Stiftung Neue Verantwortung

Workshop Paper

Market Surveillance and IT-Security – What are new roles, responsibilities and information flows based on NLF?

Wednesday, May 29th 2018, Stiftung Neue Verantwortung

The currently discussed EU Cybersecurity Act has the potential to create, for the first time, comparable and meaningful IT security certification in Europe and might even establish baseline security requirements for the European market. Recent drafts and committee reports reference the New Legislative Framework (NLF) and the possibility for manufacturers to comply with certification schemes through self-assessment – just like with today's CE marking. While self-assessment allows for quicker market adoption and avoids the potential financial burdens of 3rd party assessments, it heavily relies on responsive and effective market surveillance to identify bad actors and non-compliant products.

There are several open questions that will surely be debated during the Trilogue: Who decides which product categories fall under which assurance level (basic, substantial, high)? Who should be allowed to propose candidate certification schemes? How can involvement of all stakeholders during certification scheme development be ensured? Chances are high that the Cybersecurity Act will be approved by the end of 2018 and hopefully these questions will be resolved.

Understandably, attention currently focuses on the schemes and the supporting processes. Yet we also need to think about the future – when the Cybersecurity Act is done and the actual work begins. The idea of this workshop is to **brainstorm roles, responsibilities and information flows** between different stakeholders in a future IT security certification "ecosystem".

(Really short) intro to the European CE mark:

Certain products need a CE mark in order to be sold in the European Union. With a CE mark on the product the manufacturer states that he complies with all the relevant EU requirements such as safety, environmental aspects and health risks: "*The [CE] mark is not a confirmation of high-quality or excellent safety (top of the market), it says that the use of the product is not unacceptable dangerous (bottom line for the market). In this way, the CE mark confirms that basic EU legal requirements are met. In this way, compromising safety cannot be a competitive advantage, creating a 'level playing field' for fair competition.*" (Gerald Zwetsloot, 2011) For most product categories a Self-Declaration of Conformity (SDoC) by the manufacturer is enough. Some product categories require an independent 3rd party assessment by a Conformity Assessment Body. Market surveillance by public agencies tries to identify (a) products that have no CE mark or (b) products that have a CE mark but do not comply with statutory European requirements.

Stiftung Neue Verantwortung

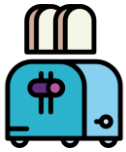
Relevant actors and key questions in the CE system:

Consumers

- Consumers have no role in the current CE framework – how can they be incorporated?
- What would be a good/scalable approach to inform consumers about the security / safety of a device before purchase? (RAPEX is not a solution)

Security Researchers

- Independent security researchers continuously find vulnerabilities in consumer IoT devices and rely on mail/twitter to inform companies. To whom should they talk if they cannot reach the original manufacturer?



IoT Device

- What should a consumer know about the device before purchasing it, regarding IT security?

Device Manufacturer

- What happens if the manufacturer bought the device from an OEM?

Distributor

- If the manufacturer is not reachable, should the distributor be held accountable for selling an insecure device?
- What would be meaningful responsibilities of the distributor regarding the security of an IoT device?

Conformity Assessment Body

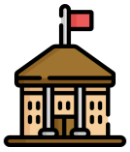
- How could Conformity Assessment be modernized so that it's easier for security researchers / students / 3rd parties to formally assess the security of IoT devices?
- How could re-certification be incentivized?

Market Surveillance Authority

- Could / Should the MSA play a more central role for consumers to receive information about the security of a device and for security researchers to disclose security vulnerabilities?

National Accreditation Body

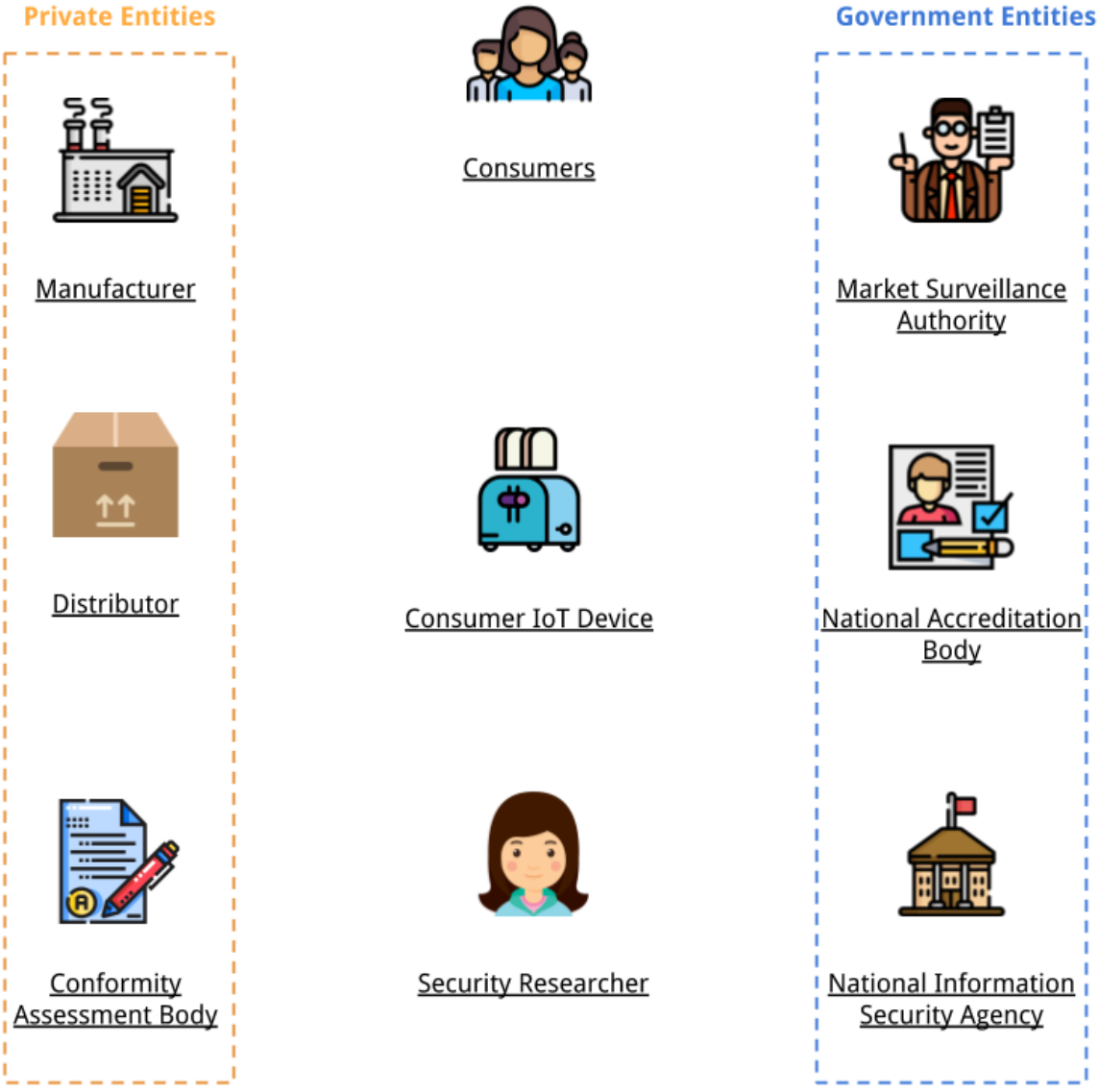
- Should there be an "Accreditation Fast-Track" for low-risk devices (ie Bluetooth Toothbrush)?



National Information Security Agency

- Should the Nat. Info. Sec. Agency perform tests of IoT devices sold on the EU market to support market surveillance?

Some of the relevant actors in the NLF/CE system



Would a database help?

The new EU Framework for Energy Labelling (EU Regulation 2017/1369) introduces the idea of a central database to collect key information about devices:

"(29) In order to set up a useful tool for consumers, to allow for alternative ways for dealers to receive product information sheets, to facilitate the monitoring of compliance and to provide up-to-date market data for the regulatory process on revisions of product-specific labels and information sheets, ***the Commission should set up and maintain a product database consisting of a public and a compliance part****, which should be accessible via an online portal.*

(30) Without prejudice to the Member States' market surveillance obligations and to suppliers' obligations to check product conformity, suppliers should make the required product compliance information available electronically in the product database. The information relevant for consumers and dealers should be made publicly available in the public part of the product database. That information should be ***made available as open data*** *so as to give mobile application developers and other comparison tools the opportunity to use it.* ***Easy direct access to the public part of the product database should be facilitated by user-oriented tools, such as a dynamic quick response code (QR code), included on the printed label.****"*

Applying this idea to the CE system and IT security, a database could store information about…

- list of all firmware updates for a device
- date of last conformity assessment / 3rd party certification
- unresolved security vulnerabilities
- average response time of the manufacturer to fix a security vulnerability
- End of Support / End of Life dates