12.3.2015

Viestintäviraston suorittamat salaustuotearvioinnit ja -hyväksynnät

Tilaajan näkökulma

Johdanto

EU:n neuvoston turvallisuussäännöstön[1] mukaan jäsenvaltioiden on nimettävä kansallinen salaustuotteiden hyväksyntäviranomainen (CAA, Crypto Approval Authority). Viestintävirasto toimii Suomen kansallisena salaustuotteiden hyväksyntäviranomaisena ja sen tehtäviin kuuluu muun muassa salaustuotteiden arviointi ja hyväksyntä kansallisen ja kansainvälisen turvallisuusluokitellun tiedon suojaamiseksi. Hyväksynnän tuloksia on mahdollista hyödyntää ja käyttää pohjana, mikäli tilaaja hakee samalle tuotteelle EU-salaustuotehyväksyntää[2]. Tässä ohjeessa kuvataan Viestintäviraston salaustuotearviointi- ja hyväksyntäprosessi tilaajan näkökulmasta.

Arvioinnin ja hyväksynnän edellytykset sekä perittävät maksut

Arvioinnin tilaajalta edellytetään, että se toimittaa riittävät tiedot arviointisuunnitelman tekoa varten, nimeää vähintään yhden soveltuvan teknisen yhteyshenkilön vastaamaan arvioinnissa esiin tuleviin kysymyksiin sekä sitoutuu arviointiprojektin aikatauluun. Tilaajalta edellytetään myös, että se omalta osaltaan mahdollistaa arviointiprojektin kannalta tarvittavat resurssit, joihin tyypillisesti sisältyy testattavan tuotteen ja pyydetyn dokumentaation toimittaminen, tuotteeseen liittyvä koulutus sekä soveltuvat henkilöstö- ja tilavaraukset.

Viestintävirasto veloittaa arvioinnista työmäärään perustuvan maksun[3]. Ennen arviointiprosessin aloittamista tilaajalla on oikeus saada Viestintävirastolta arvio työmäärästä ja maksun suuruudesta.

[1] Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (2013/488/EU). URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:FI:PDF.
[2] http://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/
[3] https://www.viestintavirasto.fi/attachments/LVM_A_Vivin_maksuista_toukokuu_2012_su.pdf

Arviointiprosessin vaiheet

Arviointiprosessi koostuu seitsemästä keskeisestä vaiheesta sekä näitä täydentävistä osavaiheista. Seuraavassa kuvataan keskeiset vaiheet sillä tarkkuudella, että se antaa tilaajalle selkeän yleiskuvan siltä vaadittavista toimista. Arviointiprosessin kulku on havainnollistettu kuvassa 1.

1. Pyyntö tai yhteydenotto Viestintävirastolle

Arviointiprosessi alkaa tilaajan sähköpostiyhteydenotolla Viestintäviraston Kyberturvallisuuskeskukseen[4]. Yhteydenotossa tulee ilmetä minkälaisesta tuotteesta on kyse, missä vaiheessa tuotteen kehitys on (suunnitteilla, valmisteilla, tuotannossa) sekä tuotteelle tavoiteltu suojaustaso. Tarvittaessa Viestintävirasto pyytää lisätietoja tilaajalta.

2. Pyynnön tarkastus ja Viestintäviraston vastaus

Vastaanotettuaan pyynnön Viestintävirasto pyrkii vastaamaan pyynnön tekijälle kahden viikon kuluessa. Edellyttäen että tuote ja sen kehitysvaihe ovat arviointiprosessin kannalta sopivalla tasolla, toimittaa Viestintävirasto tilaajalle ehdotuksen esipalaverin ajaksi sekä listan esipalaveriin vaadittavista dokumenteista.

3. Esipalaveri valmistajan ja Viestintäviraston välillä

Esipalaveri pidetään valmistajan ja Viestintäviraston arvioijien kesken.

Esipalaverissa keskustellaan asiakkaan toimittamasta dokumentaatiosta, joita ovat muun muassa:

- Tuotteen toiminnallinen kuvaus - Käydään läpi tuotelupaus, tuotteen suorituskyky sekä toiminnallisuus. Lisäksi käydään läpi tuotteen kokonaisarkkitehtuuria ja sitä ympäröiviä elementtejä sekä uhkamalleja.
- Tuotteen salaustekniikka - Käydään läpi tuotteen salaustekniset ominaisuudet ja ratkaisut sekä avaintenhallinta.
- Arvioinnin tavoitetaso - Käydään läpi arvioinnin tavoitetaso ja sen saavutettavuus tuotteella aiotussa käyttötarkoituksessa.
- Aikaisemmat arvioinnit ja testaukset - Käydään läpi aiemmin tehdyt arvioinnit ja testaukset.
- Yritysturvallisuuteen ja tuotekehitykseen liittyvät turvallisuusasiat - katselmoidaan valmistajan tietoturvallisuusjärjestelyt ja tilaajan/viranomaisen mahdollinen tarve hakea valmistajasta yritysturvallisuusselvitystä
- Viestintä - Keskustellaan asiakkaan kanssa voiko tuotteesta tai sen käynnissä olevasta arvioinnista viestiä esimerkiksi sidosryhmille.

Mikäli arviointisuunnittelun edellyttämiä tietoja ja dokumentaatiota ei saada järjestettyä esipalaveriin tai niitä ei pystytä toimittamaan esipalaverin jälkeen, arvioidaan arviointiprosessin päättäminen tapauskohtaisesti.

[4] Sähköpostiosoite caa@ficora.fi

4. Arviointisuunnitelma ja sopimuksenteko

Viestintävirasto laatii arviointisuunnitelman, jossa kuvataan yleisellä tasolla kyseisen tuotteen arviointiin liittyvät asiakokonaisuudet sekä arvioinnin aikataulutus. Tilaajalle annetaan mahdollisuus kommentoida arviointisuunnitelmaa ja suunnitelma viimeistellään yhteistyössä tilaajan kanssa.

Kun Viestintävirasto on alustavasti arvioinut salaustuotearvioinnin laajuuden ja työmäärän, solmitaan sopimus arvioinnista Viestintäviraston ja tilaajan välillä.

5. Arviointi

Tuotteen arvioinnin tarkoituksena on tutkia täyttääkö tuote sille asetetut tietoturvavaatimukset sekä toimiiko tuote kuvatulla tavalla.

Arvioinnin edetessä tilaajalle tai valmistajalle raportoidaan keskeisiä havaintoja, joiden pohjalta valmistajan on mahdollista tehdä tuotteeseen muutoksia. Mahdollisten muutosten jälkeen testit uusitaan tarvittavin osin sekä jatketaan tuotteen testaamista arviointisuunnitelman mukaisesti.

6. Loppuraportti

Kun arviointi on saatu päätökseen, annetaan arvio tuotteen vaatimustenmukaisuudesta. Vaatimustenmukaisille tuotteille myönnettävä hyväksyntä koskee tiettyä tuoteversiota ja on voimassa toistaiseksi. Hyväksytyt salaustuotteet lisätään Viestintäviraston ylläpitämälle hyväksyttyjen salaustuotteiden listalle[5], ellei arvioinnin tilaaja tai valmistaja halua pitää hyväksyntää poissa julkisuudesta.

7. Tuotteen elinkaarenhallinta

Hyväksytyn tuotteen uudet ohjelmisto- tai tuoteversiot eivät automaattisesti ole hyväksyttyjä. Mikäli muutetulle tuotteelle halutaan hyväksyntää, tulee asiasta olla yhteydessä Viestintäviraston Kyberturvallisuuskeskukseen. Arviointiprosessin aikana voidaan kuitenkin sopia valmistajan kanssa siitä, millaisia muutoksia hyväksynnän saaneelle tuotteelle voidaan tehdä ilman erillistä yhteydenottoa. Kriittisten ohjelmistohaavoittuvuuksien korjaamisen tulisi tapahtua mahdollisimman nopeasti ja asiasta tulisi olla välittömästi yhteydessä Kyberturvallisuuskeskukseen.

[5] www.ncsa.fi > Asiakirjat > https://www.viestintavirasto.fi/attachments/tietoturva/Viestintaviraston_NCSA-toiminnon_hyvaksymat_salausratkaisut.pdf

Viestintävirasto
Kyberturvallisuuskeskus

SALAUSTUOTEARVIOINTI JA -HYVÄKSYNTÄPROSESSI