EUs forslag til «Cyber Resilience Act» – Nye krav til eID systemer?

IDentitet 2023

Konferansen IDentitet 7. -8. juni 2023 i Oslo

Tobias Mahler

Senter for rettsinformatikk

ANNEX III

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

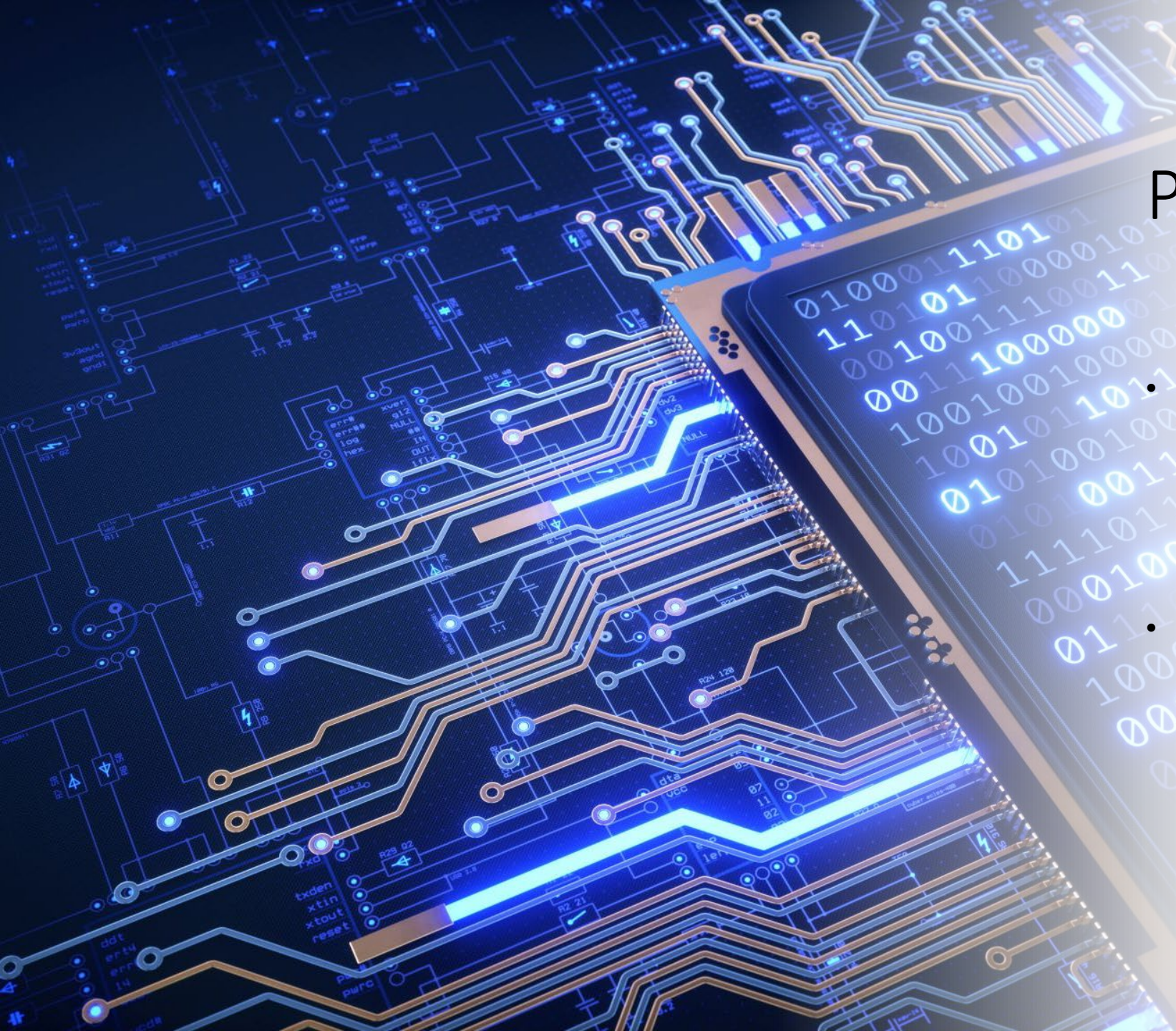
Class I

1. Identity management systems software and privileged access management software;
2. Standalone and embedded browsers;
3. Password managers;
4. Software that searches for, removes, or quarantines malicious software;
5. Products with digital elements with the function of virtual private network (VPN);
6. Network management systems;
7. Network configuration management tools;
8. Network traffic monitoring systems;
9. Management of network resources;
10. Security information and event management (SIEM) systems;
11. Update/patch management, including boot managers;
12. Application configuration management systems;
13. Remote access/sharing software;
14. Mobile device management software;
15. Physical network interfaces;

Cyber Resilience Act

introduces mandatory cybersecurity requirements

for hardware and software products, throughout their whole lifecycle



Products

- Ensure that products with digital elements placed on the EU market
  - have fewer vulnerabilities and that manufacturers remain responsible for cybersecurity throughout a product's life cycle;
- 'product with digital elements'
  - means any software or hardware product and its remote data processing solutions,
  - including software or hardware components to be placed on the market separately;

CRA fact sheet (EC)

Manufacturer's obligations

Cybersecurity is taken into account in **planning, design, development, production, delivery** and **maintenance** phase;

All **cybersecurity risks** are documented;

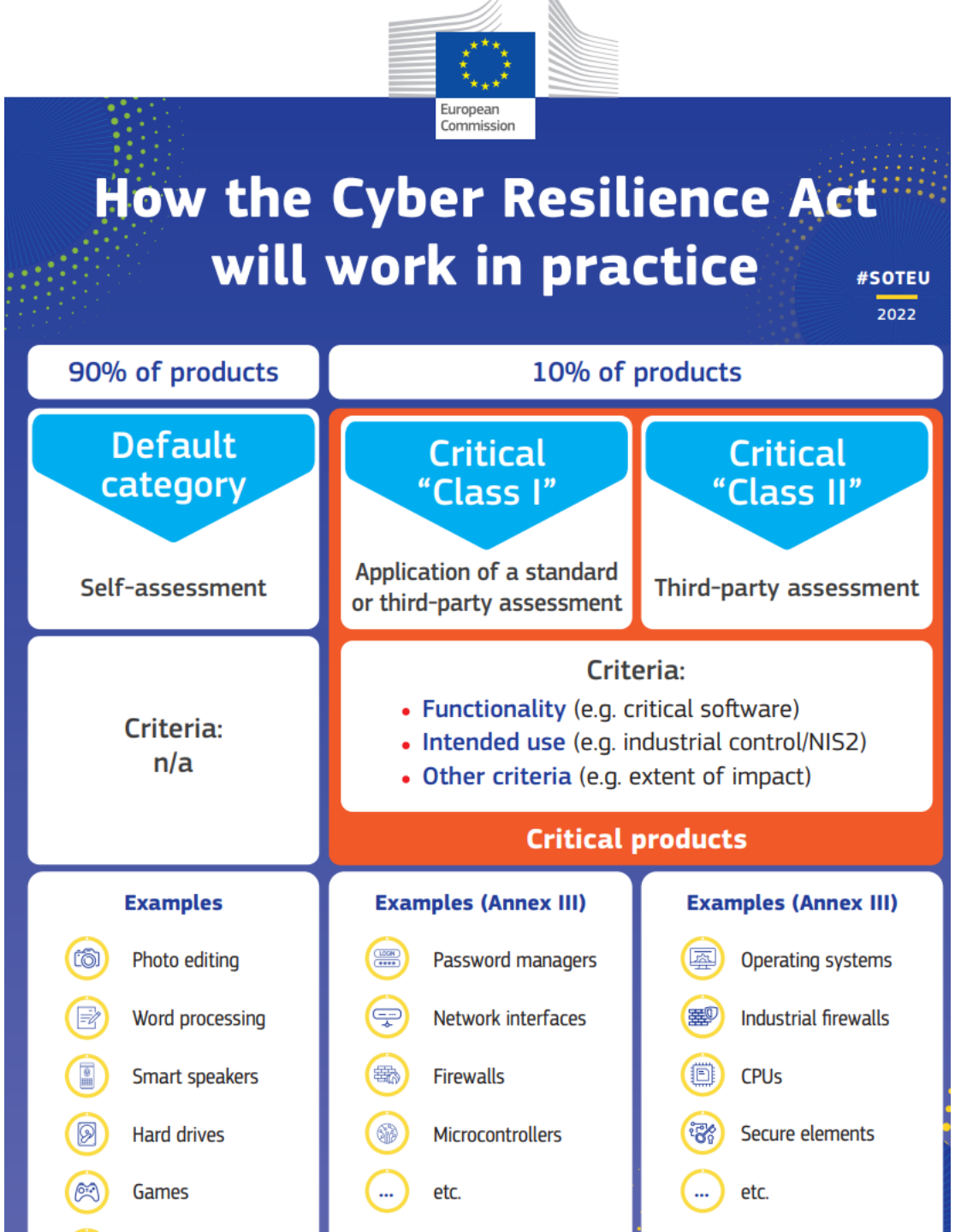
Manufacturers will have to **report actively exploited vulnerabilities and incidents**;

Once sold, manufacturers must ensure that for the **expected product lifetime** or for a period of five years (whichever is the shorter), **vulnerabilities are handled effectively**;

Clear and understandable instructions for the use of products with digital elements;

Security updates to be made **available for at least five years**.

Source: CRA fact sheet (EC)



Source: CRA fact sheet

ANNEX III

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

Class I

1. Identity management systems software and privileged access management software;
2. Standalone and embedded browsers;
3. Password managers;
4. Software that searches for, removes, or quarantines malicious software;
5. Products with digital elements with the function of virtual private network (VPN);
6. Network management systems;
7. Network configuration management tools;
8. Network traffic monitoring systems;
9. Management of network resources;
10. Security information and event management (SIEM) systems;
11. Update/patch management, including boot managers;
12. Application configuration management systems;
13. Remote access/sharing software;
14. Mobile device management software;
15. Physical network interfaces;

Spørsmål?

- Tobias.mahler@jus.uio.no