ETSI EN 303 645:
Cybersecurity voor IoT elektronische consumentenproducten

Kiwa Nederland
Wilmersdorf 50
7327 AC Apeldoorn
The Netherlands

www.kiwa.nl

ETSI EN 303 645: Cybersecurity voor IoT elektronische consumentenproducten

Koelkasten, verlichting, tv's, rookmelders, speelgoed, fitnesstrackers… Een groeiend aantal alledaagse elektronische consumentenproducten is verbonden met het internet. Deze 'slimme' apparaten maken ons leven aangenamer en vaak gemakkelijker, maar brengen ook veiligheidsrisico's met zich mee. De norm ETSI EN 303 645 bevat richtlijnen voor de veiligheid van consumentenelektronica die deel uitmaakt van het Internet of Things (IoT).

Slimme apparaten zijn tegenwoordig in bijna elk huishouden te vinden. Deze apparaten verzamelen, bewaren en verzenden meestal data van de gebruiker. Te vaak zijn deze apparaten standaard niet of onvoldoende beveiligd tegen hacks, datalekken, etc. Daarom heeft het Europees Telecommunicatie en Standaardisatie Instituut (ETSI) de standaard ETSI EN 303 645 ontwikkeld. Op basis van deze standaard test en beoordeelt Kiwa of IoT- en consumentenelektronica voldoende veilig zijn voor gebruikers.

Essentiële beveiligingsvereisten

In de standaard ETSI EN 303 645 hebben ETSI-deelnemers (fabrikanten, netwerkserviceproviders, overheden, telecomregelgevers en eindgebruikers) de meest effectieve, essentiële beveiligingseisen en best practices vastgesteld met betrekking tot cyberveiligheid en privacybescherming van consumentenelektronica die wordt verbonden met internet.

Cybersecurity IoT-consumentenproducten

ETSI EN 303 645 bevat cybersecurityvereisten en -procedures voor IoT-consumentenproducten. Dit betreft niet alleen slimme apparaten zelf, maar ook sensoren en bedieningsonderdelen van deze apparaten. Verbonden apparaten zijn vaak ook te bedienen met een smartphoneapp. De veiligheid hiervan valt niet onder ETSI EN 303 645, maar kan als optionele service door Kiwa worden beoordeeld op basis van het RARS K21048-certificatieschema.

Fabrikanten van IoT-consumentenelektronica

Certificering door Kiwa volgens ETSI EN 303 645 is van toegevoegde waarde voor ontwikkelaars en fabrikanten van consumentenelektronica die verbonden wordt met internet. Voorbeelden zijn babyfoons, slimme deurbellen, camera's, tv's, luidsprekers, draagbare gezondheidstrackers en huishoudelijke apparaten als wasmachines en koelkasten. In principe kan elk device dat een bepaalde mate van dataverkeer heeft getest worden volgens ETSI EN 303 645. Productontwikkeling volgens ETSI EN 303 645 draagt bij aan een betere veiligheid, updatemogelijkheden, transparantie, structuur, enz.

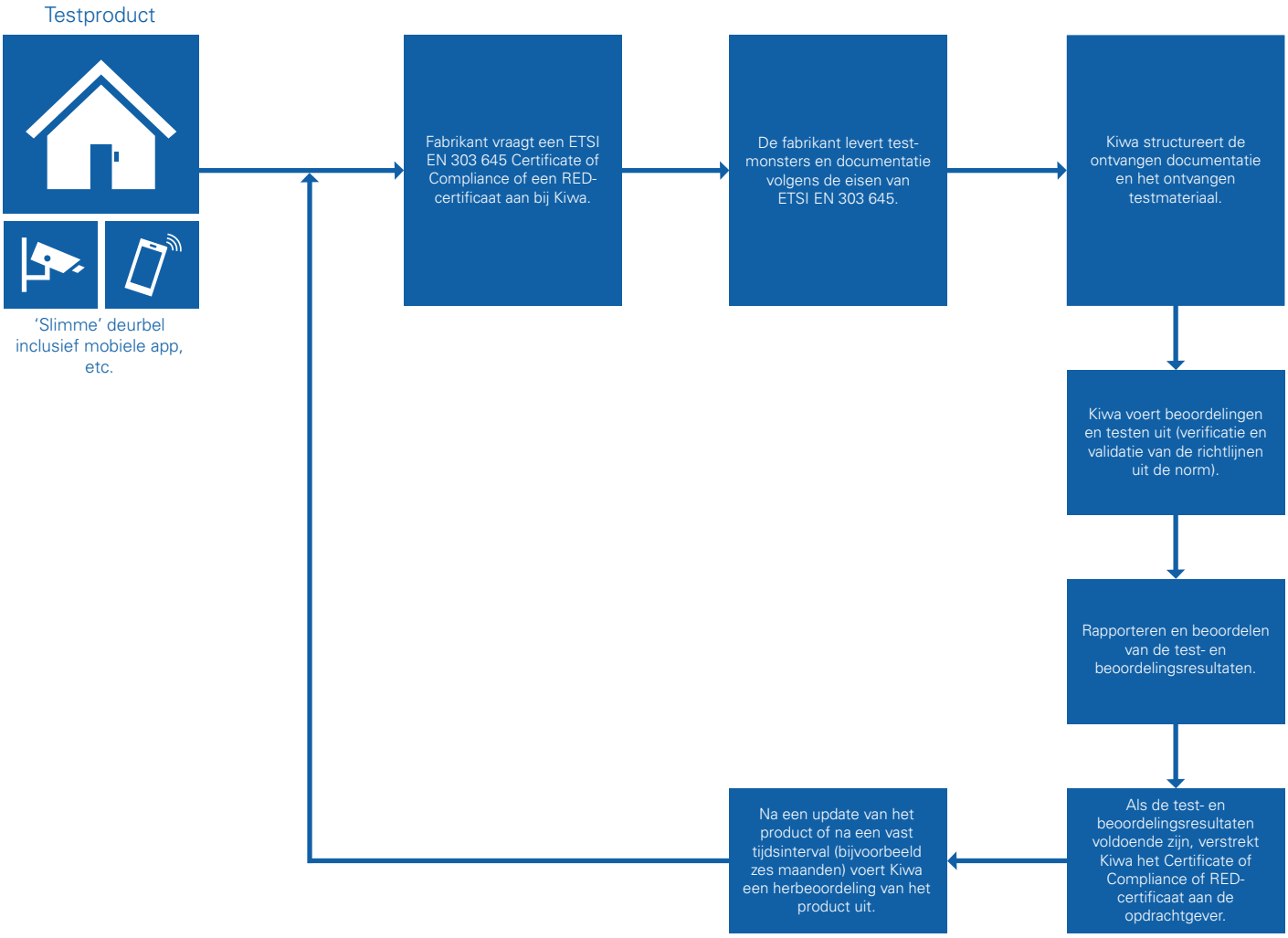
Radio Equipment Directive (RED) Compliance

Naleving van de ETSI 303 645 zorgt ervoor dat uw product voldoet aan artikel 3.3 d, e, f en i van de RED. Dit betekent dat op uw RED-certificaat ook compliance met de ETSI EN 303 645 wordt vermeld. Door aan uw belanghebbenden te communiceren dat uw RED-conformiteit ook cybersecurity voor consumentenelektronica omvat, zal uw product opvallen in een wereld waar cyberdreigingen hoogtij vieren!

ETSI EN 303 645: Cybersecurity voor IoT elektronische consumentenproducten

Certificatieproces

Aan welke eisen moet consumentenelektronica die internetfunctionaliteit gebruikt voldoen in het kader van ETSI EN 303 645? Als voorbeeld nemen we een ‘slimme’ deurbel. Deze deurbel met camera registreert wie er aanbelt en stuurt vervolgens een pushbericht naar de bewoner die vervolgens via een app kan communiceren met de bezoeker. Een mooi stukje techniek, met interessante beveiligingsaspecten. Hieronder vindt u een schematisch overzicht van het certificeringsproces voor dit product.



Welke aspecten van IoT-producten beoordelen we?

De IoT-beveiligingsexperts van Kiwa voeren tests uit op basis van de standaard ETSI EN 303 645 en beoordelen of een IoT- of ‘slimme’ applicatie voldoet aan de eisen die ervoor zorgen dat het product veilig kan worden gebruikt. Het product is hierbij onderworpen aan de eisen uit de ETSI EN 303 645. Aspecten die worden gecontroleerd en beoordeeld zijn onder meer:

- Toepassing van de standaard: Niet aan alle eisen van de standaard moet worden voldaan, maar als dat het geval is, moet dit worden gerapporteerd en gemotiveerd;
- Kwaliteit van wachtwoorden: Standaard wachtwoorden zoals 1234, admin, 0000 etc. voldoen niet aan de veiligheidseisen. Het wordt daarom aanbevolen een manier te hebben om veiligere wachtwoorden te garanderen;
- Kwetsbaarheidsrapportage: Fabrikanten moeten ervoor zorgen dat onder meer beveiligingsonderzoekers kwetsbaarheden transparant kunnen rapporteren en vervolgens op basis van de feedback de betreffende problemen kunnen oplossen;

ETSI EN 303 645: Cybersecurity voor IoT elektronische consumentenproducten

- Updatebeleid: Het tijdig ontwikkelen en implementeren van beveiligingsupdates is een van de belangrijkste maatregelen die een bedrijf kan nemen om klanten en het bredere technische ecosysteem te beschermen;
- Opslaggevoelige beveiligingsinformatie: Beveiligingsparameters (bijvoorbeeld wachtwoorden, toegangsniveaus, fail-safe mechanismen en IP-adressen) zijn belangrijk om de algemene veiligheid van een product te garanderen. Deze parameters moeten correct en veilig worden opgeslagen;
- Vermijd blootgestelde aanvalsoppervlakken: Een combinatie van technologie, processen en interacties kan 'openingen' creëren (bewust of onbewust) in software die misbruikt kunnen worden door kwaadwillenden. Dit wordt ook wel aanvalsoppervlak genoemd. Door aanvalsoppervlakken te verkleinen, waardoor kwetsbaarheden in verschillende dimensies worden verminderd, kunnen aanvallen en lekken worden voorkomen;
- Integriteit van software: Toon aan dat de software die voor het product wordt gebruikt van goede kwaliteit en veilig is en ook daadwerkelijk bedoeld is voor het product in kwestie. Dit zorgt ervoor dat software die wordt uitgevoerd door apparaten (en het omliggende ecosysteem) niet wordt beschadigd;
- Bescherming van persoonlijke gegevens: Van de fabrikant wordt verwacht dat hij ervoor zorgt dat persoonlijke gegevens worden verwerkt in overeenstemming met relevante wet- en regelgeving zoals de AVG;
- Robuustheid van het systeem: Kan het systeem storingen en storingen zo opvangen dat functionaliteit niet wordt belemmerd?
- Onderzoek telemetriegegevens: Telemetrie-gegevens van IoT-apparaten en -diensten van consumenten kunnen worden onderzocht om beveiligingsafwijkingen op te sporen;
- Mogelijkheid om persoonlijke informatie te verwijderen: Om privacyredenen moet het voor de eindgebruiker van een product mogelijk zijn om persoonlijke informatie te verwijderen;
- Installatie- en onderhoudsinstructies: Fouten tijdens installatie en onderhoud kunnen (bewust of onbewust) kwetsbaarheden veroorzaken. Procedures hiervoor moeten daarom duidelijk en eenvoudig zijn voor de eindgebruiker;
- Valideer invoergegevens: Zorg ervoor dat hoofd- en subprocessen invoer met elkaar uitwisselen die eerlijk, waar en correct is.

ETSI EN 303 645-conformiteit

Het certificeringsproces resulteert in een testrapport. Als het product voldoet aan de eisen van de norm, ontvangt de fabrikant een certificaat van overeenstemming. Als de fabrikant een RED-certificaat heeft aangevraagd, wordt onformiteit met de ETSI EN 303 645 vermeld op het RED-certificaat. Hiermee kan de fabrikant aantonen dat het product voldoet aan basiseisen op het gebied van IoT en cybersecurity die steeds belangrijker worden. Zo wekt een fabrikant niet alleen vertrouwen bij de (potentiële) gebruikers van zijn product, maar kan hij zich ook onderscheiden van andere fabrikanten.

Relevante services

We kunnen u ook helpen met de volgende diensten:

- K21048 RARS: Voor cybersecurity van systemen die externe toegang gebruiken met bijvoorbeeld mobiele applicaties;
- FCC/ISAD Market Access: testen en certificeren van uw producten voor markttoegang tot Noord-Amerika;
- IEC 62443: Cyberbeveiliging voor industriële systemen