Lausunto Liikenne- ja viestintävaliokunnalle

F-Secure kiittää mahdollisuudesta lausua asiasta U 58/2017 vp (Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi ("kyberturvallisuusasetus")). F-Secure tuottaa tietoturvaohjelmistoja sekä arvioi ja konsultoi kyberturvallisuusalan sertifiointimekanismien mukaista vaatimustenmukaisuutta.

F-Securen näkemys on, että ENISAn pysyvä mandaatti parantaa sen toimintaedellytyksiä ja mahdollistaa aiempaa pitkäjänteisemmän ja suunnitelmallisemman toiminnan. ENISAn pysyvä rooli on vahvempi ratkaisu kuin määräaikaisen mandaatin jatkaminen rajoittunein resurssein.

Tietoturvasertifiointien vaikuttavuudesta F-Securella on kahtalainen kanta: kehitys saattaa osoittautua tietoturvan tasoa parantavaksi tai kyynisen laskelmoivaan vaatimustenmukaisuuspeliin ohjaavaksi. Vasta käytäntö osoittaa, kumpi vaihtoehdoista osoittautuu vallitsevaksi.

- Tietoturvan tasoa parantava skenaario
    - Parhaimmillaan käy niin, että sertifiointivaatimus nostaa tietoturvan yleistä tasoa karsimalla heikoimmin tietoturvastaan huolehtivat toimijat pois tai pakottamalla nämä tekemään edes minimipanostuksen tietoturvaan. Tämä on yleisen edun mukaista, ja mikäli kehitystä ei muuten saada ohjattua tähän suuntaan, uuden lainsäädännön laatiminen on perusteltua.[1]
    - Velvoittavan sertifiointijärjestelmän synnyttäminen luo myös uusia markkinoita vaatimustenmukaisuudesta huolehtimista edistäville uusille palveluille ja tuotteille, joiden tarjoamiseen F-Secure luonnollisestikin osallistuu.
- Skenaario jossa vaatimustenmukaisuuteen suhtaudutaan kyynisen laskelmoivasti
    - On myös olemassa riski, että sertifiointivelvoite ajaa ohjelmisto- ja järjestelmäkehittäjiä ensisijaisesti täyttämään sertifioinnin edellyttämät minimivaatimukset ja vasta toissijaisesti edistämään tietoturvallisuutta.
    - Mikäli sertifikaatista muodostuu edellytys markkinoille pääsyyn, on erittäin todennäköistä, että toimijoiden ensisijainen intressi on saavuttaa ja säilyttää sertifioitu taso riippumatta tietoturvan todellisesta tasosta.
    - Käytännön tietoturvaloukkausten tutkinta ja ohjelmistoturvallisuuspoikkeamien analysointi on kerta toisensa jälkeen osoittanut, että sertifioitu ja vaatimustenmukainen ei tarkoita samaa kuin tietoturvallisuus, ja pahimmillaan ohjaa pahantahtoisia toimijoita markkinoilla kohdistamaan hyökkäyksensä alueisiin joita sertifiointivaatimukset eivät koske.
    - Sertifioinnin ilmaisuvoima ja siitä aiheutuvat kustannukset ovat yleensä hyvin tiukasti sidoksissa toisiinsa; laadukkaan sertifioinnin kustannukset ovat usein korkeat.

[1] F-Secure pyrkii omassa toiminnassaan ensiluokkaiseen tietoturvan tasoon jo omaehtoisesti, kuten varmasti moni muukin toimija. Valitettavasti tiedämme että käytäntömme eivät edusta koko tietotekniikka- ja ohjelmistoteollisuuden toimintakirjoa, ja koemme yleisesti tietoturvaa parantavana sen, että hyvät tietoturvakäytännöt tuodaan näkyviksi ns. minimivaatimuksiksi alueella. Toivomme että sertifiointivaatimuksia määriteltäessä kuullaan alan yrityksiä joilla on sekä tietoa vallitsevista tietoturvakäytännöistä että osaamista avustaa järkevän perusvaatimustason määrittelyssä.

Sertifiointijärjestelmien aiheuttamat kustannukset ohjelmisto- ja muulle järjestelmäkehitykselle voivat olla merkittävät. Tämä saattaa osaltaan tehdä erityisesti pienten ja keskisuurten yritysten markkinoille pääsystä hankalampaa. Eurooppalaiset ohjelmistovalmistajat ovat keskimäärin pieniä, jolloin sertifioinnista saattaa muodostua kynnys, jonka yli aloittava tai kannattavuuden kanssa kamppaileva toimija ei hevin pääse. Tämä heikentäisi erityisesti innovaatioiden ja pienten kasvuyritysten menestymismahdollisuuksia ja tekisi Euroopasta korostetusti monikansallisten suuryritysten pelikentän, samalla kun se loisi kasvuyritykselle epätasa-arvoisen aseman suhteessa Euroopan ulkopuolisiin vastaavankokoisiin toimijoihin, joita em. sertifiointivaade ei koskisi.

Jos katsotaan tämän hetken kuluttaja- ja massamarkkinatuotteiden markkinoita, tietoturvasertifiointeja ei käytännössä kommunikoida kuluttajille eikä niitä tuotteilta tai palveluilta vaadita. Ei ole täysin selvää, miten kuluttajamarkkinoilla saataisiin aikaan sertifikaatti, jolla olisi enemmän vaikutusta kuin tietoturvan huomioivalla kuluttajalainsäädännöllä olisi.

Sertifiointijärjestelmiä kehitettäessä tulisi varmistua siitä, että riittävät todisteet sertifiointikriteerien täyttämisestä voidaan kerätä normaalin ohjelmisto- ja järjestelmäkehityksen yhteydessä ja arviointilaitoksilta olisi mahdollista saada ennakkohyväksyntä tarvittavien todisteiden tyypin ja laadun riittävyyteen. Tämä vaikuttaisi todennäköisesti merkittävästi sertifioinnin kustannuksiin, koska sertifiointia tukevat toimenpiteet voitaisiin integroida osaksi jokapäiväistä tuotekehitystä ja varsinainen sertifiointi olisi kevyempi, syntyneitä todisteita arvioiva toimenpide.

Yleinen tietosuoja-asetus (GDPR, 42. artikla) pyrkii edistämään sertifiointimekanismien ja tietosuojamerkkien käyttöönottoa. Kyberturvallisuusasetusluonnos mainitsee yleisen tietosuoja-asetuksen, mutta ei ota kantaa näiden sertifiointien yhtenäistämiseen vaan ainoastaan toteaa niiden ristiriidattomuuden. Tietoturvallisuus on kuitenkin olennainen osa tietosuojaa. Esimerkiksi tietosuojadirektiivin alaisuudessa syntyneissä tietosuojasertifioinneissa kuten European Privacy Sealissa (EuroPriSe) on laajoja tietoturvavaatimuksia. F-Secure toivoo, että tietosuoja- ja tietoturvasertifiointimekanismit eivät muodostu toisistaan erillisiksi ja päällekkäisiksi.

Suomen tulisi olla aktiivisesti mukana seuraamassa ja mukana uusissa tietoturvasertifiointimenettelyhankkeissa, jotta esimerkiksi yllä mainitut aspektit tulevat huomioonotetuiksi.

Helsingissä 13.11.2017,

F-Secure Oyj

Antti Vähä-Sipilä
Principal Security Consultant