmien kanssa työskenneltäessä. On epärealistista ajatella, että Suomen kehittyneimmissä kyberalan yrityksissä voitaisiin tukeutua kaikessa yhteiskunnallisen kyberturvallisuuden rakentamisessa pelkästään kotimaisiin huippuasiantuntijoihin.

F-Secure Corporation Tammasaarenkatu 7 P.O. Box 24 FI-00181 Helsinki Finland

Tel: +358 9 2520 0700 www.f-secure.com

Business id 0705579-2 Registered office Helsinki

25.10.2021

Puolustusvaliokunta

VNS 8/2021

Kyberpuolustuksen resursoinnin ja rahoituksen arviointi

Suomi kehittää voimakkaasti yhteiskunnallisia digitaalisia palveluita. Kybertoimintaympäristö laajenee voimakkaasti ja yhteiskunnan digitaalinen asiointi asettaa uusia vaatimuksia kyberpuolustuksen kyvykkyydelle.

Puolustusselonteossa viitattu kyberturvallisuusstrategian kehittämisohjelman Liikenne- ja viestintäministeriön julkaisu *Kyberturvallisuuden Kehitysohjelma* (LMV 2021:7) kuvaa hyvät lähtökohdat kyvykkyyden kehittämiselle. Ohjelma ei kuitenkaan huomioi kaikkea tarpeellista hyökkäyksen alla tapahtuvaa yksityis- ja julkissektorin yhteistoimintaa.

Kyberturvallisuuden valvonnan ja hyökkäysten hallinnan toimenpiteiden tulee olla hajautettu ekosysteemiin palveluja tuottaville toimijoille. Toimijat tuottavat valvontatietoa omista ympäristöistään, niin että tilannekuva on mahdollista muodostaa koostamalla eri lähteistä saatavalla tiedoista. Tätä tietoa voidaan rikastaa kansainvälisen yhteistyön kautta saadulla tiedolla. Valvontatiedon välittäminen edellyttää määrätietoista kriittisien tietojärjestelmien kehitystyötä. Sen toteuttaminen ei edellytä toimijalta merkittävää taloudellista panosta, vaan kyse on pääasiassa toimintatavoista. Tiedon kerääminen ja analysointi toisaalta vaatii huomattavia investointeja ja ratkaisun tulee varmistaa, ettei siitä itsestään synny kriittistä uhkaa yhteiskunnan toiminnalle.

Yksityisellä sektorilla on kyvykkyys tarjota osaamista ja tehokkaita yhteistyöverkostoja, joita kriisin johtamisen ja omien toimenpiteiden tukena tarvitaan. Kyberhyökkäys kohdistuu harvoin yhden viranomaisen tai hallinnonalan tietojärjestelmiin. Toimiva viranomaisyhteistyö yksityisen sektorin kanssa on avainasemassa kyberpuolustuksen johtamisessa.

Liikenne- ja Viestintäministeriön kyberturvallisuuden kehittämisen ohjelman toimeenpanosuunnitelmaa tarkasteltaessa esitetty rahoitusarvio on F-Securen herkkyysarvion mukaan riittämätön hyödyntämään yksityisen sektorin erityisosaamista ja muita resursseja kehitysohjelman toteutukseen - kehitysohjelman hengen esittämällä tavalla. Lisäksi edellä esitetyt *katvealueet* (erityisasiantuntijuus kyberhyökkäyksen vahinkojen rajaamisen ja hyökkäyksestä toipumisen osa-alueilla) jäävät täysin huomioimatta toiminnan rahoitustarpeissa. Näiden rajausten puitteissa voidaan ainoastaan todeta budjetointi- ja rahoitussuunnitelmien olevan riittämättömiä.

Helsingissä 25.10.2021

Mikko Hyppönen, tutkimusjohtaja

Juha Torkkel, johtava tietoturvakonsultti

F-Secure Oyj