E 58/2023 Lausunto

Eduskunnan puolustusvaliokunta

2024-02-29

WITH secure

Lausunnon antaja

Päivämäärä	Tekijä	Muutos	Versio
2024-02-29	Antti Laatikainen, Johtava tietoturvakonsultti	Lopullinen versio	1.1

Dokumentin jakelu

Päivämäärä	Vastaanottaja	Organisaatio
2024-02-29	Puolustusvaliokunta	Eduskunta

Toimeksianto

Asia: E 58/2023 Suomen avaintavoitteet EU:n strategiseen agendaan ja tulevan komission ohjelmaan vaikuttamiseksi.

Suomen puolustusvaliokunta pyysi WithSecurea antamaan asiantuntijalausunnon Suomen suunnitelluista valtioneuvoston avaintavoitteista seuraavalle EU vaalikaudelle 2024-2029. Asiantuntijalausuntoa pyydettiin erityisesti kyberturvallisuuden EU-tasoisen kehittämisen perspektiivistä.

WithSecure perustaa seuraavan lausuntonsa omaan kokemukseensa ja näkemykseensä teollisuudenalan haasteista ja visioista, sekä valtioneuvoston kanslian perusmuistioon EU/41/2024-VNK-1 joka toimitettiin toimeksiannon pohjamateriaaliksi.

Lähtökohta lausunnolle

Kyberturvallisuus on olennainen elementti nykyaikaisen yhteiskuntarauhan, kansallisen- ja kansainvälisen turvallisuuden ja hyvinvoinnin hallinnassa ja ylläpidossa. Digitalisoituminen tuo tietojärjestelmät ja tietotekniikan kaikkien arkeen, teollisuuteen ja viranomaistoimintaan.

Kyberturvallisuus mahdollistaa digitalisaatioon liittyvien riskien hallinnan, uhkien torjumisen ja yhteiskunnallisesti merkittävien toimintojen jatkuvuuden myös poikkeusoloissa. Näin tulkiten, kyberturvallisuus mahdollistaa nykyisen yhteiskuntarakenteen toimivuuden ja luo rungon myös kriisiajan palveluille sekä kyvykkyyksille.

Tietotekniikka, ja sen mukana myös kyberturvallisuus, ovat alati muutoksessa ja näin myös altista maaperää innovaatiolle sekä uusien yritysideoiden ja tuotteiden luomiselle. Suomi on asemoitunut tällaisen innovaation tunnettuna kärkimaana, joten Eurooppalaisen kyberturvatekemisen harmonisointi ja yhteismitallistaminen tuottavat WithSecuren näkemyksen mukaan myös potentiaalia suomalaisen osaamisen viennille sekä Euroopan sisällä että Euroopan ulkopuolelle.

LAUSUNTO

WithSecure näkee tarpeelliseksi omassa lausunnossaan nostaa esille seuraavia kyberturvallisuuden hankkeita tai tavoitteita, ja ehdottaa niitä harkittavaksi Suomen avaintavoitteisiin EU:n strategista agendaa muodostettaessa.

Tilannekuvan rakentaminen

Kansainvälisen yhteistyön merkitys kyberuhkien torjunnassa korostuu entisestään, kun digitaalinen ympäristö ei tunne valtioiden rajoja. Tietoverkkoihin kohdistuvat hyökkäykset voivat olla monimutkaisia ja hankalasti jäljitettäviä, ja niiden taustalla voi olla valtiollisia toimijoita, rikollisjärjestöjä tai yksittäisiä hakkeriryhmiä. Tämä monimuotoisuus vaikeuttaa operatiivisen tilannekuvan muodostamista ja yhteistyötä eri maiden viranomaisten välillä.

WithSecure näkee tarpeellisena reaaliaikaisen, operatiivisen tilannekuvan luomisen jäsenvaltioihin kohdistuvan tietojärjestelmien vaikuttamisen ja kyberrikollisuuden valvonnan tueksi. Olennaista tämän tilannekuvan sisällöstä olisi sen tarkkuus ja konkretian taso, jotta siitä saatavalla ohjauksella voitaisiin toteuttaa konkreettisia ennaltaehkäiseviä ja suojaavia toimenpiteitä.

Tämän tilannekuvan tulisi olla jäsenmaiden viranomaisten käytettävissä erilaisiin tarkoituksiin, mukaan lukien kansainväliseen verkkorikostutkintaan.

EU voi tukea tällaisen näkyvyyden rakentumista erilaisia rajapintoja ja toimintatapoja määrittelevän lainsäädännön tai ohjeistuksen avulla, mahdollistaen viranomaisten tiedonsiirron ja yhteistyön yli rajojen. EU:n tasolla on myös ohjattava ja luotava olosuhteet teollisuudelle uusien palveluiden ja ratkaisujen kehittämiseksi. Tämä tukee myös Suomen oman puolustus- ja kyberteollisuuden kyvykkyyttä uusien palveluiden tarjoamiseen.

EU:lla on useita yhteistyötä vahvistavia- ja siihen tähtääviä aloitteita jo olemassa. Tällaisia ovat esimerkiksi Joint Cybercrime Action Taskforce (J-CAT)[1] sekä Enisan alaisuudessa toimiva European Cyber Crisis Liaison Organisation Network CyCLONe[2].

WithSecuren kuvaama operatiivinen tilannekuva ja sen käytännön toteutuksen suunnittelu voitaisiin koordinoida näiden olemassa olevien elimien kautta tai niiden kanssa. WithSecure ei kuitenkaan suoranaisesti näe nykyisten EU aloitteiden tuottavan vaikkapa kriittisen infrastruktuurin operatiiviselle tietoturvaväelle tarpeeksi ajanmukaista, ja kohdennettua näkyvyyttä toisissa jäsenvaltioissa tapahtuviin häiriöihin ja hyökkäyksiin.

Huomioonotettavana asiana tässä tilannekuvan rakentumisessa on myös tekoälyn ja kvanttilaskennan esiintulo erilaisessa verkkorikollisuudessa ja verkkohäirinnässä. Tulevassa EU:n tekoälyasetuksessa[3] määritellään hyvin kontrollikeinoja ja vaatimuksia tekoälyn ja tekoälyjärjestelmien ylläpitoon ja käyttöön. Siinä ei kuitenkaan WithSecuren näkemyksen mukaan luoda viranomaisille tarvittavaa toimivaltaa tai työkaluja tekoälyn tuomien uhkien torjumiseen, tekoälyä käyttävien hyökkäystapojen tunnistamiseen tai verkossa tekoälyä hyödyntävien laittomien tapahtumien tunnisteiden jakamiseen yllä kuvatulla kansainvälisellä tilannekuvatoiminnallisuudella.

Yhteenveto: Kansainvälisen yhteistyön vahvistaminen, tilannekuvan parantaminen ja teollisuuden tukeminen ovat keskeisiä askelia kohti parempaa kyberturvallisuutta Euroopassa. Tekoälyn tuomiin uusiin hyökkäystapoihin tulee valmistautua myös viranomaisten valvonta- ja torjuntatoimissa.

---

[1] https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce
[2] https://www.enisa.europa.eu/topics/incident-response/cyclone
[3] https://artificialintelligenceact.eu/

Rikollisuuden torjunta

Kyberhyökkäykset ovat nykyään osa arkipäivää, ja niiden monimuotoisuus tekee niiden tarkoitusperän tunnistamisesta haastavaa. Usein hyökkäysten takana voi olla valtiollisia toimijoita, jotka naamioituvat rikollisjärjestöjen taakse. Tämä vaikeuttaa motiivien selvittämistä, ja toisinaan todellinen tarkoitusperä paljastuu vasta myöhemmin tai jää kokonaan hämärän peittoon.

Verkkorikollisuuden torjunnassa on tärkeää tehdä tekijöilleen toiminta mahdollisimman hankalaksi ja kannattamattomaksi. Tutkintaan ja verkkorikollisten kiinniottoon tulisi panostaa entistä enemmän. Lisäksi viranomaisten työtä tulisi koordinoida paremmin, edellisessä kappaleessa kuvattua operatiivista tilannekuvaa hyödyntäen. Kansainvälisen yhteistyön merkitys korostuu, kun kyberuhkien torjunta ei tunne valtioiden rajoja.

Rikollisuuden torjuntaan voitaisiin EU:n tasolla harkita käyttöönotettavaksi erilaisia Cybercrime Exit [4] ohjelmia, sekä Yhdysvalloissa käyttöön otettua Rewards For Justice [5] ohjelmaa. Näillä ohjelmilla päästäisiin pureutumaan verkkorikollisuuteen sitä toteuttavien ihmisten kautta, muodostaen sekä rikollisuutta vastaan toimimisen palkitsemista, että rakentavia tulevaisuudenpolkuja ja todellisia vaihtoehtoja rikolliseen toimintaan päätyneille yksilöille.

Kyberturvallisuuden alalla ollaan yhdessä eri toimijoiden kesken harjoittelun todettu olevan erittäin tehokas tapa tehostaa erilaisiin häiriöihin ja poikkeamiin varautumista sekä niistä toipumista. Hyvänä esimerkkinä Digipoolin vuosittain järjestämät TIETO [6] harjoitukset. WithSecure näkee, että EU voisi tehostaa omaa kyvykkyyttään sekä rikollisuuden torjunnassa, että muihin häiriöihin varautumisessa, koordinoimalla vastaavanlaisia harjoituksia EU tasoisesti. Toimintamallina Suomi voisi tarjota TIETO harjoituksissa rakennettua käytännön tietotaitoa.

Yhteenveto: Kyberhyökkäysten torjunta vaatii monipuolista yhteistyötä, tehokasta tutkintaa ja koordinoitua toimintaa eri viranomaisten välillä. Tavoitteena on tehdä verkkorikollisuudesta kannattamatonta ja parantaa digitaalista turvallisuutta kaikkialla Euroopassa.

Ohjauksen harmonisointi

EU:n alueella ollaan valmistelemassa tai parhaillaan käyttöönottamassa useita kyberturvallisuutta- ja erilaista palautumista sekä varautumista vahvistavaa lainsäädäntöä. Näitä ovat muun muassa NIS2[7], DORA[8], CER[9] ja CRA[10].

Näistä DORA ja CRA tulevat voimaan sellaisenaan kaikissa jäsenvaltioissa, ja NIS2 ja CER jalkautetaan kansallisiksi lainsäädännöiksi.

Molemmat, sekä NIS2 että CER, määrittelevät minimitason riskienhallinnan kontrolleja niin sanotulle kriittiselle infrastruktuurille, eli yhteiskunnan toiminnan ja kansalaisten arjen kannalta merkittäville teollisuuden aloille ja niiden toimijoille. Molemmat direktiivit ovat vaatimuksiltaan ylätasoisia, määritellen toimijoiden vastuulle tunnistaa ja täyttää omassa toiminnassa määrittelyn mukaisia riskienhallinnan kontrollikeinoja.

---

[4] https://poliisi.fi/cybercrime-exit
[5] https://rewardsforjustice.net/rewards/foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/
[6] https://www.digipooli.fi/fi/tieto24
[7] The Network and Information Security (NIS) Directive https://digital-strategy.ec.europa.eu/fi/policies/nis2-directive
[8] Digital Operational Resilience Act (DORA) https://www.digital-operational-resilience-act.com/
[9] Critical Entities Resilience Directive (CER) https://eur-lex.europa.eu/eli/dir/2022/2557/oj
[10] EU Cyber Resilience Act https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

EU:n jäsenvaltioilla on jo nyt laajaa hajontaa siitä, miten direktiivien vaatimukset tulee määritellä kansallisissa laeissa. EU maiden välillä on eroavaisuuksia jo siinäkin, miten NIS2 direktiiviin kuuluvien yritysten ja organisaatioiden jaottelu tärkeisiin ja merkittäviin toimijoihin tulisi tulkita.

Keskinäiset erot maiden välisissä vaatimuksissa, konkretian tasolle vietynä yritysten ja organisaatioiden toiminta- ja tietojärjestelmäsuunnittelussa, aiheuttavat haasteita yhteistyön, valvonnan ja hyökkäyksen torjunnan koordinoinnissa. Eri maiden eroavat lainsäädännöt aiheuttavat myös haasteita useassa maassa toimivien yritysten lakitulkintojen välillä, ja aiheuttavat suuria määriä tarpeetonta hallinnollista selvitystyötä yritysten pohtiessa itse ratkaisuja eroavien tulkintojen välillä.

Suomen tulevassa laissa kyberturvallisuuden riskienhallinnasta[11] ollaan määritelty osio, jossa Suomen valvovat viranomaiset pidättävät oikeuden määritellä direktiivin ja lain sanaa tarkemmalla tasolla käytännön ohjeistuksia konkreettisista riskienhallinnan- ja operatiivisen tietoturvan toteutuksen tavoista.

WithSecure suosittelee EU:n tuottavan vastaavia, yritysten konkreettisia toimia määrittelevistä direktiiveistä nykyistä tarkempia operatiivisia tulkinta- ja toteutusohjeita. Ohjeiden aiheita voidaan kerätä valvovilta viranomaisilta, tarkastajilta sekä teollisuudenalan toimijoilta.

WithSecure suosittelee myös vastaisuudessa harkittavan harmonisointiin ja kansainväliseen yhteistyöhön tähtäävien määräysten olevan regulaation muodossa. Kokemuserona, verrattuna Euroopan tietosuoja-asetuksen[12] ja NIS2:en tulkinnan monimuotoisuutta ja käyttöönoton haasteita, WithSecure voi todeta omaan teollisuudenalatuntemukseensa nojaten yritysten kokevan NIS2:en huomattavasti haastavammaksi.

Yhteenveto: Nykyinen regulaatio parantaa kyberturvallisuuden minimitasoa, mutta ei yhtenäistä Euroopan käytäntöä toivotulla tavalla.

Lausunnon antaja:

Helsingissä, 29.2.2024

Antti Laatikainen

Johtava tietoturvakonsultti

WithSecure Consulting

antti.laatikainen@withsecure.com

+358406372163

Liitteet:

1) Kokoava powerpoint, esitetty Puolustusvaliokunnan tilaisuudessa 01.03.2024

[11] https://valtioneuvosto.fi/-/1410829/hallituksen-esitys-kyberturvallisuusdirektiivin-taytantoonpanemiseksi-lausunnoille

[12] General Data Protection Regulation https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016R0679