

Cyber Security

Neue Produktcompliance-Anforderungen nach dem
Cyber Resilience Act & Entwicklungen in der Cyber-
Litigation

Dr. Tobias Rothkegel
Christoph Kauffmann

 **The Legal Engine**

Powered by



Ihre Speaker



Dr. Tobias Rothkegel, CIPP/E
Partner / Data & Cyber
Osborne Clarke GmbH & Co. KG

+49 40 55436 4090
tobias.rothkegel@osborneclarke.com



Christoph Kauffmann, LL.M.
Partner / Disputes & Risk
Osborne Clarke GmbH & Co. KG

+49 221 5108 4202
christoph.kauffmann@osborneclarke.com



Contents

Neue Produktregulierung

01 Überblick neue Digitalregulierung / Abgrenzung

02 CRA: Anwendungsbereich

03 CRA: Überblick über Pflichten

Cyber-Litigation

04 Fallgruppen

05 Organpflichten der Geschäftsführung

06 Rechtsprechungsüberblick

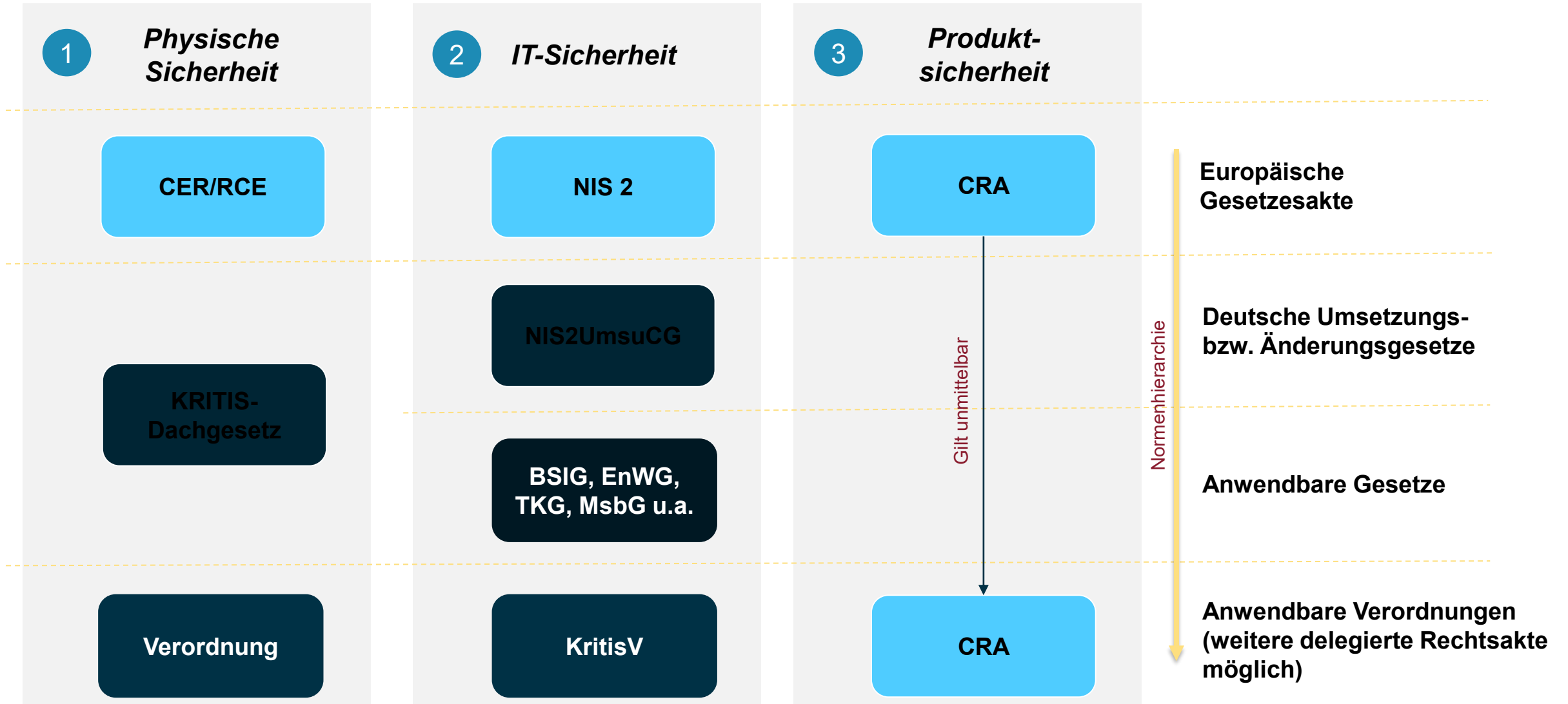
07 Incident Response / Handlungsempfehlungen



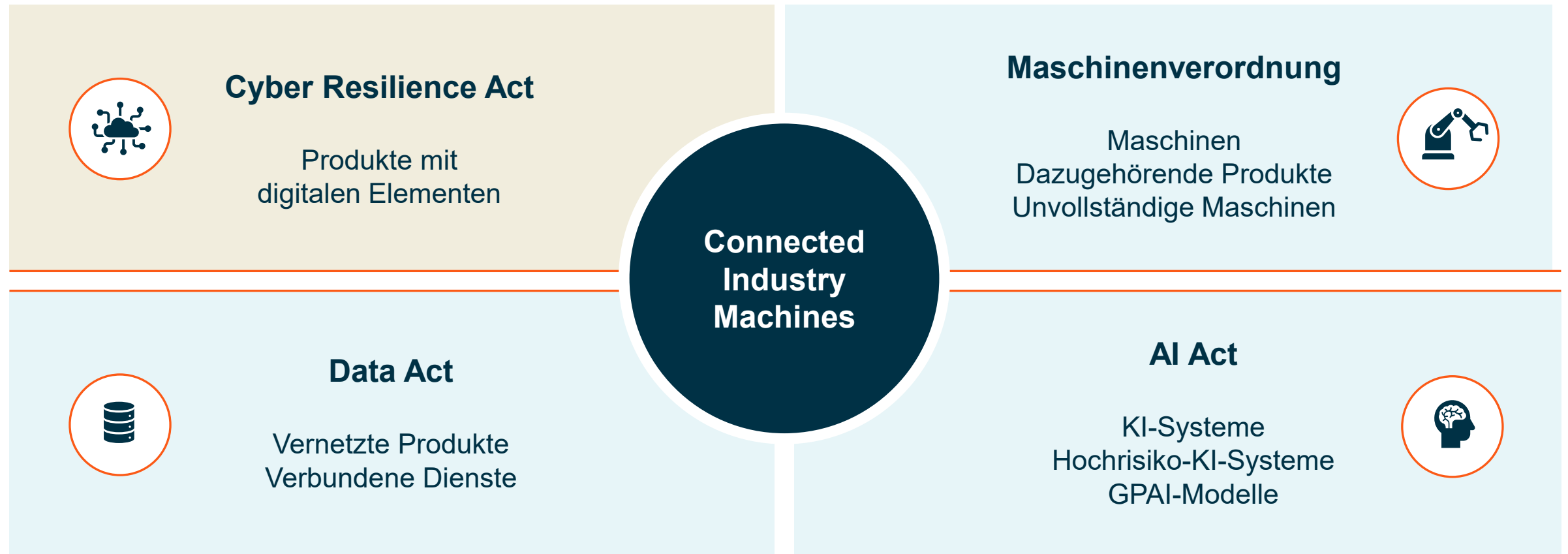
01 Überblick neue Digitalregulierung / Abgrenzung



Übersicht über Cyber-Security Rechtsakte



Übersicht produktbezogene Digitalregulierung



Cyber Resilience Act in a nutshell

- **Ziel:** Erhöhung der **Cybersicherheit vernetzter Produkte** im Binnenmarkt / Individualschutz der Käufer
- **Unmittelbare Geltung** in Mitgliedstaaten für Produkte, die nach dem **11. Dezember 2027** in Verkehr gebracht werden.
- **Achtung: Meldepflichten** gelten bereits ab **11. September 2026** und damit auch für bereits in Verkehr gebrachte Produkte!

Sachlicher Anwendungsbereich

Produkte mit digitalen Elementen



Ausnahmen:

- Medizinprodukte
- In-vitro-Diagnostika
- KFZ
- Luftfahrt
- Militär / nationale Sicherheit

Persönlicher Anwendungsbereich



Hersteller



Händler



Importeure

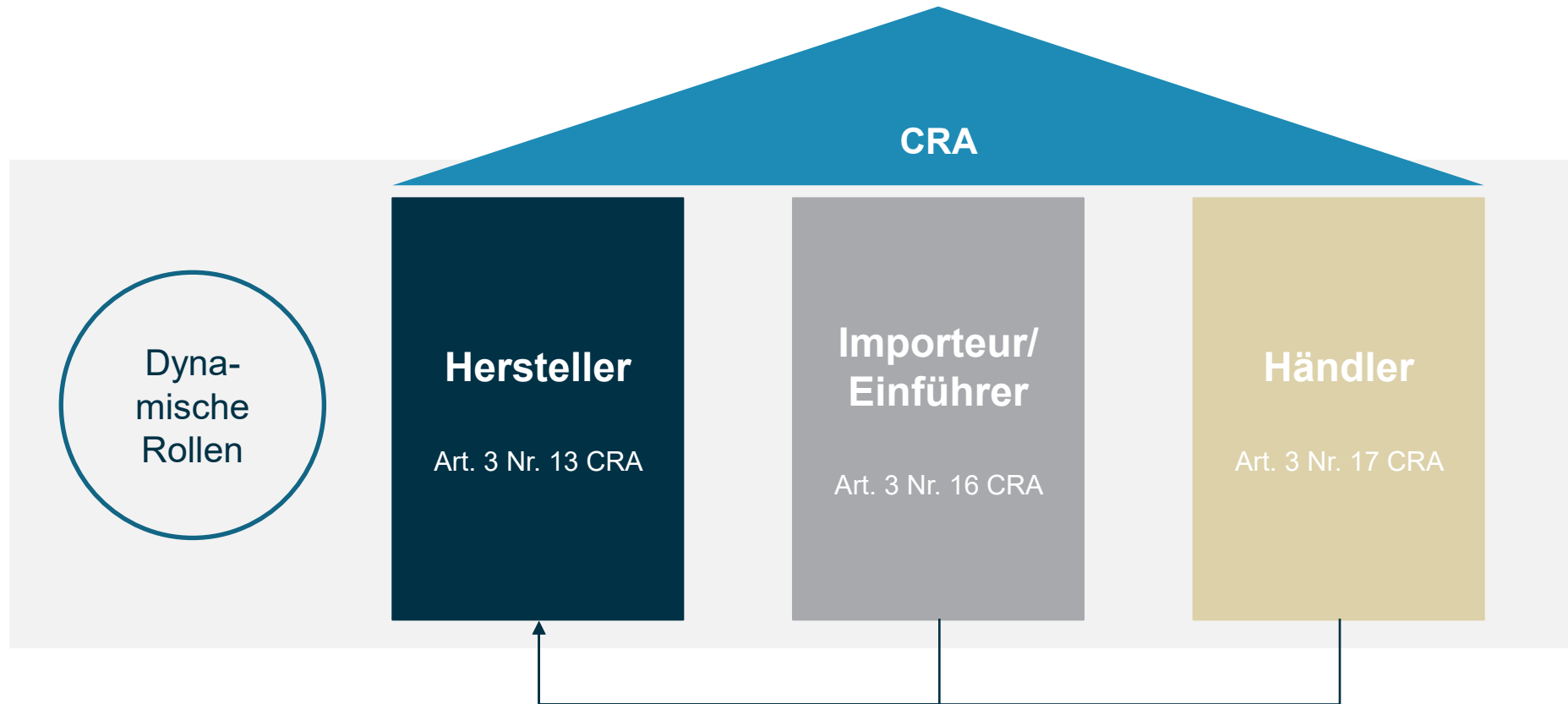
Kernpflichten für Hersteller

- Bewertung der Cyberrisiken des Produkts mit digitalen Elementen
- Erstellen technischer Dokumentation und Beifügen von Gebrauchsanweisungen
- Gewährleistung der Produkteigenschaften und Prozesse nach Anhang I
- Durchführung eines Konformitätsbewertungsverfahrens und Vorhalten der Konformitätserklärung; Produkt mit CE-Kennzeichnung versehen
- Schwachstellenbehebung während der erwarteten Produktlebensdauer (i.d.R. min. 5 Jahre)
- Vorhalten von Sicherheitsupdates für mindestens 10 Jahre

02 CRA: Anwendungsbereich

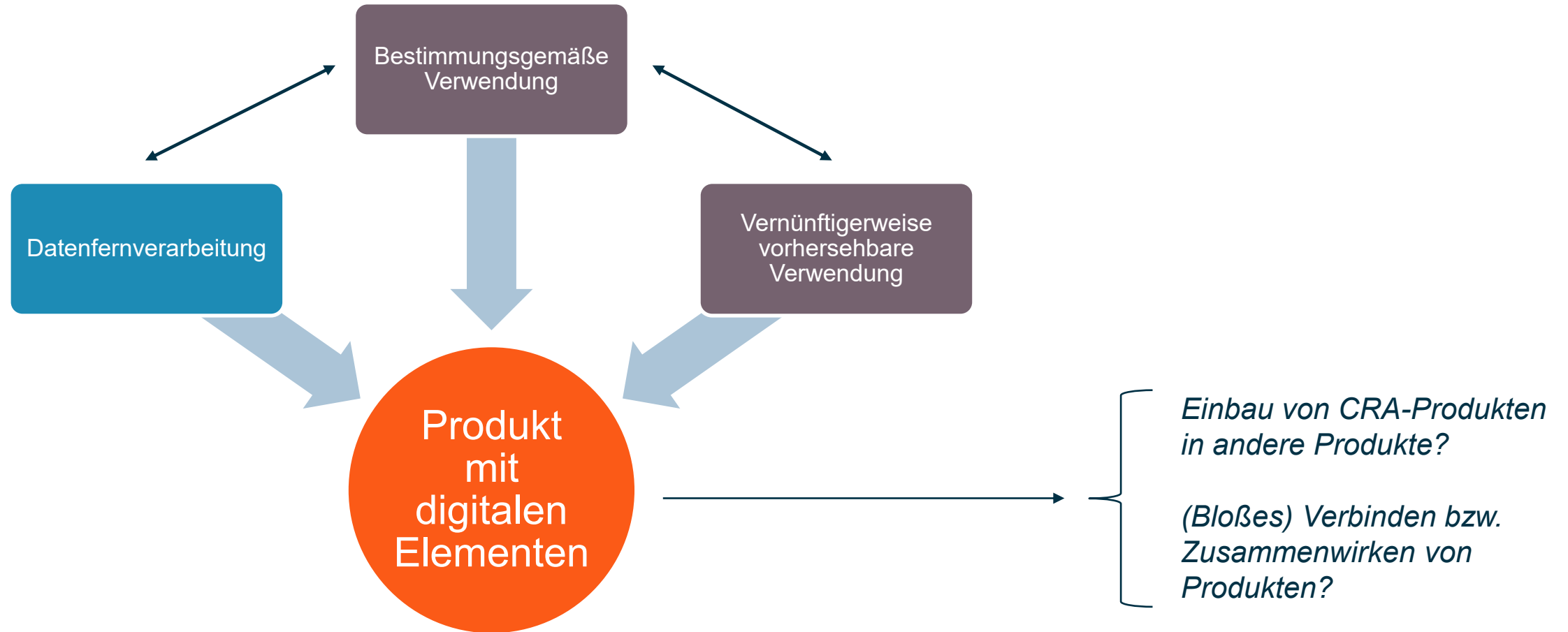


Persönlicher Anwendungsbereich des Cyber Resilience Acts



Importeure und Händler werden zum Hersteller, wenn sie ein Produkt unter ihrem Namen oder ihrer Marke in Verkehr bringen oder ein bereits in Verkehr gebrachtes Produkt wesentlich verändern.

Maßgebliche Faktoren für Anwendbarkeit des CRA



Was ist ein *Produkt* im Sinne des Cyber Resilience Acts?

- **Produkt mit digitalen Elementen**, „dessen bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt“ (Art. 2 Abs. 1 CRA)
- „Ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden“ (Art. 3 Nr. 1 CRA)

 Hardware	 Software	 Datenfernverarbeitung
• IoT-Geräte • Wearables • Vernetzte Industriemaschinen	• Apps • Betriebssysteme • Anwendungs-Software / SaaS?	+ Cloud-Funktionen von Apps oder Smart-Home Geräten

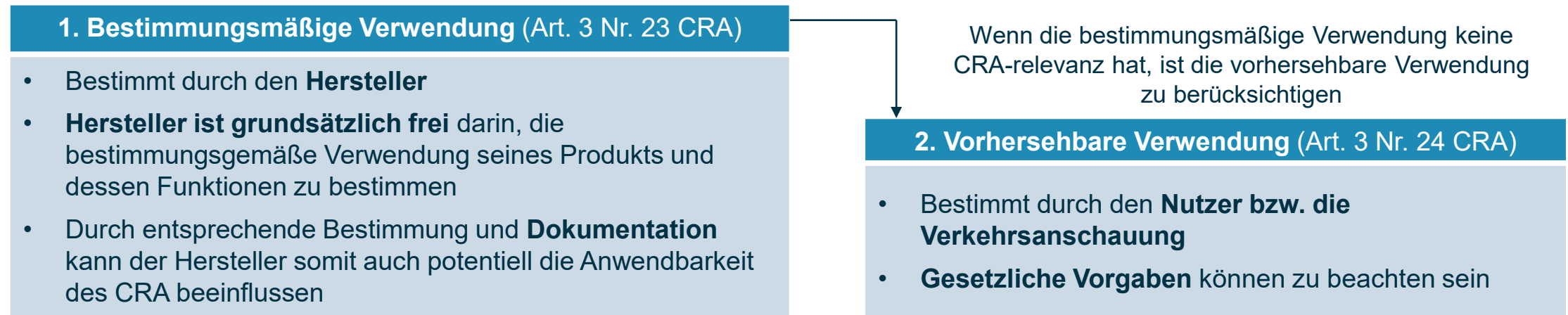


Was aber ist das *Produkt*?

- Insb. relevant bei **Zusammenwirken mehrere Komponenten**
- Keine Definition im CRA (auch nicht in Erwägungsgründen)
- Vergleichbarer Maßstab aus dem ProdHaftG und dem ProdSiG? Eher (-)
- Für CRA maßgeblich: *Bestimmungsgemäße bzw. vorhersehbare Verwendung eines Produkts* (vgl. nächste Slide)

Bestimmungsgemäße vs. vorhersehbare Verwendung

- **Bestimmungsgemäße Verwendung:** „die Verwendung, für die ein Produkt mit digitalen Elementen laut Hersteller bestimmt ist, einschließlich der besonderen Nutzungsumstände und Nutzungsbedingungen entsprechend den Angaben des Herstellers in der Gebrauchsanleitung, im Werbe- oder Verkaufsmaterial und in Erklärungen sowie in der technischen Dokumentation“
- **Vernünftigerweise vorhersehbare Verwendung:** „eine Verwendung, die nicht unbedingt der vom Hersteller in der Gebrauchsanleitung, im Werbe- oder Verkaufsmaterial und in Erklärungen und der technischen Dokumentation angegebenen Zweckbestimmung entspricht, die sich aber aus einem vernünftigerweise vorhersehbaren menschlichen Verhalten oder aus technischen Vorgängen oder Wechselwirkungen wahrscheinlich ergibt“



Einbindung von CRA-relevanten Komponenten in andere Produkte

Grundsatz: Beide Produkte werden unabhängig voneinander betrachtet
(Art. 7 Abs. 1 CRA und dem Erwägungsgrund 35)

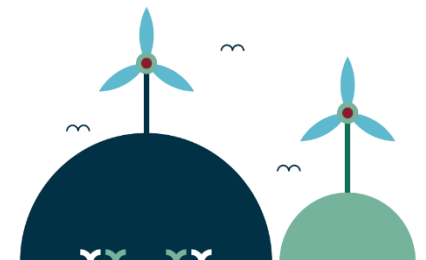
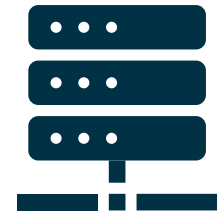
- Sowohl die eingebundene Komponente als auch das Produkt können jeweils **eigenständige Produkte mit digitalen Elementen** nach dem CRA sein (ggf. von unterschiedlichen Herstellern)
- In der Regel treffen den **Hersteller des zweiten Produkts** die **Händlerpflichten in Bezug auf das erste Produkt**
- **Das neu entstehende Produkt ist genuin danach zu bewerten, ob es CRA-Relevanz aufweist.**

Entscheidend ob neu entstehendes Produkt CRA-Relevanz hat, ist, ob durch den Einbau ein neues *Produkt mit digitalen Elementen* entsteht, oder die Produkte lediglich miteinander verbunden werden

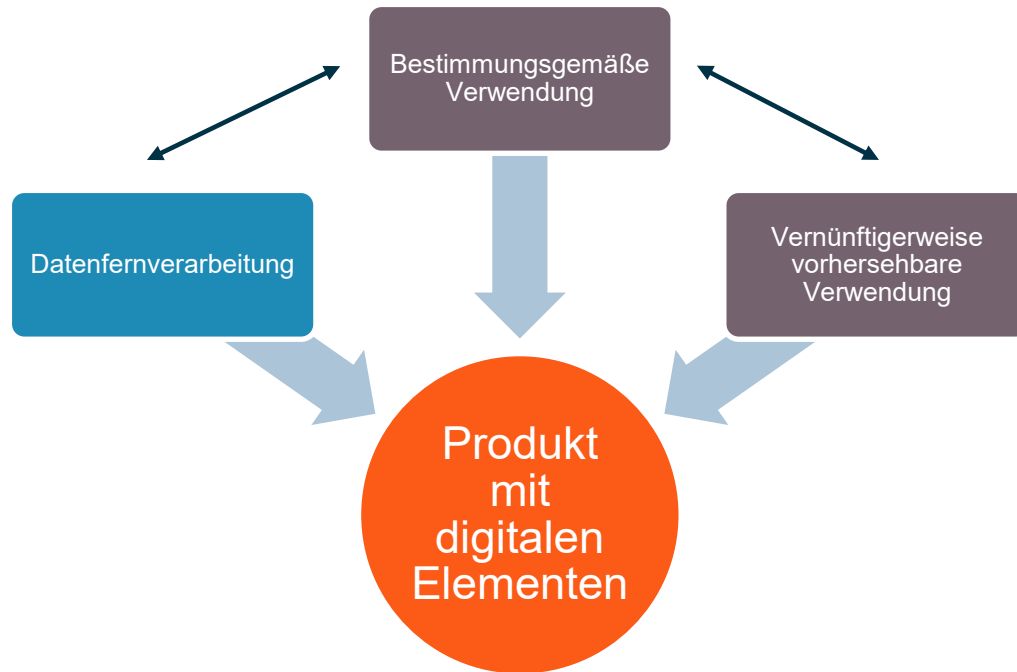
-> **Maßstab: bestimmungsgemäße oder vorhersehbare Verwendung!**

Beispiel: Einbau eines **Konnektivitätsmoduls in ein physisches Produkt**, sodass eine externe Kommunikation (Fernüberwachung oder -steuerung) ermöglicht wird

- Entsteht hierdurch ein neues *Produkt* dessen (bestimmungsgemäße) Funktionen auch die entstandene (Fern-)Kommunikation umfassen? Oder:
- Erfüllt das physische Produkt seine (bestimmungsgemäße) Verwendung auch ohne diese Kommunikation?

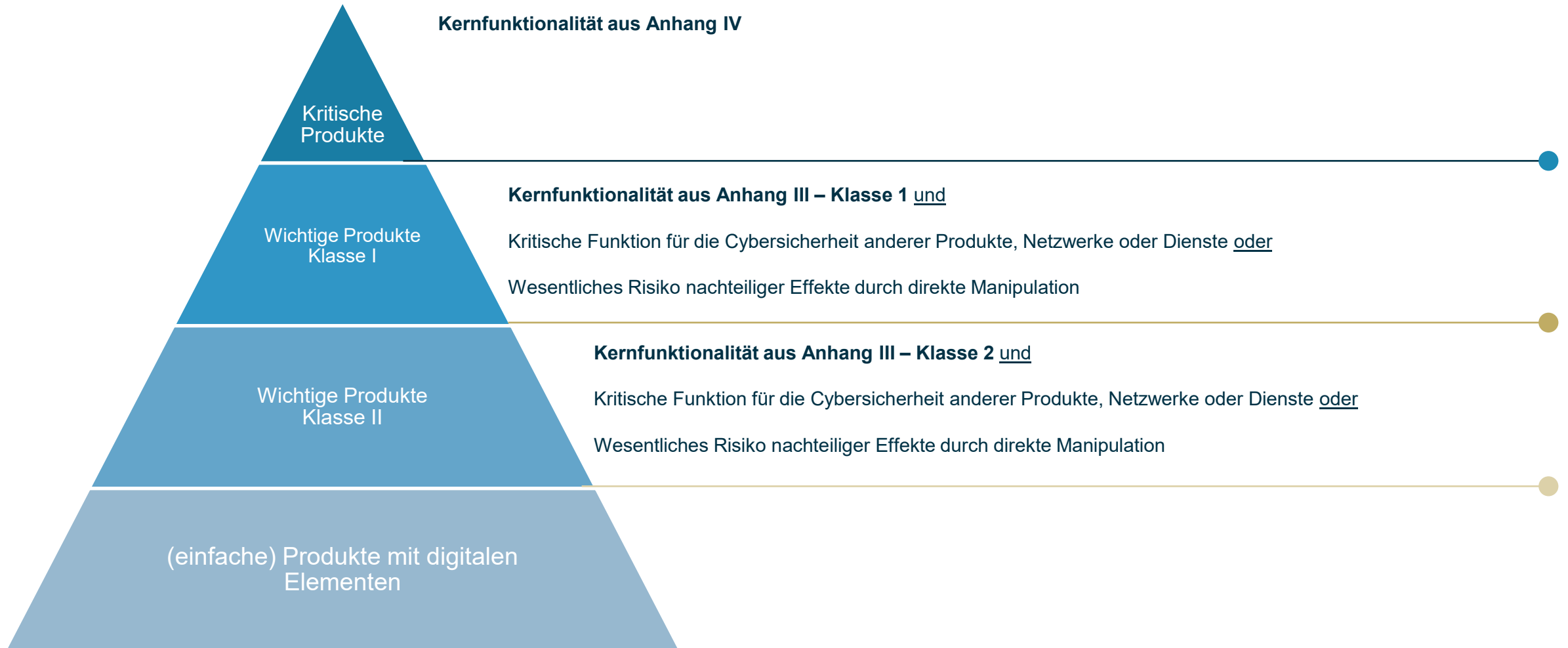


Zusammenfassung



- *CRA enthält keine Definition davon, was unter „Produkt“ zu verstehen ist*
- *Bewertung der Anwendbarkeit des CRA teilweise sehr einfach, teilweise sehr komplex (insb. bei Einbau oder Zusammenwirken von Komponenten).*
- *Grundsätzlich kann jegliche Art Hardware oder Software unter den CRA fallen (SaaS nur mit Client-Software betroffen)*
- *Entscheidend ist bestimmungsgemäße Verwendung eines Produkts (Gestaltungsmöglichkeiten für Hersteller!)*
- *Voraussichtlich vorhersehbare Verwendung bleibt zu berücksichtigen*
- *Unklar ob Datenfernverarbeitung konstitutiv für Anwendbarkeit des CRA ist (eher nein)*
- *Bei Einbau von CRA-relevanten Komponenten ist jedes Produkt gesondert zu bewerten*

Kategorien von Produkten mit digitalen Elementen



Wichtige Produkte mit digitalen Elementen

Klasse I

-  Software für Identitätsmanagementsysteme
-  eigenständige und eingebettete Browser;
-  Passwort-Manager
-  Suche, Entfernung und Quarantäne von Schadsoftware
-  VPN-Funktionen
-  Netzmanagement, physische und virtuelle Netzwerkinterfaces
-  SIEM
-  Boot Manager
-  Public Key / Digital Certificate Issuance Infrastruktur
-  Betriebssysteme
-  Router, Modems und Switches
-  Mikroprozessoren/-controller mit sicherheitsrelevanter Funktion

-  Application specific integrated circuits (ASIC) und field-programmable gate arrays (FPGA) mit sicherheitsrelevanter Funktion
-  Smart home virtual assistants und smart home Produkte mit sicherheitsrelevanter Funktion
-  Mit dem Internet verbundene Spielzeuge mit sozialen interaktiven Features oder Location Tracking
-  Wearables mit Gesundheitstracking oder zur Nutzung durch Kinder

Klasse II

-  Hypervisoren und Container-Runtime-Systeme, die eine virtualisierte Ausführung von Betriebssystemen und ähnlichen Umgebungen unterstützen
-  Firewalls und Intrusion Detection bzw. Prevention Systems
-  Tamper-resistant Mikroprozessoren/-controller

Kritische Produkte mit digitalen Elementen

Kritische Produkte

-  Hardware mit Security Boxes
-  Smart meter gateways
-  Andere Geräte für fortgeschrittene Sicherheitszwecke (z.B. Cryptoprocessing)
-  Smartcards und ähnliche Geräte



Europäische Kommission darf die Liste der wichtigen und kritischen Produkte durch delegierte Rechtsakte ergänzen und spezifizieren.

Konformitätsbewertungsverfahren

Selbstkontrolle	EU-type examination procedure	Umfassende Qualitätssicherung	European cybersecurity certification 
• Hersteller gewährleistet und erklärt auf eigene Verantwortung, dass Produkt genüge den Anforderungen in Anhang I.1 und erfülle die Anforderungen von Anhang I.2 • Hersteller erstellt technische Dokumentation • Hersteller trifft alle erforderlichen Maßnahmen, um Konformität zu gewährleisten • Hersteller bringt CE-Kennzeichnung an Produkt an (Produktwebseite genügt) • Hersteller gibt schriftliche EU-Konformitätserklärung ab und hält sie für 10 Jahre ab Inverkehrbringen vor	• Notifizierende Stelle untersucht Konzeption und Entwicklung des Produkts und bescheinigt Konformität mit Anhang I • Bewertung erfolgt auf Grundlage der technischen Dokumentation und ggf. zusätzlicher Nachweise • Nach Abschluss erhält Hersteller Prüfbescheinigung und hält sie mit allen Anhängen und der technischen Dokumentation für 10 Jahre ab Inverkehrbringen auf • Hersteller bringt CE-Kennzeichnung und Prüfbescheinigung an Produkt an (Produktwebseite genügt)	• Hersteller betreibt ein Qualitätssicherungssystem • Hersteller beantragt bei notifizierender Stelle die Bewertung seines QS-Systems • Hersteller verpflichtet sich zur Einhaltung und Neubewertung bei wesentlichen Änderungen • Notifizierende Stelle überwacht QS-System regelmäßig • Auf Grundlage von QS-System bringt Hersteller CE-Kennzeichnung an und gibt Konformitätserklärung ab	Option für wichtige Produkte Klasse II Verpflichtend für kritische Produkte
Option für alle Produkte			

03 CRA: Überblick über Pflichten



Anforderungen an Prozesse

Anlage I



Risikobewertung
und Umsetzung
von Maßnahmen



Due Diligence
Drittkomponenten



Erstellen und
Pflegen von
SBOM



Technische
Dokumentation
erstellen / pflegen



Konformitäts-
verfahren

Entwicklung / Produktion



Updatefähige
Architektur



Sichere
Distributionswege



Strategie für
Offenlegung



Meldestelle
etablieren



Pflichtinformationen /
Nutzerhinweise

Anforderungen an Prozesse



Regelmäßiges
Update
Risikobewertung



Regelmäßige
Überprüfung
der Sicherheit



Schwachstellen-
management und
-dokumentation



Sichere Standard-
konfiguration



Schwachstellen
entspr. Strategie
veröffentlichen

Vertrieb / Lifecycle

Deprecation



Bereitstellung
Sicherheitsupdates
~5+ Jahre

Kostenlos, es sei
dann tailor-made



Bereitstellung
Dokumentation,
Pflichtinformationen
und Nutzerhinweise



Aufrechterhalten
der Konformität
für ~5+ Jahre



Meldungen von
Schwachstellen
und schweren
Vorfällen

Art. 13 Abs. 10: Keine weitere
Updatepflicht für Altversionen, wenn:

- Wesentlich veränderte neue Version veröffentlicht
- Nutzer haben kostenlos Zugriff auf die neue Version
- Nutzung der neuen Version führt nicht zu zusätzlichen Kosten, um Hardware- oder Softwareumgebung anzupassen

Meldepflichten – Hersteller (Art. 14)

- Gelten ab dem 11. September 2026!
- Für alle sachlich erfassten Produkte, die bereits auf dem Markt sind!

Meldepflicht an **gemeinsame Meldestelle** des nationalen Computer-Notfallteams (CSIRT) und ENISA von:

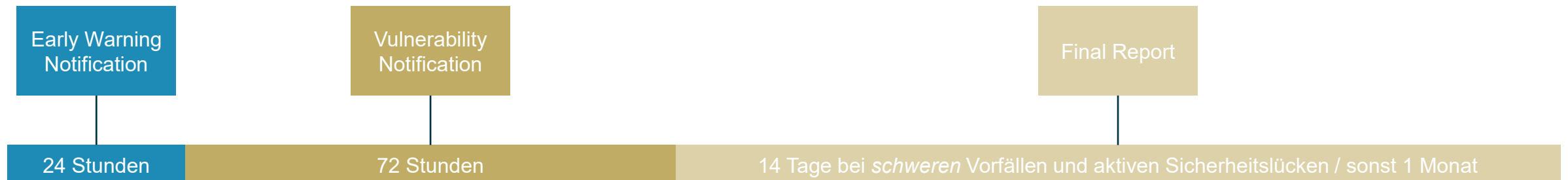
- Aktiv ausgenutzten Schwachstellen (Art. 3 Nr. 42 CRA):

eine Schwachstelle, zu der verlässliche Nachweise dafür vorliegen, dass ein böswilliger Akteur sie in einem System ohne Zustimmung des Systemeigners ausgenutzt hat

- Vorfälle mit Auswirkungen auf Sicherheit von Produkten mit digitalen Elementen (Art. 3 Nr. 44 CRA):

einen Sicherheitsvorfall, der sich negativ auf die Fähigkeit eines Produkts mit digitalen Elementen auswirkt oder auswirken kann, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Funktionen zu schützen

- Meldung muss ebenfalls an **betroffene**, und *gegebenenfalls* an **alle Nutzer** des Produkts erfolgen (Art. 14 Abs. 8 CRA).



Meldepflichten – FAQ

- Schwachstellen in integrierten Komponenten sind ebenfalls zu melden (ggf. auch vom Komponentenhersteller wenn Komponente aus sich heraus auch CRA-relevant ist).
- Hersteller müssen Kontaktstelle einrichten, an die Schwachstellen gemeldet werden können. Schwachstellen können Herstellern aber auch auf anderen Wegen bekannt werden (etwa durch Threat Intelligence Reports)
- Gilt für alle CRA-relevanten Produkte, die bereits auf dem Markt sind.
- Gilt grundsätzlich auch für alle Versionen, z.B. einer Software (Gegenteil grundsätzlich argumentierbar, arg ex. Art. 13 Abs. 10 CRA).
- ABER: Gilt nur für Schwachstellen, die nach dem 11. September 2026 bekannt werden.

04

Typische Fallgruppen



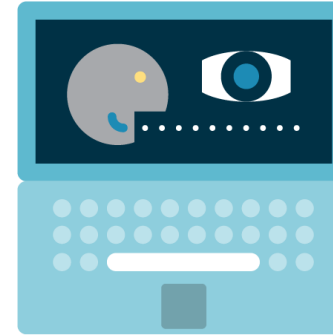
Typische Fallgruppen – Praxis



Business E-Mail Compromise

Manipulation von Zahlungsdaten
im E-Mail-Verkehr → fehlerhafte
Überweisung

Anspruchsgrundlagen: U.a. § 362
BGB (Erfüllung –); Art. 82 DSGVO;
vertragliche Nebenpflichten



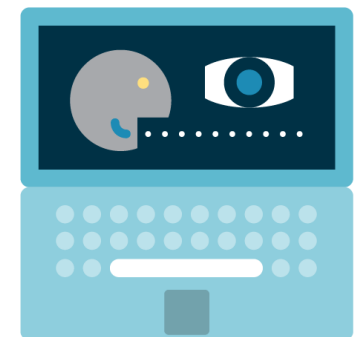
Datenschutzverletzung/Datenleck

Angriff auf Verantwortliche oder
Auftragsverarbeiter → Abfluss
personenbezogener Daten

Anspruchsgrundlage: U.a. Art. 82
DSGVO, § 823 BGB

Typische Fallgruppen - Angriffsvektoren

- Phishing & Social Engineering
- Ransomware-Angriffe
- DDoS-Angriffe (Distributed Denial of Service)
- Datenpannen & Insider-Bedrohungen
- Supply-Chain-Angriffe



05 Rechtsprechungsüberblick



OLG Karlsruhe | B2B-Rechnungsmanipulation

Sachverhalt:

- Kaufvertrag über gebrauchten Pkw; Parteien: zwei Unternehmen (B2B)
- Klägerin (Verkäuferin) übersandte Rechnung per E-Mail
- Hacker fingen E-Mail ab; zweite E-Mail mit gefälschter IBAN → Käuferin überwies 13.500 € auf Drittkonto
- DSGVO: nicht anwendbar (keine personenbezogenen Daten natürlicher Personen in der Rechnung)



Entscheidung:

§ 362 Abs. 1 BGB: Zahlung erfüllt die Schuld nicht

Keine Pflicht zur E2E-Verschlüsselung mangels Verkehrsüblichkeit im B2B-Bereich

Hilfsweise: erhebliches Mitverschulden der Käuferin (§ 254 BGB)

OLG Schleswig | B2C-Rechnungsmanipulation – Abweichende Linie

Sachverhalt:

- Werkvertrag; Klägerin = Unternehmerin;
Beklagte = Verbraucherin
- Schlussrechnung über 15.385 € per E-Mail;
Hacker manipulierten IBAN
- Beklagte überwies auf Drittkonto; Klägerin
verlangt erneute Zahlung
- DSGVO: anwendbar (personenbezogene
Daten der Verbraucherin in der Rechnung)

Entscheidung:

§ 362 BGB: Zahlung erfüllt die
Schuld nicht

Verstoß gegen Art. 5, 24, 32
DSGVO:

Transportverschlüsselung
unzureichend

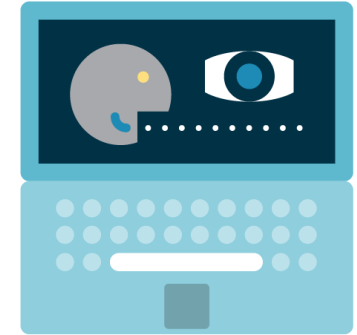
E2E-Verschlüsselung = „Mittel der
Wahl“ bei hohem finanziellem
Schadensrisiko

Kein Mitverschulden der
Verbraucherin (§ 254 BGB –)

LG Koblenz | B2C – Art. 82 DSGVO und Mitverschulden

Sachverhalt:

- Werkvertrag (Zaunbauarbeiten); Kläger = Handwerker (Unternehmer), **Beklagter = Privatmann (Verbraucher)**
- Pauschalpreis 11.000 €; E-Mail-Kommunikation über GMX-Account
- Hacker kompromittieren GMX-Account des Klägers; drei Folge-E-Mails mit falscher IBAN
- Beklagter überweist 11.000 € in zwei Raten auf Drittkonto



Entscheidung:

§ 362 BGB: keine Erfüllung

Art. 82 DSGVO: Haftung dem Grunde nach bejaht (unzureichende TOMs)

Aber: **erhebliches Mitverschulden** des Beklagten (§ 254 BGB) wegen erkennbarer „Red Flags“



OVG Münster | Kein Anspruch auf E2E-Verschlüsselung aus Art. 32 DSGVO

Sachverhalt:

- Antragsteller = Unternehmer (Sprengstoffhandel); im Transparenzregister eingetragen
- Antragsgegnerin = Bundesanzeiger Verlag GmbH (registerführende Stelle)
- Antragsteller verlangt im einstweiligen Rechtsschutz: ausschließliche Verarbeitung seiner Daten mit E2E-Verschlüsselung
- Begründung: erhöhtes Entführungs-/Raubrisiko infolge beruflicher Tätigkeit

Entscheidung:

Kein Anspruch aus Art. 18 DSGVO (Einschränkung der Verarbeitung)

Art. 32 DSGVO: kein Gebot eines bestimmten Verschlüsselungsverfahrens

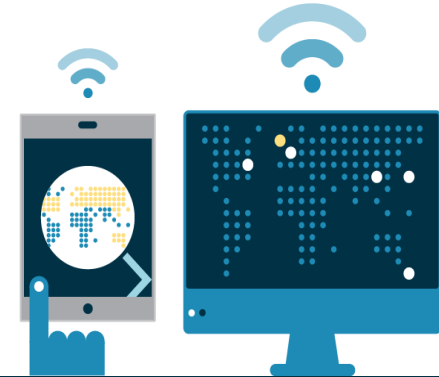
TLS + weitere TOMs + BSI-Zertifizierung = ausreichendes Gesamtsicherheitsniveau

Erhöhtes Sonderrisiko nicht glaubhaft gemacht (§ 920 Abs. 2 ZPO)

LG Krefeld | Kein schuldhafter DSGVO-Verstoß bei Zero-Day-Exploit

Sachverhalt:

- Klägerin = Verbraucherin (Riester-Vertragsnehmerin bei beklagtem Versicherungsunternehmen)
- Beklagte zu 2) = Auftragsverarbeiterin, einsetzende Software: „MOVEit“ (marktführend)
- 31.5.2023: Zero-Day-Exploit auf MOVEit → Abfluss von Name, Adresse, Geburtsdatum, Steuer-ID, Sozialversicherungsnummer
- Ca. 2.500 Unternehmen weltweit betroffen



Entscheidung:

Kein schuldhafter Verstoß gegen Art. 24, 32 DSGVO

Zero-Day + keine Vorwarnzeichen + marktführende Software → keine Pflichtverletzung feststellbar

Kein Anscheinsbeweis aus erfolgreichem Angriff

→ Klage abgewiesen

SG Nürnberg | Kein Schaden bei fehlender Kenntnis vom Datenverlust

Sachverhalt:

- Klägerin = 2018 geborenes Kind; gesetzlich krankenversichert (Beklagte zu 1); Bonusprogramm-Teilnahme
- Beklagte zu 2) = Auftragsverarbeiterin mit MOVEit-Software (identischer Exploit wie LG Krefeld)
- Betroffene Daten: Name, Bankkonto der Mutter, Krankenversicherungsnummer, Prämienbetrag
- In der mündlichen Verhandlung: Kind hatte keine Kenntnis vom Datenleck

Entscheidung:

Kein schuldhafter Verstoß (wie LG Krefeld)

Darüber hinaus: **kein nachweisbarer immaterieller Schaden**, weil die Klägerin keine Kenntnis vom Vorfall hatte

Vortrag zu Ängsten war lebensfremd und unsubstantiiert

LG Köln | Haftung wegen Verstoßes gegen Kontrollpflicht nach Art. 28 DSGVO

Sachverhalt:

- Klägerin = Nutzerin eines Musikstreaming-Dienstes (Verbraucherin); Beklagte = Streaming-Plattform (Verantwortliche, ca. 16 Mio. aktive Nutzer weltweit)
- Auftragsverarbeiter (Kundenverwaltungsdienst): Vertrag bis Ende 2020
- Nach Vertragsende: Beklagte holte keine Bestätigung der vollständigen Datenlöschung ein
- 2022: Hack des früheren Dienstleisters → Kundendaten im Darknet



Entscheidung:

Pflichtverletzung aus Art. 28 Abs. 3 DSGVO: unterlassene Löschungskontrolle

Haftung nach Art. 82 DSGVO

Immaterieller Schaden (Kontrollverlust): 100 € zugesprochen

LG München I | ISO-27001-Zertifikat schützt nicht vor Einzelpflichtverstößen

Sachverhalt:

- Kläger = Verbraucher (Kunde der Beklagten)
- Beklagte = Wertpapierinstitut (digitale Vermögensverwaltung, ISO-27001-zertifiziert)
- Ehemaliger IT-Dienstleister (Vertragsende: 2015); Zugangsdaten nach Vertragsende **nie geändert**
- 2020: Angreifer nutzen alte Zugangsdaten → 389.000 Datensätze (33.200 Kunden) entwendet (inkl. Ausweiskopien, Portraitfotos, IBAN)

Entscheidung:

Verstoß gegen Art. 32 DSGVO trotz ISO-27001-Zertifizierung

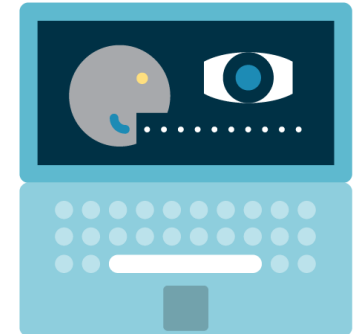
Kein ersatzfähiger immaterieller Schaden nachgewiesen

→ Klage abgewiesen

AG Duisburg | Kein schuldhafter Verstoß bei Zero-Day Exploit

Sachverhalt:

- Klägerin = Verbraucherin (Riester-Vertragsnehmerin)
- Beklagte = Versicherungsgesellschaft und Auftragsverarbeiterin (MOVEit, identischer Exploit)
- Abgeflossene Daten: Name, Anschrift, IBAN, Riester-Vertragsnummer, u. a.



Entscheidung:

Kein schuldhafter Verstoß
gegen Art. 32 DSGVO

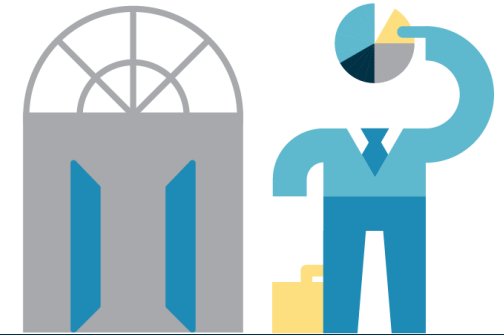
Kein Anscheinsbeweis aus
dem erfolgreichen Angriff

→ Klage abgewiesen

Fall Fasana | Sachverhalt und insolvenzrechtliche Implikation

Sachverhalt:

- Produzierendes KMU wird am 19. Mai 2025 Opfer eines Ransomware-Angriff
- Vollständiger IT- und Produktionsstillstand, täglich erhebliche Umsatzausfälle
- Insolvenzantrag: 1. Juni 2025 – 13 Tage nach dem Angriff
- Kein Verbraucher; keine DSGVO-Schadensersatzproblematik – primär Frage der Organverantwortung



Rechtliches Kernproblem:

IT-Ausfall macht Liquiditäts- und Überschuldungslage kaum ermittelbar

§ 15a InsO: keine Befreiung von der Antragspflicht wegen technischer Beeinträchtigungen

Rechtliche Hintergründe | Schadensgrundlagen

Regulatorische Pflichten / Geschäftsführungspflichten

§ 30 Abs. 1, 2 BSIG-Neu: „[Einrichtungen] sind verpflichtet [...] Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten“; Maßnahmen umfassen zumindest „Bewältigung von Sicherheitsvorfällen“

Art. 32 Abs. 1 lit. c DSGVO: „die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen“

§ 93 Abs. 1 AktG: „Die [...] Geschäftsführung [hat] die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden. Eine Pflichtverletzung liegt nicht vor, wenn das Vorstandsmitglied [...] vernünftigerweise annehmen durfte, auf der Grundlage angemessener Information zum Wohle der Gesellschaft zu handeln“

Schadensminderungspflichten bzw. -obliegenheiten ggü.:

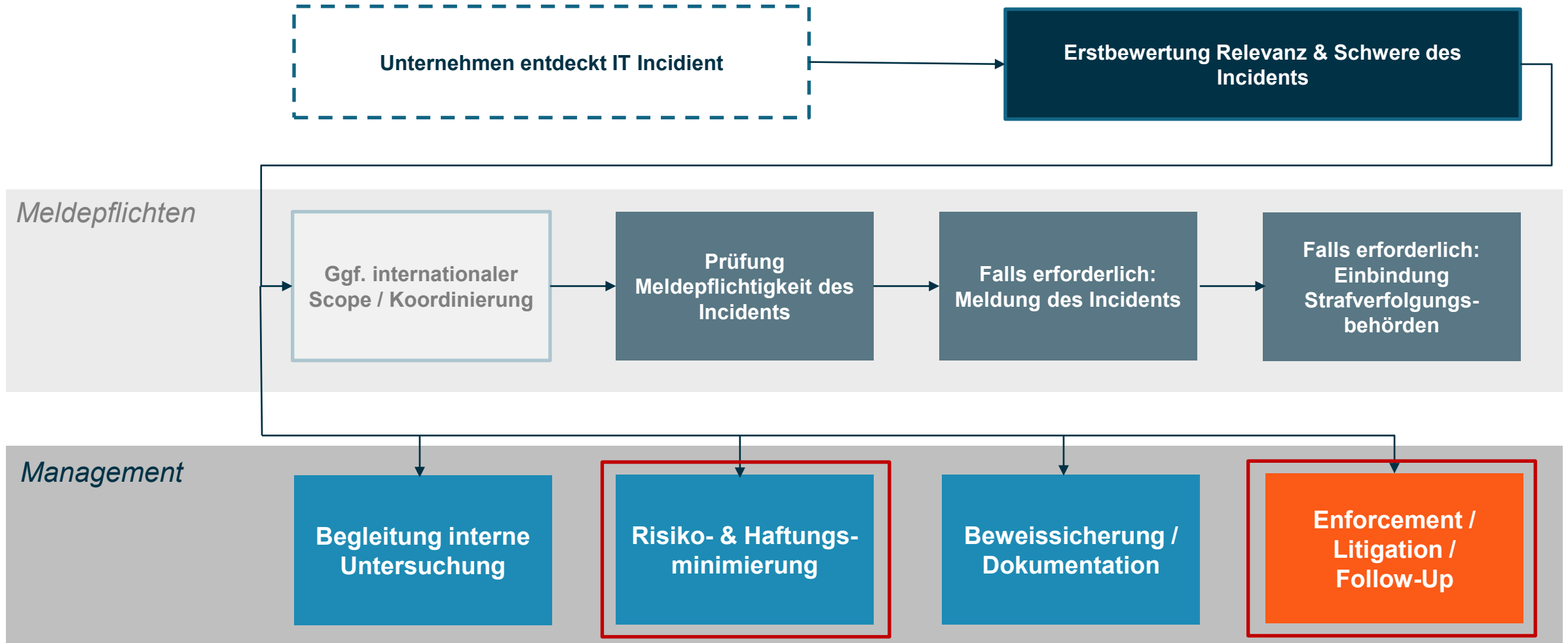
Geschädigten

Schädigern

Versicherung

- Verstoß gegen regulatorische Pflichten -> Bußgeldrisiko
- Relevanter Faktor bei Bußgeldbemessung
- Organisationsverschulden: Haftung der Gesellschaft UND persönliche Haftung der Geschäftsführung
- Erhöhung möglicher Haftung ggü. Geschädigten (ggf. Vorsatz)
- Mögliche Verringerung eigener Schadensersatzansprüche ggü. Schädigern (da Mitverschulden bei Schadensentstehung)
- Möglicher Verstoß gegen Versicherungsbedingungen -> Ausfall oder jedenfalls Verringerung Deckungsanspruch

Best Practice | Incident Management Prozess (aus rechtlicher Sicht)



Rechtssichere Kommunikation | Kunden, Behörden usw.

Übergreifend:

- Festlegung der richtigen Kommunikationsstrategie: *Beichte* vs. *Salami* vs. *Teppich*
- Vermeidung von Selbstbelastung und voreiligen Schuldeingeständnissen
- Koordination in Unternehmensgruppen elementar (Vermeidung voreiliger Meldungen)
- *Control the narrative*

Behörden / öffentlichen Stellen

- Datenschutz: nur wenn verpflichtet; Beweisverwertungsverbot in § 43 Abs. 4 BDSG beachten!
- Polizei/StA/LKA: Grds. keine Pflicht zur Strafanzeige; überlegenswert bei Asset Recovery

* Versicherungsbedingungen beachten!

Betroffene / im Unternehmen

- Regelfall: nur wenn verpflichtet (z.B. Art. 34 DSGVO)
- Bei bereits eingetretener Verbreitung (extern oder auch intern) zur Kontrolle des Narrativs denkbar

Kunden / Lieferanten / anderen Geschäftspartnern

- *Force Majeure* Schreiben
- Befreiung von vertraglichen Pflichten
- „Zwingt“ Gegenseite zur Schadensabwendung oder jedenfalls -minderung

Key Takeaways

- ***Regulatorische Pflicht zu Vorbereitungs- sowie Abhilfemaßnahmen / entscheidend für spätere Haftungsminimierung bzw. Vermeiden von Mitverschulden***
- ***Ab erster Minute der Incident-Bearbeitung unmittelbar mit Schadens- bzw. Haftungsvermeidung beginnen (insb. BCM, Force Majeure Schreiben usw.)***
- ***Kommunikationsstrategie festlegen / keine voreiligen Schuldeingeständnisse / Beweisverwertungsverbote seitens Datenschutzbehörden kennen***
- ***Mögliche Anspruchssteller bzw. -gegner und darauf erwachsende mögliche Haftung bzw. eigene Ansprüche früh einordnen und beziffern / Haftungsklauseln prüfen***
- ***Eigene Schäden genau beziffern und dokumentieren***
- ***Dokumentation / Abschlussbericht essenzieller Grundstein für jede erfolgreiche Verteidigung / Alignment mit externem forensischem Gutachten zwingend***
- ***Versicherungsbedingungen zwingend beachten / Abweichungen schriftlich bestätigen lassen***

Vielen Dank / Ihre Fragen



Dr. Tobias Rothkegel, CIPP/E
Partner / Data & Cyber
Osborne Clarke GmbH & Co. KG

+49 40 55436 4090

tobias.rothkegel@osborneclarke.com



Christoph Kauffmann, LL.M.
Partner / Disputes & Risk
Osborne Clarke GmbH & Co. KG

+49 221 5108 4202

christoph.kauffmann@osborneclarke.com

