Maksujärjestelmät-osasto

Jonna Ijäs

7.1.2021
SP/FIVA-EI RAJOITETTU
Julkinen

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Yleisenä kommenttina toteamme, että mahdollisen lainsäädännön soveltamisalaa koskien on syytä huomioida, että Suomen Pankkia koskevat tietoturvavaatimukset tulevat Euroopan keskuspankkijärjestelmän (EKPJ) tietoturvavaatimuksista, joita Suomen Pankin tulee noudattaa.

Kohta 3. Raportista ei käynyt ilmi mitä tarkoitetaan työnantajavirastolla. Termi tulisi määritellä. Lainsäädännössä tulisi mahdollistaa, että tietoturvaosaamisen on mahdollista osoittaa myös muulla tavoin kuin koulutuksella, esimerkiksi aiemmalla kouluttautumisella, työvuosilla tietoturva-asioiden parissa tai tietoturvasertifikaateilla. Raportissa sanotaan, että työnantajavirastot sitoutuvat siihen, että koulutus on pakollinen. Mielestämme parempana käytäntönä voitaisiin katsoa olevan, että työnantajavirastot sitoutuvat siihen, että resurssit organisaatiossa ovat riittävät ja tietoturva-asiantuntijoiden tietotaito ja osaaminen ovat tehtävään nähden ajantasaista ja riittävällä tasolla. Kyberturvallisuuskeskuksen tarjoama koulutus voisi olla yksi tapa hankkia riittävä ja ajantasainen osaaminen.

Kohta 5. Selvityksessä olisi syytä ottaa huomioon myös rajat ylittävä viranomaisten välinen tiedonvaihto.

Kohta 7. Tässä olisi syytä huomioida, että komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi digitaalisesta häiriönsietokyvystä rahoitusmarkkinoilla tuo yhtenäisiä määräyksiä EU-tasolla. Suomen Pankki tulisi

Maksujärjestelmät-osasto

Jonna Ijäs

7.1.2021
SP/FIVA-EI RAJOITETTU
Julkinen

jättää tämän vaatimuksen ulkopuolelle, koska Suomen Pankin tulee noudattaa Euroopan keskuspankkijärjestelmän tietoturvavaatimuksia.

Kohta 11. Raportista jäi epäselväksi, onko kyseessä tekninen vai hallinnollinen auditointi. Ulkoisten palveluntarjoajien tekninen auditointi voi olla haastavaa muuten kuin dokumentaation tai heidän omien auditointiraporttien kautta. Komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi digitaalisesta häiriönsietokyvystä rahoitusmarkkinoilla tuo pilvipalveluntarjoajat keskitetysti EU-tason valvonnan alaisuuteen. Suomen Pankin osalta tietoturvavaatimukset pilvipalveluiden käytölle tulevat Euroopan keskuspankkijärjestelmän tietoturvavaatimuksista.

Kohta 12. Raportista ei käynyt ilmi mitä tarkoitetaan kriittisten toimialojen merkittävimmillä toimijoilla ja mitä toimintoja sertifiointi kattaisi. Toimijat ja toiminnot olisi hyvä määritellä asetustasolla. Raportista jäi myös epäselväksi mitä sertifioinnilla on tarkoitus saavuttaa. Olisi syytä vielä harkita, onko sertifionti oikea kontrollointimekanismi vai riittääkö, että toiminta on esimerkiksi auditoitu ISO 27001 -vaatimuksia vasten? Olisi syytä myös selventää, että koskeeko sertifiointivaatimus myös alihankintaketjuja. Alihankintaketjuissa voi olla mukana myös pieniä toimijoita. Etenkin pienemmille toimijoille kyseinen sertifiointi voi olla liian suuri hallinnollinen taakka.

Kohta 25. Tämänkin osalta Suomen Pankin tietoturvavaatimukset tulevat Euroopan keskuspankkijärjestelmän tietoturvapolitiikasta.

Kunnioittavasti

SUOMEN PANKKI

Liitteet Kirjoita tähän

Jakelu

Tiedoksi Kirjoita tähän