Finavia Oyj

Lausunto

29.11.2023 FINAVIA 5450

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Finavia Oyj kiittää mahdollisuudesta lausua lakiesityspaketista, jolla täytäntöönpannaan kansallisesti NIS2-direktiivi. Lausuntomme keskittyy ensisijaisesti kyberturvallisuuden riskienhallinnasta annettavaan lakiin.

Kyberturvallisuuden minimitason korottaminen ja organisatorisen kyberturvallisuustyön kypsyystason kehittäminen on kannatettava tavoite. Parhaimmillaan lain tasolla velvoittavat toimenpiteet ovat organisaation sekä sen asiakkaiden ja kumppanien etu ja vastuullinen yritys tekisi toimenpiteitä kyberturvallisuuden parantamiseksi joka tapauksessa ilman ulkoista velvoitetta.

Laintasoisesti sääntelemällä varmistetaan, että markkinoille muodostuu yhteinen näkemys hyväksyttävästä minimitasosta ja jaettu ymmärrys tyydyttävän turvallisuuden saavuttamiseksi edellytettävistä keinoista. Lain kirjaimen ja myöhemmän tulkinnan painopiste tulisikin olla kyberturvallisuustoimien vaikuttavuudessa yksittäisten "temppujen" luettelemisen ja katselmoinnin sijasta.

Pahimmillaan direktiivin soveltamisalaan kuuluvat yritykset jäävät yksin ratkomaan toimitusketjut läpäiseviä kyberturvallisuuden haasteita vailla tosiasiallista kykyä ratkaista niitä. Kyberturvallisuusvelvoitteiden vieminen voimassa oleviin sopimuksiin on vaikutuksiltaan arvaamatonta, eikä pitkäikäiseksi aiottua teknologiaa ole välttämättä edes mahdollista toteuttaa toivotulla riskitasolla. Lainvalvojalta ja -säätäjältä odotetaankin aktiivista otetta, jolla markkinaa muokataan lain tavoitteden edellyttämällä tavalla ilman, että toteutusvastuu kilpistyy aina sopimussuhteen sisäiseksi asiaksi tavalla, jossa velvoitteiden alainen ostaja maksaa kaikki turvallisuusparannukset.

Soveltamisalaa koskevat huomiot

Finavia Oyj on lentoasemayhtiö, joka johtaa ja kehittää koko Suomen kattavaa lentoasemaverkostoa. Finaviassa tehdään työtä, jota ilman maailma olisi kaukana.

NIS2-direktiivin ohella toimintaamme ohjaa kansainvälinen, EU-tasoinen ja kansallinen ilmailun vertikaalia ohjaava regulaatio, joiden valmistelussa NIS2-direktiivi on jo huomioitu.

Osa toimitusketjuamme jää väistämättä NIS2-velvoitteiden ulkopuolelle. Tämä saattaa muodostua haasteeksi velvoitteiden langetessa Finavialle ilman, että käytössämme olisi tehokkaita keinoja vaikuttaa toimitusketjuumme.

Riskienhallintavelvoitetta koskevat huomiot

Laissa kyberturvallisuuden riskienhallinnasta kiteytyy edellä mainittu epäsuhta toimitusketjun eri osiin kohdistuvan sääntelystä. Perusteluissa 9 § 2 momentin kohdan 4 osalta tunnistetaan, että NIS2-velvoitteiden alaisen toimijan alihankintaverkosto ei ole kokonaisuudessaan samojen velvoitteiden alainen.

Finavia ilmaisee huolensa siitä, että lainlaatija ja laillisuusvalvoja ylenkatsovat pitkien sopimussuhteiden avaamisen tuomia riskejä ja jättävät huomioimatta pitkäikäisten teknologioiden tuomat haasteet. Mikäli toimitusketjun palvelu- ja teknologiatarjonnan kyberturvallisuuden kehittäminen jää yksinomaan sopimussuhteen puitteissa tapahtuvaksi, luodaan edellytykset kustannustason hallitsemattomalle kasvulle ja kyberturvallisuuden parantamista vain paperilla tarjoaville näennäisratkaisuille. NIS2-velvoitteiden piiriin kuuluvan ostajan neuvotteluvoima on heikko, mikäli myös myyjään ei kohdistu laintasoisia tai kansainvälisistä standardeista johdettuja velvoitteita kyberturvallisuuden laadun parantamiseksi.

Saman pykälän 4 mom 6. kohdassa viranomaiselle annetaan määräyksenanto-oikeus “perustason kyberhygieniakäytännöistä”. Hygieniakäytännöillä viitataan pykälän 2. momentin listan kohtaan 11. Esimerkkinä “kyberhygieniasta” käytetään niin kutsuttua zero-trust-filosofiaa toteuttavia pääsyn- ja järjestelmänhallinnan käytäntöjä. Luonnollisesti hyvän hygienian vaatiminen ei ole väärin eikä kohtuutonta. Kuitenkin vaarana on, että teknisten määräysten myötä yksittäisten teknologioiden soveltamista edellytetään riippumatta siitä, onko tähän tosiasiallisia edellytyksiä.

Esimerkkinä käytetty zero-trust on erityisen ongelmallinen, koska teknologian soveltaminen edellyttää modernin pilviteknologioihin perustuvaa järjestelmäarkkitehtuuria. Kriittisillä toimijoilla saattaa kuitenkin olla muista lainsäädäntövelvoitteista johtuvia vaatimuksia (erit. viranomaisen luokittelemien tietojen käsittely, varautumisvelvoitteet), jotka nimenomaan muodostavat esteitä

pilvipohjaisiin teknologioihin siirtymiselle. Vaarana on, että toimija jää lainsäädännöstä johtuvien vaatimusten ristiaallokkoon.

Raportointivelvoitetta koskevat huomiot

Laissa kyberturvallisuuden riskienhallinnasta 11 § on epäonnistunut ilmaisu: "..merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa .. asianomaiselle toimijalle taloudellisia tappioita.."

Finavian käytännön tietoturvatyössä opittu havainto on, että "taloudellisia tappioita" tulee jo pelkästään ääneen lausutun tietoturvaloukkausepäilyn tai vääräksi osoittautuneen tietoturvapoikkeamahavainnon selvittämistyöstä. Tiukasti tulkiten jokainen ylimääräinen organisaation perustehtävään liittymätön työtehtävä tai palveluntarjoajalle erillislaskutusta aiheuttava selvitystyö on omiaan aiheuttamaan taloudellisia tappioita. Näin suoranuottisen tunnusmerkistön käyttö _merkittävän poikkeaman_ määrittelemiseksi on ongelmallinen.

Esitämme, että sanamuodon tulisi olla olla esim. "merkittäviä taloudellisia tappioita" tai "huomattavia taloudellisia vaikutuksia". Tällöin ilmaisu olisi linjassa saman momentin luonnollisiin ja oikeushenkilöihin viittavan ilmaisun "huomattavaa aineellista tai aineetonta vahinkoa" kanssa.

Saman pykälän 2. momentissa velvoitetaan antamaan ensi-ilmoitus 24 tunnin sisällä. Ilmoitusvelvollisuus vuorokauden sisällä olisi kestämätön erityisesti, mikäli edellä mainittu huolimaton ilmaisu "taloudellisia tappioita" jäisi voimaan. Merkittäviksi määriteltyjen poikkeamien ja siten ilmoitusten määrä räjähtäisi käsiin, ja useimmilla velvoitteenalaisilla organisaatioilla olisi käytännössä valittava panostaako tietoturvaloukkauksen selvittämiseen ja ratkaisemiseen vaiko viranomaisilmoitusten tehtailemiseen.

Olettaen, että ilmoitustaso kuitenkin lausuntokierroksen myötä tulleen palautteen johdosta asettuu kohtuulliseksi, Finavia muistuttaa, että ilmoitusvelvollisilla organisaatioilla on perusteltu syy odottaa saavansa ilmoitusten myötä konkreettista tukea ja apua poikkeaman hallinnassa ja kyberturvallisuuden tilanneymmärryksen syventämiseksi.

Käytännössä kyberturvallisuusturvapoikkeaman aiheuttaja, turvallisuusongelman juurisyy tai edes vaikutus ei nimittäin ole aina ilmeinen havainnon tehneessä tai hyökkäyksen kohteeksi joutuneessa organisaatiossa. Varsinkaan tuoreeltaan. Ilman organisaatio- tai sektori- ja valtiorajat ylittävää tiedustelutietoa ei ole mahdollista päätellä mitään uhkatoimijasta saati tämän motiiveista, kyvykkyyksistä, menetelmistä ja päämääristä. Ilman tietoa hyväksikäyttömenetelmistä voi olla vaikea arvioida omien kybersuojauksen menettelyjen efektiivistä tehoa. Ilman tietoa hyökkäyksen tunnusmerkistöistä voi olla vaikea suorittaa uhkanmetsästystä tai edes löytää poikkeamahavaintoja tapahtumavirrasta. Kyberturvallisuuspoikkeamaan annettavan ensivasteen laajuus, kohdistus, kesto

ja menettelyt edellyttävät kattavaa ymmärrystä siitä, mitä havainnot kertovat ja mitä voidaan olettaa tapahtuvan pimennossa. Lopulta vahingosta toipuminen saattaa esimerkiksi edellyttää ymmärrystä siitä, missä määrin teknisen infrastruktuurin hallinta on menetetty. Finavian mielestä ei ole kohtuuton vaatimus, että poikkeamaraportteja vastaanottava virnaomaistaho aktiivisesti hyödyntää kartuttamaansa tietoa velvoitteidenalaisten auttamiseksi silloin kun on ilmeistä että raportoitu poikkeama liittyy ilmiöön, josta viranomaisella on jo täydentävää tietoa.

Paitsi, että ilmoitusvelvoitteen tulee palvella kyberturvallisuuspoikkeaman menestyksekästä ja tehokasta ratkaisua, tulee ilmoituksen jättämisen olla helppoa, varmaa ja nopeaa. Poikkeamaepäilyn ensi vaiheiden selvittelyn yhteydessä olisi kestämätöntä, mikäli selvitystyöhön kytketyn henkilöstön aika kuluisi viranomaisen raportointimenettelyn parissa.

Esimerkki laajasti hyödylliseksi tunnustetusta kyberpoikkeamien raportointipalvelusta on kyberturvallisuuskeskus NCSC-FI, entinen CERT-FI. Moni organisaatio raportoi havaintojaan ja epäilyjään kyberturvallisuuskeskukselle matalalla kynnyksellä, koska raportointi on helppoa ja mutkatonta ja lähes poikkeuksetta NCSC-FI pystyy antamaan vastineeksi täydentävää tietoa, jonka avulla poikkeaman aiheuttama riski on mahdollista arvioida tarkemmin ja selvitystoimet on mahdollista suunnata tarkoituksenmukaisesti. NCSC-FI on toistuvasti myös ottanut aktiivisen roolin usean toisistaan riippumattoman ja toisistaan tietämättömän organisaation tietoturvaloukkauksiin antamien vastatoimien koordinoimiseksi.

Esimerkkinä vastakkaisesta toimii esimerkkinä tietosuoja-asetuksen edellyttämä raportointi tietosuojavaltuutetulle. Dynaamisen lomakkeen täyttämiseen kuluu harjaantuneeltakin helposti yli tunnin verran aikaa. Lomakkeesta ei jää ilmoittajalle omaa kopiota, joten oikeusvarmuussyistä ilmoittaja joutuu tekemään ylimääräistä työtä kopioidakseen lomakkeelle syötettävistä tiedoista käsipelillä tietoja kenttä kentältä omaan asianhallintajärjestelmään. Lomakkeeseen syötettävän tietomäärän kartuttaminen voi edellyttää suurten aineistomäärien läpikäyntiä ja useiden toisistaan riippumattomien sisäisten ja ulkoisten toimijoiden selvitystyön koordinointia. Jopa triviaaleissa tapauksissa organisaatiolla voi olla vaikeuksia raportoida GDPR:n edellyttämässä 72 tunnin aikaikkunassa. Tietosuojavaltuutettu ei myöskään lähtökohtaisesti tarjoa vastineeksi syvempää tilannekuvaymmärrystä eikä neuvontaa siitä, miten vastaavat tilanteet on aiemmin ratkaistu. On jopa niin, että tietosuojavaltuutetulle lähettyihin raportteihin ei aina tule edes vastaanottokuittausta, jolloin raportointivelvoitteen alaiselle jää epäselväksi onko viranomainen vastaanottanut raporttia ensinkään. Ylikansallisissa tapauksissa raportointia saatetaan joutua tekemään usealle kansalliselle viranomaiselle rinnakkain.

Finavia edellyttää, että raportointi on sujuvaa ja tuottaa lisäarvoa.

Finavia kiinnittää ilolla huomiota siihen, että lain 17 §:ssä valvovalle viranomaiselle säädetään tehtäväksi tiedottaa tietosuojavaltuutettua silloin, kun se poikkeaman luonne huomioiden on tarpeen.

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

-

Koivunen Erka
Finavia Oyj - Kyberturvallisuusjohtaja