THREAT MODELING CONNECT
German Online Meetup

DACH-Region

THREAT MODELING CONNECT | DEUTSCHSPRACHIGE ZWEIGSTELLE

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

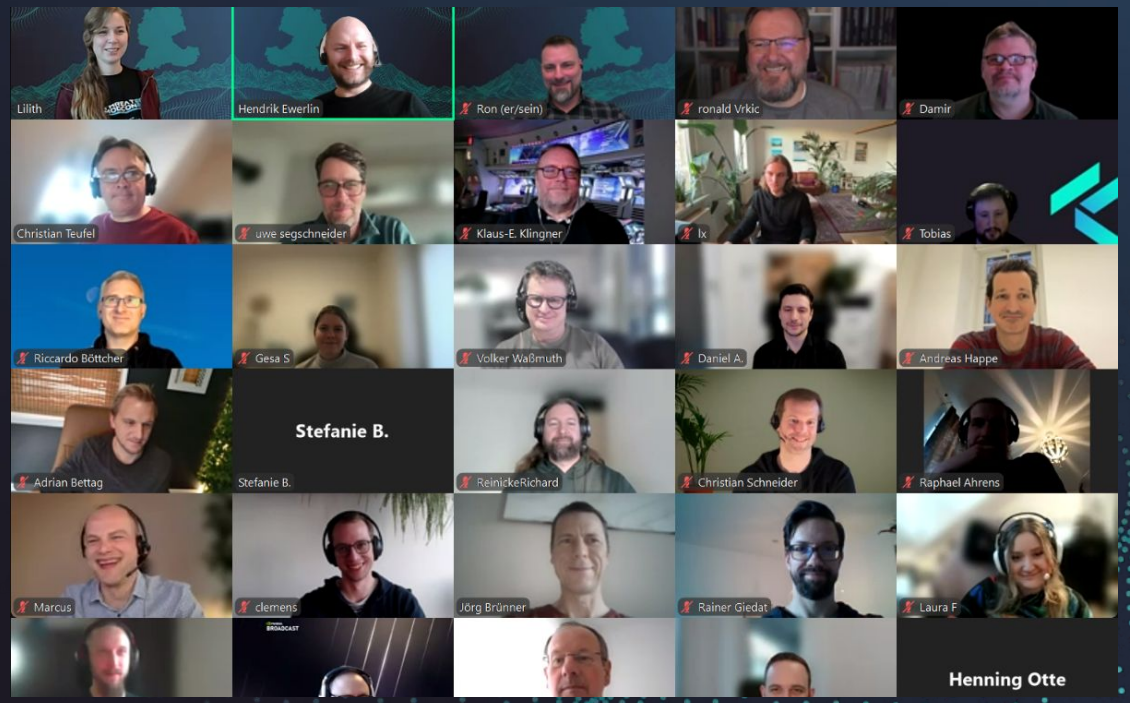
THREAT MODELING CONNECT | POWERED BY IRIUSRISK

TMC DACH

Cyber Resilience Act trifft auf BSI

03.12.2025 17:30 Uhr

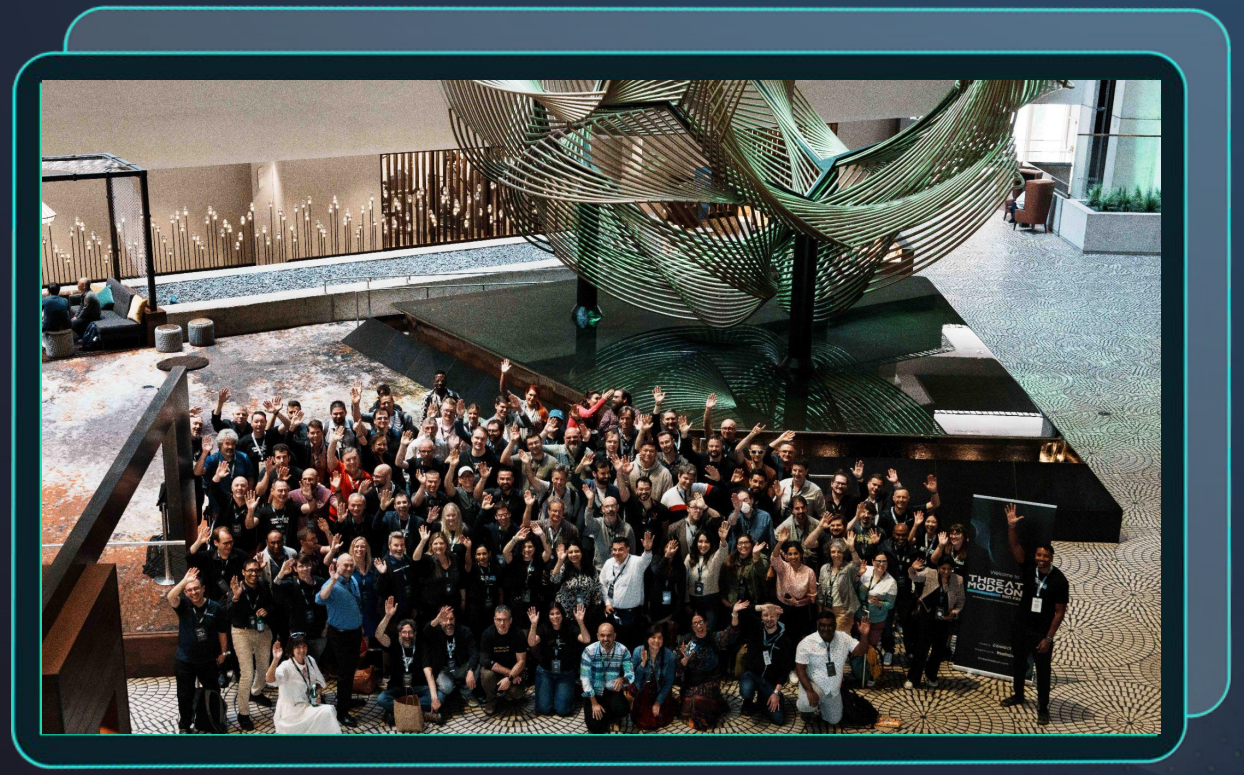
Willkommen zur Threat Modeling Connect (TMC) Gemeinschaft!



THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Wer wir sind

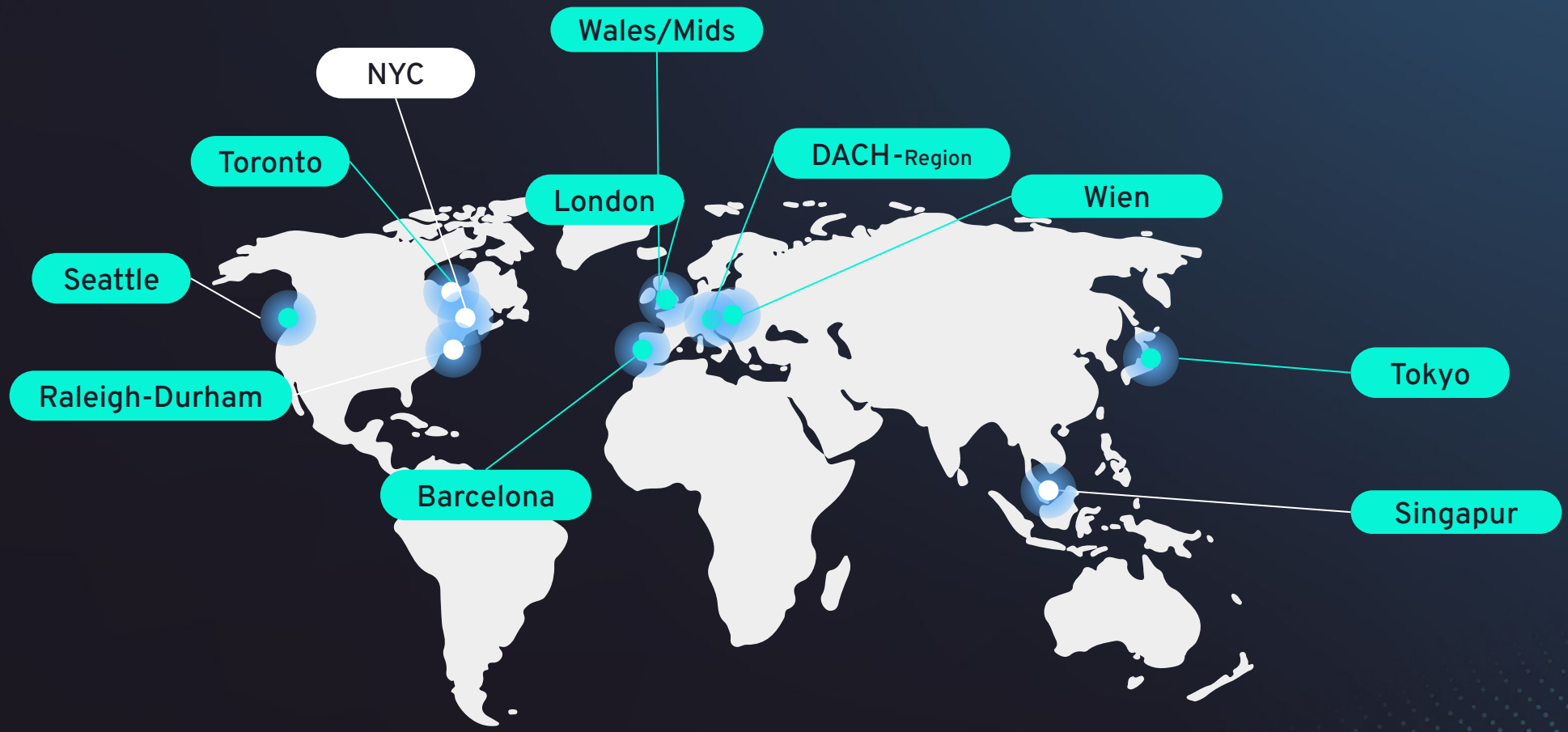
TMC ist eine offene Gemeinschaft für Bedrohungsmodellierung, die von IriusRisk ins Leben gerufen wurde. Sie hat sich zum Ziel gesetzt, die Weichware und Systeme, die die moderne Welt am Laufen halten, durch Bedrohungsmodellierung zu schützen.



TMC
lokale Kapitel / Zweigstellen ;-)

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Kommt bald



THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Was wir tun

脅威モデリング コネクト | 東京

TMC Lokale Treffen

Lokale Veranstaltungen, organisiert von Chapter-Führerinnen und -führern und weltweit im Aufschwung.

THREAT MODCON 2025 BARCELONA

ThreatModCon

Zwei mal im Jahr stattfindende Konferenz mit USA und EU Versionen — die einzige Konferenz mit Fokus auf Bedrohungsanalyse in dem Gebiet.

Threat Modeling Hackathon

Der größte Bedrohungsmodellierungs-Hackathon in der Branche

THREAT MODELING CONNECT | FORUM

TMC Forum

Eine spezialisierte Online-Gemeinschaft von Bedrohungsmodellierenden — echte Profis und Fans von Bedrohungsmodellen.

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Gemeinschafts- und Veranstaltungsförderer

IriusRisk


OLYMPUS
OM-D
VOIGTLÄNDER
NOKTON
25mm F0.95 Type II

Was ist der CRA?

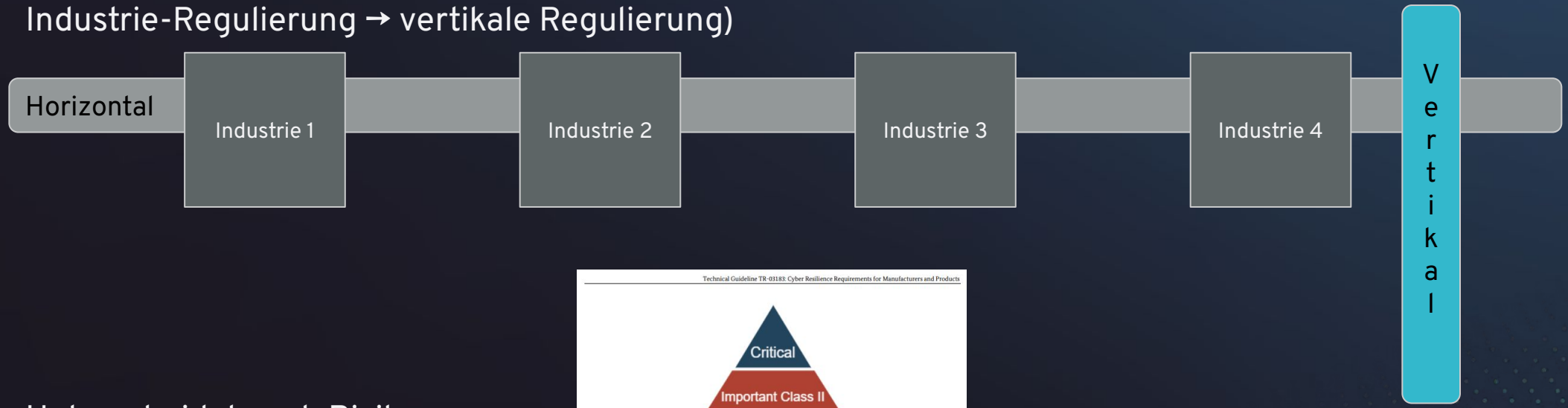
- Europäische Regulierung zur Sicherheit von Produkten mit digitalen Elementen (Products with digital elements)

- Genauer: eine Verordnung
  - gilt unmittelbar in allen EU Staaten
  - keine Umsetzung in nationales Recht notwendig!

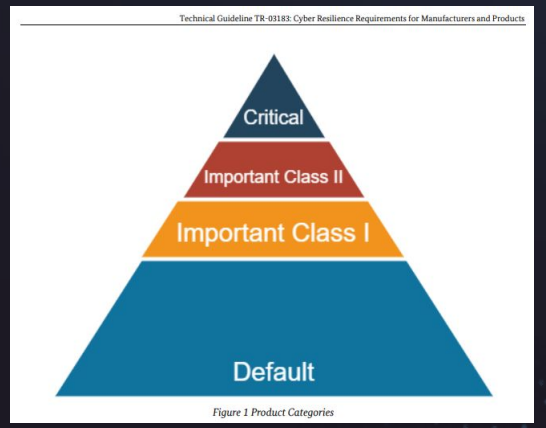
https://european-union.europa.eu/sites/default/files/styles/oe_theme_ratio_3_2_medium/public/2024-08/EU-countries_2_0.jpg?h=ef1d7280&itok=9GsAkAha

Fakten über Cyber Resilience Act

- horizontale Regulierung → Betrifft alle Produkte mit digitalen Elementen (Keine Branchen- oder Industrie-Regulierung → vertikale Regulierung)



- Unterscheidet nach Risikogruppen



Zeitlinie des Cyber Resilience Acts?

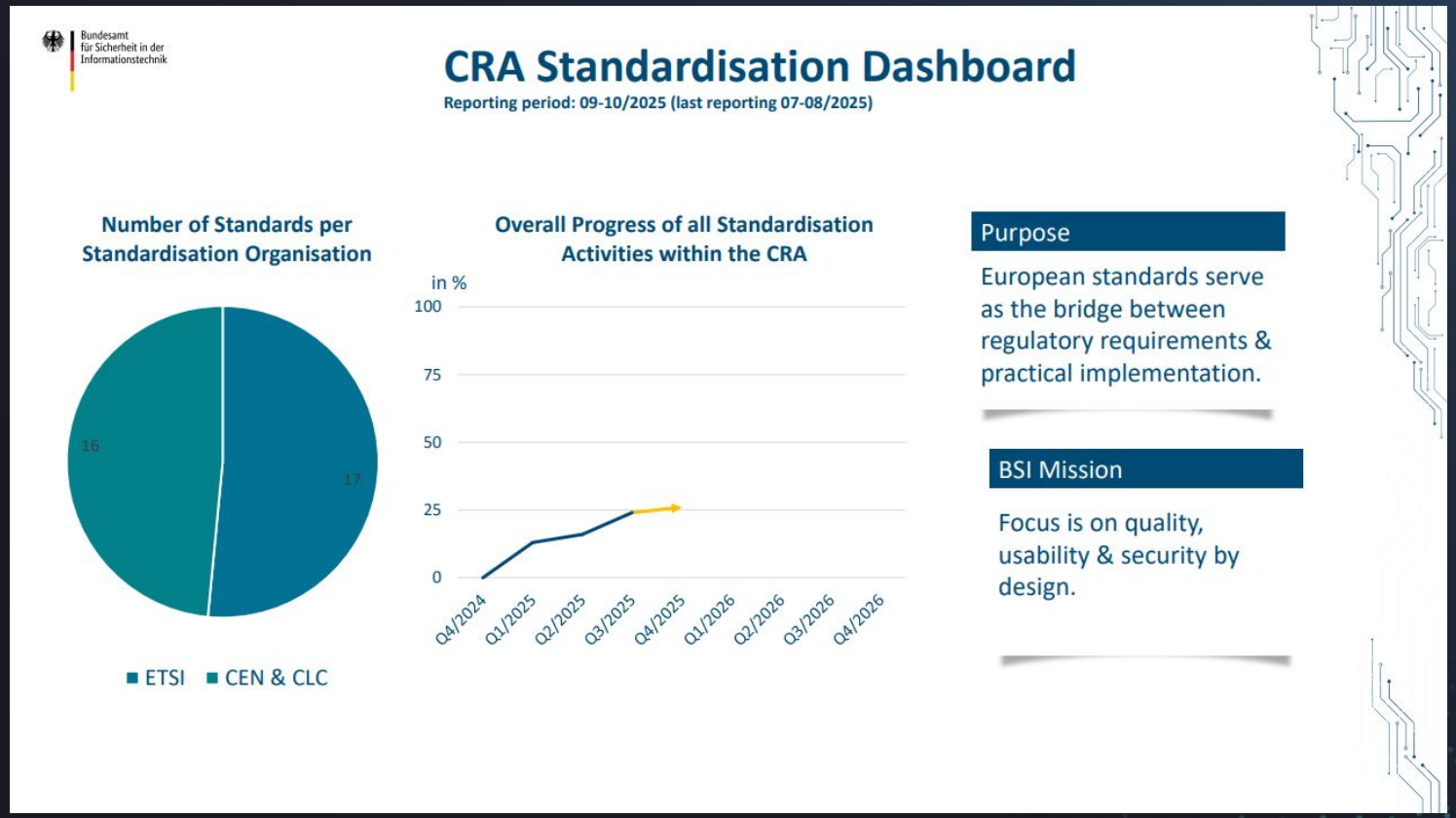
Fakten über Cyber Resilience Act

- Gilt für Hersteller von HW/SW bei der möglichkeit sich mit einem Netzwerk zu verbinden, bei SW betrifft es den Software-”Autor”, aber auch Importeure, etc.

- Ist ergänzend anderen gesetzlichen Vorhaben zu sehen, Ausnahmen für bereits regulierte Produkte wie
  - Medical Devices → Regulation (EU) 2017/745 or under the Regulation (EU) 2017/746 (Article 2(2) CRA)
  - Motor vehicles and their trailers → regulation (EU) 2019/2144 (Article 2(2) CRA)
  - Products with digital elements that are certified in accordance with the common rules in the field of civil aviation, Regulation (EU) 2018/1139 (Article 2(3) CRA)
  - Marine equipment that falls into the scope of Directive 2014/90/EU of the European Parliament and of the Council (Article 2(4) CRA)
  - Aber auch → OSS (keine kommerzielle Intention), Produkte für nationale Sicherheit oder Verarbeitung von geheimen Daten, reine Cloud Dienste (ohne Client Komponente!!!)

- Standardisierungsverfahren sind noch am Laufen

Aktueller Stand der Standardisierung BSI - Dashboard



Aktueller Stand der Standardisierung
BSI - Dashboard

Aktueller Stand der Standardisierung
BSI - Dashboard

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Essentielle Anforderungen des Cyber Resilience Act

Teil I Cybersicherheitsanforderungen in Bezug auf die Eigenschaften von Produkten mit digitalen Elementen

(1) Produkte mit digitalen Elementen werden so konzipiert, entwickelt und hergestellt, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

(2) Auf der Grundlage der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,

a) ohne bekannte ausnutzbare Schwachstellen auf dem Markt bereitgestellt werden,
b) mit einer sicheren Standardkonfiguration auf dem Markt bereitgestellt werden, sofern zwischen dem Hersteller und dem gewerblichen Nutzer in Bezug auf ein maßgeschneidertes Produkt mit digitalen Elementen nichts anderes vereinbart wurde, und die Möglichkeit bieten, das Produkt in seinen ursprünglichen Zustand zurückzusetzen,
c) sicherstellen, dass Schwachstellen durch Sicherheitsaktualisierungen behoben werden können, gegebenenfalls auch durch automatische Sicherheitsaktualisierungen, die als Standardeinstellung innerhalb eines angemessenen Zeitrahmens installiert werden sowie über einen klaren und benutzerfreundlichen Opt-out-Mechanismus verfügen, bei dem die Nutzer über verfügbare Aktualisierungen informiert werden und sie vorübergehend verschieben können;
d) durch geeignete Kontrollmechanismen Schutz vor unbefugtem Zugriff bieten, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, und einen möglicherweise unbefugten Zugriff melden,
e) die Vertraulichkeit gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten schützen, z. B. durch Verschlüsselung relevanter Daten, die gespeichert sind oder gerade verwendet oder übermittelt werden, durch modernste Mechanismen und durch den Einsatz anderer technischer Mittel,
f) die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, ob personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer vom Nutzer nicht genehmigten Manipulation oder Veränderung schützen und deren Beschädigung melden,
g) die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und von Bedeutung sind, und auf das für die Zweckbestimmung des Produkts mit digitalen Elementen erforderliche Maß beschränken („Datenminimierung“),
h) die Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach einem Sicherheitsvorfall, einschließlich über Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe), sicherstellen,
i) die negativen Auswirkungen von den Produkten selbst oder von vernetzten Geräten auf die Verfügbarkeit der von anderen Geräten oder Netzen bereitgestellten Dienste minimieren,
j) so konzipiert, entwickelt und hergestellt werden, dass sie – auch bei externen Schnittstellen – möglichst geringe Angriffsflächen bieten,
k) so konzipiert, entwickelt und hergestellt werden, dass die Auswirkungen eines Sicherheitsvorfalls durch geeignete Mechanismen und Techniken zur Minderung der möglichen Ausnutzung verringert werden,
l) sicherheitsbezogene Informationen durch Aufzeichnung und/oder Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen und Änderungen daran bereitstellen und den Nutzern einen Opt-out-Mechanismus zur Verfügung stellen,
m) den Nutzern die Möglichkeit bieten, alle Daten und Einstellungen dauerhaft sicher und einfach zu löschen, und, wenn diese Daten auf andere Produkte oder Systeme übertragen werden können, sicherstellen, dass dies auf sichere Weise geschieht.

Essentielle Anforderungen des Cyber Resilience Act

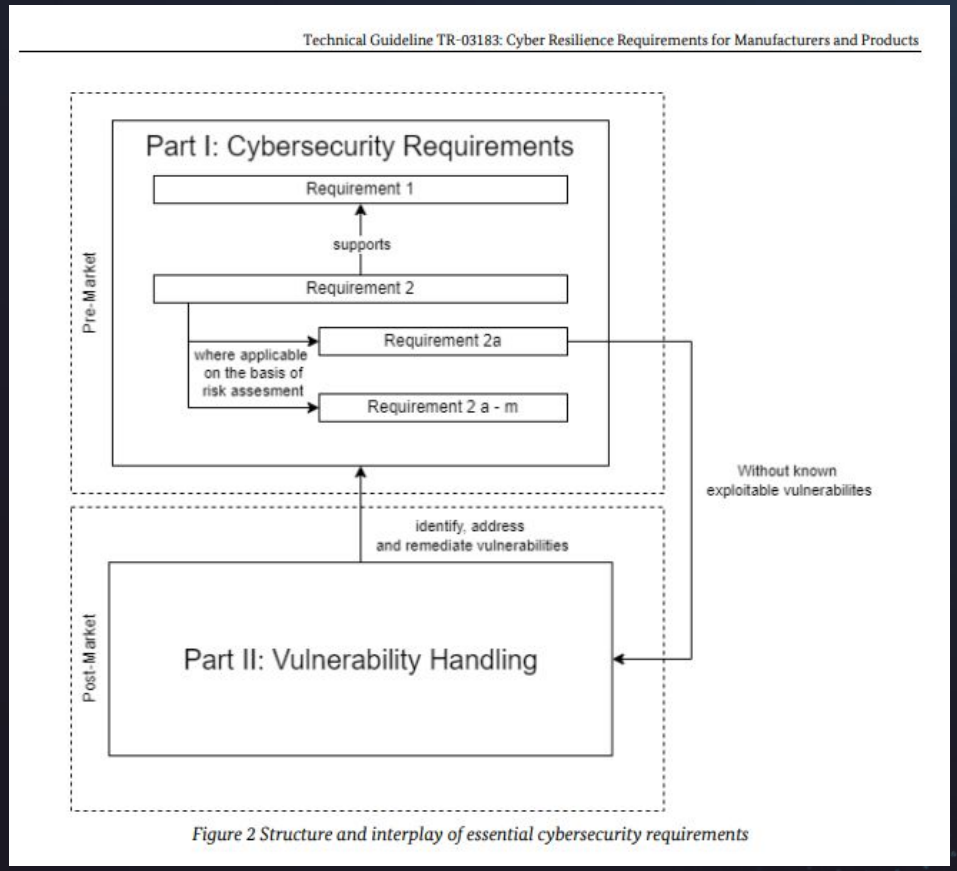


Figure 2 Structure and interplay of essential cybersecurity requirements

Was ist eine Technische Richtlinie (BSI)?

BSI: Das Ziel der technischen Richtlinien des BSI (BSI-TR) ist die Verbreitung von angemessenen IT-Sicherheitsstandards. Sie ergänzen die technischen Prüfvorschriften des BSI und liefern Kriterien und Methoden für Konformitätsprüfungen sowohl der Interoperabilität von IT-Sicherheitskomponenten als auch der umgesetzten IT-Sicherheitsanforderungen.

Ursprünglich haben BSI-TR Empfehlungscharakter; verbindlich werden sie erst, wenn sie durch Gesetze, Verordnungen, Verwaltungsvorschriften oder vertragliche Vorgaben (z. B. in Projekten der Bundesverwaltung oder als Grundlage für BSI-Zertifizierungen und Produktzulassungen) ausdrücklich gefordert oder referenziert werden.

Technische Richtlinie des BSI zum CRA

- **Das Bundesamt für Sicherheit in der Informationstechnik (BSI)**
  - **ist die zuständige Aufsichtsbehörde und notifizierende Behörde für den CRA in Deutschland**
  - **beteiligt sich am Standardisierungsprozess und erarbeitet Technische Richtlinien**

- **Technical Guideline TR-03183: Cyber Resilience Requirements for Manufacturers and Products**
  - Enthält DREI Teile
    - Part 1: General requirements Entwurfsfassung 0.10.0 → **heutiges Thema**
    - Part 2: Software Bill of Materials (SBOM) Version 2.1.0
    - Part 3: Vulnerability Reports and Notifications Version 1.0.0
  - Keine Verpflichtung → ABER geben die Interpretation des CRA durch das BSI wieder
  - Einhaltung garantiert nicht die Einhaltung des CRA
  - Wird durchgehend erweitert und ggf. durch europäische Standardisierung ersetzt

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

TR-03183-1 Version 0.9.0 vs. 0.10.0

0.90 und 0.10.0 sind wie zwei Welten

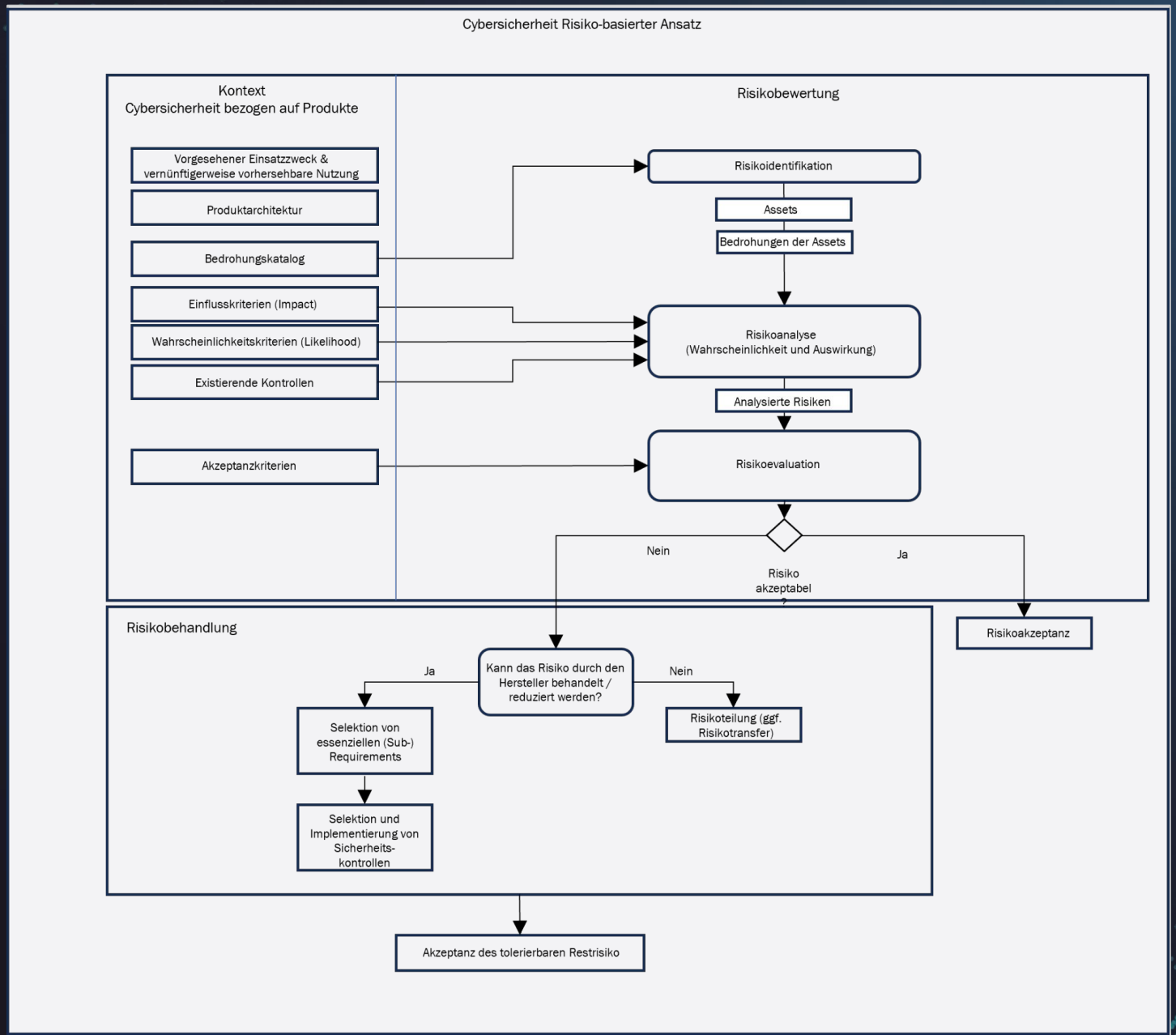
Eindeutiger Fokus auf Risk Assessment und Threat Modelling → Plus Dokumentatíon und Kommunikation für Risk Sharing / Risikoteilung im Vergleich zu Risikotransfer

Zahlen:

Version	**0.9.0**	**0.10.0**
Requirements / Recommendations	33	10 (als Controls auf Prozessaktivitäten)
Erwähnung Threat Modeling	0 x	4 x → Threat Modelling wird zur **Kernaktivität!**

Risikoprozess in der BSI TR-03183-1

THREAT MODELING CONNECT | POWERED BY IRIUSRISK



Controls in Version 0.10.0

Risiko Identifikation

➜ Asset Discovery (Was bauen wir bzw. was verarbeiten / leisten wir?)

➜ Risiko / Bedrohungsidentifizierung (Was kann schief gehen?)

5.8.1.1.3 Control

The manufacturer MUST identify all assets of the PwDE.

➜ Asset-Driven Approach

5.8.1.2.3 Control

The manufacturer MUST identify threats to the assets and the potentially affected components of the PwDE.

-> Bedrohungen aus Sicht von Angreifern aber auch versehentlicher Missbrauch (Misuse). Aber keine absichtlicher Missbrauch wie Jai

Controls in Version 0.10.0

Risikoanalyse → Wie schlimm ist es?

5.8.2.3 Control

The manufacturer MUST analyse the risks of the PwDE in regard to their likelihood and potential impact.

→ **Diskussionswürdig (Blog-Beitrag von Adam Shostack: Risk ist not a Hammer and not all Threats are Nails)**

5.8.3.3 Control

The manufacturer MUST evaluate whether the analysed risks of the PwDE can be accepted or not.

→ **klassische Risikobehandlung (analog ISO 31000) mit Vermeidung, Akzeptanz, Mitigierung, Transfer (Kommunikation)**

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Controls in Version 0.10.0

Risikobehandlung

Evaluation, Design und Implementierung von Kontrollen (Was werden wir dagegen tun?)

5.9.1.3 Control

The manufacturer MUST select applicable essential cybersecurity requirements of Annex I Part I and appropriate controls to treat the evaluated risks and to reduce them to an acceptable level and include the selected controls in the design of the product.

5.9.3.3 Control

The manufacturer MUST implement the selected controls and verify their effectiveness and correctness, in accordance with the associated risk.

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Controls in Version 0.10.0

Risikoteilung - “Betroffene zu Beteiligten machen”

Kommunikation und Verantwortungsübernahme für Restrisiken

5.9.2.1.3 Control → Zulieferer

If sharing risks with a third-party supplier, the manufacturer MUST exercise due diligence by ensuring that the manufacturer of the integrated component is legally obliged, contractually required or otherwise able and willing to treat the risk accordingly.

5.9.2.2.3 Control → User

If sharing the risk with the user, the manufacturer MUST ensure that the shared risks are within the foreseeable expectations of the user and that sufficient guidance documenting the risks and the expected mitigation by the user according to 8 is provided.

→ **Hilft hier Veröffentlichung des Bedrohungsmodells (zumindest teilweise)?**

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Controls in Version 0.10.0

Implementierung von Kontrollen und deren Verifizierung

5.9.3.3 Control

The manufacturer MUST implement the selected controls and verify their effectiveness and correctness, in accordance with the associated risk.

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Controls in Version 0.10.0

Prozessdokumentation - “Papier schwarz machen”

5.10.3 Control

The manufacturer MUST document the results of the risk assessment in a comprehensive manner. This includes the risk context, the evaluated risks including the corresponding implemented controls and shared risks as well as the applicable essential cybersecurity requirements.

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Controls in Version 0.10.0

Überführung in einen Regelkreislauf- “Risikomanagement und Bedrohungsanalyse wird lebende Praxis”

5.11.3 Control

The manufacturer MUST update the risk assessment when the risk context of the PwDE changes and treat new unaccepted risks accordingly.

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Controls in Version 0.10.0

Umfassende User Dokumentation

8.1.1.1 Control

The user documentation related to the PwDE MUST contain the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website with the means to contact the manufacturer

8.1.2.1 Control

The user documentation related to the PwDE MUST contain the name and type and any additional information enabling the unique identification of the PwDE.

8.1.3.1 Control

The user documentation related to the PwDE MUST contain the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates.

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Controls in Version 0.10.0

Umfassende User Dokumentation

8.1.4.1 Control

The user documentation related to the PwDE MUST contain detailed information on the necessary measures during initial commissioning and throughout the lifetime of the PwDE to ensure its secure use.

8.1.5.1 Control

The user documentation related to the PwDE MUST contain detailed information on how modifications to the PwDE can affect the security of data.

8.1.6.1 Control

The user documentation related to the PwDE MUST contain detailed information on how security relevant updates can be installed.

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Controls in Version 0.10.0

Umfassende User Dokumentation

8.1.7.1 Control

The user documentation related to the PwDE MUST contain detailed information on the secure decommissioning of the product with digital elements, including information on how user data can be securely removed.

8.1.8.1 Control

The user documentation related to the PwDE MUST contain detailed information on how the default setting enabling the automatic installation of security updates can be turned off.

8.1.9.1 Control

The user documentation related to the PwDE MUST contain detailed information on where the PwDE is intended for integration into other products with digital elements and the information necessary for the integrator to comply with the essential requirements.

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Was ist noch neu in Version 0.10.0

BSI setzt bei Cybersecurity Controls auf OSCAL

Open Security Control Assessment Language

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Nächste Veranstaltungen

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

TMC DACH "Na und?! Warum ist das sensibel?" TMC DACH Threat Modeling Feierabend

📅 Dienstag, 03.02.26
17:30 Uhr

THREAT MODELING CONNECT | POWERED BY IRIUSRISK

Aufrufe zum Handeln

Wenn du magst...

- Abonniere unseren Kalender
- Slack 1/2: Komm ins TMC Slack
- Slack 2/2: Tritt unserem Kanal #tmc-dach bei
- Komm ins TMC Forum
- Sei bei internationalen TMC-Veranstaltungen dabei (ThreatModCon, Hackathon, ...)
- Melde dich bei uns, wenn du etwas beitragen möchtest