HE 57/2024 Lausunto DRAFT

Liikenne- ja viestintävaliokunta

2024-09-27

WITH secure | Consulting

Lausunnon antaja

Päivämäärä	Tekijä	Muutos	Versio
2024-09-27	Antti Laatikainen, Johtava tietoturvakonsultti	Lopullinen versio	1.0

Dokumentin jakelu

Päivämäärä	Vastaanottaja	Organisaatio
2024-09-27	Liikenne- ja viestintävaliokunta	Eduskunta

Toimeksianto

Asia: HE 57/2024 vp Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi.

WithSecure perustaa seuraavan lausuntonsa omaan konsultointityön aikaiseen kokemukseensa teollisuudenalan haasteista NIS2-vaatimustemukaisuuden arvioinnissa ja toteutuksessa, sekä lakivaliokunnan esitykseen HE_57+2024.pdf joka toimitettiin WithSecurelle pohjamateriaaliksi.

Lähtökohta lausunnolle

Nykyaikainen suomalainen yhteiskunta tarvitsee toimiakseen taustalla toimivia tietojärjestelmiä. Yhteiskunnan palveluiden mahdollistavien järjestelmien häiriönkesto, luotettavuus ja saatavuus ovat suorassa yhteydessä ihmisten turvallisuudentunteeseen, yhteiskuntarauhaan ja yhteiskunnan toimintakykyyn.

Suomessa yhteiskunnan toiminnalle kriittisen infrastruktuurin muodostavat tuhannet yritykset, liikkeenharjoittajat ja liikelaitokset. Jotta kansalaiset voisivat luottaa kaikkiin yhteiskunnan palveluihin, on tärkeää määritellä yhteiset tavoitteet ja minimitasot kyberturvallisuuden riskeille.

WithSecuren konsultoinnin asiakkuuksiin kuuluu laaja kirjo NIS2-direktiivin ja kyberturvallisuuslain alaisuuteen kuuluvia kriittisen infrastruktuurin toimijoita. Näiden toimijoiden valmiudet vastata lain vaatimuksiin vaihtelevat suuresti riippuen toimialasta, aiemmasta sääntelystä ja riskienhallinnan kypsyydestä.

LAUSUNTO

WithSecuren näkökulmasta ehdotettu kyberturvallisuuslaki on hyvin laadittu, kattava, relevantti ja erittäin tarpeellinen.

Yhteiskunnan kybersietoisuuden kannalta WithSecure pitää tällaista riskienhallinnan ja hallintakeinojen minimitasoa määrittelevää lainsäädäntöä erittäin tärkeänä.

WithSecuren lausunnossa käsitellään riskienhallinnan käytäntöjä ja haasteita sekä sitä, miten käsittelyssä oleva laki voisi tukea näitä vielä tehokkaammin.

Riskiymmärrys

Kyberturvallisuuslaissa ei mainita yhteiskunnallisen vaikuttavuuden arviointia osana riskienhallintaa.

Riskienhallinta on yrityksen tai organisaation päätöksentekoa tukeva rakenne, jonka avulla pyritään käyttämään resursseja mahdollisimman tehokkaasti. Jokaisella organisaatiolla on rajalliset resurssit, ja riskienhallinnassa tavoitetilan asettelulla on suuri merkitys, sillä se määrittää, mihin riskejä verrataan. Yrityksen liiketoimintariskit eivät aina ole samat kuin yhteiskunnalle tarjottavan palvelun riskit. Selvin havaittava ero näiden välillä on riskien käsittelyyn käytettävissä toimintatavoissa. Riskejä voidaan käsitellä esimerkiksi vähentämällä, siirtämällä, poistamalla tai jakamalla. Yksi vaihtoehto on riskien hyväksyminen, ja kaikilla riskeillä on aina jäännösriski.

Jos yritys tai organisaatio käsittelee vain omaan toimintaansa liittyviä riskejä, he saattavat pitää jäännösriskien ja riskien hyväksymistä päätöksenä, jonka he voivat tehdä puhtaasti liiketaloudellisten ja operatiivisten tavoitteidensa perusteella. Jos yhteiskunnallista näkökulmaa ei oteta huomioon tai laki ei ohjaa siihen, näin ei WithSecuren kokemuksen mukaan aina tehdä. Riskipäätökset hallintakeinojen resurssoinnista, hankinnasta tai käyttöönotosta voidaan tehdä yrityksen oman riskinottohalukkuuden perusteella, vaikka päätös olisi objektiivisesti katselmoituna kestämätön yhteiskuntaan kohdistuvien riskien näkökulmasta.

Kyberturvallisuuslain johdanto-osuudessa sekä vaikuttavuuden arvioinnissa mainitaan, että riskien hallintakeinojen oikeasuhteisuuden arvioinnissa tulee ottaa huomioon riskin yhteiskunnallinen vaikuttavuus, ja sen tulee olla määrittävä tekijä riskin pienentämiseksi nähtävän vaivan ja rahan määrittelyssä. Alkuperäisessä NIS2-direktiivissä todetaan, että toimenpiteiden oikeasuhteisuutta arvioitaessa on otettava huomioon toimijan altistuminen riskeille, toimijan koko sekä poikkeamien todennäköisyys ja vakavuus, mukaan lukien niiden yhteiskunnalliset ja taloudelliset vaikutukset.

Ehdotetussa kyberturvallisuuslaissa käytetty kieli ohjaa arvioimaan riskejä suhteessa “toiminnoissa ja palveluntarjonnassa käytettävien tietojärjestelmien turvallisuuteen ja jatkuvuuteen”. Riskienhallintatoimenpiteiden edellytetään olevan suhteessa tietojärjestelmille aiheutuviin riskeihin ja niiden merkitykseen toiminnan ja palveluntarjonnan kannalta. Tämä luo vaikutelman, että laki tähtää yrityksen oman liiketoiminnan ja palveluntarjonnan toimintavarmuuden parantamiseen, mikä eroaa yhteiskunnalle kriittisen palvelun varmistamisesta.

WithSecuren suositus

Lakitekstiin lisätään NIS2-direktiivin ja perusteluosion mukaisesti suora maininta yhteiskunnalle tarjottavan palvelun merkityksellisyyden arvioinnista relevanttina elementtinä riskienhallintakeinoja määriteltäessä.

Kokemuksemme mukaan useiden teollisuudenalojen toimijoiden kanssa väärin ymmärretty lähtökohta riskienhallinnassa johtaa käytännössä yhteiskunnallisten vaikutusten ja NIS2:n tavoitteiden kannalta kestämättömiin jäännösriskeihin ja riskien hyväksymisiin edellä mainituista syistä.

Riskienhallinnan hallintakeinojen ohjeistus

Yritykset ja organisaatiot, jotka kuuluvat NIS2-direktiivin piiriin, joutuvat käyttämään rahaa ja resursseja riskienhallintakeinoihin. Valvontakeinojen tulee lain määritelmän mukaan olla “suhteutettuja toiminnan laatuun ja laajuuteen, poikkeamasta kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeamien todennäköisyyteen ja vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä ajantasainen kehitys huomioon ottaen käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka[1].”

Useilla lain piiriin kuuluvilla organisaatioilla on haasteita oman toiminnan riskien tunnistamisessa, ja varsinainen työ niiden käsittelyssä ja hallinnassa alkaa vasta tunnistamisen jälkeen. Lakiteksti on hyvä, mutta se tarvitsee rinnalleen paljon konkreettista ohjeistusta, jotta se avautuu lukijoille tavalla, joka johtaa tehokkaaseen kansallisen kyberturvallisuuden parantamiseen.

WithSecuren suositus

Riskienhallinnan hallintakeinojen valinta, niiden tarkoituksenmukainen käyttöönotto sekä tehokas ylläpito ja valvonta edellyttävät perustietämystä siitä, millaisia hallintakeinoja on mahdollista ja tehokasta käyttää. Lain käyttöönotto vaikuttaa moniin teollisuudenaloihin, joiden lähtökohdat kyberturvallisuuteen ovat alhaiset. Kattaviin ohjeistuksiin, neuvontapalveluihin ja mahdollisiin rahoitustukitoimiin on hyvä varautua tarvittavien tahojen resurssoinneissa.

WithSecurella on käytännössä tullut vastaan tilanteita, joissa tunnistetaan riskienhallintakeinojen käyttöönoton tarpeellisuus yhteiskunnallisen merkittävyyden kannalta, mutta konsultoitavalla yrityksellä ei ole tarvittavia resursseja tai rahaa hankintaan. Suosittelemme toimintamallin kuvausta tällaisiin tilanteisiin kyberturvallisuuslain jalkauttamisen tukemiseksi.

[1] HE 57/2024 vp Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi, Kyberturvallisuuslaki, 9 §

Valvonta ja poikkeamista ilmoittaminen

Monet Kyberturvallisuuslain piiriin kuuluvat organisaatiot ovat kaupallisia yrityksiä. Erilaisten toimintakulttuurien, riskienhallintametodien, käytettävissä olevien resurssien ja osaamisen tasojen vuoksi riskienhallinnan rakenteet ja hallintakeinot vaihtelevat huomattavasti kattavuudeltaan ja tehokkuudeltaan. Riskienhallinnassa voidaan tehdä virhearviointeja tai arviointimetodista voi puuttua olennaisia elementtejä, kuten edellä kuvattu “riskiymmärrys”. Jäännösriskien ja riskien hyväksymisen suhteen voidaan tehdä taloudellisiin intresseihin perustuvia päätöksiä, jotka ovat yhteiskunnallisen vastuun kannalta kestämättömiä. Tärkeiden toimijoiden jälkikäteisvalvonta tarkoittaa käytännössä, että vahingon on ensin tapahduttava.

Kyberturvallisuuslain mukainen viranomaisvalvonta kattaa vain osan toimijoista ja on aina rajoitettu valvovien viranomaisten resursseista. Yritysten työntekijöiden omatoiminen puutteiden ilmoittaminen ja palveluita käyttävien kansalaisten ilmoitusten hyödyntäminen viranomaisten työn tehokkaassa kohdentamisessa puuttuu ehdotetusta lakitekstistä. Tämä jättää aukkoja valvontaan ja voi johtaa siihen, että merkittäviä riskejä jää havaitsematta ja käsittelemättä ajoissa.

WithSecuren suositus

Lakiin tai sitä tukeviin ohjeistuksiin tulisi sisällyttää toimintamalli whistleblower-kanavasta sekä muista keinoista, joilla voidaan ilmoittaa yritysten riskienhallinnan räikeistä puutteista valvoville viranomaisille.

Lausunnon antaja:

Helsingissä, 27.9.2024

Antti Laatikainen

Johtava tietoturvakonsultti

WithSecure Consulting

antti.laatikainen@withsecure.com

+358406372163

Liitteet:

1) Kokoava PowerPoint-esitys, esitetty Liikenne- ja viestintävaliokunnan tilaisuudessa 27.09.2024