anapur AG

OT-CYBERSECURITY: LEGAL REQUIREMENTS

NAMUR 2024

ERWIN KRUSCHITZ, VORSTAND ANAPUR AG

Ausbildung:

Ingenieur Elektrotechnik
Engineering Management

Aktuelle fachliche Tätigkeit:

Assessments & Beratung

OT-Security, GMP, Functional Safety

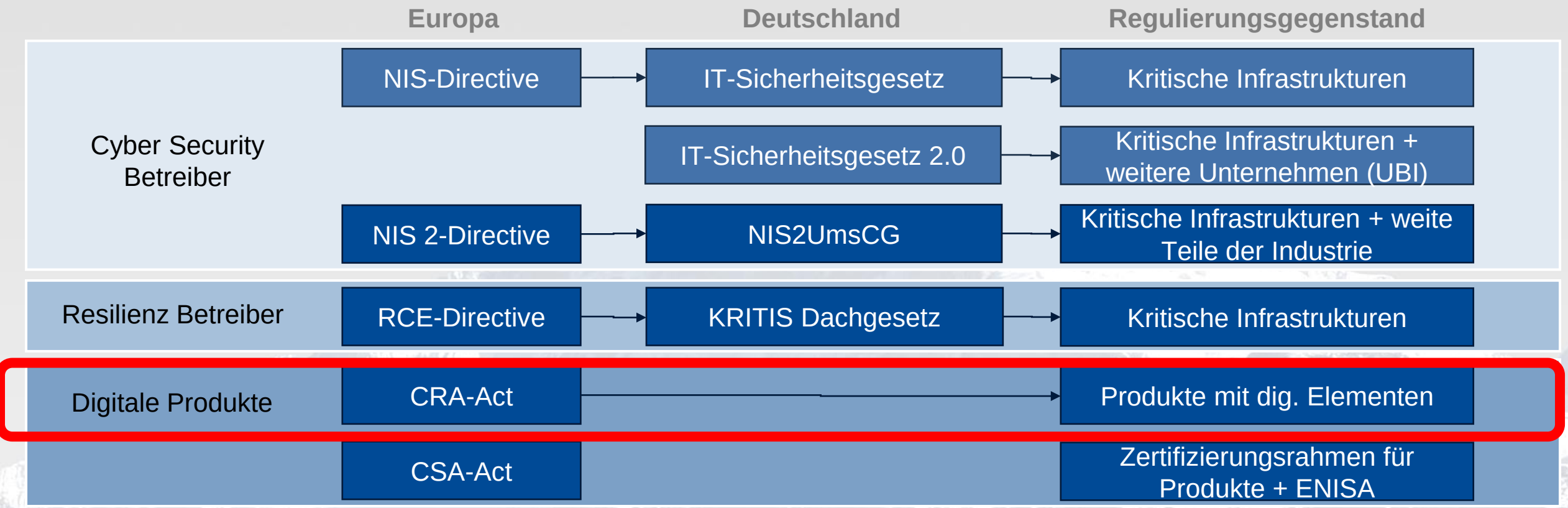
Gemeinschaftsaktivitäten:

- NAMUR AK 4.18 Automation Security (Obmann)
- VCI AK IT-Sicherheit
- DIN/DKE/VDE 931.1 Automation Security
- IEC62443 / ISA99
- Allianz for Cyber Security
- GAMP DACH
- ISPE

AGENDA

1. **Überblick Cybersicherheitsregularien**
2. **CRA EU Cyber Resilience Act**
3. **NIS 2 EU Network and Information Security Directive**
4. **Arbeitsschutz TRBS1115-1, Störfallschutz KAS51**

SECURITY REGULIERUNG
ALLGEMEINE SECURITY GESETZE



CYBER RESILIENCE ACT (CRA) - ALLGEMEINES

Das Wesentliche:

Cyber-Security wird Teil der europäischen CE-Kennzeichnung

Gültig für: ALLE „Produkte mit digitalen Elementen“
Start: ab 2027
Strafen: max. 15 Mill. EUR oder bis zu 2,5 % des weltweiten Jahresumsatzes

CE-Selbsterklärung für Automatisierungskomp. (harmonisierte EU-Normen)
Support Zeitraum min. 5 Jahre + Anwendererwartung & Verwendungszweck

Pflichten für Hersteller:

Bewertung von Cybersicherheitsrisiken
Due-Diligence-Prüfung für Komponenten von Drittanbietern
Das Produkt erfüllt grundlegende Cyber-Anforderungen
Umgang mit Schwachstellen
Anleitungen für Nutzer

CRA: GRUNDLEGENDE CYBERSEC ANFORDERUNGEN

ANNEX I

a) Auslieferung ohne Schwachstellen
b) Sichere Standardkonfiguration
c) Schwachstellen aktualisierbar
d) Schutz vor unberechtigtem Zugriff
e) Schutz der Vertraulichkeit (z.B. durch Verschlüsselung)
f) Schutz der Integrität und Meldung von Verfälschungen
g) Datenminimierung
h) die Verfügbarkeit wesentlicher Daten auch nach Vorfall gewährleisten
i) die negativen Auswirkungen auf andere Geräte zu minimieren
j) Begrenzung der Angriffsflächen, einschließlich externer Schnittstellen;
k) Verringerung der Auswirkungen eines Vorfalls durch Techniken zur Eindämmung der Ausbeutung;
l) Aufzeichnung relevanter interner Aktivitäten (Zugriff, Änderung)
m) sichere Löschung bzw. Migration der Einstellungen

CRA: ANFORDERUNGEN ZUM UMGANG MIT SCHWACHSTELLEN

ANNEX I PART II

(1) Schwachstellen identifizieren & dokumentieren (maschinenlesb. Software-Stückliste)
(2) Schwachstellen unverzüglich beseitigen
(3) wirksame und regelmäßige Sicherheitstests des Produkts durchführen
(4) Informationen über behobene Schwachstellen weitergeben & öffentlich machen
(5) koordinierte Offenlegung von Schwachstellen einführen und durchsetzen
(6) die Weitergabe von Informationen steuern
(7) Mechanismen zur sicheren Verteilung von Updates bereitstellen
(8) die unverzügliche und kostenlose Verbreitung von Updates gewährleisten
(eine Ausnahme ist nur für maßgeschneiderte Produkte möglich)

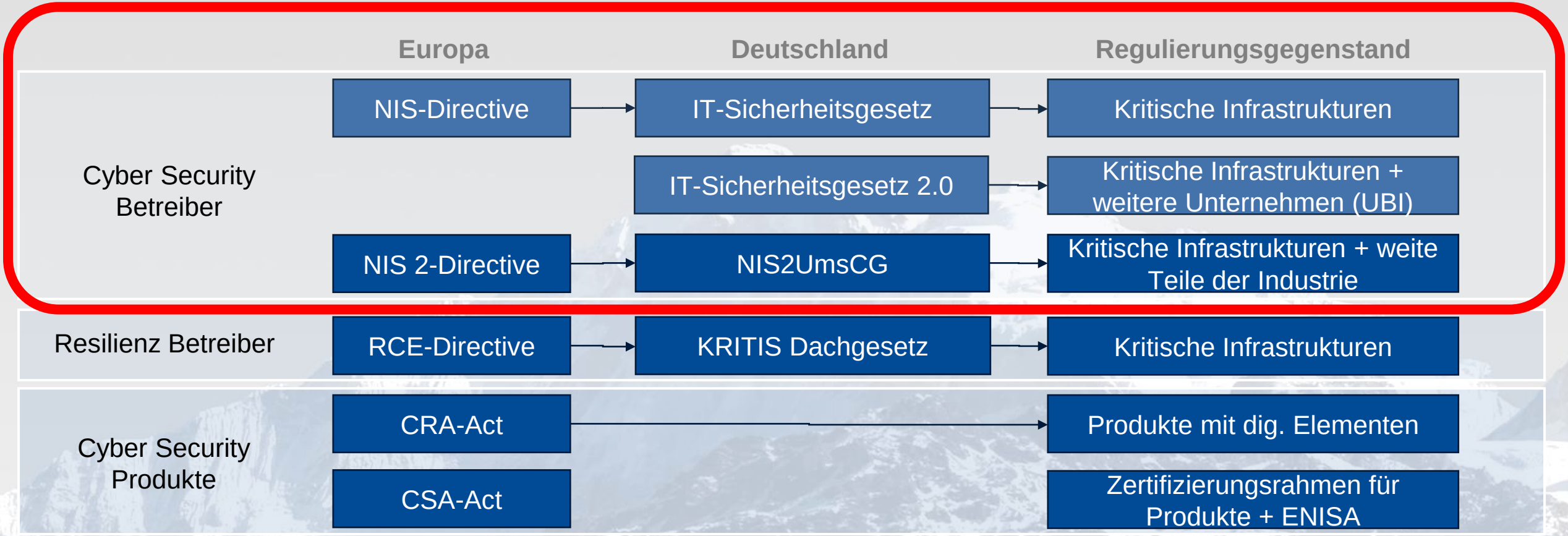
CRA: ANLEITUNGEN FÜR DEN NUTZER

ANNEX II

1..3 Adresse / digitaler Kontakt

4. den Verwendungszweck des Produkts einschließlich der Sicherheitsumgebung der wesentlichen Funktionen des Produkts
5. alle bekannten oder vorhersehbaren Umstände, die zu erheblichen Cybersicherheitsrisiken führen können;
6. die Internetadresse, unter der die EU-Konformitätserklärung abgerufen werden kann;
7. die Art und das Enddatum der technischen Sicherheitsunterstützung
8. detaillierte Anweisungen
    - (a) die erforderlichen Maßnahmen bei der Erstinbetriebnahme und während der Lebensdauer des Produkts
    - (b) wie sich Änderungen auf die Sicherheit der Daten auswirken können;
    - (c) wie sicherheitsrelevante Updates installiert werden können;
    - (d) die sichere Außerbetriebnahme einschließlich Informationen zur sicheren Entfernung von Benutzerdaten
    - (e) wie die automatischen Updates abgeschaltet werden können;
    - (f) Informationen für den Integrator zur Einhaltung der grundlegenden Cybersicherheitsanforderungen

SECURITY REGULIERUNG
ALLGEMEINE SECURITY GESETZE



NIS2 ALLGEMEINE INFORMATION

Artikel 21 Forderung an ALLE (Chemie):

1. Risikoanalyse
2. Bewältigung von Sicherheitsvorfällen,
3. Backup- und Wiederherstellung, Krisenmanagement
4. Sicherheit der Lieferkette
5. Sicherheitsmaßnahmen bei Erwerb von IT
6. Bewertung der Wirksamkeit von Maßnahmen
7. Cyberhygiene und Schulungen
8. Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Zugriffskontrolle
10. Multi-Faktor-Authentifizierung

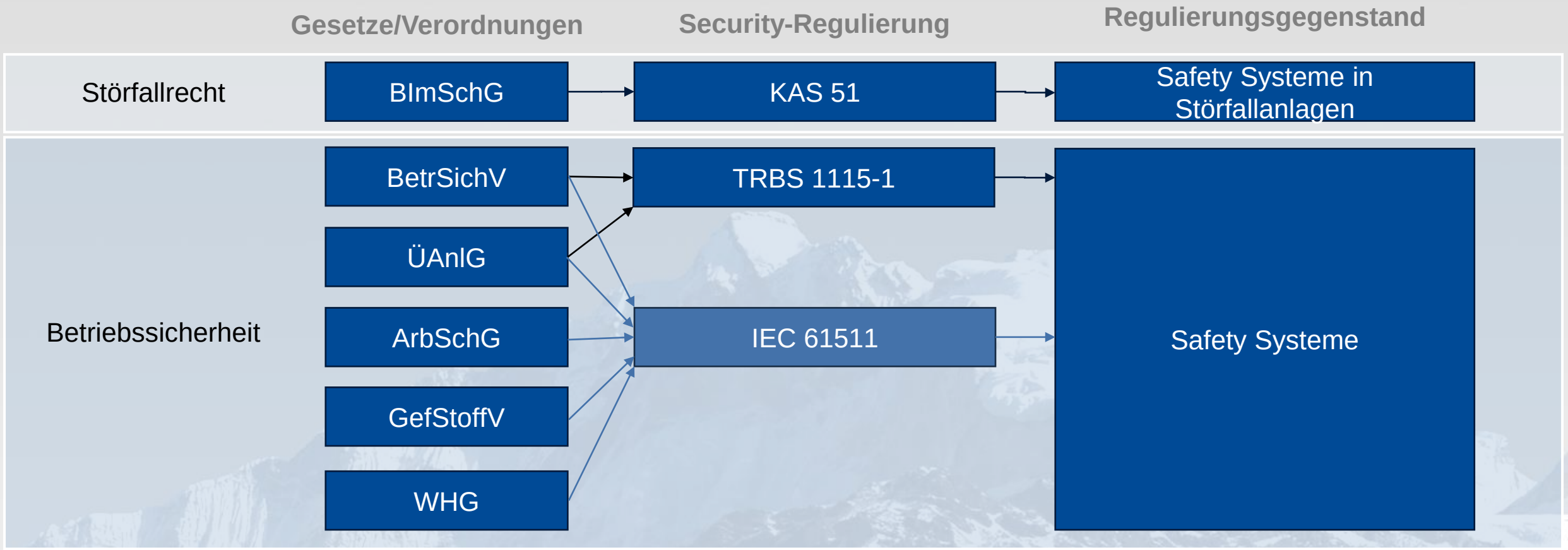
Ausführung nach „Stand der Technik"

Besonders wichtige Einrichtungen - zusätzlich:

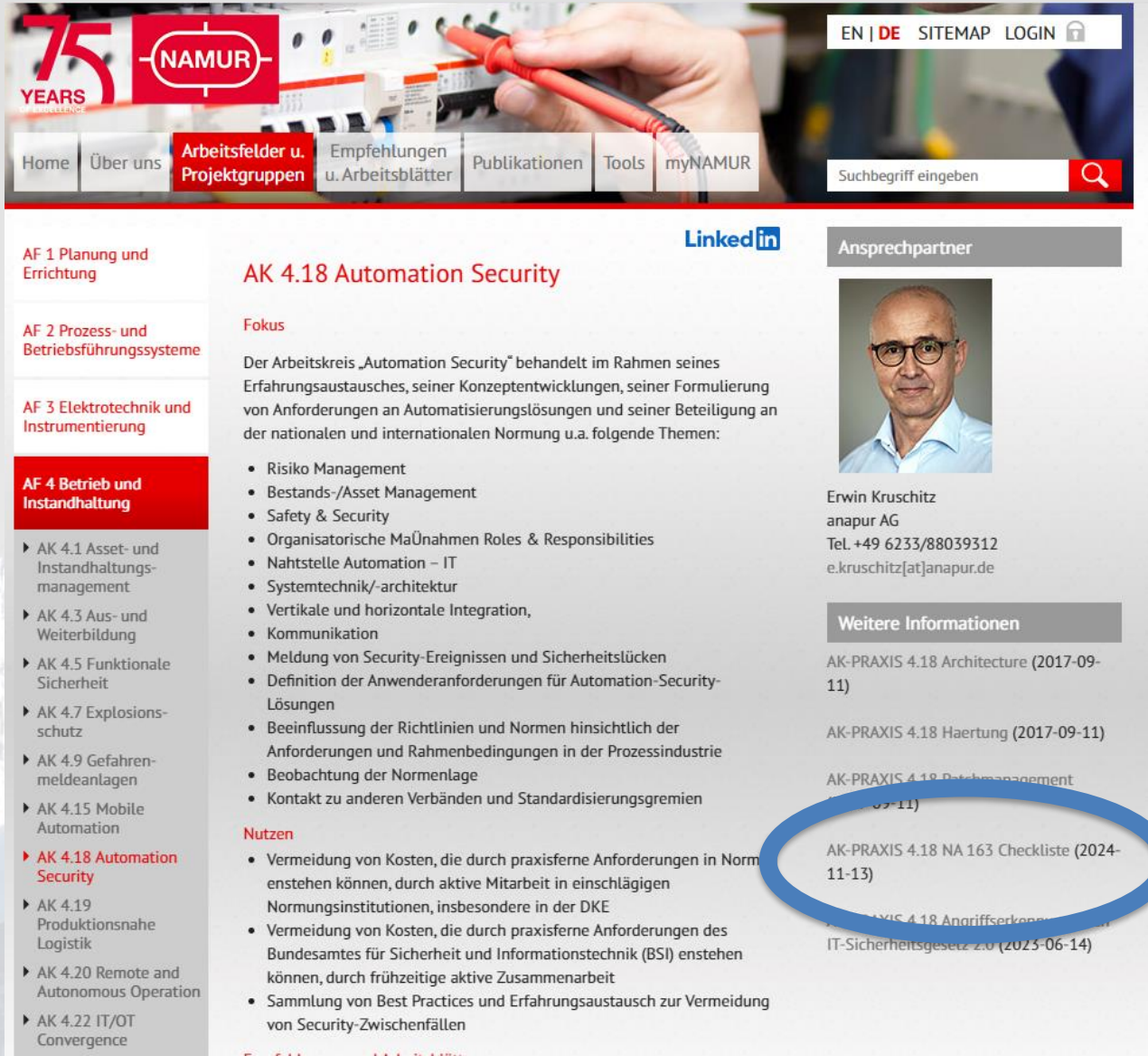
- Registrierungspflicht
- Meldepflicht
- Nachweis (Audit durch qualifizierten Prüfer)
- Angriffserkennung (§8 IT-SIG 2)

Wird eine Maßnahme nicht vollständig oder nicht rechtzeitig ergriffen oder,…die **Einhaltung der Verpflichtung …nicht vollständig dokumentiert**, ist das eine Ordnungswidrigkeit. Sanktionen in der Chemie max. 7 Mill. EUR bzw. 1,4% des weltweiten Jahresumsatzes

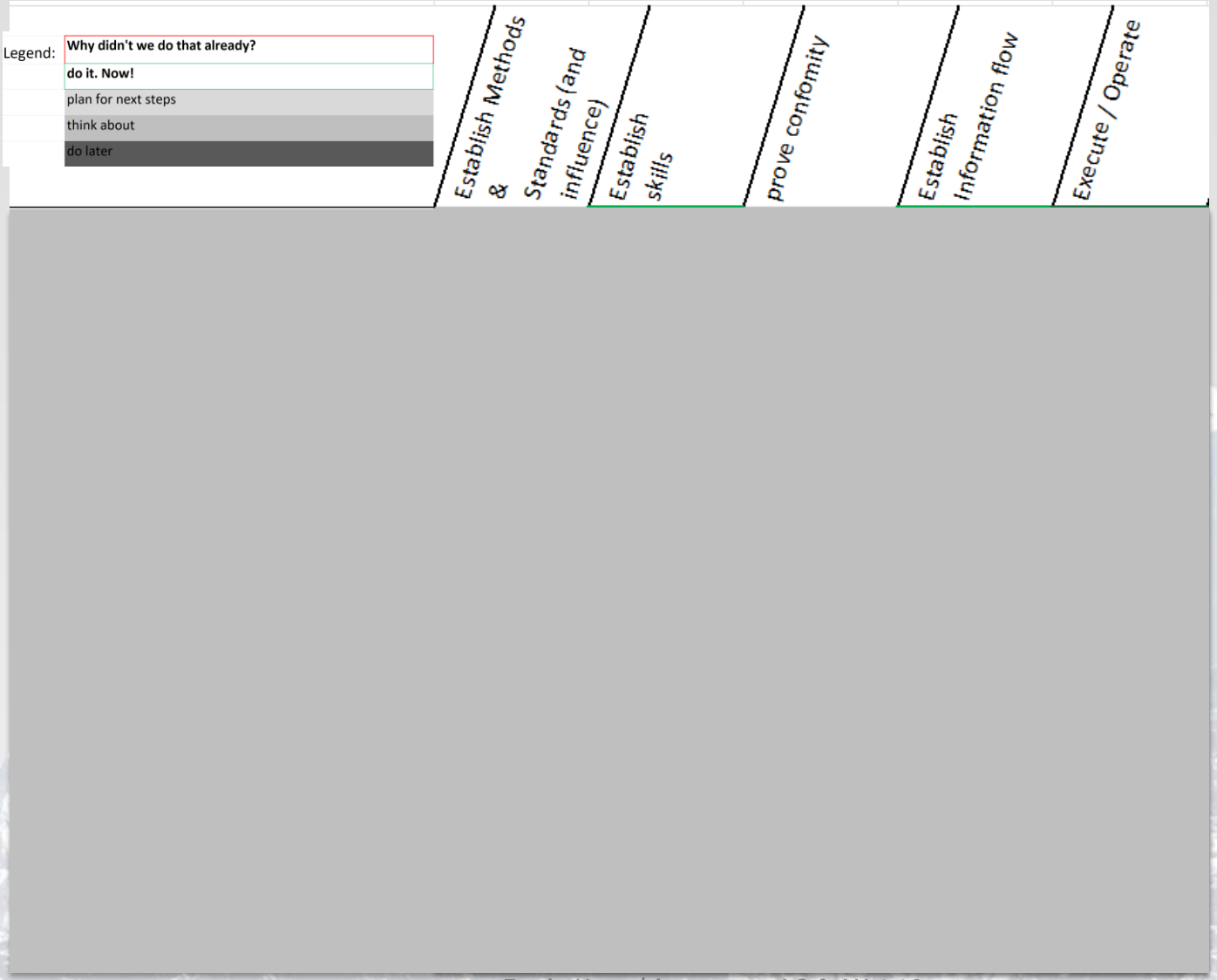
SECURITY REGULIERUNG
SECURITY FOR SAFETY (IN DEUTSCHLAND)



- BDI Position Cybersicherheitsregulierung
  - *„Die deutsche Industrie fordert, dass die gesetzlichen Maßnahmen überlappungs- und widerspruchsfrei sind. Doppelprüfungen und Audits müssen vermieden werden.“*
  - https://bdi.eu/publikation/news/cybersicherheitsregulierung


NAMUR
75 YEARS
EN | DE SITEMAP LOGIN
Home
Über uns
Arbeitsfelder u. Projektgruppen
Empfehlungen u. Arbeitsblätter
Publikationen
Tools
myNAMUR
Suchbegriff eingeben
AF 1 Planung und Errichtung
AF 2 Prozess- und Betriebsführungssysteme
AF 3 Elektrotechnik und Instrumentierung
AF 4 Betrieb und Instandhaltung
AK 4.1 Asset- und Instandhaltungs-management
AK 4.3 Aus- und Weiterbildung
AK 4.5 Funktionale Sicherheit
AK 4.7 Explosions-schutz
AK 4.9 Gefahren-meldeanlagen
AK 4.15 Mobile Automation
AK 4.18 Automation Security
AK 4.19 Produktionsnahe Logistik
AK 4.20 Remote and Autonomous Operation
AK 4.22 IT/OT Convergence
AK 4.18 Automation Security
Fokus
Der Arbeitskreis „Automation Security" behandelt im Rahmen seines Erfahrungsaustausches, seiner Konzeptentwicklungen, seiner Formulierung von Anforderungen an Automatisierungslösungen und seiner Beteiligung an der nationalen und internationalen Normung u.a. folgende Themen:
Risiko Management
Bestands-/Asset Management
Safety & Security
Organisatorische MaÜnahmen Roles & Responsibilities
Nahtstelle Automation – IT
Systemtechnik/-architektur
Vertikale und horizontale Integration,
Kommunikation
Meldung von Security-Ereignissen und Sicherheitslücken
Definition der Anwenderanforderungen für Automation-Security-Lösungen
Beeinflussung der Richtlinien und Normen hinsichtlich der Anforderungen und Rahmenbedingungen in der Prozessindustrie
Beobachtung der Normenlage
Kontakt zu anderen Verbänden und Standardisierungsgremien
Nutzen
Vermeidung von Kosten, die durch praxisferne Anforderungen in Norm enstehen können, durch aktive Mitarbeit in einschlägigen Normungsinstitutionen, insbesondere in der DKE
Vermeidung von Kosten, die durch praxisferne Anforderungen des Bundesamtes für Sicherheit und Informationstechnik (BSI) enstehen können, durch frühzeitige aktive Zusammenarbeit
Sammlung von Best Practices und Erfahrungsaustausch zur Vermeidung von Security-Zwischenfällen
Ansprechpartner
Erwin Kruschitz
anapur AG
Tel. +49 6233/88039312
e.kruschitz[at]anapur.de
Weitere Informationen
AK-PRAXIS 4.18 Architecture (2017-09-11)
AK-PRAXIS 4.18 Haertung (2017-09-11)
AK-PRAXIS 4.18 NA 163 Checkliste (2024-11-13)

DER WEG NACH VORNE



Status Quo:

NE153
NA163
NA169
CSAF
AK-Praxis

anapur AG

anapur AG

DANKE / THANK YOU