ETSI EN 303 645:
Beveiliging IoT consumenten-electronica

Kiwa Fire Safety & Security
Wilmersdorf 50
7327AC Apeldoorn
Nederland

www.kiwa.com

ETSI EN 303 645: Beveiliging IoT consumentenelectronica

Koelkasten, verlichting, tv's, rookmelders, speelgoed, fitness trackers… steeds meer gebruiksvoorwerpen die we dagelijks gebruiken zijn verbonden met het internet. Die 'slimme' apparaten maken ons leven leuker en vaak ook gemakkelijker, maar brengen ook veiligheidsrisico's met zich mee. De standaard ETSI EN 303 645 bevat richtlijnen voor de beveiliging van consumentenelektronica die deel uitmaakt van het Internet of Things (IoT).

In vrijwel elk huishouden zijn tegenwoordig meerdere smart devices te vinden. Vaak verzamelen, bewaren en verzenden deze apparaten gegevens van de gebruiker. Nog té vaak zijn deze apparaten standaard niet of onvoldoende beveiligd tegen hacks, datalekken, etc. Het Europees Telecommunicatie en Standaardisatie Instituut (ETSI) heeft daarom de standaard ETSI EN 303 645 ontwikkeld. Kiwa test en toetst op basis van deze standaard of IoT-producten voldoende veilig zijn voor eindgebruikers.

Essentiële beveiligingseisen

In de ETSI EN 303 645 hebben de deelnemers van het ETSI (fabrikanten, leveranciers van netwerkdiensten, overheden, telecomtoezichthouders en eindgebruikers) doelmatige, essentiële beveiligingseisen en best practices vastgelegd rondom cyberveiligheid en privacybescherming van consumentenelektronica met een internetverbinding.

Cyberveiligheid IoT consumentenproducten

De ETSI EN 303 645 bevat eisen en procedures voor de cyberveiligheid van IoT-consumentenproducten. Het gaat daarbij niet alleen om smart devices zelf, maar ook om sensoren en bedieningsonderdelen van deze apparaten. Vaak kunnen connected devices ook bediend worden met een smartphone-app. De veiligheid daarvan wordt niet door de ETSI EN 303 645 afgedekt, maar als optionele service kan Kiwa aan de hand van het RARS-schema de veiligheid hiervan beoordelen.

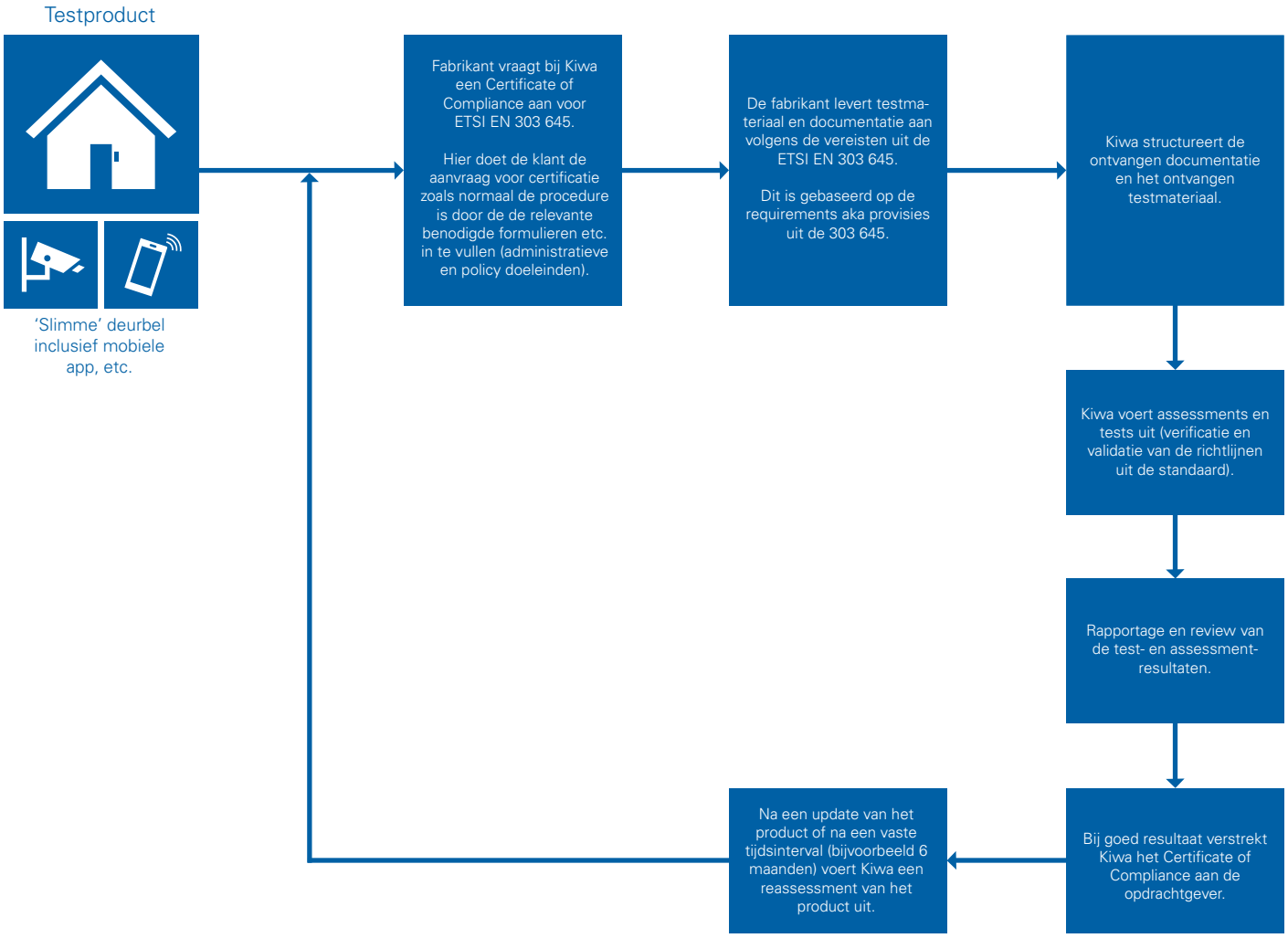
Voor fabrikanten van IoT consumentenelektronica

Certificering door Kiwa volgens de ETSI EN 303 645 is van toegevoegde waarde voor ontwikkelaars en fabrikanten van consumentenelektronica die verbonden kan worden met het web. Voorbeelden zijn onder meer babyfoons, slimme deurbellen, camera's, tv's en speakers, wearable health trackers en connected huishoudelijke apparatuur als wasmachines en koelkasten. Productontwikkeling volgens de ETSI EN 303 645 draagt bij aan betere veiligheid, updatebaarheid, transparantie , structuur, etc.

ETSI EN 303 645:
Beveiliging IoT consumentenelectronica

Certificeringstraject

Waaraan moet consumentenelektronica die gebruik maakt van internetfunctionaliteit voldoen om het ETSI EN 303 645-certificaat te krijgen? Als voorbeeld nemen we een 'slimme' deurbel. Deze deurbel met camera legt vast wie er aanbelt en stuurt dan een pushbericht naar de bewoner die vervolgens, via een app, kan communiceren met de bezoeker. Een mooi staaltje techniek, met ook de nodige veiligheidsaspecten. Hieronder een schematisch overzicht van het certificeringstraject van dit product.



Waar letten we op?

De IoT Security experts van Kiwa voeren aan de hand van de ETSI EN 303 645 testen uit en evalueren of een IoT- of smart toepassing voldoet aan de eisen die ervoor moeten zorgen dat het product door alle betrokkenen veilig gebruikt kan worden. Het product wordt hierbij onderworpen aan de eisen van de ETSI EN 303 645. Aspecten die hierbij worden gecheckt en beoordeeld zijn onder meer:

- Toepassing van de norm: Niet aan alle eisen uit de norm hoeft te worden voldaan, maar dan moet wél gerapporteerd en gemotiveerd zijn waarom dit het geval is.
- Kwaliteit wachtwoorden: Wachtwoorden als 1234, admin, 0000 etc. voldoen logischerwijs niet aan de veiligheidseisen.
- Mogelijkheden voor het melden van kwetsbaarheden: Fabrikanten moeten ervoor zorgen dat onder meer beveiligingsonderzoekers kwetsbaarheden op transparante wijze kunnen melden en deze vervolgens oplossen.
- Updatebeleid: Het tijdig ontwikkelen en implementeren van beveiligingsupdates is een

ETSI EN 303 645:
Beveiliging IoT consumentenelectronica

van de belangrijkste acties die een bedrijf kan ondernemen om klanten en het bredere technische ecosysteem te beschermen.

- Opslag gevoelige beveiligingsinfo: Security parameters (bijvoorbeeld wachtwoorden, access levels, fail safe-mechanismes en IP-adressen) zijn belangrijk voor het waarborgen van de algemene security van een product. Deze parameters moeten goed en secuur opgeslagen worden.
- Vermijd blootliggende 'attack surfaces'. Door een combinatie van techniek, processen en interacties kunnen in software (bewust of onbewust) 'openingen' ontstaan die door kwaadwillenden misbruikt kunnen worden. Dit kan worden voorkomen door deze af te schermen.
- Integriteit software: Toon aan dat de software die voor het product gebruikt wordt kwalitatief goed en veilig is en ook daadwerkelijk voor het betreffende product bedoeld is.
- Beveiliging persoonsgegevens: Van de fabrikant wordt verwacht dat hij ervoor zorgt dat persoonsgegevens worden verwerkt in overeenstemming met relevante wet- en regelgeving als de AVG.
- Robuustheid systeem: Kan het systeem uitval en verstoringen zodanig opvangen dat de functionaliteit niet word gehinderd?
- Onderzoek telemetriegegevens: Telemetriegegevens van IoT-apparaten en -diensten van consumenten kunnen worden onderzocht om beveiligingsafwijkingen op te sporen.
- Mogelijkheid verwijderen privé-informatie: Met het oog op de privacy moet het voor de eindgebruiker van een product mogelijk zijn om persoonlijke informatie te verwijderen.
- Installatie- en onderhoudsvoorschriften: Fouten tijdens installatie en onderhoud kunnen zorgen voor kwetsbaarheden(bewust of onbewust). Procedures hiervoor moeten dus helder en eenvoudig zijn voor de eindgebruiker.
- Valideer input data: Zorg ervoor hoofd- en subprocessen input met elkaar uitwisselen die integer, waar en juist is.

ETSI EN 303 645-certificaat

Het certificatietraject levert een testrapport op. Als het product aan de standaard voldoet, ontvangt de fabrikant een ETSI EN 303 645-certificaat. Hiermee kan hij aantonen dat het product voldoet aan de basiseisen op het gebied van IoT-veiligheid. Hiermee creëert een fabrikant niet alleen vertrouwen bij de (potentiële) gebruikers van zijn product, maar kan hij zich ook onderscheiden ten opzichte van andere fabrikanten.