Lumen 2/2016 TEEMA-ARTIKKELI

Kybertuvallisuuteen panostetaan Lapissa

Harri Ihalainen, tietohallintojohtaja, Rovaniemen kaupunki
Pekka Iivari, erityisasiantuntija, MTI, Lapin ammattikorkeakoulu
Kenneth Karlsson, lehtori, Teollisuuden ja luonnonvarojen osaamisala, Lapin ammattikorkeakoulu

Asiasanat: kyberturvallisuus, harjoitukset, varautuminen

Esipuhe

EU on lanseerannut Digital Single Market agendan, jossa henkilöiden vapaa liikkuvuus, palveluiden ja pääomien vapaa liikkuvuus taataan. Tämä tarkoittaa, että kansalaiset ja yritykset voivat saumattomasti käyttää ja harjoittaa digitaalisia palveluita. Taustalla on ajan ja paikan riippumattomuus sekä syrjimättömyys. Tämä EU:n Digital Single Market agenda tuo paineita myös yhteiskunnan kyberturvallisuuteen.

Yhteiskuntamme on voimakkaasti riippuvainen tietoverkkojen ja tietojärjestelmien toiminnasta ja olemme erittäin haavoittuvia niihin kohdistuville häiriöille. Kaikessa toiminnassamme lisääntynyt tietointensiivisyys ja digitalisoituminen, toimintojen ulkoistaminen, tieto- ja viestintäjärjestelmien keskinäinen integraatio, kaikille avointen tietoverkkojen käyttö sekä lisääntynyt riippuvuus sähköstä asettavat uudenlaisia vaatimuksia organisaatioiden perustoimintojen turvaamiseksi normaalioloissa, normaaliolojen vakavissa häiriötilanteissa ja poikkeusoloissa.

EU ja Suomen valtion kyberturvallisuusstrategia

Suomen kyberturvallisuusstrategiassa (Valtioneuvoston periaatepäätös 2013) tästä keskinäisriippuvaisesta ja moninaisesta sähköisessä muodossa olevan tiedon käsittelyyn tarkoitetusta ympäristöstä on kansainvälisesti ryhdytty käyttämään termiä kybertoimintaympäristö.

Kyberturvallisuusstrategian mukaan kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus on turvallisuuden osa-alue, jolla pyritään sähköisen ja verkotetun yhteiskunnan turvallisuuteen. Tärkeää on tunnistaa, ehkäistä ja varautua sähköisten ja verkotettujen järjestelmien häiriöiden vaikutuksiin yhteiskunnan kriittisiin toimintoihin, joita ovat energian, veden ja lämmön tuotanto ja jakelu, tietoyhteiskunta palveluineen, kuljetukset ja logistiikka sekä finanssiala. Kyberturvallisuusajattelussa yhdistyy tietoturvallisuuden, jatkuvuuden hallinnan ja yhteiskunnan kriisivarautumisen ajattelua.

Stuxnet-tietokonemadon pääsy Iranin Natanzin rikastuslaitoksen järjestelmään lienee maailmalla tunnetuimpia kyberhyökkäyksiä. Hyökkäyksestä raportoitiin kesäkuussa 2010. Kohteena oli yhteiskunnan elintärkeiden toimintojen kannalta kriittinen järjestelmä, jonka sabotoiminen olisi voinut aiheuttaa laajaa tuhoa. Kyberiskut ydinvoimalaitoksiin, sotilaallisiin kohteisiin ja kansainvälisiin energiajärjestelmiin eivät olisi enää uhka pelkästään yhteiskunnan kriittisille toiminnoille vaan verkottuneiden yhteiskuntien (valtioiden) muodostamalle globaalille järjestelmälle.

Kyberturvallisuus käsitteenä ja toimintaympäristöön liittyneenä

Uudet teknologiat vaikuttavat PK-yritysten toimintaan ratkaisevasti, mutta yritysten valmiudet vastata kyberuhkiin vaihtelevat. Tämä selittyy sillä, että harva yritys on joutunut kohtaamaan kyberturvallisuustapahtumia tai tapahtumia ei yksinkertaisesti ole havaittu. Yritysten kannattaa kuitenkin sisällyttää kyberuhkat riskianalyyseihin ja prosessien kehittämiseen. Kyberturvallisuus on usein esillä silloin kun johonkin organisaatioon on tunkeuduttu tieto- ja viestintäjärjestelmiä hyväksi käyttäen.

Kyberturvallisuutta ja tietoturvallisuutta pidetään synonyymeina. Molempiin termeihin törmäämme arjessa usein ja niitä käytetään usein päällekkäin ja vähän huolimattomasti. Tietoturvallisuus on sitä, että voimme olla varmoja tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Kyse on siis tiedon, sähköisen, kirjoitetun tai muun, turvaamisesta. Se on tietoturvallisuusasia, jos et saa oikeaa tietoa yrityksesi intranetistä tai jos yrityksen verkossa leviää kaikkien saataville vain sinulle tarkoitettuja tietoa. Kyberturvallisuutta puolestaan on se, että kunnan tytäryhtiönä toimivan sähkö- ja lämpölaitoksen järjestelmiin ei pääse kukaan luvatta tunkeutumaan ja katkaisemaan tuotantoprosesseja. Määritelmien sekamelskaan sisältyy

myös termi tietoverkkorikos, joka on poliisin mukaan kyberrikoksen synonyymi (Leppänen et al. 2016).

Tietoverkkoihin tunkeutujat voidaan jakaa valkohattuihin, rikollisiin, terroristeihin ja valtiollisiin toimijoihin. Valkohatut (niin sanotut hyvikset) ajavat jotakin missiota ja julkisuutta mutta eivät halua tuhota järjestelmiä. Klassiset rikolliset eli mustahattuiset krakkerit puolestaan hakevat tuottoa ja rahaa. Terroristit tunnetusti toteuttavat poliittista/uskonnollista agendaa tuhon kautta ja valtiolliset toimijat haluavat tietoa. Nämä toisistaan poikkeavat tavat ja motiivit suorittaa kyberhyökkäyksiä edellyttävät puolustajilta erilaisia taktiikoita ja toimintatapoja. Esimerkiksi rikollisten ollessa kyseessä heidän tunkeutuminen pitää eristää, toiminta katkaista ja verkot on kytkettävä irti. Sen sijaan valtiollisten toimijoiden (vaikkapa vakoilijoiden) tunkeutumista ei välttämättä keskeytetä koska heidän käyttäytymisen seuraaminen antaa mahdollisuuden päästä kiinni laajemmin kiinni vakoiluverkostoon. Tällaisissa tapauksissa yhteyksien katkaiseminen osoittaisi vakoilijalle, että hän on paljastunut.

Kyberrikollisuusuhat

Keskusrikospoliisin mukaan palvelunestohyökkäykset ovat keskeinen osa kyberrikollisuutta. Rikollisuus kohdistuu Suomessa pääosin julkishallinnon palveluihin ja pankkeihin. Viimeaikaiset pankkipalveluihin kohdistuneet hyökkäykset ovat olleet nuorten suomalaisten järjestämiä. Hyökkäyksen tekeminen on halpaa ja jäljittäminen vaikeaa. KRP:n mukaan toinen kyberrikollisuuden muoto on luottokorttitietojen väärinkäyttö, joka on ollut jyrkässä kasvussa vuodesta 2015 lähtien. Skimmauksen eli kortin kopioinnin lisäksi maksukorttitietoja anastetaan tietomurtojen yhteydessä (Muurman, 2016).

Haittaohjelmista kiusallisia ovat erityisesti Ransomware eli kiristysohjelmat. Keskusrikospoliisi kehottaa olemaan maksamatta kiristäjille vaikka tiedossa onkin, että jotkut yritykset ovat varanneet rahaa lunnasvaatimusten maksamiseen. Kiristysohjelmahyökkäyksiä on kohdistunut jopa sairaaloihin ja siellä ne voivat aiheuttaa vakavia ongelmia.

Kybertorjunnan haasteita ovat lainsäädännön jälkeenjääneisyys, virtuaalivaluutat, hitaat oikeusapumenettelyt, kryptaukset ja tekijöiden verkottuminen sekä rikosseuraamusten lievyys. Tiedustelulainsäädännön puuttuminen vaikeuttaa viranomaisten mukaan tietoverkkouhkien torjuntaa. Merkittävä osa verkossa tapahtuvista aisoista on valvonnan ulkopuolella. Nykyisen lainsäädännön mukaan kaduilla voidaan kyllä suorittaa valvontaa mutta ei tietoverkoissa.

Tietoverkkojen turvallisuusuhkat ovat nousseet perinteisten turvallisuusuhkien rinnalle osaksi arjen turvallisuuden kokonaisuutta.

Kyberuhkiin varautuminen

Viestintäviraston mukaan hyökkäyksen tai kiristysten sattuessa on yritettävä dokumentoida (mitä, kuka, miten, milloin on tehty) ja yritysten kannattaa ylläpitää lokeja poikkeamahavainnoista. Myös tietoturvallisuuden resursointiin ja ulkoistuksen hallintaan kannattaa kiinnittää huomiota. Teknisistä torjuntakeinoista viestintävirasto suosittelee segmentoimaan verkkorakenteita (joskus on hyvä olla irti ulkopuolisista järjestelmistä) ja ajantasaistamaan tietoturvapäivityksiä. Tehokas keino tieturvallisuuden kohottamisessa on järjestää yrityksen ulkopuolisen ja sisäpuolisen verkon yhtäaikainen monitorointi. Tämä estää myös yrityksestä ulos lähtevät tietoturvaloukkaukset, jotka voivat olla tahallisesti tai tahattomasti leviäviä.

Tärkeä ennaltaehkäisyn keino on myös viranomaisten ja yritysten välinen yhteistyö. Yrityksen kannattaa ilmoittaa tietoliikenne- ja viestintäverkkoon kohdistuvista epämääräisestä toiminnasta Viestintäviraston Kyberturvallisuuskeskukseen. Toinen vaihtoehto on ilmoittaa suoraan poliisille. Viranomaisilta sekä tieto- ja kyberturvallisuuspalveluita tarjoavilta yrityksiltä saa konkreettisia ohjeita varautumiseen. Lisäksi osaamista ja suorituskykyä pitäisi testata. Kansallisesti pitäisi etsiä parhaita käytänteitä ja pohtia vaikka vakuutusten räätälöintiä kyberuhkia vastaan.

Vaikka kriittinen infrastruktuuri on pääosin yksityisten yritysten omistamaa ja hallinnoimaa, ovat kunnat edelleen avainasemassa kyberturvallisuuden tuomisessa arjen tasolle. Kunnat ovatkin viime aikoina heränneet kyberturvallisuuden merkitykseen. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) yhteydessä toimiva kuntajaosto edistää verkostomaisen toimintatavan kehittämistä kuntien tieto- ja kyberturvallisuustyössä.

Kyberturvallisuus osana organisaation johtamista – CASE Rovaniemi

Rovaniemen kaupunki on Suomen ensimmäisiä kuntia, joissa kyberturvallisuutta on jalkautettu harjoituksin. Rovaniemi järjesti vuonna 2014 harjoituksen SOTE–sektorilla ja vuonna 2015 testattiin koulutoimen valmiuksia. Elokuussa 2016 pidettiin kyberturvallisuuden varautumisharjoitus, jossa harjoituksen aiheena oli kyberuhkien toteutuminen alueella ja tarkastelun kohteena kaupungin johdon toiminta simuloidussa kriisitilanteessa.

Varautumisharjoitusten tavoitteena on tunnistaa kyberturvallisuusuhat ja kehittää uhkamalleihin liittyvää osaamista sekä johtamista.

Elokuun 2016 harjoituksessa oli mukana myös matkailuala, jota edustivat Santa's Hotel Santa Claus ja Sava-Group Oy. Matkailualan mukana olo toi harjoituksen suunnitteluun erittäin ajankohtaisen ja realistisen skenaarion, joka toteutettuna osaltaan lisäsi harjoitukseen osallistuvien mahdollisuutta eläytyä tilanteeseen. Napapiirin Energia ja Vesi tarjosi myös asiantuntija osaamista harjoitusskenaarion rakentamiseen. Harjoitusten valmistelusta ja harjoituksen johtamisesta on vastannut Rovaniemen kaupungin tietohallinto-osasto sekä turvallisuuspäällikkö. Kaupungin johdon sitoutuminen harjoitukseen oli ensiarvoisen tärkeää. Kaupunginjohtajan määräys harjoituksesta koski kaupungin johtoryhmän jäseniä, tietohallintoyksikön työntekijöitä sekä turvallisuuspäällikköä.

Harjoitusten keskeiset havainnot liittyvät johtamiseen, viestintään ja verkostoitumiseen. Organisaatioissa kannattaa mahdollisimman aikaisessa vaiheessa ryhmäytyä ongelman ratkaisemiseksi. Koskipa tämä koulujen rehtoreita, yritysten hallituksia tai kuntien johtoryhmiä. Viestintävastuut ja –tavat tulee olla ennalta suunniteltuja ja ulkopuolisia asiantuntijoita kannattaa kiinnittää mukaan ongelman ratkaisuun hyvissä ajoin. Harjoituksissa kävi ilmi myös se, että olisi tärkeää tunnistaa uhkatilanteiden kehittyessä tarvittava hiljaisten signaalien huomaamisen liittyvä keskeinen osaaminen ja tilannekuvan muodostamisen ja analysoinnin vaatimat taidot. Turvallisuushenkilöstö on tottunut tällaiseen havainnointiin ja kykenee muodostamaan heikoista signaaleista tilannekuvan sekä arvioimaan miten siihen tulee reagoida. Sama epätavallisen toiminnan havaintoherkkyys tulisi jalkauttaa organisaatioiden johtoon eri tasoille. Turvallisuusajattelun arkipäiväistäminen harjoittelun kautta antaa mahdollisuuksia toimia tämän tavoitteen saavuttamiseksi.

Kyberturvallisuuteen tarvitaan osaavia verkostoja

Rovaniemen kaupungin kyberturvallisuusharjoituksen suunnittelu ja toteutus osoitti sen, että kyberuhkien ennalta estämiseen ja harjoitteluun tarvitaan osaavia ja sitoutuneita verkostoja. Rovaniemen esimerkki toi esiin sen, että Rovaniemi kaupunki toimii matkailun, opetuksen ja yrityselämän keskiössä. Näitä on arvioitava kyberuhkien kannalta usealta ulottuvuudelta. Esimerkiksi sähkön, veden, jätteen ja monien muiden perusasioiden haavoittuvuus voi mahdollisesti tuoda suuria ongelmia koko kaupungin systeemille, jota voidaan kutsua kybersysteemiksi.

Lapin ammattikorkeakoulun asiantuntijoita on osallistunut vuosina 2015 ja 2016 Rovaniemen kaupungin kyberturvallisuusharjoitusten suunnitteluun ja seurantaan. Aktiivinen osallistuminen kyberharjoituksiin on vienyt omalta osaltaan eteenpäin Lapin ammattikorkeakoulun turvallisuusosaamisen painoalaa sekä työelämäyhteyksiä. Lisäksi ammattikorkeakoulun opettajat ja asiantuntijat saavat ajankohtaista tietoa omien valmiuksiensa kehittämiseksi.

Vaikka viestintäviraston toimialakatsauksessa 1/2016 todetaan, että karkeasti katsottuna toimivuushäiriöiden esiintymistiheys on viime vuosina pysynyt samalla tasolla, niin on tärkeää harjoitella häiriötilanteita silmällä pitäen ennakolta kaikkien osa-alueiden mahdollisimman saumattoman yhteistyön varmistamiseksi.

Viitteet

EU, Digital Singel Market, Digital Economy & Society. 2016.

Leppänen Anna, Lindeborg Karl ja Jarkko Saarimäki (2016). Tietoverkkorikollisuuden tilannekuva. Valtioneuvoston selvitys ja tutkimustoiminnan julkaisusarja 17/2016.

Muurman Tero, 2016. Rikoskomisario Tero Muurman, KRP kyberrikostorjuntakeskusToukokuussa 2016 pidetyillä turvallisuusalan neuvottelupäivillä kyberrikollisuudesta

https://www.viestintavirasto.fi/attachments/toimialatieto/Toimialaka