CYBERSECURITY FOR CONSUMER IOT

RUSNĖ JUOZAPAITIENĖ
ANEC representative in ETSI TC Cyber

The value of ANEC

- Established in 1995

- Aims to represent and defend the European consumer interest in a **continuum** of consumer protection and welfare

  - ✓ the development and revision of European policies & laws related to standards, consumer protection & welfare

  - ✓ (key mission) of standardisation (governance & technical levels of CEN, CENELEC & ETSI; sometimes technical level in ISO & IEC)

  - ✓ the use of standards (conformity assessment, accreditation, market surveillance & enforcement)

- In 2018, ANEC participates in over **175 technical bodies** of CEN, CENELEC & ETSI, and in over **25 technical bodies** of ISO & IEC

The use of standards can:

- raise consumer protection and reduce the risk of accidents
- help to promote environmental protection and sustainability
- make the quality of services more consistent
- ensure that people of all ages and abilities have equal access to products and services
- serve to underpin the digital age and the information society

- ISO PC 317

  - ISO 31700 : Consumer protection: Privacy by Design for consumer goods and services

- ETSI TC CYBER
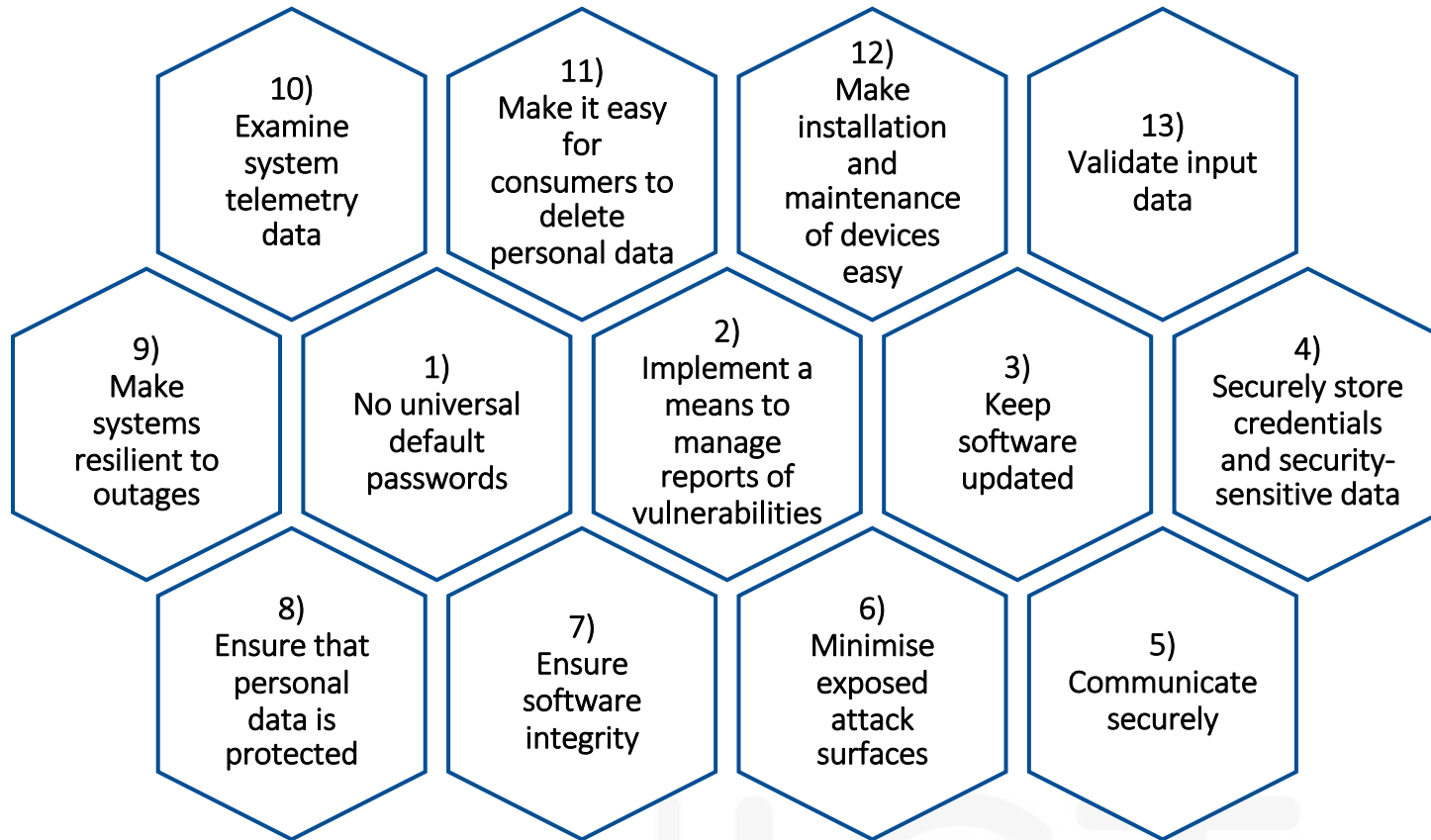
  - Cybersecurity for Consumer IoT

ETSI TC CYBER

- TC CYBER is ETSI's Centre of Excellence and focal point for Cybersecurity.
- TC CYBER works on a range problems –from Privacy, to IoT, to protecting personal data and Quantum Cryptography.
- Works on both industry security challenges and EU security mandates to address global Cybersecurity problems.

Consumer IoT

- Estimated 12.9 billion consumer IoT devices by 2020 (Gartner 2017)

- Poorly secured IoT devices threaten people's privacy, online security and safety.

- They can be misused for large-scale DDoS attacks.

Cybersecurity for Consumer IoT

- ETSI TC Cyber has published Technical Specification (TS) 103 645 Cybersecurity for Consumer Internet of things in February 2019

Content of TS 103 645

10) Examine system telemetry data

11) Make it easy for consumers to delete personal data

12) Make installation and maintenance of devices easy

13) Validate input data

9) Make systems resilient to outages

1) No universal default passwords

2) Implement a means to manage reports of vulnerabilities

3) Keep software updated

4) Securely store credentials and security-sensitive data

8) Ensure that personal data is protected

7) Ensure software integrity

6) Minimise exposed attack surfaces

5) Communicate securely

Supporting European Experts Presence in
International Standardisation Activities in ICT

Challenges

- DIN SPEC 27072 IoT capable devices

- ETSI TC CYBER and CEN-CENELEC JTC 13 joint meeting

- TS 103 345 being revised into a European Standard EN intended for potential use with Cybersecurity Act (CSA).

- Further TC Cyber recommendations through applying Critical Security Controls to IoT.

-TR 103 305-3: Critical Security Controls Part 3.

An increasing number of schemes provide assurance against TS 103 645, for example:

- BSI Kitemark certification for Internet of Things connected devices

- DTG a 'Secure by Design' cyber security conformance scheme [for smart TVs]

- IoT Security Compliance Framework"

- ETSI TC CYBER test / compliance specifications also under development (TS 103 701 Cybersecurity assessment for consumer IoT products)

- Work item adopted in September 2019

- Aiming for publication in summer 2020

Next steps

- Raise awareness and encourage industry uptake of TS 103 645

- Support NSO consultation on EN 303 645 to achieve swift publication of first version

- Develop TS 103 701 to support assurance and certification schemes