40 years
Delivering technology advantage. Since 1984.

Der Cyber Resilience Act als Katalysator für die Sicherheit von IoT-Ökosystemen

asut IoT-Konferenz, 11. April 2024

ergon

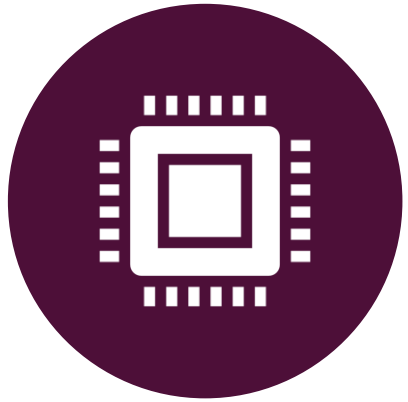
Gefährlich, kostspielig und häufig:
Cyberangriffe auf IoT-Ökosysteme

2015
Forscher hacken Geländewagen und übernehmen Lenkung und Bremsen

2016
Mirai Botnet legt 900’000 Router lahm

2020
Unautorisierter Zugriff auf Überwachungs-kameras in Spitälern, Gefängnissen, Fabriken, usw.

2021
Pipeline Hack: Gas pipeline shutdown wegen Ransomeware infizierter IoT Geräte



2023
Cryptojacking**:** Botnets aus IoT Geräten für Crypto-currency Mining

ergon

Gefährlich, kostspielig und häufig:
Cyberangriffe auf IoT-Ökosysteme

> 10 Millionen

DDoS Attacken 2021[1]

$ 300'000

Durchschnittskosten erfolgreicher Angriffe[2]

1) European Commission, Directorate-General for Communications Networks, Content and Technology, *Cyber resilience act – New EU cybersecurity rules ensure more secure hardware and software products*, European Comission, 16. Dec. 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_239
2) Irdeto Global Connected Industries Cybersecurity Survey https://resources.irdeto.com/media/new-2019-global-survey-iot-focused-cyberattacks-are-the-new-normal

ergon

Zunahme von Cyberangriffen auf IoT-Ökosysteme

IoT malware attacks **grew more than 400%** in the Zscaler cloud compared to the same period in 2022.

Zscaler IoT & OT Report 2023

Number of IoT devices (bots) engaged in botnet-driven DDoS attacks rose **from around 200’000** a year ago **to approx. 1 million** devices.

Nokia Threat Intelligence Report 2023

Cyber Resilience Act

Ziel

– Konsumenten und Unternehmen vor Cybersecurity Bedrohungen schützen

– Hohe volkswirtschaftliche Kosten verhindern

– CE gekennzeichnete Produkte erfüllen ein vernünftiges Mass an Cybersicherheit

Bussgelder von 15 Mio Euro oder 2,5% des Jahresumsatzes

ergon

Cyber Resilience Act

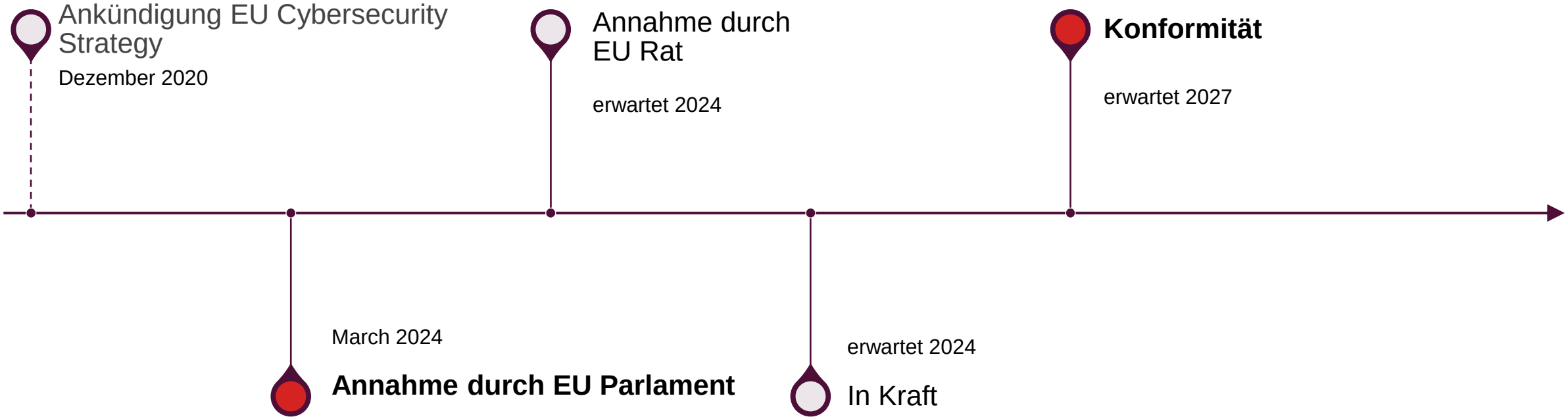
Produkte mit digitalen Elementen

Default Kategorie	Klasse I	Klasse II
– Smart Speakers – Bildbearbeitung – Games – etc.	– Browser – Router – Firewall – etc.	– Betriebssysteme – Industrielle Firewall – HSM – etc.
Selbstbeurteilung	**harmonisierter Standard** **Beurteilung durch Dritte**	**Beurteilung durch Dritte**

ergon

Cyber Resilience Act

Timeline



ergon

Cyber Resilience Act

Kerninhalte

Sicherheitsanforderungen an Produkte mit digitalen Elementen (PDE)

Anforderungen an den Product Lifecycle

Schwachstellen-Management

ergon

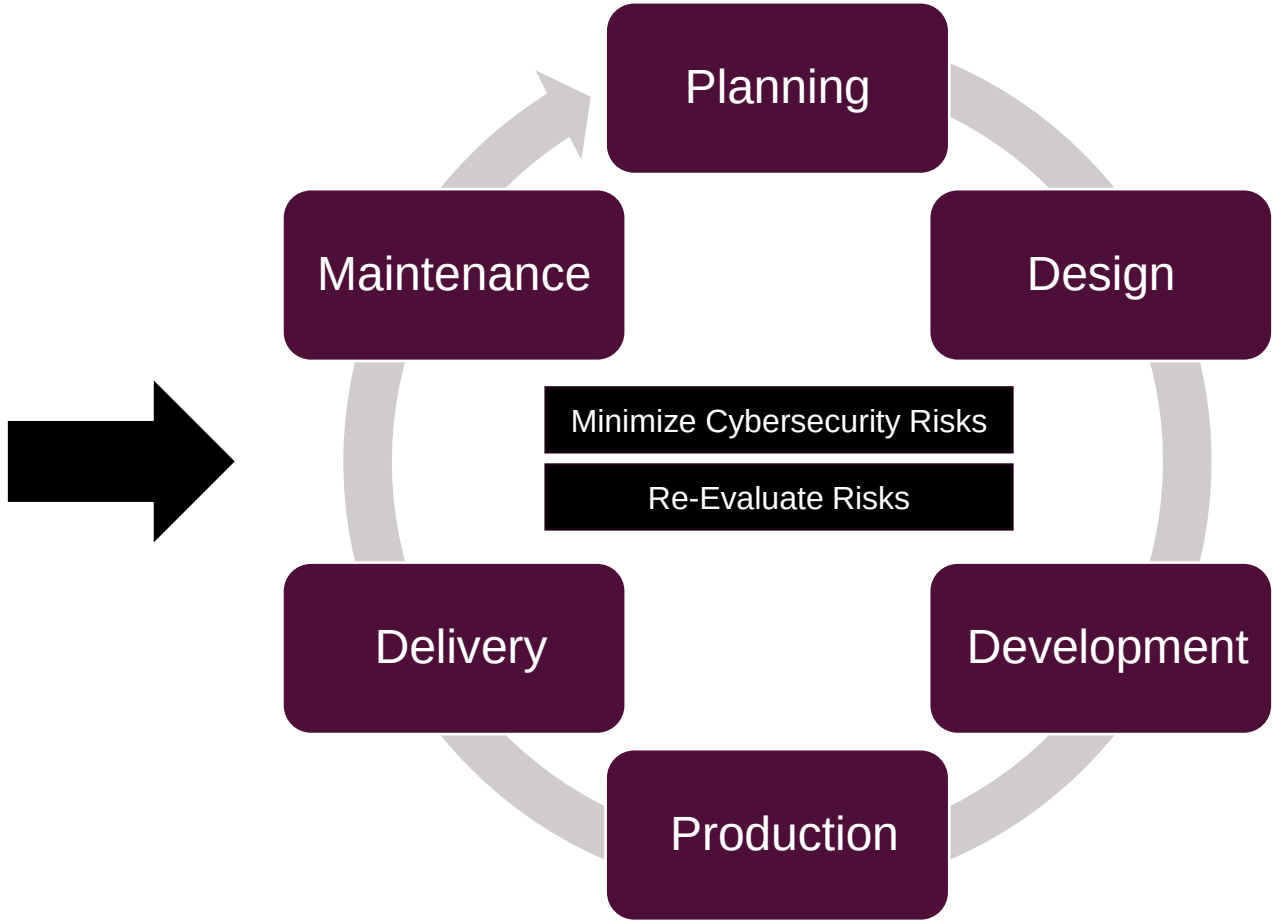
Sicherheitsanforderungen an Produkte mit Digitalen Elementen (PDE)

Kontrollmechanismen zum Schutz vor unbefugtem Zugriff	Sicherheitsupdates	Vertraulichkeit / Integrität gespeicherter Daten	
Minimierung eigener negativer Auswirkungen auf andere	Minimierung Angriffsfläche über externe Schnittstellen	Sichere Standardkonfiguration	Vertraulichkeit / Integrität bei Verarbeitung von Daten
DoS Mitigation	Datenminimierung	Aufzeichnung sicherheitsrelevanter Vorgänge	Vertraulichkeit / Integrität bei der Übermittlung von Daten

ergon

Product Lifecycle
Anforderungen

Cybersecurity Risk Assessment



ergon

Schwachstellen-Management

Software Bill of Materials

Vulnerability Scanning

Report Exploited Vulnerabilities

Notify User

Update Vulnerable Software

ergon

Zunahme von Cyberangriffen auf IoT-Ökosysteme

IoT malware attacks **grew more than 400%** in the Zscaler cloud compared to the same period in 2022.

Zscaler IoT & OT Report 2023

Number of IoT devices (bots) engaged in botnet-driven DDoS attacks rose **from around 200’000** a year ago **to approx. 1 million** devices.

Nokia Threat Intelligence Report 2023

Warum werden IoT-Ökosysteme angegriffen?

IoT Edge Geräte sind oft schlecht gesichert, wenig überwacht und werden nicht aktualisiert.

Wie wurden IoT Edge Geräte 2023 angegriffen?

“There are two main IoT infection routes: brute-forcing weak passwords and exploiting vulnerabilities in network services.”

IoT Threat Report, SECURELIST by Kaspersky

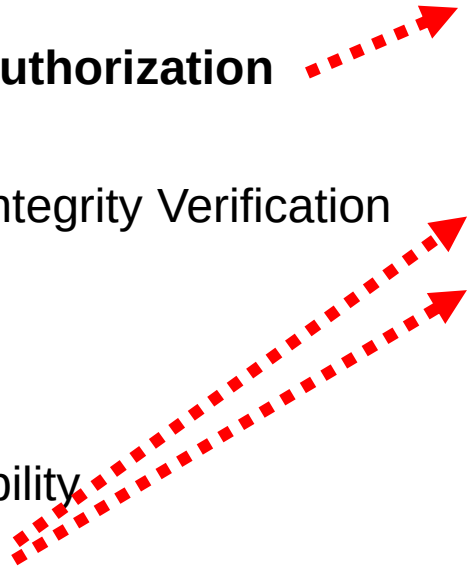
https://securelist.com/iot-threat-report-2023/110644

ergon

OWASP Top 10 IoT Vulnerabilities

OWASP IoT Top 10 Vulnerabilities 2014

1. Insecure Web Interfaces
2. **Insufficient Authentication/Authorization**
3. Insecure Network Services
4. Lack of Transport Encryption/Integrity Verification
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interfaces
8. Insufficient Security Configurability
9. **Insecure Software/Firmware**
10. Poor Physical Security

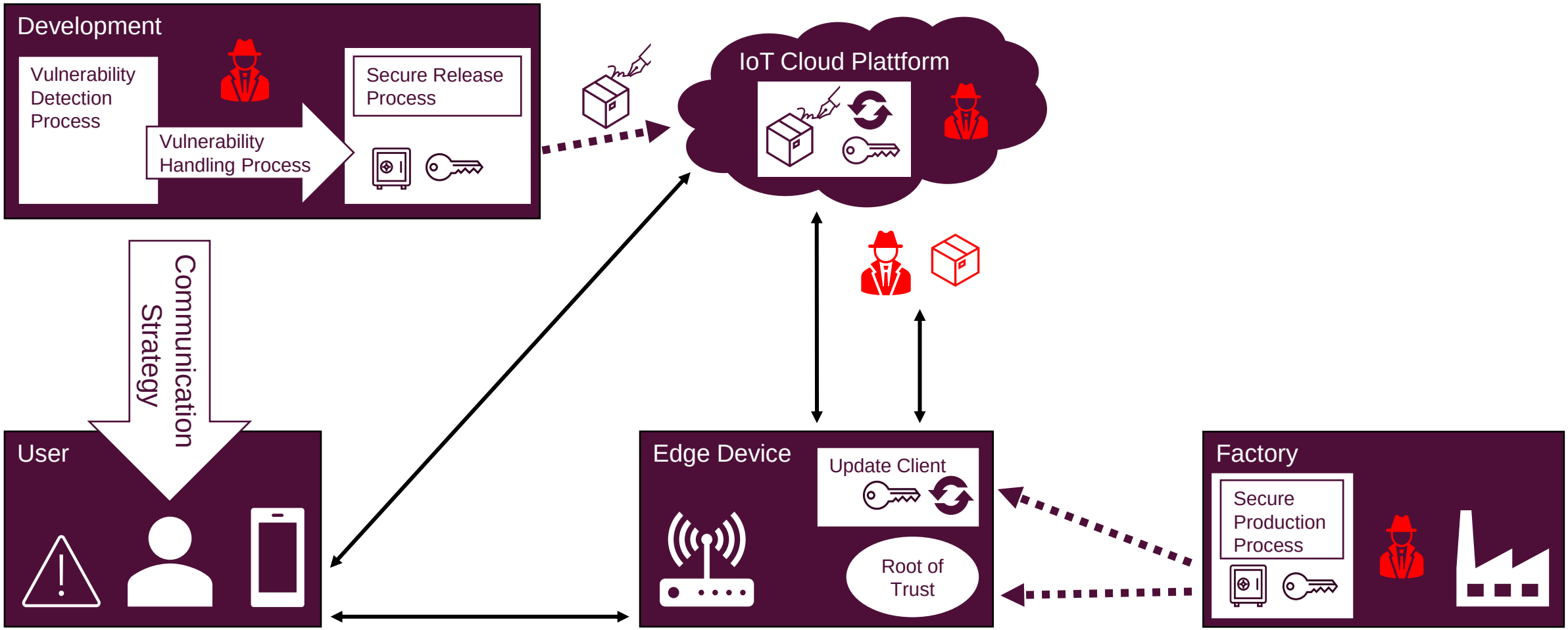


OWASP IoT Top 10 Vulnerabilities 2018

1. **Weak, Guessable, or Hardcoded Passwords**
2. Insecure Network Interface Services
3. Insecure Ecosystem Interfaces
4. **Lack of Secure Update Mechanism**
5. **Use of Insecure or Outdated Components**
6. Insufficient Privacy Protection
7. Insecure Data Transfer and Storage
8. Lack of Device Management
9. Insecure Default Settings
10. Lack of Physical Hardening

ergon

Sicherheitsupdates im IoT-Ökosystem



ergon

Fazit

Was schon lange «Best Practice» war, wird mit dem Cyber Resilience Act zur Pflicht.

ergon

Vielen Dank
für Ihre Aufmerksamkeit

Fabian Stelling

Software Engineer, Ergon Informatik AG

fabian.stelling@ergon.ch
ergon.ch

ergon