TÜV AUSTRIA GRUPPE

CRA, AI-Act, RED und NIS - Zusammenhänge mit der MVO

WKO NÖ SAFETY DAY – CE-Kennzeichnung & Normen

Alex Zeppelzauer / Oktober 2024

Inhalt

- ✓ ENISA
- ✓ KI Act
- ✓ NIS
- ✓ CRA
- ✓ RED
- ✓ Zusammenhänge

ENISA

ENISA (European Union Agency for Cybersecurity)

- ✓ zentrale Agentur der EU für Cybersicherheit
- ✓ unterstützt die Mitgliedstaaten und EU-Institutionen bei der Verbesserung ihrer Cybersicherheitskapazitäten und –fähigkeiten
- ✓ wichtige Rolle bei der Entwicklung und Umsetzung von Cybersicherheitsstandards und -richtlinien

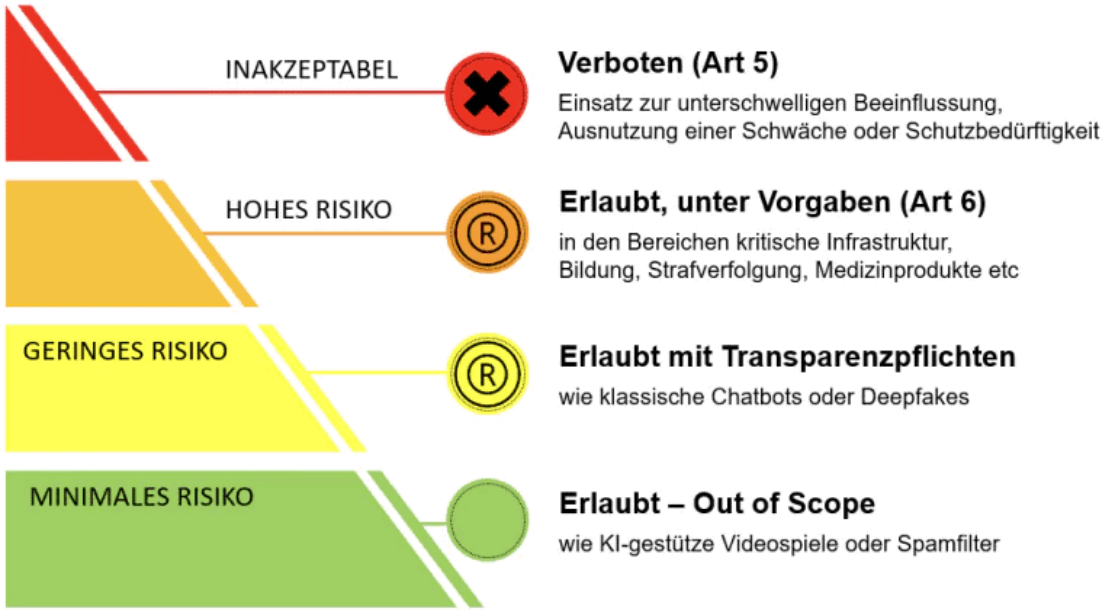
AI-Act & Risikoklassen

AI-Act (Artificial Intelligence Act)

- ✓ ein Vorschlag der Europäischen Kommission zur Regulierung von Künstlicher Intelligenz (KI) in der EU.
- ✓ einheitliches Regelwerk, das die Sicherheit und Grundrechte der Bürger schützt und gleichzeitig Innovationen fördert
- ✓ sieht eine risikobasierte Klassifizierung von KI-Systemen vor und legt spezifische Anforderungen an Hochrisiko-KI-Systeme fest, einschließlich Cybersicherheitsanforderungen

4 Risikoklassen

- ✓ Allgemeine Anforderungen an alle KI-Systeme
  - Registrierungspflicht
- ✓ Transparenzanforderung für bestimmte KI-Systeme mit geringem Risiko (Art. 52)
  - Beispiel – Ein Chatbot muss zu erkennen geben, dass er ein Chatbot ist.
- ✓ Risikomanagement für Hochrisiko-KI-Systeme (Art. 6-51)
  - Durchführung von Prüfungen und Konformitätsbewertungsverfahren
- ✓ Verbot bestimmter KI-Praktiken (Art. 5)
  - Beispiele: Social Scoring, Betrieb von Systemen zur biometrischen Identifizierung im öffentlichen Raum, …



https://www.eylaw.at/wp-content/uploads/2023/01/AI-Act-EU-Startups-risk-approach-chatgpt-Artificial-inteligence-KI-oesterreich-ey-law-news.png

Network and Information Security Directive

NIS 2

- ✓ zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit
- ✓ erweitert die Anforderungen der ursprünglichen NIS-Richtlinie von 2016
- ✓ zielt darauf ab, ein hohes gemeinsames Sicherheitsniveau für Netz- und Informationssysteme in der EU zu gewährleisten

Wichtigste Punkte der NIS-2-Richtlinie

- ✓ Erweiterter Anwendungsbereich
  - für mehr Unternehmen und Organisationen in 18 kritischen Sektoren, einschließlich Gesundheitswesen, Energie, Verkehr und digitale Infrastruktur
- ✓ Strengere Sicherheitsanforderungen
  - Implementierung umfassenderer Sicherheitsmaßnahmen
  - regelmäßige Risikobewertungen
- ✓ Meldepflichten
  - Verpflichtung, erhebliche Cybervorfälle innerhalb von 24 Stunden zu melden
- ✓ Erhöhte Strafen

CRA & Cybersecurity Framework

CRA (Cyber Resilience Act)

- ✓ zielt darauf ab, die Cybersicherheit von Produkten mit digitalen Elementen zu verbessern
- ✓ legt Anforderungen an die Cybersicherheit während des gesamten Lebenszyklus dieser Produkte fest, von der Entwicklung bis zur Nutzung und Entsorgung
- ✓ soll sicherstellen, dass Produkte sicher in der EU verwendet werden können und dass Hersteller entsprechende Sicherheitsmaßnahmen implementieren

Cybersecurity Framework

- ✓ einheitliche Zertifizierungsschemata, die EU-weit gültig sind
- ✓ Stellt sicher, dass zertifizierte Produkte und Dienstleistungen bestimmten Sicherheitsanforderungen entsprechen

Drei Zertifizierungssysteme in Entwicklung

- ✓ **EU5G:** Ein Zertifizierungssystem für 5G-Netzwerke
- ✓ **EUCC:** Basierend auf Common Criteria (international anerkannter Standard für die Sicherheitsbewertung von IKT-Produkten)
- ✓ **EUCS:** Ein Zertifizierungssystem für Cloud-Dienste

Red - Radio Equipment Directive

- Deutsch: „Funkanlagenrichtlinie“ Richtlinie 2014/53/EU

  „… elektrisches oder elektronisches Erzeugnis,
  das zum Zweck der Funkkommunikation und/oder
  der Funkortung bestimmungsgemäß Funkwellen ausstrahlt
  und/oder empfängt …“

- Umsetzung in Österreich:
  - BGBl. I Nr. 57/2017
  - Funkanlagen-Marktüberwachungs-Gesetz - FMaG 2016

EN 18031 & RED

EN 18031

- ✓ neue Normenreihe, die speziell entwickelt wurde, um die Cybersicherheitsanforderungen der RED zu erfüllen

Drei Teile

- ✓ EN 18031-1: Bezieht sich auf Funkanlagen mit Internetanschluss
  - stellt sicher, dass solche Geräte robuste Sicherheitsmaßnahmen implementieren, um Netzwerksicherheit, Schutz der Privatsphäre und Betrugsprävention zu gewährleisten
- ✓ EN 18031-2: Deckt Funkgeräte ab, die Daten verarbeiten.
- ✓ EN 18031-3: Bezieht sich auf internetfähige Funkgeräte, die virtuelles Geld oder Geldwerte verarbeiten

Überblick CE-Richtlinien

TÜV TRUST IT
TÜV AUSTRIA Group

Für Maschinen und Anlagen:

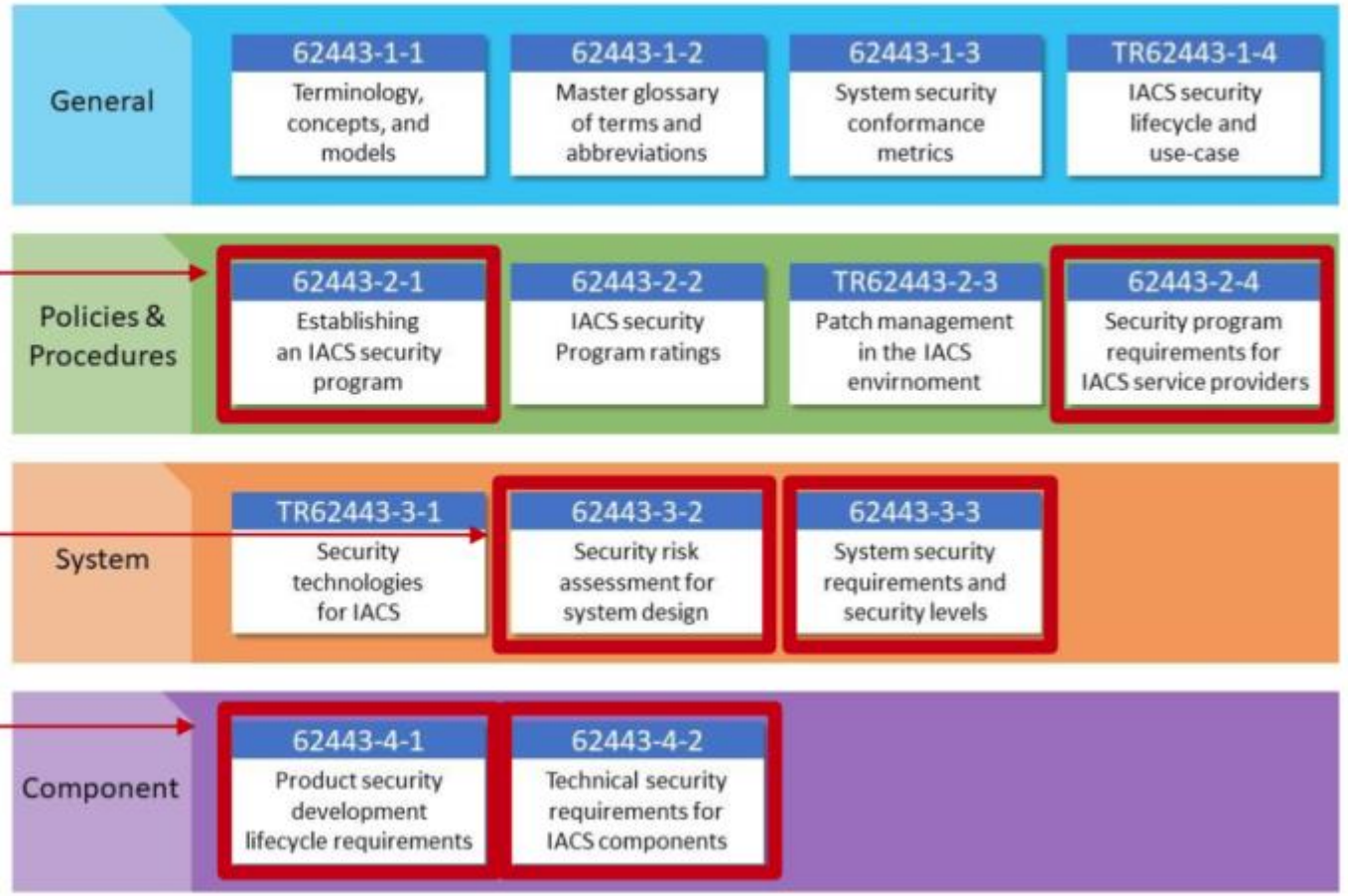
- Die Maschinenrichtlinie 2006/42/EG
- Maschinenverordnung 2023/1230 (Übergangsfrist bis 14.01.27!)

Für Betriebsmittel und elektrische Geräte:

- Niederspannungsrichtlinie 2014/35/EU
- RoHS 2011/65/EU
- Funkanlagen (RTTE bzw. RED) 2014/53/EU
- EMV-Richtlinie 2014/30/EU
- Eco-Design-Richtlinie 2009/125/EG

Richtlinien, Gesetze und die IEC 62443

NIS II
CRA (Cyber resilience act)
Maschinenverordnung
Funkanlagenrichtlinie



TÜV AUSTRIA is an accredited inspection and certification body

DANKE für Ihre Aufmerksamkeit!

Alexander Zeppelzauer
Mobil: +43 664 604546276
Email: alexander.zeppelzauer@tuv.at