TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Havaintoja älylaitteiden tietoturvasta

Tietoturvamerkki Tampereella 18.4.2023

Kimmo Koskenheimo

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tietoturvamerkki

Älylaitteiden Tietoturvamerkki

- Ensimmäinen valtiollinen tietoturvamerkki, perustettu 2019
- Tavoitteena riittävä tietoturvan perustaso kuluttajille
- Suojaaminen tavanomaisilta internet-uhilta
- Selkeä kuluttajaviestintä älylaitteiden kyberturvallisuudesta

Älylaitteiden Tietoturvamerkki

- 18 pakollista vaatimusta Eurooppalaisen ETSI-standardointijärjestön EN 303 645 -vaatimuksista.
- Vaatimusten valinnalla pyritään keskittymään kuluttajien tärkeimpiin kipukohtiin
  - Saavutetaan riittävä turvataso vaatimatta syvällistä IT-osaamista
  - Läpinäkyvyys tietoturvakontrollien toteuttamisessa ja tietosuojassa
- Korostaa valmistajan vastuuta tuotteen turvaamisessa sen elinkaaren ajan.

Kuluttajaa suojaavat vaatimukset

- Tukijakso
- Turvaohjeistus ja turvallisuuden tekeminen yksinkertaiseksi käyttäjälle (turvalliset oletusasetukset)
- Vahvat ja yksilölliset salasanat
- Ennakoiva haavoittuvuuksien hallinta ja ajantaisaiset turvapäivitykset
- Ymmärrettävät yksityisyyden suojan periaatteet
- Salattu tiedonsiirto ja turvalliset verkkorajapinnat

Tietoturvamerkin tarkastusten painopisteet

Riippumaton ja toistuva arviointi

- Sidosryhmäpalautte oli selkeää – itsearviointi ei riitä, riippumaton arviointi lisää luottamusta.
- Vuosittaisilla tarkasteluilla varmistetaan turvatason säilymistä ja uhka-arvion ajantasaisuutta.

Uhkamallinnus ja riskiarvio

- Kohteen kannalta olennaisten nykyisten ja lähitulevaisuudessa todennäköisten uhkien tunnistaminen.
- Vaatimusten ja testauksen kohdentaminen tärkeimpiin uhkiin.

Tuote ekosysteemissään

- Laitteen toiminnan kannalta olennaisten palveluiden, mobiilisovellusten ja muiden ekosysteemirajapintojen huomiointi arvioinnissa.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Havaintoja

Havaintoja tuotteiden kypsyydestä

- Tuotteet jakautuvat turvamielessä kahteen ryhmään. Osa tuotteista täyttää vaatimukset helposti, toisilla on taas suuria ongelmia.
  - Tuotteiden hylkäysprosentti on 40 tätä edeltävästä itsearvioinnista huolimatta.
  - Osasta tuotteista löytyy selkeitä puutteita jo ennen tarkastusta.
- Valmistajien käsitys tuotteidensa turvallisuudesta voi helposti olla ylioptimistinen.

Havaintoja tuotteiden kypsyydestä

- Monet valmistajat eivät tule pitämään tietoturvallisuutta riittävässä arvossa, jos turvattomuus ei johda selkeisiin seuraamuksiin.
- Havaintojen korjaaminen tarkastuksen aikana vie aikaa.
  - Turvallisuusasioiden huomioiminen aikaisin tuotekehitysvaiheessa auttaisi valmistajia kypsyyden luomisessa.

Havaintoja tuotteiden kypsyydestä

- Hyväksynnän hakijalla ei aina ole ymmärrystä siitä, kuinka tuote toimii, tai hyvää keskusteluyhteyttä tuotekehittäjiin
  - Tuotteen ongelmat ja turvallisuuden kannalta ongelmalliset toiminnot voivat tulla yllätyksinä
  - Tämä voi osaltaan johtua ulkoistuksista tai yleisemmin pitkistä tuotantoketjuista.
- Tuotekehityksessä kerääntyy helposti teknistä velkaa, joka on ongelma myös turvallisuusmielessä.

Avoin lähdekoodi

- Avoimen lähdekoodin kirjastot ja muut komponentit ovat usein hyvä valinta sekä turvallisuuden että toiminnallisuuden osalta.
- Kirjastojen valinnassa pitää kuitenkin olla tarkkana.
- Valmistajien referenssitoteutusten käyttö on harvoin hyvä valinta.

Haavoittuvuuksien hallinnasta

- Eri tietoturvamerkkien pitäisi kannustaa valmistajia turvapäivityksiin. Joissain vanhoissa sertifiointimalleissa näin ei ole ollut.
- Haavoittuvuuksien hallinta ja valmistajien omaehtoinen turvallisuuden kehitys on vastuullista toimintaa jo nyt, ja jatkossa siihen tullee erilaista pakottavaa sääntelyä.
- SBOM (Software Bill of Materials) olisi hyvä työkalu kolmansien osapuolten komponenttien haavoittuvuuksien hallintaan. SBOM-listan luominen tuotteen valmistuksen jälkeen on työlästä, joten se kannattaisi ottaa osaksi tuotekehitystä alusta asti.

Yleisimmät merkin saantia estäneet viat

- Vanhat ja haavoittuvat ohjelmistoversiot
- Turvattomat päivitykset
- Pääsy kehitystoiminnallisuuksiin
- Referenssitoteutusten käyttö sellaisenaan
- Laaja hyökkäysrajapinta, paljon avoimia portteja ja tarpeettomia palveluita
- Dokumentoimattomat, usein kovakoodatut tunnukset
- Dokumentoimattomat hallintarajapinnat
- Turvaton syötteen käsittely
- Perusongelmat www-rajapinnoissa
- Turvattomat radiorajapinnat
- Turvaton WiFi-verkkoon liittyminen
- Rittämätön kypsyys - tuote näyttää varhaisen vaiheen prototyypiltä

Lopuksi

- Tietoturvamerkki tähtää koko tuotteen elinkaareen kattavaan perusturvatasoon, joka ei vaadi käyttäjiltä ylimääräistä vaivaa.
- Tarkastuksissa on havaittu, että tuotteiden kypsyystasot vaihtelevat suuresti. Valmistajien käsitykset tuotteistaan ovat usein puutteellisia. Jopa 40% tuotteista hylätään, vaikka valmistajat ovat arvioineet niiden turvallisuuden riittäväksi.
- Tuotteiden turvahaasteet kärjistyvät tuotantoketjun monimutkaistuessa ja tuotteen integraatioiden monimutkaistuessa komponenttien ja ekosysteemin kesken.
- Radiolaitesääntelyn lisäksi tuleva Cyber Resilience Act (CRA) tulee tuomaan tietoturvavaatimuksia kaikille tuotteille, joissa on digitaalisia osia. Tietoturvamerkki on hyvä tapa valmistautua tähän sääntelyyn.