CSC-Tieteen tietotekniikan keskus Oy

Lausunto

06.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

CSC – Tieteen tietotekniikka Oy kiittää mahdollisuudesta antaa lausunto väliraporttiin selvityksestä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla.

Työryhmä on lyhyessä ajassa ennakkoluulottomasti tunnistanut tietoturvan ja tietosuojan rakenteellisia ongelmia sekä esittänyt laaja-alaisesti ja kattavasti toimenpide-ehdotuksia ongelmien ratkaisemiseksi.

Myös palveluita tuottavien organisaatioiden turvallisuusjohdossa tunnistetaan hyvin suojaamistoimien molemminpuoliset kannustinloukut sekä ero yleisen tietoturvakiinnostuksen (”tietoturvateatteri” kuten eräs suomalaisen tietoturvayrityksen tietoturvajohtaja ilmaisi asian julkisuudessa) varmistetun ja kattavan operatiivisen tietoturvan välillä.

Tietoturva ei ole ilmaista tuottajalle eikä tilaajalleen vaan edellyttää taloudellista panostusta mm palveluiden ja palvelukomponenttien säännölliseen kovetukseen, turvallisuussuunnitteluun – sekä testaukseen, muutoshallintaan, riskienhallintaan, henkilöstön koulutukseen, kyberharjoituksiin osallistumiseen, johdon katselmointeihin, jne. Nämä ovat kuluja jotka tulisi yhteisesti tunnistaa määritellä sekä palveluiden tilaajan että palveluiden toimesta. Olemassa oleviin palveluihin on mahdollista sopia tietoturvatason nosto.

Väliraportin muut osat, kommentit:

Varsinkin kriittisillä toimialoilla tietoturvavaatimukset tulisi olla selkeitä ja explisiittisiä jo hankintavaiheessa. Nykyisten käytössä olevien turvallisuussopimusten vaatimukset ovat pääosin

kirjattu yleisellä ja monin tavoin tulkittavalla tasolla, olisi huomattavan paljon selkeämpää jos turvallisuussopimuksessa todetaan esim. että palvelun tulee täyttää KATAKRI TL IV tai PiTuKri:n henkilötietokasautuman vaatimuksia.

Julkishallinnossa palveluiden tilaajat eivät yleisesti ole hankintamenettelyissä edellyttäneet tai lukeneet hyväksi että palveluntuottaja on sisällyttänyt palvelun ISO 27001 sertifiontinsa kattavuuteen. Tietoturvan ja tietosuojan vahvistamiseksi kriittisillä toimialoilla sertifiointia tulisi joko edellyttää (Ehdotus 12. jota puollamme) tai sen tulisi antaa merkittävää hyötyä hankintamenettelyissä.

Järjestelmähankintoja tehtäessä tietoturva ja tietosuoja tulisi ottaa huomioon jo hankintaprosessin alussa, sillä näin voidaan parhaiten varmistua siitä, että tietosuoja- ja tietoturvavaatimukset ovat sisäänrakennettuna erilaisiin prosesseihin ja järjestelmiin. Kilpailutushankintaprosesseissa tulisikin kiinnittää aktiivisemmin huomiota esimerkiksi eri toimijoiden tarjoamien palvelujen ja järjestelmien sertifioinnin tasoon.

Vaikutustenarviointi (Ehdotus 29.) tulisi integroida osaksi toimijoiden riskienhallintaa. Tietosuojasertifionnit (Ehdotus 30.) olisi syytä sisältää vaatimuksia myös tietoturvan osalta, nyt riskinä on tietosuojan siiloutuminen sopimushallintoon.

Siltä osin kun operatiiviset tietoturvavaatimukset säädetään velvoittaviksi, tulisi tätä varten luoda myös taloudellinen suunnitelma joka kattaa sekä hankinnoista vastaavat viranomaiset että kriittisten toimialojen yritykset. Varmistettu tietoturva saattaa varsinkin siirtymävaiheessa lisätä kevyesti tuotetun palvelu kustannuksia jopa monikertaisiksi.

Ongelmaksi palvelutuotannossa jää palvelutuottajien omien palvelukomponenttien vastaavien alihankkijoiden tietoturvan ja tietosuojan varmistaminen. Tähän tarkoitukseen KATAKRI , PiTuKri sekä ISO 27001 sertifiointi ovat liian raskaita, myös yleisen tason henkilötietojen käsittelyn ehdot (teknistä ja organisatorisista toimenpiteistä ”huolehdittava”) eivät käytännössä jalkaudu. Tätä ongelmaa ratkaisemaan ehdotamme että yhteistyössä elinkeinoelämän ja kriittisten toimijoiden kanssa luodaan ketterät mutta tietoturva- ja tietosuojavaatimukset varmistavat käytännön toteutusohjeet ja arviointikriteerit.

Huomiomme kiinnittyi myös siihen, raportin ehdotuksissa poliittisiksi linjauksiksi huomioidaan EU- ja kv-yhteistyön merkitys ainoastaan tietoturvavaatimusten (Ehdotus 7.) ja kriittisten alojen (Ehdotus 10.) määrittelyssä. Myös NIS-direktiivin uudelleenarviointityöhön halutaan vaikuttaa kriittisten alojen määrittelyn suhteen (Ehdotus 21.).

Raportissa voisi myös mainita EU- ja kv-yhteistyön vahvistamisen (ja uuteen NIS-direktiiviin vaikuttamisen) myös viranomaisten ja muiden alan toimijoiden välisen yhteistyön ja tietojenvaihdon osalta. Komission strategiassa tällä on vahva painotus (ks. esim. luku 1.2. Building a European Cyber Shield), ja tietojenvaihdon lisääminen on myös yksi NIS-direktiivin uudistuksen tavoitteista (kuten CSC:n lausunnossa myös toivottiin (https://www.csc.fi/-/291475-12).

Toinen komission tärkeä tavoite, jolle voisi ilmaista tukea, on kyberturvallisuuslainsäädännön yhdenmukaistaminen eri puolilla Eurooppaa. Lisäksi mietimme, painottaako LVM:n raportti riittävän vahvasti osaamisen kehittämistä (vrt. Jennin huomio ihmisestä turvallisuusratkaisujen heikoimpana lenkkinä + komission strategian kokonainen luku 1.8 A Cyber-skilled EU workforce), mutta ehkä nämä molemmat kuuluvat ennemmin Suomen kyberturvallisuusstrategian ja sen ensi vuonna valmistuvan toimeenpano-ohjelman scopeen? Laajemmassa kyberturvallisuuskeskustelussa voisi ehkä jatkossa tuoda esiin myös Arctic Connectin kyberturvallisuusnäkökohtia.

Näiden kommenttien täydentämänä pidämme työryhmän ehdotuksia oikeansuuntaisina ja kannatettavina.

Urpo Kaila

Tietoturvapäällikkö

CSC – Tieteen tietotekniikan keskus Oy

Kaila Urpo
CSC-Tieteen tietotekniikan keskus Oy