Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them. – Project: 101190180.

Which Products Fall Under the CRA

Digital Innovation Hub Trakia

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

OSCRAT Open-Source Cyber Resilience Act Tools

Introduction

1

“Products with digital elements” = hardware + software + connectivity.

2

CRA applies to both consumer and industrial products.

3

Security becomes a *legal requirement* for all connected products.

Definition of “Products with Digital Elements”

1

IoT Devices

smart TVs, home assistants, industrial sensors, connected cars.

2

Software

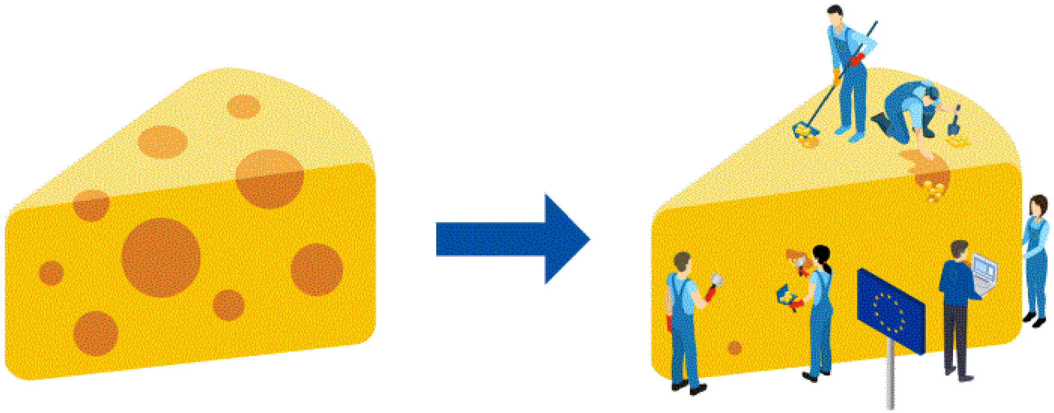
operating systems, antivirus, productivity tools, firmware, apps.

3

Embedded Hardware

routers, PLCs, smart meters, medical devices.

The EU’s Mission: Filling the Security Gaps in Digital Products



CRA Product Classification

- **Important products** (Annex III): general connected devices, business and consumer software.
- **Critical products** (Annex IV): high-impact items such as security software, network management systems, industrial control equipment.
- **Class I and II** for critical products, depending on risk and functionality.

In scope: *“Products with Digital Elements”*

Hardware products *(including components placed on the market)* – laptops, smart appliances, mobile phones, network equipment, CPUs

Software products *(including components placed on the market)* – operating systems, word processing, games or mobile apps, software libraries *...including their remote data processing solutions!*

Outside the Scope

❌ **Non-commercial products**
(e.g. hobby or research devices not sold on the market)

❌ **Services, in particular standalone SaaS**
(websites, web-only tools — covered by NIS2 or DORA)

❌ **Outright exclusions**
(cars, medical devices, certified aeronautical and marine equipment)

💡 *CRA applies only to “products with digital elements” placed on the market.*

Real-World Examples

- A **smart thermostat** (IoT): needs security updates, vulnerability management, CE marking.
- A **mobile banking app** (software): must handle data securely and report vulnerabilities.
- A **connected medical device** (embedded hardware): must meet stricter requirements — likely a *critical product*.
- A **cloud-based network monitoring tool**: falls under both CRA and the EUCS (Cloud Services Scheme).

Key Takeaways

- CRA covers *any connected product* — IoT, software, embedded hardware.
- Two levels of control: *Important* and *Critical products*.
- Ensures *secure by design* principles.
- Builds consumer trust and supports the EU’s *Digital Single Market*.

Thank you!

Miroslav Mitev, PhD
+359 896 198 875
m.mitev@dihtrakia.org