RISIKO MEDIZINPRODUKT

IT-Security, Risk Management & Produkthaftung sind Chefsache!

virtuell, 28. April 2025

Dieses Bild wurde mit Hilfe von DALL-E (OpenAI) generiert.

Referentin: Michaela Berg

1 Darstellung der „neuen“ Spannungsfelder anhand gesetzlicher & regulatorischer Vorschriften

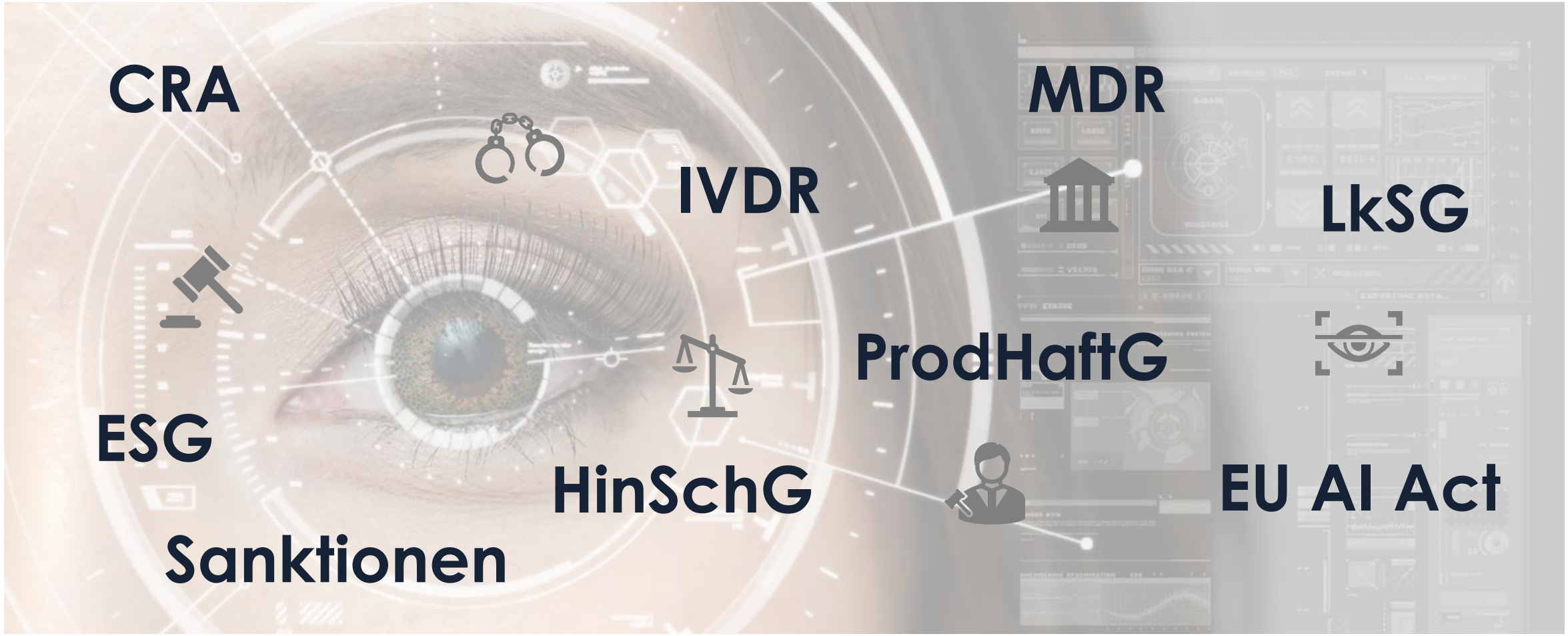
2 Vom Risikomanagement zum Risikotransfer

01 | Darstellung der neuen Spannungsfelder

Auswirkungen der aktuellen gesetzlichen & regulatorischen Vorschriften auf das Risikomanagement und die Versicherungen

Gesetzliches und regulatorischen Umfeld

Neue und aktuelle Spannungsfelder



Gesetzliches und regulatorischen Umfeld

Auswirkungen auf das Risiko-Management

- **Regulatorik fordert systematisches Risikomanagement**
- **Lieferketten = zentrales Risikofeld**
- **ESG (Environmental, Social, Governance) = neue Risikodimensionen**
- **Cyberrisiken steigen stark an**

Gesetzliches und regulatorischen Umfeld

Auswirkungen auf das Versicherungskonzept

- **Kürzere Innovationszyklen → Anpassung der Versicherungskonzepte für neue Produkte notwendig**
- **Höhere Versicherungs- und Deckungssummen notwendig**
- **Steigende Kosten für Versicherungsprämien durch wachsende Risiken**
- **Risiken durch geopolitische Spannungen und Sanktionen (Lieferketten, Exportverbote)**
- **Unterschiedliche Anforderungen in internationalen Märkten (z. B. USA vs. EU)**
- **Erweiterte Anforderungen an Produktsicherheit in der Lieferkette**

Gesetzliches und regulatorischen Umfeld

Cyber Regulatorik & Versicherung | Auswirkungen und Praxisbeispiele

1. **Produkthaftpflichtversicherung**

Auswirkung: Produkthaftung durch fehlende Absicherung vernetzter Komponenten – trotz technischer Zulassung

Beispiel: implantierbares Herzgerät mit Cybersicherheitslücke

2. **IT-Haftpflichtversicherung**

Auswirkung: Erhöhtes Schadenpotenzial bei Systemausfällen in kritischer Infrastruktur

Beispiel: Cloud-basierter Dienstleister für Klinikdatenverwaltung erleidet einen Serverausfall

Gesetzliches und regulatorischen Umfeld

Cyber Regulatorik & Versicherung | Auswirkungen und Praxisbeispiele

3. D&O-Versicherung

Auswirkung: Persönliche Haftung des Managements bei Nicht-Umsetzung regulatorischer IT-Vorgaben

Beispiel: KI-gestütztes Dermatoskop zur Hautkrebsfrüherkennung

IHRE MEINUNG IST GEFRAGT

Scannen Sie den QR oder verwenden Sie den Link, um teilzunehmen

https://forms.office.com/e/Q8jgBgGfsk

Link kopieren

0 Antwort übermittelt

Wie gut sind Sie mit den Anforderungen der Cyber-Security im Rahmen der MDR vertraut?

sehr gut	gut	teilweise
kaum	gar nicht	

Treemap | Bar

1 von 6

02 | Vom Risikomanagement zum Risikotransfer

Grundlagen des Risikomanagements für MedTech-Unternehmen | Versicherungslösungen

Vom Risikomanagement zum Risikotransfer

Anforderungen an das Risiko- und QM-Management gemäß MDR

Einführung eines Systems	Anwendung im Lebenszyklus	Nutzen-Risiko-Bewertung	Kontrolle und Überwachung
„Risikomanagement-system einrichten und dokumentieren“ (Art. 10)	„Systematisch über gesamten Produktlebenszyklus hinweg anwenden“ (Anhang I)	„Positives Nutzen-Risiko-Verhältnis sicherstellen“	„Risiken kontinuierlich bewerten und kontrollieren“

Vom Risikomanagement zum Risikotransfer

Anforderungen an das Risiko- und QM-Management gemäß MDR

Die MDR ist rechtsverbindlich – ISO-Normen sind „anerkannte Werkzeuge“ zur Umsetzung

- Die MDR (EU-Verordnung 2017/745) ist verbindlich für alle Hersteller, Importeure und Händler von Medizinprodukten in der EU.
- ISO-Normen wie ISO 14971 (Risikomanagement) und ISO 13485 (Qualitätsmanagement) sind keine Gesetze, aber sie gelten als „harmonisierte Normen“ bzw. anerkannte Standards zur Umsetzung der MDR-Anforderungen.

Vom Risikomanagement zum Risikotransfer

ISO 14971 vs. ISO 13485 – Was ist der Unterschied?

🧩 KRITERIUM	📘 ISO 14971 – Risikomanagement	📕 ISO 13485 – Qualitätsmanagement
Ziel	Systematischer Umgang mit Risiken bei Medizinprodukten	Aufbau und Steuerung eines QM-Systems für sichere Produkte
Fokus	**Produktlebenszyklus:** Risikoidentifikation, -bewertung, -kontrolle	**Unternehmensprozesse:** Entwicklung, Produktion, Dokumentation
Geltungsbereich	**Produktbezogen** (Einzelprodukt oder Produktfamilie)	**Organisation/Unternehmen** (alle qualitätsrelevanten Bereiche)
Verbindung zur MDR	Erfüllt Anforderungen aus Anhang I der MDR	Grundlage zur Umsetzung der Artikel 10 (Pflichten der Hersteller)
Verpflichtung	Praktisch verpflichtend durch MDR & Benannte Stellen	Voraussetzung für CE-Kennzeichnung (indirekte Verpflichtung)
Verknüpfung	Muss ins QM-System (nach ISO 13485) eingebettet sein	Muss ein Risikomanagementsystem (nach ISO 14971) berücksichtigen
 **Kurz gesagt**	**ISO 14971 ist der Werkzeugkasten fürs Risikomanagement**	**ISO 13485 ist das Betriebssystem, in dem dieser Werkzeugkasten sauber integriert und verwendet wird.**

Vom Risikomanagement zum Risikotransfer

Anforderungen an das Risiko- und QM-Management gemäß MDR

❓ Sind ISO-Normen verpflichtend für Hersteller? 🔍 Formal: Nein – Praktisch: Fast immer Ja

- Theoretisch kann ein Hersteller andere Methoden verwenden, um die Anforderungen der MDR zu erfüllen.
- Praktisch akzeptieren Benannte Stellen (z. B. TÜV, DEKRA) fast ausschließlich anerkannte Normen wie ISO 13485/14971 als Nachweis der Konformität.
- Wer davon abweicht, muss gleichwertige oder bessere Verfahren nachweisen – was extrem aufwändig und risikobehaftet ist.

Vom Risikomanagement zum Risikotransfer

Gesetzliche und regulatorische Anforderungen für Cyber-Security

MDR – (EU) 2017/745 Art. 10 (9)

- ✓ Hersteller müssen im Rahmen des Risikomanagements auch Cybersicherheitsrisiken berücksichtigen und die möglichen Auswirkungen auf die Patientensicherheit und die Funktionalität des Medizinprodukts bewerten.
- ✓ Cybersicherheitsanforderungen müssen in der technischen Dokumentation festgehalten werden, insbesondere für vernetzte Medizinprodukte

NIS-Richtlinie (EU-Richtlinie 2016/1148)

- ✓ Diese Richtlinie betrifft die Cybersicherheit von Netz- und Informationssystemen und verlangt von Unternehmen im Gesundheitssektor, Sicherheitsvorkehrungen zu treffen, um kritische Infrastrukturen vor Cyber-Angriffen zu schützen.
- ✓ Medizinprodukte-hersteller, die als Betreiber kritischer Infrastrukturen gelten, müssen Risiken aus Cyber-Bedrohungen identifizieren, bewerten und geeignete Schutzmaßnahmen implementieren.

ISO/IEC 27001 – Informationssicherheitsmanagementsystem (ISMS)

- ✓ Es wird empfohlen, für die Cybersicherheit ein umfassendes Informationssicherheitsmanagementsystem (ISMS) einzuführen, um Risiken im Umgang mit Daten, Netzwerken und Systemen zu minimieren.
- ✓ Diese Norm legt fest, wie ein systematisches Risikomanagement zur Absicherung der IT-Infrastruktur aussehen sollte und fordert eine kontinuierliche Verbesserung.

IEC 62443 – IT-Sicherheit in der Automatisierungstechnik

- ✓ Relevant für Hersteller von vernetzten Medizingeräten (IoMT – Internet of Medical Things).
- ✓ Diese Norm umfasst ein vollständiges Set an Anforderungen zur Sicherung von Systemen gegen Cyber-Bedrohungen. Sie behandelt sowohl Hardware- als auch Softwareaspekte und legt Standards für den sicheren Betrieb vernetzter Systeme fest..

FDA Cybersecurity Guidance (USA)

- ✓ Die FDA fordert in ihren Richtlinien für Medizinprodukte die Berücksichtigung von Cybersicherheitsaspekten im Rahmen der Produktentwicklung und Zulassung. Sie verlangt, dass Hersteller von vernetzten Medizinprodukten detaillierte Sicherheitskonzepte präsentieren und Cyber-Risiken im Rahmen der klinischen Evaluation bewerten.

Vom Risikomanagement zum Risikotransfer

Der Prozess im Überblick

Vom Risikomanagement zum Risikotransfer

Risikotransfer durch Versicherungen

VERSICHERUNGS-SPARTE	Kurzbeschreibung	Auswirkungen bei fehlender Absicherung	Bemerkung
Produkthaftpflicht-Versicherung	Personen-/Sachschäden Dritter durch fehlerhafte Produkte	existenziell	Software als Produkt
Feuer-Versicherung	Absicherung Sachwerte und Ertragsausfall	existenziell	Basisabsicherung für Gebäude, Betriebs-einrichtung und Vorräte
Elementarschaden-Versicherung	Absicherung Sachwerte und Ertragsausfall	hoch	Hohe Nachfrage auch für Ertragsausfall
Betriebshaftpflicht-Versicherung	Personen-/Sachschäden Dritter durch betriebliche Tätigkeiten	hoch	Basisabsicherung für betriebliche Tätigkeiten
Rückrufkosten-versicherung	Kosten für Rückrufaktion (inkl. Kommunikation, Entsorgung etc.)	hoch	Bedingte Marktdurchdringung bei exponierten Risiken
Umwelthaftpflicht-Versicherung	Personen-/ Sachschäden übertragen durch Boden, Wasser, Luft	hoch	Ansprüche Dritter bei Explosion

Vom Risikomanagement zum Risikotransfer

Risikotransfer durch Versicherungen

VERSICHERUNGS-SPARTE	Kurzbeschreibung	Auswirkungen bei fehlender Absicherung	Bemerkung
D&O-Versicherung	Befriedigung von Schadenersatzansprüchen / Abwehr unberechtigter Ansprüche in Folge einer Pflichtverletzung der Entscheider	hoch	Verschärfte Haftung durch höhere Anforderungen an Compliance, Regulatorik etc.
Cyber-Versicherung	Datenschutzverletzungen, Cyberangriffe, Betriebsunterbrechung	hoch	Personenbezogene Daten / Schnittstelle zur kritischen Infrastruktur
Vertrauens-schaden-Versicherung	Schäden durch Wirtschaftskriminalität (Dritte und eigene Mitarbeiter)	hoch	Nahezu jedes Unternehmen hatte schon derartige Fälle
Transport-Versicherung	Schäden/Verluste bei Gütern in Bewegung	mittel	Besonderheiten bei temperaturgeführten Gütern
Strafrechtsschutz-Versicherung	Verteidigung bei strafrechtlichen Ermittlungen	mittel	Absicherung des gesamten Personals / Sonderfunktionen

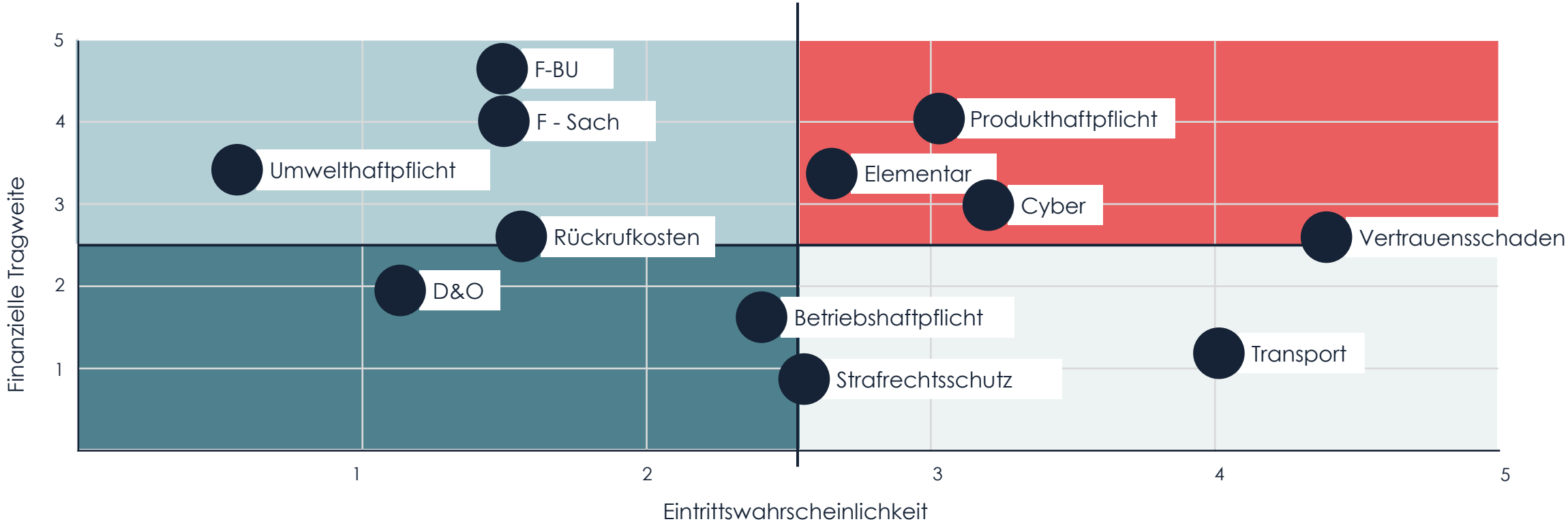
Vom Risikomanagement zum Risikotransfer

Risikotransfer durch Versicherungen

VERSICHERUNGS-SPARTE	Kurzbeschreibung	Auswirkungen bei fehlender Absicherung	Bemerkung
Maschinen-Versicherung	Maschinenbruchversicherung	mittel	Erweiterung Betriebsunterbrechung bei Schlüsselmaschinen möglich
Elektronik-Versicherung	Allgefahrenversicherung für elektronische Geräte	mittel	Pauschal oder ausgewählte, elektronische Geräte
Umweltschaden-Versicherung	Biodiversitätsschäden (öffentlich-rechtliche Ansprüche)	mittel	Nur wenige Schäden in Deutschland in der Grunddeckung bekannt
Firmenrechtsschutz -Versicherung	Kosten bei gerichtlichen Auseinandersetzungen im Zusammenhang mit Firmen- und Arbeitsrecht	mittel	Umfangreicher Ausschlusskatalog und prämienintensiv

Vom Risikomanagement zum Risikotransfer

Schadeneintrittswahrscheinlichkeit und finanzielle Tragweite



Finanzielle Tragweite

1 – sehr gering
2 – gering
3 – mittel
4 – groß
5 – existenzbedrohend

Eintrittswahrscheinlichkeit

1 – unwahrscheinlich
2 – vorstellbar
3 – selten
4 – gelegentlich
5 – häufig

Vom Risikomanagement zum Risikotransfer

Abgrenzung Produkthaftpflicht, IT-Haftpflicht & Cyber | Fallbeispiel

1. Ausgangslage

Ein Medizintechnikunternehmen bringt eine vernetzte Medikamentenpumpe auf den Markt. Die Pumpe ist softwaregesteuert, über eine Cloud-Anbindung fernüberwachbar und wird in mehreren Kliniken eingesetzt.

2. Der Schadenfall

- ✓ Ein Hackerangriff über eine ungepatchte Schwachstelle in der Cloud-Schnittstelle führt zu einem Zugriff auf mehrere Pumpen.
- ✓ Infolge des Angriffs wird die Dosisregelung der Software manipuliert, was bei einem Patienten zu einer Überdosierung und anschließend zu gesundheitlichen Komplikationen führt.
- ✓ Die betroffene Klinik muss mehrere Pumpen außer Betrieb nehmen – der IT-Ausfall führt zu einem erheblichen Betriebsunterbruch und Notbetrieb auf der Station.
- ✓ Bei der anschließenden Prüfung wird festgestellt: Die Software enthielt Programmierfehler, die eine Absicherung gegen Fremdzugriffe erschwerten.

Vom Risikomanagement zum Risikotransfer

Abgrenzung Produkthaftpflicht, IT-Haftpflicht & Cyber

KRITERIUM	Produkthaftpflicht	IT-Haftpflicht	Cyber-Versicherung
Zielsetzung	Schutz bei Personen-/Sachschäden durch fehlerhafte Produkte	Schutz bei Vermögensschäden durch fehlerhafte IT-Dienstleistungen	Schutz bei Schäden durch Cyberangriffe und IT-Ausfälle
Typische Schadenursachen	Mangelhaftigkeit des Produkts	Programmierfehler, fehlerhafte Beratung oder Implementierung	Hacking, Malware, Datenverlust, Betriebsunterbrechung
Versicherte Schäden	Dritte erleiden Personen- oder Sachschäden	Vermögensschäden Dritter durch fehlerhafte IT-Leistung	Eigenschäden (z. B. IT-Wiederherstellung, Betriebsunterbrechung) und Drittschäden
Versicherte Leistungen	Prüfung von Ansprüchen, Abwehr unberechtigter Forderungen, Schadenersatz	Prüfung und Regulierung berechtigter Vermögensschäden	Kosten für Forensik, Krisen-PR, Betriebsunterbrechung, (DSGVO-Bußgelder)

IHRE MEINUNG IST GEFRAGT

FRAGEN?

VIELEN DANK!

MICHAELA BERG

Head of Life Sciences

GGW GmbH - Köln

+49 221 – 94 97 48 23

+49 172 – 85 388 21

michaela.berg@ggw.de