

EU Cyber Resilience Act - Wie ich bei meinem Produkt 15 Millionen € gespart habe

Act - Wie ich bei meinem Produkt 15 Millionen € gespart habe



Sprecher
André Lutermann
Microsoft Deutschland

Simon Brockschmidt
PwC Cyber Security Services

Agenda

- 1 Introduction
- 2 Cyber Resilience Act: What about it?
- 3 Cyber Resilience Act: Deep Dive
 - # Anwendbarkeit
 - # Kritische Produkte
 - # Konformität
- 4 Solution
 - # PwC METUS Security
- 5 Q&A



Cyber Resilience Act: What about it?

- Stellt die Cybersicherheit von **Produkten mit digitalen Elementen** sicher
- Gilt für Produkte die auf dem **Markt der europäischen Union** angeboten werden (B2B, B2C)
- Stellt spezifische **technische** und **organisatorische** Anforderungen, u.a.

Risiko Assessments

Updatepflicht

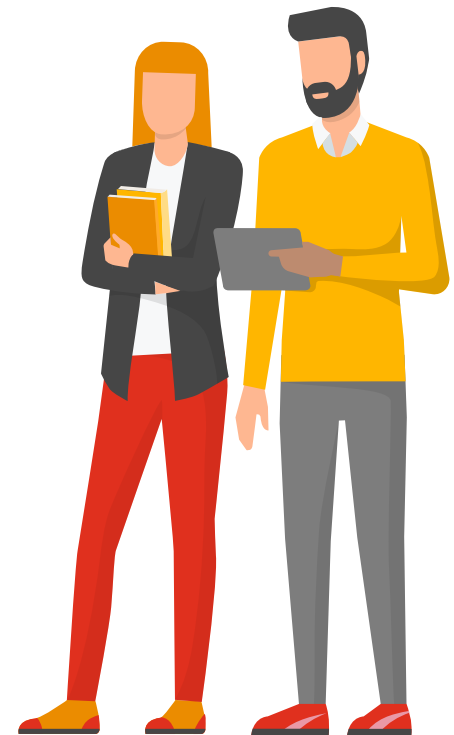
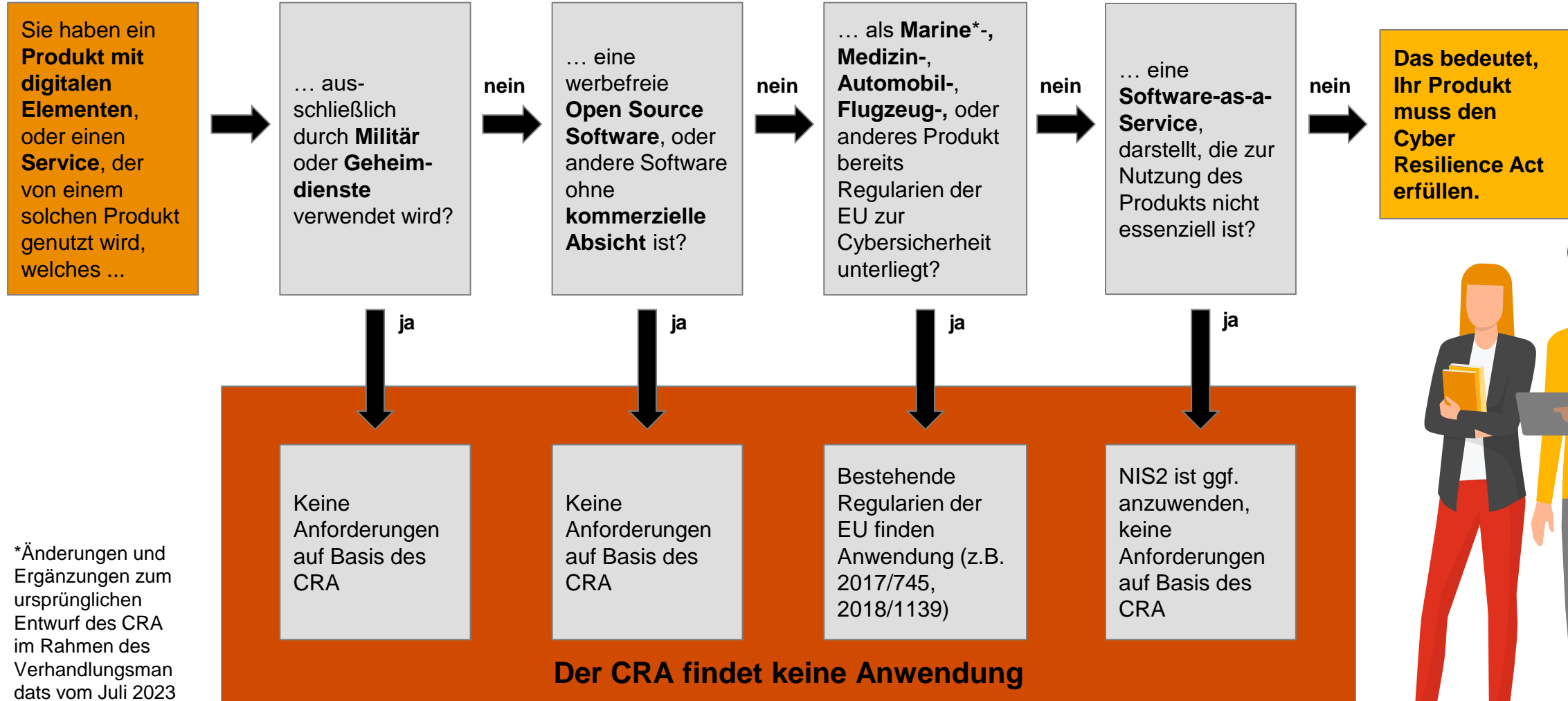
SBOM

Incident Reporting (24h)

- **Verabschiedung 2024** erwartet; erste Vorgaben gelten nach 12-18 Monaten, alle weiteren nach 24-36 Monaten
- Verstöße werden mit **Bußgeldern** i.H.v. **€15 Mio.** oder **2,5% des globalen Jahresumsatzes** belegt



Cyber Resilience Act: Anwendbarkeit



*Änderungen und Ergänzungen zum ursprünglichen Entwurf des CRA im Rahmen des Verhandlungsmandats vom Juli 2023

CRA findet Anwendung

Anhang IIIa:
 a) Wichtig für Cybersicherheit in kritischen Sektoren der NIS-2-Richtlinie (Anhang I), oder
 b) Können Versorgungsketten im EU-Binnenmarkt empfindlich stören

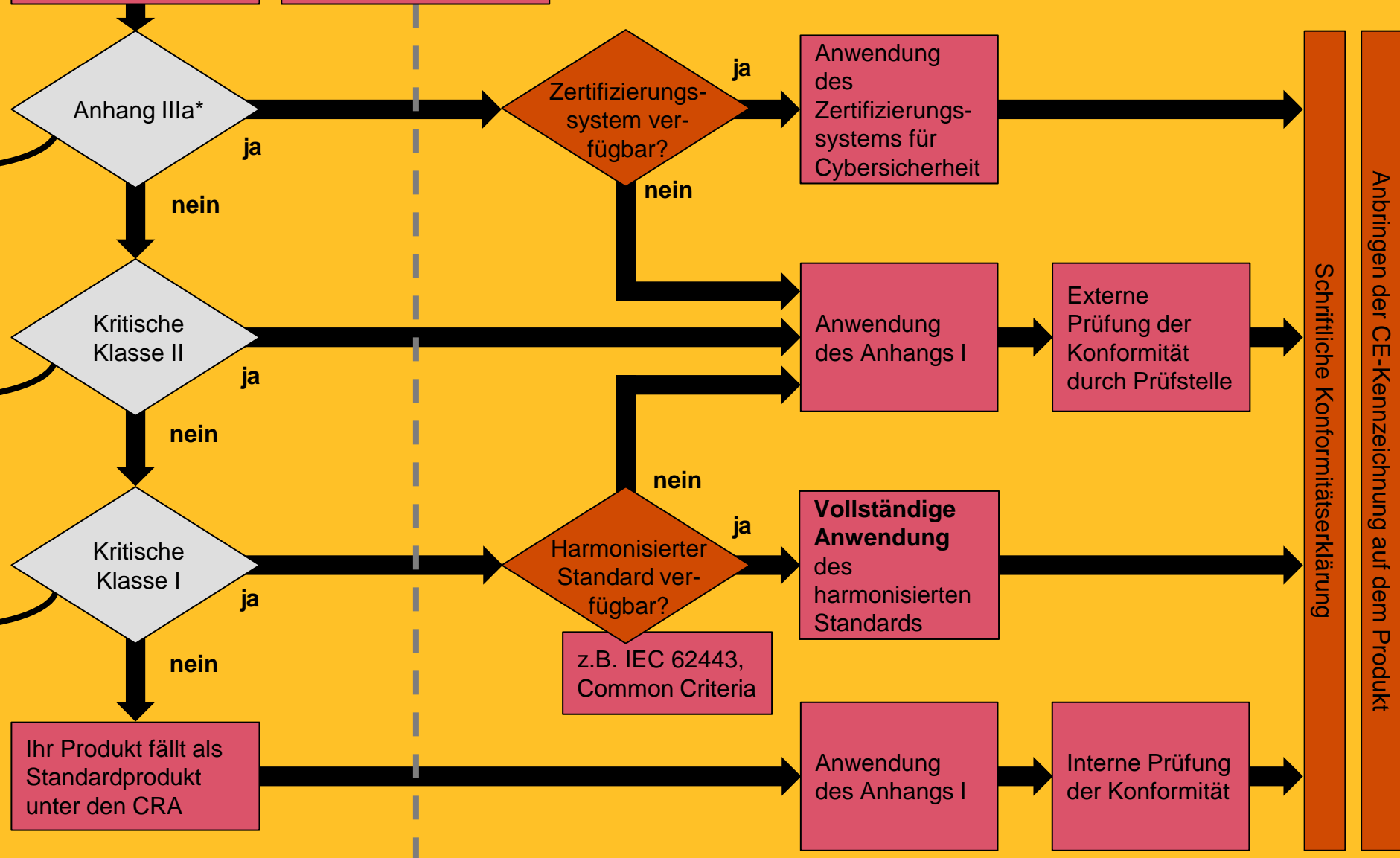
Hardwarekomponenten wie Geräte mit Security Boxen, Smart Meter Gateways, sichere Krypto Prozessoren, Smartcards u.ä., sowie Secure Elements.

Kritische Klasse II:
 a) Erfüllen primär eine cybersicherheitsrelevante Aufgabe, und
 b) Stellen Funktionen bereit, die bei Manipulation große Auswirkungen auf andere Produkte haben

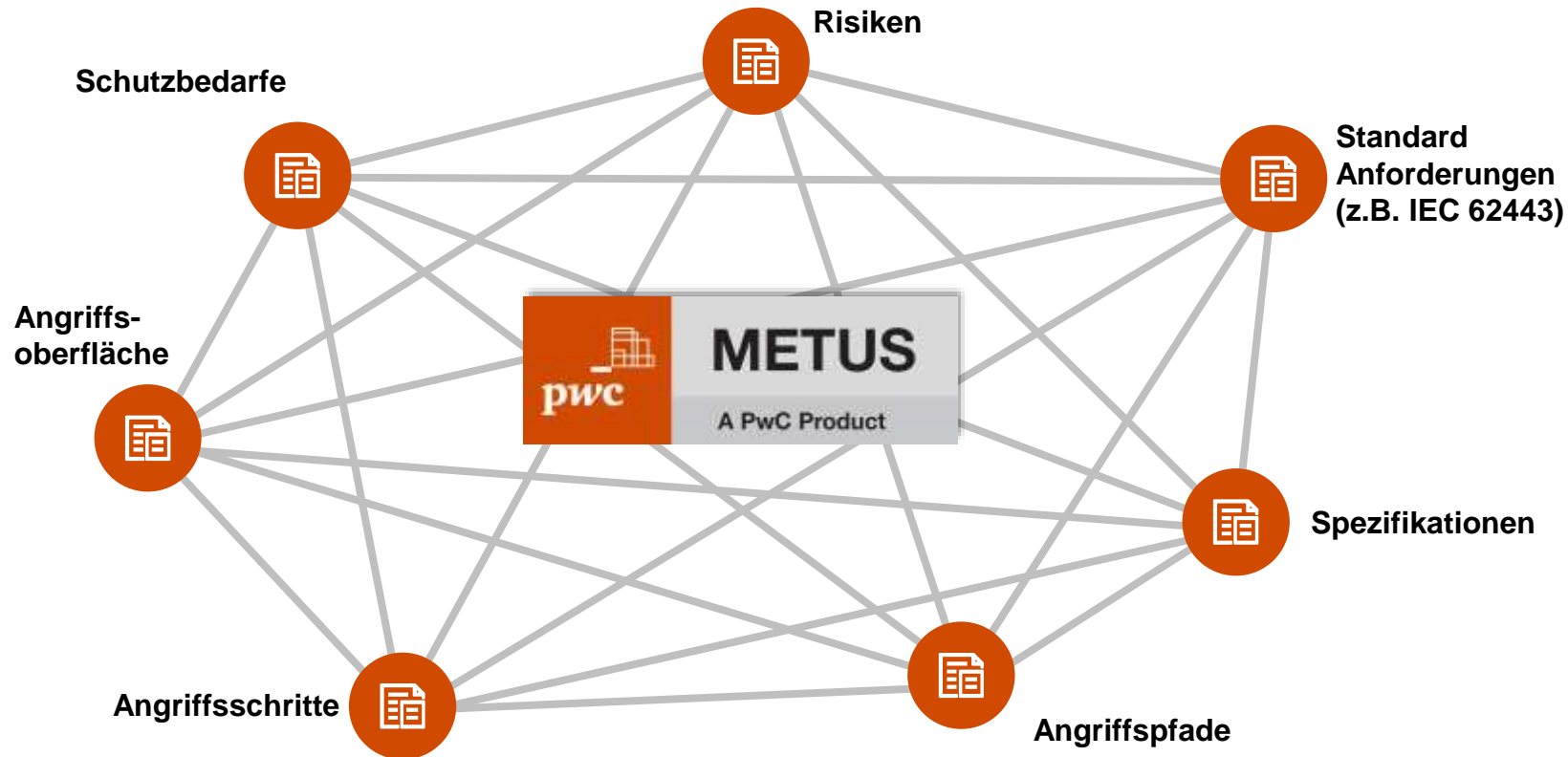
Z.B. Firewalls und Intrusion Detection/Prevention Systems.

Kritische Klasse I:
 Produkte erfüllen nur eine der Bedingungen der kritischen Klasse II, z.B. Antivirensoftware, Boot Manager und Public Key Infrastruktur, sowie Software zum Ausstellen digitaler Zertifikate.

Ist Ihr Produkt Teil des Anhangs III(a*)?
 Führen Sie ein Risiko Assessment zur Cybersicherheit durch



Solution: METUS Security



Funktionsumfang

- Systematische Erfassung der Angriffsfläche und Schutzbedarfe (Nutzung von Schnittstellen zu Asset Discovery Tools und Datenbanken möglich)
- Angriffsschritte werden automatisch zu verschiedenen Angriffspfaden kombiniert und visualisiert
- Aus allen Angriffspfaden werden die Risiken priorisiert, welche die größten Auswirkungen auf das Gesamtsystem haben
- Nutzung von integrierten Bedrohungs- und Anforderungskatalogen
- Unterstützung gängiger Dateiformate, sowie Schnittstellen zur Integration mit Drittsystemen

Cyber Resilience Act

Ihre Kontakte in Halle 7 am Microsoft Stand (629)



Dr. Oliver Hanka
Partner

Industrial & Product
Cyber Security

Bernhard-Wicki-Str. 8
80636 München

+49 160 5105836
Oliver.Hanka@PwC.com



Simon Brockschmidt
Senior Associate

Industrial & Product
Cyber Security

Bernhard-Wicki-Str. 8
80636 München

+49 1515 1043948
Simon.Brockschmidt@PwC.com



Finden Sie uns:
Halle 7
Microsoft
Stand 629

