TietoEVRY Oyj

Lausunto

05.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

TietoEVRY Oyj pitää Liikenne- ja viestintäministeriön työryhmän pohdintaa tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla tarpeellisena. Viimeaikaiset keskustelua herättäneet tietomurtotapaukset ovat toimineet hyvinä herättäjinä sekä yksityisille että Valtionhallinnon toimijoille huomioimaan yhteiskunnan kriittisten toimintojen mahdollisia heikkouksia. On kuitenkin mahdollista, että vastaavia rikoksia toteutuu auditoinneista, sertifioinnista ja valvonnasta huolimatta. Siksi tulevaisuudessa on tärkeää varautua myös vahinkojen rajoittamiseen, ripeään tutkintaan, tiedottamiseen sekä oppien keräämiseen ja jakamiseen.

Väliraportissa on tervetulleita ehdotuksia vaatimusten ja vastuiden selkiyttämiseksi sekä tietoturva- ja tietosuojaresurssien lisäämiseksi. Erityinen kiitos tietoturvan ja tietosuojan tarkastelusta taloustieteen ilmiönä ja yritysten kannustimien näkökulmasta. On tärkeätä huomioida, että tietoturva ja tietosuoja verkottuneessa yhteiskunnassa ovat kompleksisia haasteita, jolloin luonnollisesti ratkaisutkin ovat monitahoisia ja vaativia. Tietoturvapoikkeamilta on mahdotonta välttyä kokonaan, joten on tärkeää ymmärtää kokonaiskuva ja välttää ylilyöntejä. Yksityissektorin toimijoihin kohdistettavien kannustimien liittäminen julkisiin, hintakriteeriä painottaviin tietojärjestelmäkilpailutuksiin vaatii huolellista harkintaa.

Lakisääteiset vaatimukset ja valvonta ovat tärkeitä varmistaaksemme yhteiskunnan kriittisten palveluiden tietoturvan hyvän perustason. On myös huomioitava, että tietoturva ei toteudu tarkastamalla, vaan organisaatioiden päivittäisessä työssä johdon kannustamana, riittävin resurssein ja riittävällä osaamisella. Väliraportissa peräänkuulutetaan lisää vaatimuksia, tarkastuksia, sertifiointeja ja resursseja nimenomaan valvontaan ja tarkastamiseen. Samalla on kuitenkin varmistettava, että Suomessa on riittävästi osaamista organisaatioiden saatavilla tietoturvan toteuttamiseen. Hyvän tietoturvan toteuttaminen on vaativampi ja enemmän resursseja vaativa tehtävä kuin sen tarkastaminen tai sertifiointi.

Yksityisen sektorin rooli ja yhteistoiminta viranomaisten kanssa on hyvin huomioitu perusteluissa. Väliraportin laadinnassa elinkeinoelämää ei ilmeisesti ole ollut mukana ja lausuntopyynnön jakelussakin vähäisessä roolissa. Erityisesti ICT palveluntarjoajat ovat merkittävässä roolissa tulevien vaatimusten toteuttamisen osalta. Palveluntarjoajan näkökulmasta on tärkeää, että organisaatiot panostavat hankintaosaamiseensa siten, että tietoturvavaatimukset ovat selkeät ja oikein mitoitetut. Eri toimialoille kohdistetut vaatimukset kohtaavat ICT palveluntarjoajien palveluissa ja järjestelmissä. Toimialarajat ylittävät ja toimialakohtaiset yhtenäiset perusvaatimukset mahdollistavat kustannustehokkaammat palvelut.

Työryhmän 7-kohtaiseen yhteenvetoon tietoturvan ja tietosuojan parantamiseen kriittisillä toimialoilla on helppo yhtyä ja sen pohjalta on hyvä lähteä suunnittelemaan ja toteuttamaan toimenpiteitä. Kaikkia askeleita on kehitettävä tasapainossa, yhteistyössä, tietoa jakaen ja osaamista kartuttaen - huomioiden sekä yhteiskunnan kriittisten toimintojen suojaamisen, että elinkeinoelämän intressit. Kaikilla on varmasti yhteinen tahto varmistaa suomalaisen yhteiskunnan toimivuus.

Kommentit ehdotuksiin poliittisiksi linjauksiksi.

Linjaus 1:

Viranomaisten yhtenäinen säädöspohja on kannatettava. On kuitenkin varmistettava, ettei Kyberturvallisuuskeskuksen luottamuksellinen asema elinkeinoelämän keskuudessa vaarannu. Tällä hetkellä KTK:lle voi kertoa havainnoistaan ilman, että tieto siirtyy muille viranomaisille ilman ilmoittajan hyväksyntää. On myös syytä selkiyttää kansallisen ja kansainvälisen lainsäädännön tulkintaa siten, että tärkeitä tietoja ei jää luovuttamatta tai tietojen luovutus viivästyy lakitulkintojen epäselvyyksien takia.

Linjaus 2:

Resurssien lisääminen on hyvä asia. Muistettava, että merkittävä osa kriittisestä infrastruktuurista on yksityisten toimijoiden hallussa, joten viranomaisten keskinäisen kommunikoinnin lisäksi on huomioitava elinkeinoelämä.

Linjaus 5:

Tietojen vaihtaminen yksityisten yritysten kanssa on myös syytä huomioida. Ratkaisujen tulisi olla yleisesti käytettäviin ratkaisuihin (esim. O365) integroituvia siten, että yrityksiltä ei edellytetä erillisiä kommunikointityökaluja viranomaisyhteyksiin.

Linjaus 7:

Painotettava erityisesti ”selkeät” ja ”oikeasuhtaiset”. Vaatimukset on säilytettävä sellaisella tasolla, että palveluntarjoajat voivat valita itselleen parhaiten toimivat ratkaisut ja toimintamallit. Mikäli tietyille toimialoille on tarjottava erityisratkaisuja, on tiedostettava kustannusvaikutukset.

Linjaus 8:

Ei ole selkeää, kehen velvoite kohdistuu. Onko tarkoitus, että velvoite koskee yksittäisiä toimialojen organisaatioita vai toimialan yhteiseksi määriteltyjä vaatimuksia? Palveluntarjoajia velvoittaa asiakasorganisaation kanssa tehty sopimus, ei viranomaisten toimialalle asettama regulaatio. Toimialan yritysten on varmistettava, että mahdolliset lausunnot on saatu ja havainnot korjattu jo tarjouspyyntöihin. Toimeenpanon auditointivelvoitteet kustannuksineen on huomioitava myös sopimuksissa.

Linjaus 11:

Auditoinnit ovat raskaita toimenpiteitä ja vaativat paljon resursseja myös organisaation käyttämiltä palveluntarjoajilta. Organisaatioiden mahdollisuus tukeutua mahdollisimman paljon palveluntarjoajien omaehtoisesti tekemiin auditointeihin säästää merkittävästi kaikkien osapuolten kustannuksia.

Linjaus 12: Tietoturvasertifiointi kansainvälistä ISO 27001 standardia hyödyntäen on periaatteessa kannatettavaa. Sertifioinnin pakollisuuden laajuutta on kuitenkin syytä harkita huolellisesti. Merkittävien toimijoiden määrittäminen on tehtävä yksiselitteisesti. Raportissa mainittiin kriittisillä toimialoilla olevan lähes 58000 yritystä. Huoltovarmuuskriittisiä organisaatioita Suomessa lienee alle 2000. ISO 27001 sertifikaatteja on Suomessa alle 100 yrityksellä. On myös syytä määrittää, millä laajuudella organisaation sertifiointia edellytetään. Koko organisaation toimintojen sertifiointi ei kaikissa tapauksissa ole tarkoituksenmukaista.

Sivulla 31 viitattiin sertifioinnin kokonaiskustannusarvioon 76 480€ perustuen opinnäytetyöhön, joka kattoi sertifikaatin hankinnan ja kolmen vuoden kokonaiskustannusten arvion 6:n hengen ohjelmistoyrityksessä, jonka lähtötilanne koettiin hyväksi. Tähän arvioon ei pidä laskelmia pelkästään perustaa. Kustannukset voivat olla moninkertaisia riippuen toimialasta, yrityksen koosta ja tietoturvan lähtötilanteesta.

Linjaus 13:

Tietoturvan arviointilaitosten määrän ja vaihtoehtojen lisääminen on kannatettavaa.

Linjaus 21:

NIS-direktiivin kansallisen implementoinnin ja muun kansallisen regulaation yhteensopivuus on varmistettava.

Linjaus 23:

Katakri edellyttää TL IV -tason tietojen sähköisen käsittely-ympäristön olevan tietyille kriittisille palveluille kokonaisuudessaan Suomen lainsäädännön alaisuudessa, toimivaltaisten viranomaisten toimivallan piirissä. On syytä täsmentää termiä ”kriittinen palvelu” ja vaatimuksia palveluiden tuottamiselle Suomessa.

Linjaukset 24-25:

On suositeltavaa hyödyntää mahdollisimman paljon kansainvälisiä standardeja ja sertifikaatteja. Globaalisti toimivat yritykset joutuvat joka tapauksessa tukeutumaan kansainvälisiin standardeihin. Kansallinen PiTuKri on hyvä työkalu pilvipalvelujen hankinnan tueksi, mutta sitä ei pidä käyttää pakollisena vaatimusluettelona. Julkisen sektorin toimijoita on ohjeistettava PiTuKrin (ja Katakrin) oikeaan käyttöön siten, että vaatimukset on sovitettu palveluntarjoajilta hankittaviin palveluihin.

Linjaus 35:

Palvelussa on mahdollistettava ilmoitukset sekä kerralla useammalle viranomaiselle että vain yhdelle viranomaiselle.

Väliraportin muut osat, kommentit:

Tietoturvapoikkeamien ja niiden taloudellisten vaikutusten ennustaminen on vaikeaa. Samoin kuin tietoturvainvestointien taloudellisten hyötyjen ja takaisinmaksuajan laskeminen. Regulaatiolla on siksi roolinsa viranomaisten ja yritysten tietoturvan ja tietosuojan perustason varmistamisessa. On kuitenkin tärkeää mahdollistaa organisaatiokohtainen joustavuus huomioiden organisaation toiminta, resurssit ja riskitilanne. Tasapainon löytäminen on haastavaa.

Perusteluissa mainitaan riittävän tietoturvan olevan poliittisesti määriteltävissä ja sääntely vaikuttavan positiivisesti tietoturvan huomioimiseen. Poliittisesti voidaan edellyttää sopivaa perustasoa, mutta ”riittävä” tietoturvataso on kunkin organisaation itse arvioitava. Sääntely toki lisää tietoturvan huomioimista yrityksissä, mutta se pakottaa kohdistamaan resurssit ensisijaisesti ulkopuolelta annettuihin, ”keskiarvostettuihin” tietoturva- ja tietosuojakontrolleihin. Mikäli organisaation voimavarat riittävät vain regulaation edellyttämiin toimenpiteisiin, organisaation erityishaasteet ja riskit ovat vaarassa jäädä huomiotta. Pakolliset, laajasti suunnatut tietoturvavaatimukset tuskin ovat riittäviä läheskään kaikille organisaatioille.

Liika regulaatio voi jähmettää organisaation toimintaa. Teknologia kehittyy valtavalla nopeudella ja uudesta teknologiasta löytyy väistämättä tietoturvahaasteita. Organisaatioille on kuitenkin tärkeää

arvioida ja ottaa käyttöön uusia, palveluita parantavia teknologisia mahdollisuuksia. Liian rajoittava regulaatio voi pahimmillaan hidastaa innovaatioita ja palveluiden kehittymistä.

Tietoturva- ja tietosuojaosaajien puute on tunnistettu, mutta samalla halutaan merkittävästi lisätä ko. resursseja. Tämä on haastava yhtälö. Huomio kiinnittyi myös siihen, että resursseja halutaan erityisesti tarkastamiseen ja valvontaan. Suuri resurssilisäys näille alueille haastavassa osaajamarkkinassa voi tarkoittaa sitä, että tietoturva- ja tietosuojaosaajien saatavuus tärkeämmille osa-alueille – organisaatioiden palveluiden, tuotteiden ja tietoteknisten ratkaisujen tietoturvalliseen toteuttamiseen sekä jatkuvien tietoturvapalvelujen tuottamiseen – heikkenee entisestään. Kuten väliraportin johdannossa todetaan, tietosuoja ja tietoturva on huomioitava toiminnan koko elinkaaren aikana tuote-, järjestelmä- ja palvelukehityksen lähtökohtana, eikä jälkikäteen päälle liimattavana laastarina.

Perusteluissa oli mainittu luottokorttitietojen olevan paremmin suojattu kuin terveystiedot. Luottokorttitietojen tietoturvavaatimukset (esim. PCI DSS vaatimukset) on määritelty toimialan sisällä, ei viranomaisten toimesta. Toimiala myös arvioi ja uudistaa vaatimuksia säännöllisesti. Maksukorttitoimijoiden kannustimena olivat taloudelliset perusteet, jotka edellyttivät asiakkaiden ehdotonta luottamusta toimijoihin. On myös hyvä ymmärtää, että uudet vaatimukset aiheuttivat toimialalla merkittäviä muutoksia ja kustannuksia: pienimmät toimijat poistuivat markkinoilta koska eivät enää kyenneet vastaamaan vaatimuksiin, syntyi uusia luottokorttimaksuihin erikoistuneita palveluntarjoajia ja yritykset joutuivat tekemään merkittäviä arkkitehtuuri- ja tietojärjestelmämuutoksia. Uusien tietoturvavaatimusten leviäminen organisaatioihin pakotettiin merkittävin sanktioin ja muutos kesti useita vuosia. On syytä huolellisesti arvioida regulaation vaikutukset toimijakenttään.

Tilannekuvan tärkeys mainitaan useampaan kertaan. Tilannekuvasta on hyötyä vain, jos se on ajantasainen ja saatavilla. On syytä varmistaa, että tilannekuvaa ei välitetä yksisuuntaisesti ”alhaalta ylös”, vaan että riittävä tilannekuva on kaikkien kriittisten toimintojen tuottamiseen liittyvien osapuolten käytettävissä.

Pirhonen Jari
TietoEVRY Oyj - Konsernin turvallisuusyksikkö, Jari Pirhonen