Pvm

Tietoturvamerkin vaatimustenmukaisuuslomake

Lomakkeen käyttö

Tämä lomake tarjoaa tietoa IoT-tuotteen tietoturvallisuudesta kansalliselle tietoturvaviranomaiselle sekä teknisesti orientoituneille kuluttajille. Lomake julkaistaan osana tietopakettia kuluttajille aina, kun uusi Tietoturvamerkki myönnetään.

Osio 1 tarjoaa yleistä tietoa merkin saaneesta tuotteesta ja siihen liittyvästä ekosysteemistä, kuten mobiilisovelluksista ja kolmannen osapuolen tarjoamista pilvipalveluista. Osio 2 käsittelee kuluttajien kannalta merkityksellisiä tietoturvauhkia sekä niiden torjumiseen käytettäviä tietoturvallisuusvaatimuksia. Vaatimuskohtien yhteyteen on liitetty taulukoita, joita voi käyttää apuna lomakkeen täyttämisessä silloin, kun se on mahdollista ja järkevää. Lomakkeessa annetaan myös esimerkkejä tavoista, joilla tuotteen tietoturvallisuusominaisuuksia voidaan kuvata.

Tämän tekstin viittaukset ETSIin ovat vaatimuksia, jotka esitetään standardissa ETSI EN 303 645 "CYBER; Cyber Security for Consumer Internet of Things". Standardi saatavilla osoitteessa https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Yhteystiedot

Yrityksen nimi:	
Y-tunnus	
Yhteyshenkilö:	
Sähköposti:	
Puhelinnumero:	

Hakemus lähetetään osoitteeseen tietoturvamerkki@traficom.fi

1 Tuotekuvaus

Kuvaa tuote tai tuoteperhe (Tuote), jolle merkkiä haetaan. Kuvaa myös valmistajan tai Tuotteen toiminnan kannalta olennainen kolmansien osapuolten tarjoama ekosysteemi (Palvelu).

1.1 Tuen kesto

Valmistajan tulee ilmaista käyttäjälle selvällä ja läpinäkyvällä tavalla Tuotteelle taattava tukijakso (ETSI 5.3-13). Määrittele tukijakso ja kerro, kuinka siihen liittyvä tieto on käyttäjän saatavilla.

1.2 Tietoturvaohjeistus

Valmistajan tulee tarjota käyttäjille ohjeet Tuotteen turvalliseen käyttöönottoon (ETSI 5.12-2). Kerro, missä tietoturvaohjeistus on saatavilla suomeksi.

1.3 Muut sertifikaatit ja merkit

Kuvaa muut sertifikaatit, joiden vaatimukset Tuote täyttää. Esimerkiksi CE-merkki ja/tai FCC-merkki; Tuotteella on sertifikaatti X (esim. UK:n tietoturvamerkki, lisää linkki); taho Y on todentanut tuotteessa käytetyt palvelukomponentit

2 Suojautuminen tyypillisiä IoT-uhkia vastaan

Tuote on suojattu tyypillisiltä IoT-uhilta seuraavissa osioissa kuvatuilla tavoilla.

2.1 Heikot, helposti arvattavat tai kovakoodatut salasanat

Salasanoja koskeva vaatimustaso on kuvattu seuraavassa. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Tuotteen salasanojen täytyy aina olla yksilöllisiä ja laitekohtaisia tai käyttäjän itsensä määrittelemiä, jos Tuote ei ole tehdasasetustilassa (ETSI 5.1-1).	☐	☐	☐	☐

Kuvaa miten Tuote on suojattu heikkojen tai kovakoodattujen salasanojen muodostamalta uhalta. Kuvaa, miten vahvoja ja yksilöllisiä salasanoja vastaava tietoturvallisuustaso on saavutettu. Esimerkkinä: jos tuote on esimerkiksi suojattu muutoin kuin käyttäjän tunnistusta hyödyntäen tai jos käyttäjän tunnistaminen tapahtuu muutoin kuin salasanan avulla.

2.2 Turvattomien tai vanhentuneiden komponenttien käyttö

Turvattomien tai vanhentuneiden komponenttien käyttöä koskevat vaatimukset ovat seuraavat. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Muiden kuin hyvin kapasiteetiltaan hyvin rajallisten laitteiden tulee sisältää turvallisen päivityksen mahdollistava päivitysmekanismi (ETSI 5.3-2).	☐	☐	☐	☐
Päivitysten asentamisen pitää olla käyttäjälle yksinkertaista (ETSI 5.3-3).	☐	☐	☐	☐
Päivitykset on toimitettava kohtuullisessa ajassa (ETSI 5.3-8).	☐	☐	☐	☐
Valmistajan tulee kertoa käyttäjälle selkeästi ja ymmärrettävästi vaadittavista tietoturvapäivityksistä sekä riskeistä, joilta päivitykset suojaavat (ETSI 5.3-11).	☐	☐	☐	☐
Valmistajan tulee asettaa haavoittuvuuksien hallintapolitiikkansa julkisesti saataville (ETSI 5.2-1).	☐	☐	☐	☐

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Valmistajan tulee jatkuvasti havainnoida, tunnistaa ja poistaa tietoturvallisuuteen liittyviä haavoittuvuuksia tuotteissa ja palveluissa, joita se myy, tuottaa tai on tuottanut (ETSI 5.2-3).	☐	☐	☐	☐

Kuvaile kuinka Tuote tai Palvelu on suojattu turvattomien ja vanhentuneiden komponenttien aiheuttamalta uhalta. Kuvaa esimerkiksi, miten kaikkien komponenttien haavoittuvuuksia seurataan alihankintaketjuissa, mukaan lukien käyttöjärjestelmät, verkkopalvelut sekä ohjelmistokirjastot. Kuvaa, miten oikea-aikaisuus, asennuksen helppous, laadunvarmistus ja turvallinen tiedonsiirto ja asennus on varmistettu Tuotteen päivityksessä. Päivitysväli vaihtelee tyypillisesti 30–90 päivän välillä, mutta tämä voi vaihdella merkittävästi tuotetyypeittäin.

2.3 Riittämätön tietosuoja

Tietosuojaa koskee seuraava vaatimus. Osoita vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Valmistajan tulee tarjota kuluttajille palveluista ja tuotteista selkeää ja läpinäkyvää tietoa siitä, mitä henkilötietoa käsitellään, miten sitä käytetään, kuka sitä käyttää ja mihin tarkoitukseen. Tämä koskee myös Tuotteeseen liittyviä kolmansia osapuolia, kuten mainostajia (ETSI 6.1).	☐	☐	☐	☐

Kuvaa kuinka varmistetaan, että Tuotteen tai Palvelun sisältämää yksilöivää henkilötietoa käsitellään ja varastoidaan käyttäjälle läpinäkyvällä tavalla ja siten, että se rajoittuu vain toiminnallisuuden kannalta välttämättömään.

Voit käyttää seuraavaa taulukkoa yksilöivän henkilötiedon kuvaamiseen. Tietojen luettelointi auttaa niiden arvioinnissa.

Yksilöivä henkilötieto	Tuote/Palvelu/Komponentti	Tarkoitus	Henkilötiedon käsittelijä

2.4 Turvaton tiedon siirto ja varastointi

Tiedon siirtoa ja säilytystä koskevat seuraavat vaatimukset. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Tietoturvamielessä arkaluontoiset parametrit tulee pysyvässä säilytyksessä tallentaa laitteeseen turvallisesti (ETSI 5.4-1).	☐	☐	☐	☐

IoT-kuluttajalaitteessa tulee käyttää kryptografian parhaita käytäntöjä turvallisen viestinnän varmistamiseksi (ETSI 5.5-1).	☐	☐	☐	☐
Valmistajan tulee noudattaa tietoturvallisia hallintaprosesseja laitteen kriittisten tietoturvaparametrien käsittelyssä (ETSI 5.5-8).	☐	☐	☐	☐

Kuvaa, miten Tuote ja/tai Palvelu sekä niiden välinen viestintä on suojattu salauksen ja pääsynhallinnan puutteita vastaan. Salasanojen suojaamisessa tässä käytetään tyypillisesti tiivistysfunktioita.

2.5 Turvattomat verkkopalvelut ja ekosysteemirajapinnat

Verkkopalveluita ja ekosysteemirajapintoja koskevat seuraavat vaatimukset. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
Verkon kautta tehtävät, tietoturvan kannalta merkittävät muutokset vaativat tunnistautumista (ETSI 5.5-5).	☐	☐	☐	☐
Kaikki toiminnallisuuksien kannalta tarpeettomat verkon ja loogiset rajapinnat tulee poistaa käytöstä (ETSI 5.6-1).	☐	☐	☐	☐
Ohjelmiston tulisi toimia mahdollisimman vähillä käyttöoikeuksilla huomioiden sekä tietoturvan että toiminnallisuudet (ETSI 5.6-7).	☐	☐	☐	☐

IoT-kuluttajalaitteen tulee tarkastaa kaikki eri rajapintojen kautta tulevat syötteet. Erityisesti käyttöliittymän ja verkkorajapintojen kautta tulevat (ETSI 5.13-1).	☐	☐	☐	☐

Kuvaa miten Tuote on suojattu haavoittuvuuksilta avoimissa verkkopalveluissa, kuten verkkorajapinnoissa ja etähallinnassa. Ota huomioon myös radiorajapinnat.

Kuvaa miten Tuotteen avoimet verkkorajapinnat on suojattu esimerkiksi luvattomalta tunkeutumiselta tai tietovuodoilta.

Nämä rajapinnat liittyvät tyypillisesti pilvipalveluihin ja etähallintaan.

Seuraavaa taulukkoa voidaan käyttää vastattaessa kohtiin 2.4 ja 2.5. Tuotteen ja/tai Palvelun testaamisessa käytettävien työkalujen ja menetelmien listaaminen auttaa niiden arvioimisessa.

Verkkoportti / Radioteknologia	Salaus / Pääsynhallinta	Käyttö

2.6 Turvattomat oletusasetukset

Turvattomia oletusasetuksia koskee seuraava vaatimus. Osoita kunkin vaatimuksen toteutuminen käyttäen tarkastuslistaa.

	Vaatimustenmukainen	Ei sovellu	Ei tietoa	Vaatimus ei täyty
IoT-kuluttajalaitteen kuluttajalta vaatimat päätökset käyttöönotossa ja ylläpidossa tulee minimoida. Lisäksi tulee noudattaa tietoturvallisuuden käytettävyyden parhaita käytäntöjä (ETSI 5.12-1).	☐	☐	☐	☐

Kuvaa miten Tuote ja/tai Palvelu on suojattu turvattomilta tehdas- tai oletusasetuksilta. Kuvaa myös, miten käyttäjää opastetaan ylläpitämään turvallisia asetuksia.