WithSecure Oyj

Lausunto

29.11.2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

NIS2 on yleisesti ottaen erittäin hyvä edistysaskel eteenpäin tietoturvan osalta, ja riskienhallintavelvoitteet parantavat tietoturvan tasoa kriittisessä infrastruktuurissa. Täytäntöönpanoehdotus sisältää kuitenkin soveltamiseen liittyviä haasteita, joita avaamme seuraavissa kohdissa.

Soveltamisalaa koskevat huomiot

Keskeisiksi toimijoiksi on lueteltu kriittinen infrastruktuuri, mutta tietoturvapalveluiden tarjoajien lukeminen samaan luokkaan ei käytännön kannalta ole ongelmatonta, sillä tietyt velvollisuudet ovat hyvin vaikea, jopa mahdotonta toteuttaa. Esitämme, että kansallisen liikkumavaran salliessa NIS2-direktiivin soveltamisalaan lisätty tietoturvapalveluntarjoajat määriteltäisiin kansallisessa laissa tarkkarajaisemmin. Lain soveltamisalan piiriin tulisi lukea vain sellaiset yritykset, joihin kohdistuva kyberhyökkäys muodostaisi kriittisen uhan kansalliselle infrastruktuurille.

Monet yritykset toimivat kansainvälisesti, mikä voi tehdä paikallisen lainsäädännön yhteensovittamisesta muiden lainkäyttöalueiden lakien ja määräysten kanssa haastavaa, jos niissä on merkittäviä eroja. Ehdotus saattaa edellyttää muutoksia sopimusoikeudellisiin velvoitteisiin globaalien asiakkaiden kanssa, erityisesti niiden, jotka katsotaan keskeisiksi toimijoiksi, eikä kaikkia velvollisuuksia pysty sellaisenaan vyöryttämään sopimuksin sopimusosapuolille. Tämä edellyttää oikeudellisia tarkasteluja ja mahdollisia uudelleenneuvotteluja. Vaatimukset tulisi yhtenäistää mahdollisimman paljon muiden EU:n jäsenvaltioiden kanssa.

Riskienhallintavelvoitetta koskevat huomiot

Ehdotuksen 2 § 18 kohdan yksityiskohtaiset perustelut määrittelevät kyberriskin melko tiukasti, ja 7 § määrittelee sen organisaation kontekstissa. Tulisi selventää, että kyberriskien hallinta on organisaation riskienhallinnan alaista ja se lähtee tuloksista (outcomes), joilla organisaatio haluaa

vähentää riskiä. Määritelmää ei tulisi rajata vain luottamuksellisuuteen, saatavuuteen, eheyteen ja aitouteen, koska se pakottaa organisaatiot pitämään kiinni vain ennalta määritetystä standardista.

Kaikki vaaratekijät huomioiva lähestymistapa (all-hazard approach) on laaja ja se edellyttää tunnistamista ja suunnittelua kaikkia mahdollisia uhkia vastaan, olivatpa ne sitten luonnon, ihmisten tai teknologian aiheuttamia. Vaikka ehdotus vaatii kattavaa lähestymistapaa, ei ole selvää, miten yritysten tulisi punnita erilaisia riskejä, mikä tekee ehdotuksesta monimutkaisen ja mahdollisesti tulkinnanvaraisen tulkita ja toteuttaa. Tarvitaan tarkempia ohjeita tai vakioituja kehyksiä, jotta ehdotuksen velvollisuuksia on helpompi noudattaa. Tulisi lisäksi harkita portaittaista lähestymistapaa riskienhallintavaatimuksiin organisaation koon ja luonteen sekä järjestelmien kriittisyyden perusteella.

Ehdotus ei ole selkeä siltä osin, mitä “oikeasuhtaiset toimenpiteet” tarkoittavat. Se voi johtaa erilaisiin tulkintoihin, mikä voi aiheuttaa haasteita toteutuksessa. Selvennys näiden toimenpiteiden vertailuarvoista tai standardeista voisi olla hyödyllistä.

NIS2-direktiivissä luetellaan esimerkkeinä perustason kyberhygieniakäytännöistä joitakin sellaisia menettelytapoja, jotka saattavat olla haasteellisia toteuttaa etenkin direktiivin soveltamisalaan kuuluvissa pienemmissä yrityksissä. Esimerkkinä tällaisista menettelyistä on erityisesti nollaluottamuksen periaate eli ns. Zero Trust, joka ulottuu perustason kyberhygieniaa pidemmälle. Asianmukaiset identiteetin- ja pääsynhallinnan (IAM) toimenpiteet voivat olla yhtä turvallisia (kuten esimerkiksi monivaiheinen tunnistaminen (MFA)) ja niiden tulisi riittää tapauskohtaisesti. Mikäli Zero Trustia vaadittaisiin, edellyttäisi se Zero Trust -määritelmää tässä säädöksessä.

Raportointivelvoitetta koskevat huomiot

Vaatii käytännön esimerkkejä, mikä on merkittävä poikkeama ottaen huomioon kaikki keskeiset toimijat ja heidän toimialansa. Tällainen määritelmä olisi syytä lisätä lakiin, sillä siinä on oma riskinsä, jos hyökkäyksen merkittävyyden arviointia annettaisiin hyökkäyksen alla olevien yritysten itsensä arvioitavaksi. Esimerkiksi tietoturvapalveluita tarjoavan yhtiön merkittävä poikkeama voi liittyä yhtiön palveluiden taustatoimintoihin (back end), mutta se ei tarkoita, että poikkeama välttämättä vaarantaisi kriittistä infrastruktuuria. Turhaa ilmoittelua tulee välttää.

Raportointivelvollisuuden määräaika on erittäin tiukka (24h), eikä sitä ole mahdollista nykyisillä resursseilla toteuttaa, mikäli yrityksissä ei ole ympärivuorokautista (24/7) valvontaa käytössä, esimerkiksi iltaisin ja viikonloppuisin. Raportointivelvoitteen tulisi olla yhteneväinen tietosuojaloukkausilmoitusten kanssa, koska kyberhyökkäykset voivat sisältää henkilötietoja. Raportointivelvoitteen tulisi alkaa siitä, kun poikkeamasta tultiin tietoiseksi (sallien sen tapahtuvan toimistotyöaikana, huomioiden viikonloput, pyhät ja ajat, jolloin yritys on kiinni, kun kyse ei ole kriittisestä infrastruktuurista), ja aikataulun tulisi olla pidempi, jotta poikkeamia ehditään tutkia sisäisesti ennen niistä ilmoittamista.

Viranomaiselle tulisi raportoida kyberturvallisuusuhista ja läheltä piti -tilanteista, jotka ovat vaikeasti määritettävissä ja alttiita subjektiivisille tulkinnoille tietoturva- ja kyberturva-alalla. Tämä voi aiheuttaa hyvin paljon turhaa raportointia, mikäli tapauksia ei ehditä tutkia sisäisesti, ja mikäli kyseessä on false positive -tilanne. Tulee selventää, mikä on läheltä piti -tilanteen kynnys, sillä on vaikeaa tulkita, mikä on jotain, mikä olisi voinut olla riski, jos mitään ei ole vielä tapahtunut.

Tulisi myös laatia vakioitu menetelmä, jonka kautta yritykset voivat täyttää ilmoituksen, jotta aikataulu on mahdollista pitää. Pakollisen ja vapaaehtoisen ilmoitusvelvollisuuden sekä muualla laissa olevien raportointivelvoitteiden (GDPR, CER, DORA) kannalta direktiivin tavoitteiden sekä toimijoiden hallinnollisen taakan kohtuullistaminen edellyttää keskitettyä, nopeaa ja tehokasta verkkopalvelua samojen tai toisiinsa liittyvien ilmoitusten välittämiseksi kerralla useammalle viranomaiselle. On erittäin tärkeätä, että lain täytäntöönpanossa huomioidaan myös vielä ehdotusvaiheessa olevien lakiehdotusten, kuten kyberkestävyyssäädöksen vaikutus toimijoiden raportointivelvoitteisiin.

Haavoittuvuustarkastus tulisi suorittaa tunkeilemattomasti (non-intrusive) ja ennakoidusti sopien yritysten kanssa tarkastuksista. Potentiaaliset löydökset toimijan ympäristöstä täytyy pitää luottamuksellisena viranomaisen ja ko. toimijan välillä, koska tällaisen tiedon vuotaminen aiheuttaa kasvavan riskin toimijalle potentiaalisen hyökkäyksen osalta.

Tulisi selventää, liittyykö koordinoituun haavoittuvuuden julkistamiseen ilmoitusvelvollisuus toimijalta itseltään CSIRT:lle vai koskeeko tämä kenen tahansa kolmansien/ulkopuolisten tahojen CSIRT:lle ilmoittamia haavoittuvuuksia.

Tietovuodon riski kasvaa, kun sensitiivistä dataa haavoittuvuuksista ja poikkeamista kerätään yhteen paikkaan. Poikkeama- ja haavoittuvuusrekisteri on houkutteleva kohde tietomurroille. Tulee selventää, kenellä tähän tietokantaan olisi pääsy ja mikä on peruste tällaisen tietokannan koostamiselle. Kyseiselle tietokannalle tulee olla erittäin tiukat tietoturvavaatimukset ja se tulee lukea osaksi kriittistä infrastruktuuria. Kyseisiä haavoittuvuuksia ja poikkeamia ei tulisi julkistaa – tai lähtökohtaisesti edes tallettaa rekisteriin – yleisesti ennen kuin kyseiset haavoittuvuudet on korjattu. Muussa tapauksessa se aiheuttaa suuria tietoturvariskejä kriittisissä toimijoissa.

Tietojen siirto yhdeltä toimijalta toiselle on aina riski, ja turhia tiedonsiirtoja tulisi välttää.

Valvontaa koskevat huomiot

Pääsynhallinta ja tiedon luottamuksellisuus ovat tietoturvan kulmakiviä. Myöskään viestin suojaa ei voi tällä lailla heittää romukoppaan – tulee säätää selkeät säännöt sille, miten viestin suojaa voi loukata tietoturvan nojalla.

Lakiehdotuksen 27 §:ssä annetaan laaja kuvaus siitä, mitä tietoja valvontaviranomainen voi pyytää tiettyyn tapahtumaan liittyen. Kun kyse on CSIRT:stä ja tapahtumiin reagoinnista, ainoa tarvittava tieto on käsillä olevaan tapahtumaan liittyvät tiedot, varsinkin jos organisaatio ei pysty vastaamaan tapahtumaan itse. Esimerkiksi riskienhallinnan toimintamallilla ei ole merkitystä kaikissa tapahtumissa, Riskienhallinta on kyberturvallisuusohjelman hallinto-osaa, kun taas poikkeamiin reagointi, johon CSIRT:lle tehtävät ilmoitukset kuuluvat, on reagointia ja toipumista varten.

Pääsy on rajattava tiukasti tapahtumaan liittyviin tietoihin. CSIRT-toimijan tulisi olla vastuussa tietojen turvallisesta tallentamisesta ja asianmukaisten tietojen säilytysrajojen asettamisesta, jotta ne poistetaan viipymättä tietyn ajan kuluttua.

Tämän ehdotuksen alla keskeiseksi toimijaksi luetulla yrityksellä voi olla tämän lain toimialaan kuulumattomien julkishallinnon toimijoiden salassapidettäviä tietoja. Niiden jakaminen valvovalle viranomaiselle olisi lain tarkoitusperien vastaista. Ehdotuksessa tulee selventää tähän liittyvä poikkeus, ja selventää tämän lain suhde muuhun lainsäädäntöön.

Tietojen luovuttaminen usealle ulkopuoliselle osapuolella olisi lain tarkoitusperien vastaista, koska tiedonsiirto ja tallentaminen tarpeettomasti on aina riski.

Ehdotuksen 29 §:n mukainen tarkastusoikeus antaisi kolmannelle osapuolelle oikeudet yrityksen tietojärjestelmiin ja tietoihin, mitä ei voi tehdä. Kyseiset tiedot voivat sisältää hyvin luottamuksellista tietoa yrityksen asiakkaiden riskeistä – mukaan lukien julkishallinnon asiakkaiden. Velvoite ei ole tällaisenaan toteutettavissa, ja sitä tulisi tarkentaa. Olisi täysin lain tarkoitusperien vastaista antaa kolmannelle osapuolelle täydet oikeudet toimijan tietojärjestelmiin ja tietoihin, kun organisaatiolta vaaditaan tietoturvan ja riskienhallinnan hyvää hallintaa.

Ulkopuolinen tarkastuksen suorittaja on tietoturvapalveluiden tapauksessa väistämättä suora kilpailija, joten tämä on ehdottoman ongelmallinen tilanne, eivätkä yritykset voi sitä sellaisenaan noudattaa.

Esimerkiksi “saastuneet viestit” voivat olla muutakin kuin kalasteluviestejä ja ne voivat sisältää henkilötietoja. Näihin ei tulisi antaa automaattista pääsyä ulkopuolisille, vaan tämän tulisi olla muun viestinnän salaisuuden sääntelyn alainen oikeus.

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ehdotuksessa todetaan: "IP-osoitealueet ovat melko vakaita, joten niitä koskevien tietojen pitämisen ajan tasalla ei pitäisi olla suuri taakka."

Jos organisaatio (tässä tapauksessa julkinen sektori) käyttää palveluna tarjottavaa infrastruktuuria (IaaS) tai ohjelmistoa palveluna (SaaS) osana palveluitaan, tämä voi olla taakka. Velvollisuus toimii, mikäli julkisen sektorin palvelut toimivat on-premise-ratkaisuina tai kiinteillä IP-osoitteilla.

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

Ehdotus parantaa yritysten ja julkisen sektorin kyberturvallisuutta. Kuitenkin näiden vaatimusten täyttämiseksi yritysten on investoitava raskaasti henkilöstöön, teknologiaan ja jatkuvaan seurantaan. Tämä voi olla erityisen haastavaa pienille ja keskisuurille yrityksille. Pienemmille organisaatioille tulisi harkita avustuksia tai verohelpotuksia noudattamiskustannusten kompensoimiseksi.

Muut huomiot ja avoin palaute esityksestä

-

Metsärinne Noora
WithSecure Oyj