Cybersecurity in ‘products’

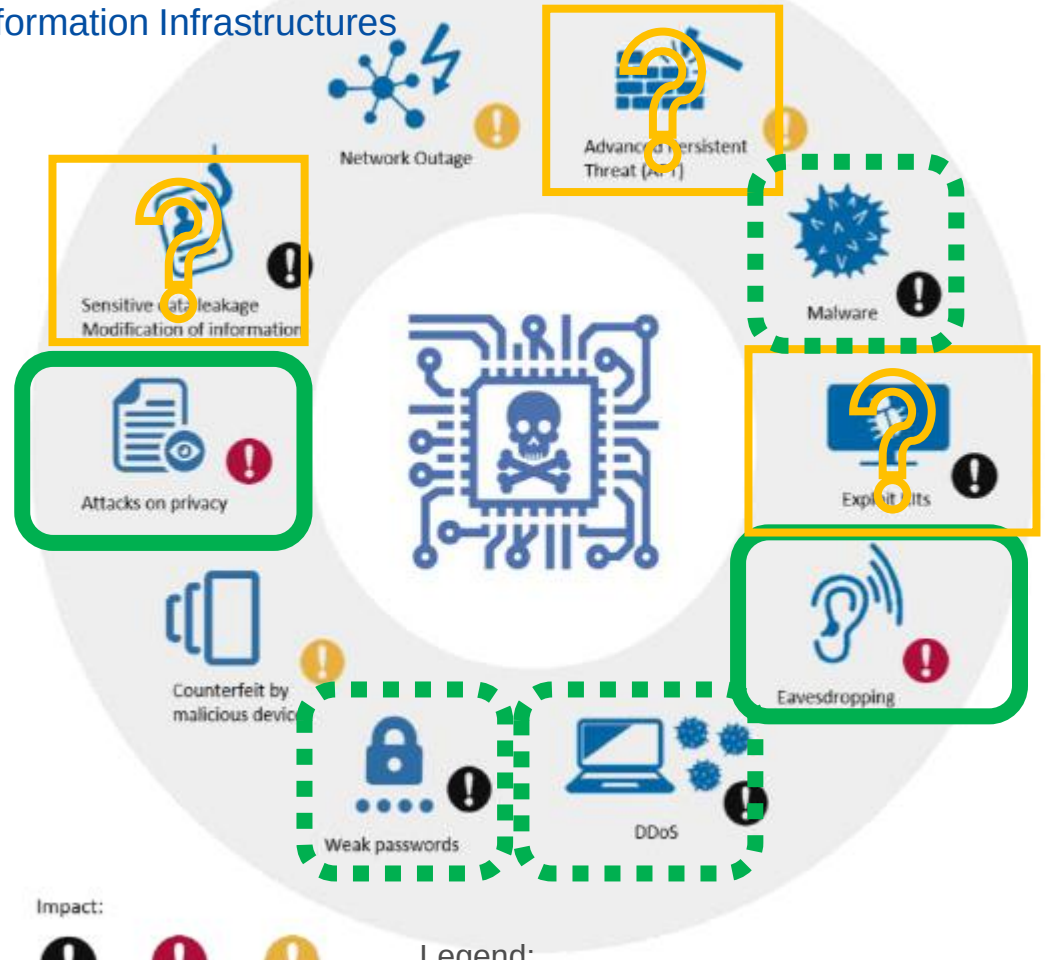
A horizontal approach to cybersecurity in digital products

Aristotelis TZAFALIAS - DG CNECT.H2 Cybersecurity and Digital Privacy Policy

Pier Francesco SAMMARTINO - DG GROW.C3 Engineering, Maritime and. Rail Industries

Cyber threats and the existing framework

Image source: ENISA - Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures



Expected full coverage

At least partial coverage
(e.g. on the radio equipment but not on the network)

To be fully assessed
(some technical solutions under Article 3(3) of the RED may help mitigating some risks but a case-by-case assessment is needed)

Legend:
Eavesdropping: the possibility of intercepting users' conversations/messages
DDoS: Distribute Denial of Service
Malware: malicious software

European Commission

Ensuring complementarity and complete coverage of cybersecurity in all connected products

RED **will cover**

"internet-connected radio equipment and wearable radio equipment" – with specific justified exceptions

Radio components (e.g. radio modules)

Protection of privacy, of the networks and against fraud

Compliance at the upload of software (subject to another delegated act whose study is ongoing)

RED **will not cover**

Wired-only connected products

Non-radio components (e.g. processors)

Certain cybersecurity risks to the availability, integrity, confidentiality of products processing non-personal data (which may yet be covered indirectly)

Duty of care, life cycle (e.g. patches)

Disclosure of vulnerabilities

Requirements for services/networks

Horizontal regulation* **will cover**

All residual connected products (wireless and wired products)

All residual components in the value chain

All residual cybersecurity risks to availability, integrity, confidentiality

Duty of care, life cycle (e.g. patches)

Disclosure of vulnerabilities

Timeline

- April 2020: Publication of the IA study on “internet-connected radio equipment and wearable radio equipment”
- August 2020: Launch of an exploratory “Study on the need of Cybersecurity requirements for ICT products”
- December 2020: Council Conclusions on the cybersecurity of connected devices (ST 13629/20)
- December 2020: “Cybersecurity Strategy” – announcement of the possibility for “new horizontal rules” and the adoption of the delegated acts under RED
- Q2 2021: Expected adoption of a delegated act on Article 3(3)(d/e/f) of the RED
- tbd/tbc: New legislative proposal

Ongoing work (RED)

- Coherency: this has been discussed and scrutinised by the COM services for more than 2 years
  - See documents EG RE (03)12 and EG RE (04)05.
- Preparedness and implementation:
  - Existing technical solutions in support of the Delegated act have been asked in Q4 2019 and have been communicated to the EG RE, see EG RE (04)13 and EG RE (04)19.
  - A mapping (working document) with the correspondence between technical solutions and the essential requirements has been presented to the EG RE in July 2020 EG RE (06)07. Further meetings and exchanges occurred. An update is being awaited. This document also reports possible gaps to facilitate future work.
- Draft delegated act and draft standardisation request to be shared at the same time

Horizontal approach – Guiding principles

- Coherence with the delegated acts being prepared under the Radio Equipment Directive
- Starting point: New legislative framework
  - Essential requirements
  - Selection of appropriate conformity assessment modules covering both design and production
  - Determine the role of notified bodies
  - Use of harmonised standards

Horizontal approach – Guiding principles: “NLF+”

- Address entire lifecycle (security updates, vulnerability handling and disclosure).
- Benefit from the European Cybersecurity Certification Framework

  Art 54 para 3 of Regulation (EU) 881/2019 (Cybersecurity Act): “*Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act*.”