Sichere Industrieprodukte

The good, the bad and the ugly

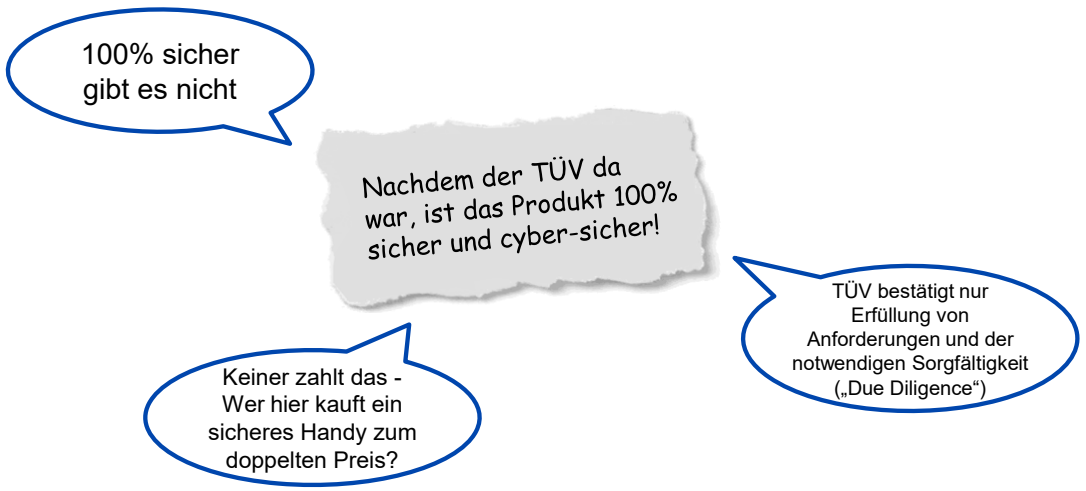
Add value.
Inspire trust.

Who I am

Michael Hermes

- OT Security Expert at TÜV SÜD
- Responsible for IEC 62443 Assessments & Certifications
- Studied Computer Science
- 10 years experience in IT, Security, software development for medical devices, cybersecurity for medical devices, DoD IA assurance
- Standardisation committees:
  - ISA Secure Technical Steering Committee

TÜV? Das sind doch die mit dem Siegel [1)]



1) https://www.youtube.com/watch?v=Qp0xUNC-_Jc

Provokante These, aber auch Erwartungshaltung der Hersteller sowie der Käufer

Ist aus zwei Gründen falsch

Wirtschaftlich sinnvoll: Oft kommt derzeit noch Bequemlichkeit dazu. Viele Systeme für Cybersicherheit gängeln die Benutzer (Passwortänderungen, Sicherheitsfragen….)

Was gehört zur Herstellung eines sicheren Produktes?

1 Organisation

- Organisation ist vorbereitet
- Personen sind trainiert
- QMS existiert
- Interne Systeme werden geschützt

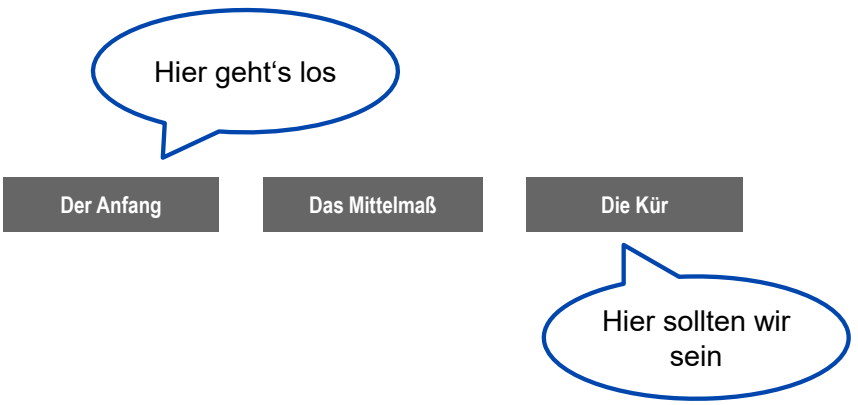
2 Entwicklung

- Entwicklungs- / Designprozess ist vorbereitet
- SDLC existiert mit Risikomanagement, Anforderungen, Design, Test, Freigabe …

3 Produkt

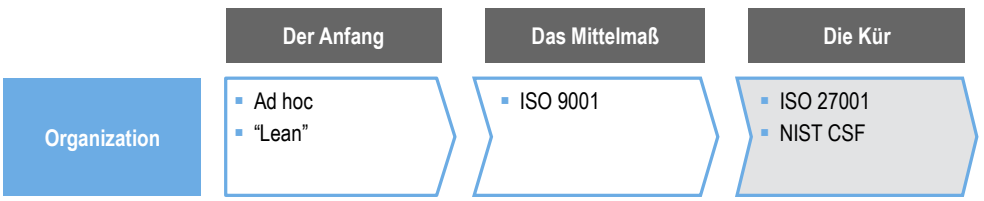
- Produkt mit ausreichend Sicherheitsfähigkeiten wird entwickelt, hergestellt, ausgeliefert und betrieben
- Benötigte Sicherheitsfähigkeiten ergeben sich aus den Produktfunktionen sowie dem Risikomanagement

Wie vergleichen wir das jetzt?



Zertifizierung = Vergleichbare Eigenschaften

The Good: Sichere Organisation



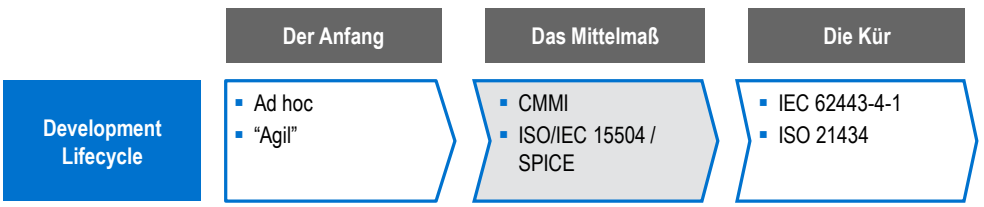
Dank etablierter Standards sind viele Organisationen beim Thema Informationssicherheit schon sehr weit

Ad Hoc = Zufällige Arbeitsweisen, damit auch zufällige Ergebnisse und Produkte

Grundlagen, Voraussetzungen schaffen. QMS ‚Denke‘, Sichere Entwicklungsumgebung, Klare Verantwortlichkeiten

Grau: Wo wir stehen / aktueller Industriekonsens / State of the art

The Bad: Sichere Entwicklung

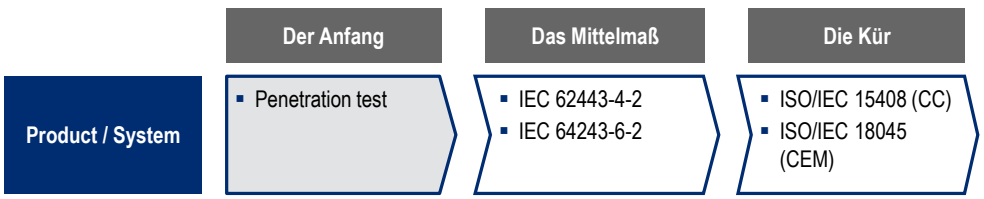


Viele Organisationen haben mit sicherer Entwicklung angefangen

Festlegen von Regeln für einen cybersicheren Entwicklungslebenszyklus, starten beim Design
- Welche Sicherheitsfeatures benötiget das Produkt (auch in den Phasen Operation, Decomissioning)
- Risikoanalyse mit dem Ergebnis welche Risiken kontrolliert werden müssen
- Testen!

Oft ein Hauptwissensträger. Der sorgt für ‚gute‘ Produkte.
z.B. ein Mobil/Handy-Spiel kann zufällig das Beste der Welt sein.
=> Eine integrierte Software mit verschiedenen Funktionen kann nie ‚zufällig‘ cybersicher sein, egal wie gut die Entwickler sind.
=> Sicherheit

The Ugly: Sichere Produkte

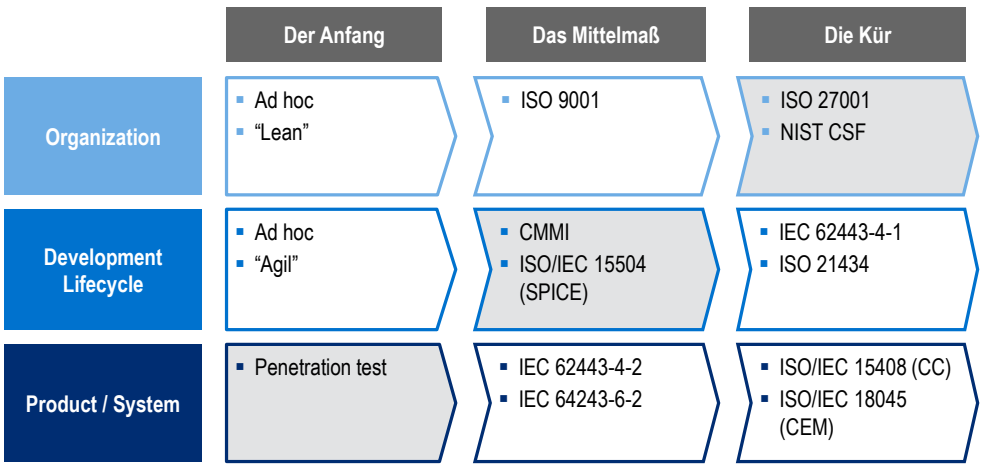


/// **Beim Thema Produktsicherheit stehen viele Unternehmen noch am Anfang**

Produkt hat grundlegende Funktionen die Cybersicherheit bedingen
z.B. Produkt kann kommunizieren -> Kommunikation muss abgesichert werden (Authentication of Partner, MAC)
Anhand der identifizierten Risiken werden Gegenmaßnahmen ergriffen

-4-2 Sicherheitsanforderungen, -6-2 Methoden zur Evaluierung
CC Sicherheitsanforderungen, CEM (CC evaluation methodology) Methoden zur Evaluierung

Die Großwetterlage



Wie machen es die anderen?

- Cybersichere Organisation, Entwicklungsumfeld, QMS
- Pflicht seit 2018

- Cybersichere Entwicklung
- Pflicht seit 2022

- Gewissheit (assurance) über cybersichere Produkte
- Verpflichtung noch nicht geplant

Automobil (spezielle Lieferketten-Situation: Wenige große OEMs mit viel Macht auf die Lieferkette)
TISAX (~27001) gefordert für sicheres Entwicklungsumfeld
TISAX: Für Zulieferer, Zuerst Eingruppierung Zuliefererklasse, Dann Pflichtanforderungen aus 27001. Angereichert durch Vertraulichkeit.

21434 (62443-4-1 auf Automobil zugeschnitten) – Pflicht ab 2022 für Zulieferer

QMS = QualitätsManagementSystem

Wie kommen wir weiter?

- Offen zur Diskussion
- Wir wollen alle mehr als minimales Pentesting

Ab sofort Common Criteria für alle?

- Für die meisten ist CC / FIPS 140 nicht wirtschaftlich
- 12+ Monate / 0.5+M€
- Viele Cybersicherheitsfeatures müssen implementiert und aktuell gehalten werden
- Für viele Gerätetypen ist CC zu viel Aufwand / nicht wirtschaftlich
- Für spezielle Gerätetypen (secure element, TPM-chip, MS Windows Security Reference Monitor) ist CC sinnvoll

Individueller Ansatz

- QMS auf den Stand der Technik bringen
- Secure Development Lifecycle umsetzen
- Risikoanalyse durchführen und je nach Risiko oder Produkttyp
  - 62443-4-2 / 62443-3-3
  - CC / FIPS 140
  - PCI DSS
  - DoD IA

Auf Cyber Resilience Act warten?

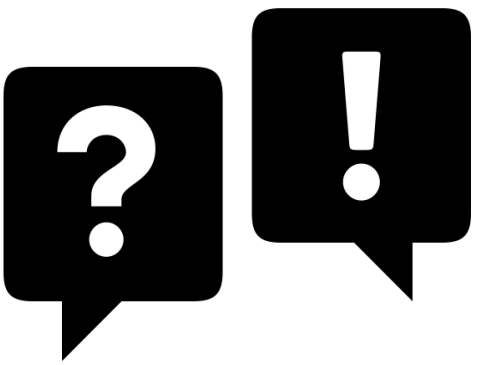
- Cyber Resilience Act (CRA)
- Konformität zu einem Standard wird Pflicht werden
- Aktuell bekannte Anforderungen sind alle ähnlich zur 62443

FIPS 140: Aus USA, Ähnlich strikt wie CC

Questions & Answers

Kontakt:

Website: www.tuvsud.com/iec62443
Email: sns@tuvsud.com



Bonus-Slides Cyber Resilience Act (CRA)

Quellen

- https://ec.europa.eu/newsroom/dae/redirection/document/89543 (vorgeschlagene Regulierung - PDF)
- https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act (Webseite, Überblick)
- https://ec.europa.eu/newsroom/dae/redirection/document/89528 (Factsheet)

CRA - Status

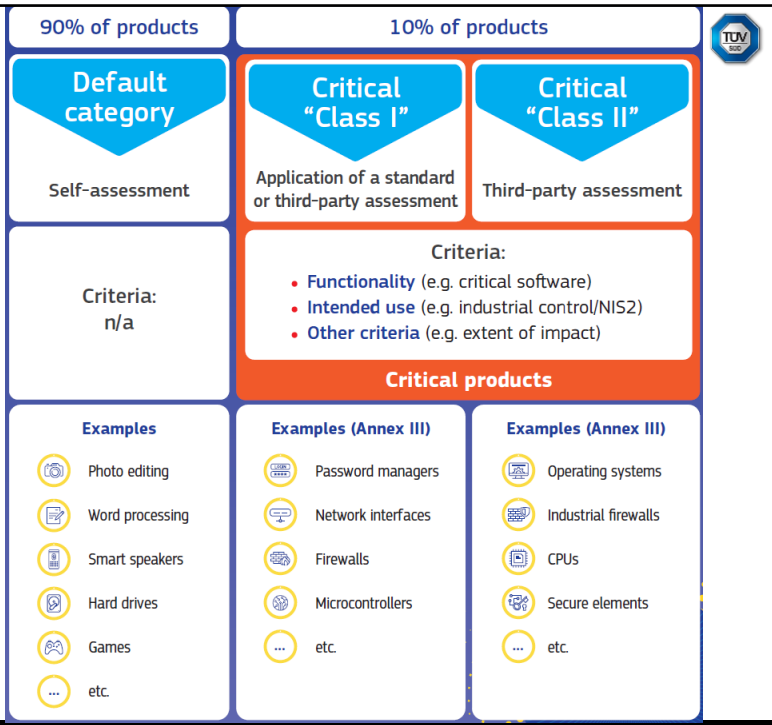
- September 2022: Vorschlag erarbeitet
- ~2022 – 2023: Untersuchung durch EU Parlament und Council, Offizielles Inkrafttreten
- ~2023 – 2024 (Inkrafttreten + 1 Jahr): Pflicht ausgenutzte Schwachstellen zu Berichten
- ~2024 – 2025 (Inkrafttreten + 2 Jahre): Alle Mitgliedsstaaten müssen den CRA voll übernommen haben

- Es wird ein Katalog harmonisierter Standards geben – bislang sind hierfür keine Kandidaten bekannt.
- Solange der Katalog noch nicht fertig ist oder Standards noch nicht herausgegeben sind kann die EU auch Anforderungen als ‚Act' erlassen

CRA Beurteilung

Fazit:

- Alle industriellen Komponenten oder Lösungen die Software beinhalten werden unter Class I oder Class II fallen.
- Beurteilung nach einem Standard wird Pflicht.



CRA - Content

The essential cybersecurity requirements and obligations mandate that all products with digital elements shall only be made available on the market if, [..] properly installed, maintained and used for their intended purpose or under conditions, which can be reasonably foreseen, they meet the essential cybersecurity requirements set out in this Regulation.

→ Gültig für alle Produkte die digitale Elemente beinhalten

The essential requirements and obligations would mandate manufacturers to factor in cybersecurity in the design and development and production of the products with digital elements, exercise due diligence on security aspects when designing and developing their products, be transparent on cybersecurity aspects that need to be made known to customers, ensure security support (updates) in a proportionate way, and comply with vulnerability handling requirements.

Cybersec beachten in Design, Entwicklung, Produktion. (identisch 62443-4-1 SM).
Kunden entsprechend informieren (identisch 62443-4-1 SG)
Definierte Behandlung von Schwachstellen (identisch 62443-4-1 DM & SUM)

CRA – TÜV SÜD Sichtweise

- Unsicherheit ob 62443 harmonisiert wird oder ein anderer Standard
- 62443 ist ein etablierter Standard der alle Funktionen in der industriellen Welt abdeckt, 62443 wird bereits von branchenspezifischen Standards kopiert (21434, 81001-5-1) => gute Chancen, dass 62443 harmonisiert wird, oder der neue Standard von 62443 kopiert
- 62443 deckt die selben Themengebiete ab die auch im CRA gefordert werden

Self-Assessment 62443-4-1 ist eine sichere Methode um gut vorbereitet zu sein.