Pvm

Kyberturvallisuuskeskuksen IoT-tietoturvamerkin vaatimuksenmukaisuusilmoitus

Ilmoituksen rakenne ja täyttöohjeita

Ilmoituslomakkeen tarkoituksena on tarjota tietoja IoT-tuotteen turvallisuudesta sekä Kyberturvallisuuskeskukselle että teknisesti valveutuneille kuluttajille. Se julkaistaan osana kuluttajille jaettavaa materiaalia merkin myöntövaiheessa.

Ilmoituksen kappaleessa 1 listataan yleistietoja IoT-tuotteesta ja siihen liittyvästä ekosysteemistä kuten mobiilisovelluksista ja valmistajan tai kolmansien osapuolten tarjoamista verkkopalveluista. Kappaleen 2 alakohdat käsittelevät kuluttajien kannalta merkittävimpiä IoT-tietoturvauhkia. Kohdissa on lueteltu relevantteja vaatimuksia jotka täyttämällä vähennetään altistusta näille uhkille. Vastaamisen helpottamiseksi vaatimuksia on pyritty mahdollisuuksien mukaan kokoamaan taulukoihin. Kohdissa ehdotetaan myös kuvailevia tekstejä, joiden tarkoituksena on lisätä ymmärrystä valmistajan tietoturvatoimista.

Eri kohdissa mainitut ETSI-vaatimukset viittaavat standardin ETSI TS 103 645 "CYBER; Cyber Security for Consumer Internet of Things" kohtiin. Standardi on saatavilla osoitteesta https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

1 Tuotteen kuvaus

Kuvaa tuote tai tuoteperhe, jolle tietoturvamerkkiä haetaan (jatkossa Tuote), ja sen toimintojen kannalta olennainen valmistajan tai kolmannen osapuolen ekosysteemi (jatkossa Palvelu).

1.1 Tuen kesto

Ilmoita päivämäärä, johon saakka minimissään Tuote on tietoturvapäivitysten piirissä (ETSI 4.3-4). Mikäli Tuotetta tai sen osaa ei voida päivittää, on tästä viestittävä kuluttajalle selkeästi. Ilmoita tukijakso, jonka aikana tällaiset komponentit ovat vaihdettavissa (ETSI 4.3-8, 4.3-9).

1.2 Tietoturvallisuusohjeet

Tuotteen suomenkieliset tietoturvallisuusohjeet löytyvät verkosta osoitteesta http://example.com/valmistaja/security/Tuote[1] (ETSI 4.12-1).

1.3 Muut tuotteen täyttämät vaatimukset

Tuote on CE-merkitty. Tuotteelle on haettu tietoturvasertifikaatti X (linkki, esim. brittiläinen IoT-leima). Tuotteen palvelukomponttien turvallisuus on tarkastettu tavalla Y (linkki) tai niille on haettu sertifikaatti Z (linkki, esimerkiksi Cloud Security Alliancen STAR -sertifikaatti).

2 Turvaamistoimet yleisimpiä IoT-uhkia vastaan

Tuote on turvattu yleisimpiä uhkaskenaarioita vastaan seuraavissa kappaleissa luetelluilla tavoilla.

2.1 Heikot, helposti arvattavat tai kovakoodatut salasanat

Kaikkien Tuotteen salasanojen tulee olla yksilöllisiä eikä niitä saa pystyä palauttamaan yksittäistä laitetta laajemmassa käytössä oleviin oletusarvoihin (ETSI 4.1-1).

Kuvaa, miten Tuotteessa on suojauduttu heikkojen tai kovakoodattujen salasanojen aiheuttamilta uhkilta. Jos uhka on kompensoitu esimerkiksi siten, että käyttäjä tunnistetaan muulla tavalla kuin salasanalla tai laitteen käyttäjää ei tarvitse muiden turvallisuuskontrollien vuoksi tunnistaa, kuvaa miten näillä saavutetaan vahvaa salasanaa vastaava tietoturvallisuustaso.

[1] Korvaa tämä linkki omallasi.

2.2 Turvattomien tai vanhentuneiden komponenttien käyttö

Kaikkien Tuotteen ohjelmistokomponenttien tulisi olla turvallisesti päivitettävissä (ETSI 4.3-1). Päivitystarpeesta tulee tiedottaa kuluttajalle jokaisen komponentin osalta (ETSI 4.3-2, 4.3-5). Päivitykset tulisi tuottaa saataville pian tietoturvaongelman havaitsemisen jälkeen (ETSI 4.3-3) ja päivittämisen tulisi olla käyttäjälle yksinkertaista (ETSI 4.3-5). Valmistajien tulee tarjota julkinen haavoittuvuuksien raportointipiste (ETSI 4.2-1).

Kuvaa, miten Tuotteessa ja Palvelussa on suojauduttu turvattomien ja vanhentuneiden ohjelmistokomponenttien aiheuttamia uhkia vastaan. Kuvaa esimerkiksi, miten Tuotteessa käytettyjen ohjelmistokomponenttien, kuten käyttöjärjestelmän, palvelinohjelmistojen ja ohjelmistokirjastojen, haavoittuvuuksia seurataan kattaen koko ohjelmiston tuotantoketju. Kuvaa miten Tuotteessa on toteutettu ohjelmistopäivityksien ajantasainen saatavuus, helppo asennettavuus, laatu ja turvallinen välitys. Tyypillinen päivityssykli on 30 - 90 päivää, mutta erityyppisissä tuotteissa päivitysten tiheys voi vaihdella suuresti.

2.3 Riittämätön yksityisyyden suojaaminen

Kuluttajille tulee viestiä selkeästi, kuinka Tuotteessa ja Palvelussa käsitellään henkilötietoja, mikä on tiedon käsittelyperuste ja kuka tietoja käsittelee. Tämä koskee myös kolmansia osapuolia kuten mainostajia. (ETSI 4.8-1)

Kuvaa, miten Tuotteessa ja Palvelussa on varmistuttu siitä, että henkilötietojen tallennus ja käsittely tapahtuvat käyttäjälle läpinäkyvällä tavalla ja niiden laajuus perustuu palvelun toteuttamiseen liittyvään tarpeeseen. Kohtaan 2.3 vastaamisen apuna voi käyttää seuraavaa taulukkoa:

Henkilötieto	Tuote/Palvelu/Komponentti	Käyttötarkoitus	Käsittelijä

2.4 Turvaton tiedonsiirto ja säilytys

Turvallisuuden kannalta olennaiset tiedot ja toiminnot, mukaan lukien etähallintapalvelut, tulee suojata tarkoitukseen soveltuvilla salausmenetelmillä (ETSI 4.5-1). Salausavaimia tulee hallita turvallisella tavalla (ETSI 4.5-2). Valtuutustiedot ja muut turvallisuuskriittiset tiedot on talletettava turvallisesti Tuotteessa ja Palvelussa (ETSI 4.4-1).

Kuvaa, miten Tuotteessa ja Palvelussa, sekä Tuotteen ja Palvelun välisessä viestinnässä, on suojauduttu puutteellisen tiedon salauksen sekä puutteellisen pääsynhallinnan aiheuttamaa uhkaa vastaan. Salasanojen osalta tämä tyypillisesti tarkoittaa tiivistemekanismien käyttöä.

2.5 Turvattomat verkkopalvelut ja ekosysteemirajapinnat

Tuotteen toiminnan kannalta tarpeettomat verkkopalvelut tulisi poistaa käytöstä (ETSI 4.6-1). Ohjelmistojen tulisi käyttää pienimpiä toiminnallisuuden ja turvallisuuden kannalta mahdollisia oikeuksia (ETSI 4.6-5). Käyttöliittymärajapintojen, ohjelmistorajapintojen (API) ja verkkorajapintojen välityksellä annettavat syötteet tulee tarkastaa (ETSI 4.13-1).

Kuvaa, miten Tuotteessa on suojauduttu verkkoon näkyvien palveluiden (esimerkiksi web-käyttöliittymät ja etähallintaprotokollat) heikkouksien ja haavoittuvuuksien aiheuttamilta uhkilta. Huomioi myös Tuotteen käyttämät radiorajapinnat.

Kuvaa, miten Palvelussa (esimerkiksi tuotteen pilvipalvelupohjainen hallinta tai tietojen tallennus) on suojauduttu näiden aiheuttamia uhkilta, kuten luottamuksellisten tietojen paljastumiselta tai tuotteen oikeudettomalta haltuunotolta.

Kohtiin 2.4 ja 2.5 vastaamisen apuna voi käyttää seuraavaa taulukkoa. Tuotteen ja Palvelun kehityksen yhteydessä tehdyssä testauksessa käytettyjen menetelmien ja työkalujen luettelointi helpottaa arviointia.

Portti / Radiotekniikka	Salaus ja pääsynhallinta	Käyttötarkoitus

2.6 Turvattomat oletusasetukset

IoT-laitteiden käyttöönoton ja ylläpidon tulisi olla suoraviivaista ja seurata käytettävyyden parhaita käytäntöjä (ETSI 4.12-1).

Kuvaa, miten Tuotteessa ja Palvelussa on suojauduttu turvattomien tehdas- ja oletusasetuksien aiheuttamaa uhkaa vastaan. Kuvaa myös, miten käyttäjää ohjataan pitämään asetukset tietoturvallisina.

2.7 Yrityksen yhteystiedot

Yrityksen nimi:

Y-tunnus:

Yhteyshenkilön nimi:

Sähköposti:

Puhelinnumero:

Täytetyt lomakkeet lähetetään sähköpostitse osoitteeseen tietoturvamerkki@traficom.fi