EDUSKUNNAN LIIKENNE- JA VIESTINTÄVALIOKUNNALLE

MUUTTUNUT TURVALLISUUSTILANNE JA UHKAKUVAT

ASIANTUNTIJALAUSUNTO

PROF MARTTI LEHTO

10.4.2018

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

Asia: HE 198/2017 vp, HE 199/2017 vp, HE 202/2017 vp, HE 203/2017 vp

1. TURVALLISUUSYMPÄRISTÖN MUUTOS

Kuten hallituksen esityksessä on todettu, Suomen turvallisuusympäristö on kiistatta monimutkaistunut. Uudet haasteet ja tehtävät edellyttävät viranomaisilta asianmukaista suorituskykyä. Turvallisuusympäristön muutoksiin on vastattava ajanmukaistamalla turvallisuusviranomaisten tilannekuvaa, toimivaltuuksia sekä parantamalla viranomaisten suorituskykyä.

Sisäisen turvallisuuden selonteon mukaan Venäjän ja lännen suhteiden huononeminen, kansainvälinen terrorismi, kyberuhat ja laajamittainen laiton maahantulo ovat merkittävimmät viimeaikaiset muutokset turvallisuusympäristössä. Kybervaikuttaminen ja informaatiovaikuttaminen liittyvät kiinteästi hybridivaikuttamiseen ja siksi turvallisuusviranomaisilla tulee olla sekä kyky havaita uhkat riittävän ajoissa että riittävät voimavarat pitkäkestoisenkin tilanteen hallitsemiseksi.

2. DIGITAALINEN KYBERMAAILMA

Modernin yhteiskunnan toiminta perustuu kansallisen kriittisten infrastruktuurin useiden eri osien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu yhä enemmän kyberturvallisista ja korkean käyttövarmuuden omaavista sähköjärjestelmistä ja tiedonsiirtoverkostoista sekä muista luotettavista ja tietosisällöltään eheistä hallinnon ja kansalaisten palveluista. Teknologinen kehitys on johtanut tuotannon, palvelujen ja koko yhteiskunnan digitalisoitumiseen, verkostoitumiseen ja keskinäisten riippuvuuksien kasvuun. Kyse on myös kansalaisten luottamuksen ylläpitämisestä yhteiskunnan toimintaan. Kyberhyökkäykset, haittaohjelmat, palvelunestohyökkäykset ja erilaiset informaatiovaikuttamisen muodot lisääntyvät jatkuvasti. Tämän kehityksen vuoksi on lisättävä edelleen varautumista kyberuhkiin ja -häiriötilanteisiin, jotka vaarantavat yhteiskunnalle välttämättömien tietoteknisten järjestelmien ja rakenteiden toimivuutta jo normaalioloissa. Suomalaisen yhteiskunnan ja yritysten riippuvuus kybertoimintaympäristöstä kasvaa entisestään tulevina vuosina.

Digitalisaatiokehitys on ollut nopeaa:

- Vuonna 1998 3,6 prosenttia maailman väestöstä käytti internettiä. Nyt käyttäjiä on noin 3,885 miljardia (51,7 % maailman väestöstä).
- Päivittäin maailmalla lähetetään yli 200 miljardia sähköpostiviestiä, lähetetään 500 miljoonaa twiittiä ja käytetään Googlen hakukonetta 3,5 miljardia kertaa.
- Matkapuhelinten käyttäjiä maailmassa on yli 4,77 miljardia (73 %).
- Arvioiden mukaan tänä vuonna verkkoon kytkettyjä laitteita (IoT) on noin 9 miljardia, joista kaksikolmasosaa on kuluttajalaitteita

Kybermaailmassa muutosajureita on useita, niistä keskeisin on aika. Kyberhyökkäyksen valmistelu on mahdollista toteuttaa salassa ja pitkän ajan kuluessa, mutta itse hyökkäys voidaan toteuttaa erittäin lyhyessä ajassa. Tammikuussa 2003 verkkomato Slammer levisi noin 10 minuutissa hyökkäyksen aloittamisesta arviolta 90 prosenttiin suunnitelluista kohteista (internettiä ohjaavat palvelimet). Slammer aiheutti internetin toi-

minnan maailmanlaajuisen hidastumisen. Arvioiden mukaan Slammer-verkkomadon kustannukset nousivat 750 miljoonaan euroon.

Lähes 15 vuotta myöhemmin toukokuussa 2017 levisi internetin kautta WannaCry kiristys-haittaohjelma, joka saastutti yli 200 000 konetta yli 150 maassa muutamassa vuorokaudessa. Arvioiden mukaan hyökkäyksen taloudelliset menetykset voivat nousta 4 miljardiin dollariin.

Palvelunestohyökkäyksin voidaan vaikeuttaa merkittävästi internet-pohjaisiin palveluihin. Vuonna 2016 nimipalveluyhtiö Dyn joutui Mirai-botnetilla toteutetun massiivisen kyberhyökkäyksen kohteeksi. Botnettiin oli kaapattu verkkoon kytkettyjä IoT-laitteita (Internet of Things) kuten turvakameroita, printtereitä, digibokseja, itkuhälyttimiä, kotireitittimiä. Tämän botnetin avulla voitiin estää kymmenien palveluntarjoajien toiminta kuten Twitter, Amazon, CCN, New York Times, AirBnB, Spotify ja Netflix. Hyökkäysten haittaliikenne oli huippukohdissaan yli terabitin sekunnissa, joten se riitti estämään palvelun suurimmiltakin kohteilta.

Joulukuussa 2015 hakkerit iskivät ukrainalaiseen energiayhtiöön ja onnistuivat katkaisemaan sähkönjakelun. Tämä usealla eri tavalla toteutettu kyberhyökkäys jätti 225 000 ukrainalaista ilman sähköä kuudeksi tunniksi. Samanlainen hyökkäys toteutettiin Kievin alueella joulukuussa 2016. Hyökkäyksen takana epäillään olleen valtiollisen toimijan.

Kesäkuussa 2017 Petya-haittaohjelma saastutti Ukrainassa laajasti käytetyn M.E.Doc -kirjanpito-ohjelmiston, jonka kautta se levisi nopeasti ukrainalaisiin ja kansainvälisiin toimijoihin, joilla yhteys tuohon kirjanpito-ohjelmaan. Ukrainassa mm. pankit, ministeriöt, sanomalehdet ja sähköyhtiöt joutuivat kohteeksi. Yli 80 prosenttia kohteista oli Ukrainassa, mutta kymmenet kansainväliset toimijat olivat myös kohteina. Tähän saakka hyökkäyksestä aiheutuneet kustannukset ovat olleen yli 2,2 miljardia dollaria.

Em. esimerkit osoittavat, kuinka kriittistä infrastruktuuria vastaan hyökätään ja aiheutetaan vakavia vaurioita yhteiskunnan elintärkeille toiminnoille ja pahimmassa tapauksessa ihmisten hengelle ja terveydelle. Arvioiden mukaan länsimaissa kyberhyökkäykset aiheuttavat 1-2 % menetykset bkt:stä.

Tietoverkkoihin ja -järjestelmiin kohdistuu yhä enemmän kohdistettuja hyökkäyksiä, tietoturvaloukkauksia sekä haittaohjelmatartuntoja. Vuosien 2012-2017 aikana vuoden aikana havaittujen haittaohjelmien määrä on kasvanut 100 miljoonasta yli 700 miljoonaan (400 000 uutta haittaohjelmaa joka päivä). Hyökkäyksiä kohdistetaan kansallisiin salassa pidettäviin tietoihin, aineettomiin pääomiin ja henkilötietoihin. Tiedusteluorganisaatiot pyrkivät keräämään heitä kiinnostavaa tietoa poliittisen, taloudellisen tai sotilaallisen edun saavuttamiseksi.

Nykyään taloudellisiin hyötyihin tähtäävien kyberrikollisten ja kehittyneiden valtion sponsoroimien hyökkääjien toiminta ja kyvykkyystaso eivät ole vain hämärtyneet - niitä ei enää ole olemassa. Kyberhyökkäystekniikat ja -työkalut ovat laajasti levinneet eri

motivaatioilla toimivien kyberhyökkääjien käyttöön. On tapahtunut konvergenssi, jossa toimijoiden nimeäminen ja heidän motivaationsa paljastaminen yhä vaikeampaa.

Kybertoimintaympäristön ominaisuuksiin kuuluu kehityksen suuri nopeus, tapahtumien hektisyys ja eri järjestelmien kompleksisuus. Informaatioteknologian kehityssykli on lyhyt ja sama trendi koskee eri kyberhyökkäysmuotoja ja haittaohjelmia. Kybertoimintaympäristölle on leimallista muutosnopeus, mikä edellyttää kaikelta toiminnalta nopeaa reagointikykyä – ketteryyttä, sekä varautumista myös tilanteisiin, joita ei täysin kyetä ennakoimaan.

Erityisen haitallisia ovat olleet kohdistetut hyökkäykset (APT), joissa kohde on valittu tarkasti ja kohteesta on myös kerätty tarvittava määrä tietoa hyökkäyksen mahdollistamiseksi. Kohdistetuissa hyökkäyksissä hyökkääjä hyödyntää aktiivisesti löydettyjä kohdeorganisaation palvelujen haavoittuvuuksia ja heikkouksia. Haavoittuvuuksia on ihmisten toiminnassa, organisaatioiden turvallisuusprosesseissa ja teknologiassa (ohjelmistoissa ja laitteissa). Hyökkäyksiä voidaan muuntaa ja kehittää, jotta voidaan hyödyntää kohdeorganisaation heikkouksia mahdollisimman hyvin. Kohdistetut hyökkäykset toteutetaan usein kampanjoina, jolloin ne koostuvat sarjasta epäonnistuneita ja onnistuneita yrityksiä päästä syvemmälle ja syvemmälle kohdeorganisaation verkkoon.

3. KYBERTIEDUSTELUN MAAILMA

Tiedustelun siirtyminen verkkoon on tapahtunut samassa tahdissa yhteiskuntien digitalisaation kanssa. Kybertiedustelun voimakkaan kasvun alku ajoittuu 2000-luvun puoliväliin. Kehittyneimmille vakoiluohjelmille on ollut tyypillistä, että ne on havaittu vasta vuosia operaation alkamisesta.

Vuonna 2011 havaittiin siihen saakka merkittävin verkkovakoiluoperaatio. Operaatiossa Shady RAT onnistuttiin tunkeutumaan 72 järjestön, yrityksen ja hallituksen järjestelmiin pääasiassa länsimaissa. Toiminta oli jatkunut jo viiden vuoden ajan.
Samana vuonna havaittiin verkossa Duqu-haittaohjelma, joka keräsi tietoa teollisuuslaitoksista kyberhyökkäysten valmistelemiseksi. Duqun arvioitiin toimeen verkossa neljä vuotta.

Vuonna 2012 löydettiin Flame-haittaohjelma, joka hyvin monipuolisesti kykeni käyttämään saastuttamansa tietokoneen resursseja. Se oli ensimmäinen usean megatavun kokoinen haittaohjelma, kun aikaisemmin ohjelmat ovat olleet kooltaan satoja kilotavuja. Haittaohjelmatartunnat keskittyivät Lähi-Itään. Tämän ohjelman arvioitiin toimineen verkossa viisi vuotta.

Vuonna 2013 raportoitiin NetTraveler-haittaohjelmasta, joka oli ollut toiminnassa vuodesta 2004. Tässä ainakin vuoteen 2016 jatkuneessa operaatiossa kohteena on ollut yli 350 organisaatiota 40 maasta. Hyökkäyskohteita ovat olleet avaruus-, nano, energia-, ydin-, laser- ja tietoliikenneteknologian sekä farmasian tietovarannot.

Vuonna 2014 havaittiin Regin-haittaohjelma, joka oli ollut käytössä jo vuodesta 2008 asti. Regin on enemmän ohjelmisto kuin yksittäinen ohjelma ja se oli tuolloin historian

kehittynein ja monipuolisin. Tämä monitasoinen vakoiluohjelma kykeni hallitsemaan kohdettaan täydellisesti ja leviämään tehokkaasti. Kohteita oli ainakin 14 maassa.

Vuonna 2015 Yhdysvaltain Office of Personnel Management (OPM) ilmoitti, että se oli joutunut tietomurron kohteeksi, jossa siltä anastettiin noin 21,5 miljoonan liittovaltion työntekijän (nykyisiä ja entisiä) henkilörekisteritietoja kuten sosiaaliturvatunnus, nimi, syntymäaika ja -paikka sekä osoite.

Vuonna 2016 raportoitiin Remsec-haittaohjelma-alustasta (ProjectSauron). Sen arvioidaan toimineen vuodesta 2011. Kohteita sillä on ollut ainakin 30 useassa maassa ja se kykenee asentamaan takaovia, varastamaan tietoja ja tallentamaan näppäimistön käyttöä.

Keskeistä kehitykselle on ollut haittaohjelmien monimutkaisuuden ja kyvykkyyden kasvu samalla kun niiden havaitseminen on käynyt yhä vaikeammaksi.

4. SISÄPIIRI UHKANA

Yhä enenevässä määrin yrityksen sisäpiiriläiset ovat merkittävä kyberuhka. Eri arvioiden mukaan sisäpiiriläiset (nykyiset tai entiset työntekijät, palveluntarjoajat, sopimuskumppanit, konsultit, toimittajakumppanit ja liiketoimintakumppanit) tekevät tai ovat osallisina noin 60 % kaikista hyökkäyksistä. Näistä sisäpiiriläisistä kolmasosa oli loppukäyttäjiä, joilla oli käyttöoikeudet luottamukselliseen tietoon. Motivaationa hyökkääjillä oli joko suora taloudellinen hyöty (34 %) tai vakoilu (25 %).

5. KOHTI 2020-LUKUA: TURVALLISTA TOIMINTAYMPÄRISTÖÄ EI ENÄÄ OLE

Eri arvioiden mukaan kyberturvallisuutta eniten muokkaavat voimat ovat yhä laajeneva kyberhyökkäysala, hyökkääjien osaamisen parantuminen, kyberrikollisuuden teollistuminen ja tietovuodot. Kybermaailmassa erityisesti esineiden internet (IoT), pilvipalvelut, suuret datamassa ja lisääntyvä mobiilipäätelaitteiden käyttö luovat hyökkääjille uusia hyökkäyskohteita. Pilvipalveluiden lisääntyminen tarkoittaa uusia mahdollisuuksia kyberhyökkääjille. Pilvipalvelut ovat usein kolmansien osapuolien toimittamia, jolloin asiakkaalla ei ole kunnollista näkymää palvelun laatuun tai turvallisuuteen. Älykkäitä Big data -sovelluksia käytetään jo paljon, mutta uhkana on, että suurien datavarastojen (Data lake) lisääntyessä, lisääntyvät riskit tahattomille tai tahallisille väärinkäytöksille. Mobiliteetista ja uusista päätelaitteista haetaan tehokkaampia tapoja toimia ja osa ihmisten työstä tehdään mobiilisti. Tämä kehitys on lisännyt merkittävästi haittaohjelmia ja hyökkäyksiä mobiilipäätelaitteisiin.

Digitalisaation kehityksessä on uskottu siihen, että kehittämämme IT-toimintaympäristöt ovat turvallisia niihin käyttötarkoituksiin, joihin olemme ne suunnitelleet. Erilaisilla teknisillä turvallisuusratkaisuilla (palomuuri, virustorjunta, tietoliikenteen salaus) ja käyttäjien hallinnalla (tunnistaminen, käyttöoikeudet, pääsyn valvonta) tilannetta on pyritty hallitsemaan, mutta turvallisia käyttöympäristöjä ei enää ole. Kybermaailmassa toimintaa hallitsevat internet-palveluntarjoajat (ISP), ohjelmistojen palveluntarjoajat ja alustapalvelun tarjoajat (IPP). Näiden palveluiden avulla sisällöntuottajat (ICP) tarjoavat palveluita loppuasiakkaille heidän erilaisiin käyttöliittymiin

(tietokoneet, tabletit, älypuhelimet). Kehitykselle on leimallista toiminnan keskittyminen suurien palveluntarjoajien käsiin. Toinen merkittävä muutostrendi on internetympäristön hajoaminen, jossa Venäjä ja Kiina pyrkivät luomaan omat internetympäristönsä (RuNet, ChinaNet) vastapainoksi Yhdysvaltain dominanssille.

Ennusteiden mukaan myös valtioiden kybersodankäynnin kyvykkyydet tulevat edelleen kehittymään sekä hyökkäysten laajuudessa, että edistyksellisyydessä. Valtioiden tekemät kyberhyökkäykset vaikuttavat poliittisiin suhteisiin ja globaaleihin valtarakenteisiin. Valtioiden käyttämät työkalut valuvat jollakin aikavälillä myös kyberrikollisryhmien käyttöön.

6. KYBERTIEDUSTELU JA -VALVONTA – TILANNEYMMÄRRYKSEN PERUSTA

Kybertoimintaympäristö on muuttanut perinteisiä kansainvälisiä valta-asetelmia. Se antaa pienillekin valtioille ja ei-valtiollisille toimijoille mahdollisuuden toimia tehokkaasti. Kybermaailmassa suuruus ja massa eivät enää ole hallitsevia, vaan osaaminen. Kybertoimintaympäristössä tapahtuva kansainvälinen kehitys lisää uusien uhkien mahdollisuutta meitä vastaan. Julkishallintoon ja elinkeinoelämään kohdistuu jatkuvia järjestelmähaavoittuvuuksien hyväksikäyttö- tai murtoyrityksiä. Hyökkäyksissä korostuu ammattimaisuus, mikä näkyy hyökkäysmenetelmien tehokkuudessa ja kohdistuksessa.

Kybermaailman avoimuus mahdollistaa hyökkäykset eri puolilta maailmaa käyttäen hyväksi järjestelmien haavoittuvuuksia. Monimutkaisia ja kehittyneitä haittaohjelmia vastaan on vaikea suojautua ja hyökkääjiä on vaikea tunnistaa tai löytää heidän todellinen identiteettinsä ja motivaationsa.

Haittaohjelmista vaikeimmin havaittavia ja samanaikaisesti suurinta vahinkoa kansalliselle turvallisuudelle aiheuttavia ovat valtiolliset vakoilu- ja muut haittaohjelmat. Sekä tietoliikennetiedustelun että ulkomaantiedustelun tarkoituksena olisi hankkia kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa vakavista kansainvälisistä uhista.

Jokainen organisaatio tarvitsee toimiakseen tietoa ympäristöstään ja sen tapahtumista sekä niiden vaikutuksesta omaan toimintaansa. Tarkoituksenmukainen ja nopea, oikeisiin tietoihin ja arvioihin perustuva tilannetietoisuus korostuu häiriötilanteissa, jolloin joudutaan nopeasti tekemään hyvinkin laaja-alaisesti vaikuttavia päätöksiä. Voidakseen tehdä oikeita ratkaisuja päätöksentekijöiden on tiedettävä päätöstensä perusta, seuraukset, miten muut niihin reagoivat ja mitä riskejä päätöksiin sisältyy. Tästä syystä päätöksentekijöillä tulee olla kaikilla toimintatasoilla riittävä tilannetietoisuus ja -ymmärrys, joka on väline oikea-aikaiseen päätöksentekoon ja toimintaan. Tilannetietoisuus ja -ymmärrys edellyttävät yhteistoimintaa ja osaamista, jotka mahdollistavat kokonaisvaltaisen toimintaympäristön seurannan, informaation analysoinnin ja kokoamisen, tiedon jakamisen, tutkimustarpeiden tunnistamisen ja verkostojen hallinnan. Tietojärjestelmien tulee mahdollistaa systemaattinen tietolähteiden käyttö ja yhteistoiminta sekä siihen liittyvä joustava tilannetietojen jakaminen.

Reaaliaikaisen tilannekuvan muodostaminen ja jaetun tilannetietoisuuden aikaansaaminen on torjunnan kannalta aivan keskeistä. Perusteet vastatoimenpiteiden käytölle pitää syntyä vastustajaa nopeammassa päätösprosessissa tuotettua tilannekuvaa sekä vastustajan toimintatapoja, tavoitteita ja kyvykkyyttä analysoimalla. Tilannetietoisuuden kehittäminen edellyttää tehokasta havainnointikykyä ja siksi tiedustelulaki on välttämätön kybertiedustelun ja -valvonnan suorituskyvyn kehittämisen ja ennakkovaroituksen kannalta.

Euroopan parlamentti päätöslauselmassa Euroopan unionin kyberturvallisuusstrategiasta todetaan mm., että kyberturvallisuuteen liittyvien vaaratilanteiden havaitseminen ja niistä ilmoittaminen ovat keskeisellä sijalla edistettäessä tietoverkkojen kestävyyttä unionissa. NIS-direktiivin katsotaan olevan tärkeä osa EU:n kyberstrategiaa, jonka tavoitteena on kehittää avoin ja turvallinen kyberympäristö, joka reagoi kyberhäiriöihin ja -hyökkäyksiin sekä pyrkii ehkäisemään niitä.

Tiedustelulaki antaa säädöspohjan, jotta suomalaisen yhteiskunnan mahdollisuuksia suojautua kansalliseen turvallisuuteen kohdistuvilta kaikkein vakavimmilta uhkilta voidaan parantaa. Tämän lisäksi tulee tiedustelukyvykkyyttä kehittää mm. älykkäiden valvontaohjelmistojen avulla, jotka suodattavat tehokkaasti tietoliikennettä ja reagoivat poikkeuksellisiin ja mahdollisesti riskialttiisiin tapahtumiin. Tarvitaan älykkyyttä havaita kansallista turvallisuutta vaarantava toiminta, paljastaa operaatioiden takana olevat toimijat ja haitallista koodia sisältävät ohjelmistot ja sovellukset.

Professori, ST Martti Lehto
Informaatioteknologian tiedekunta
Jyväskylän yliopisto
martti.lehto@jyu.fi