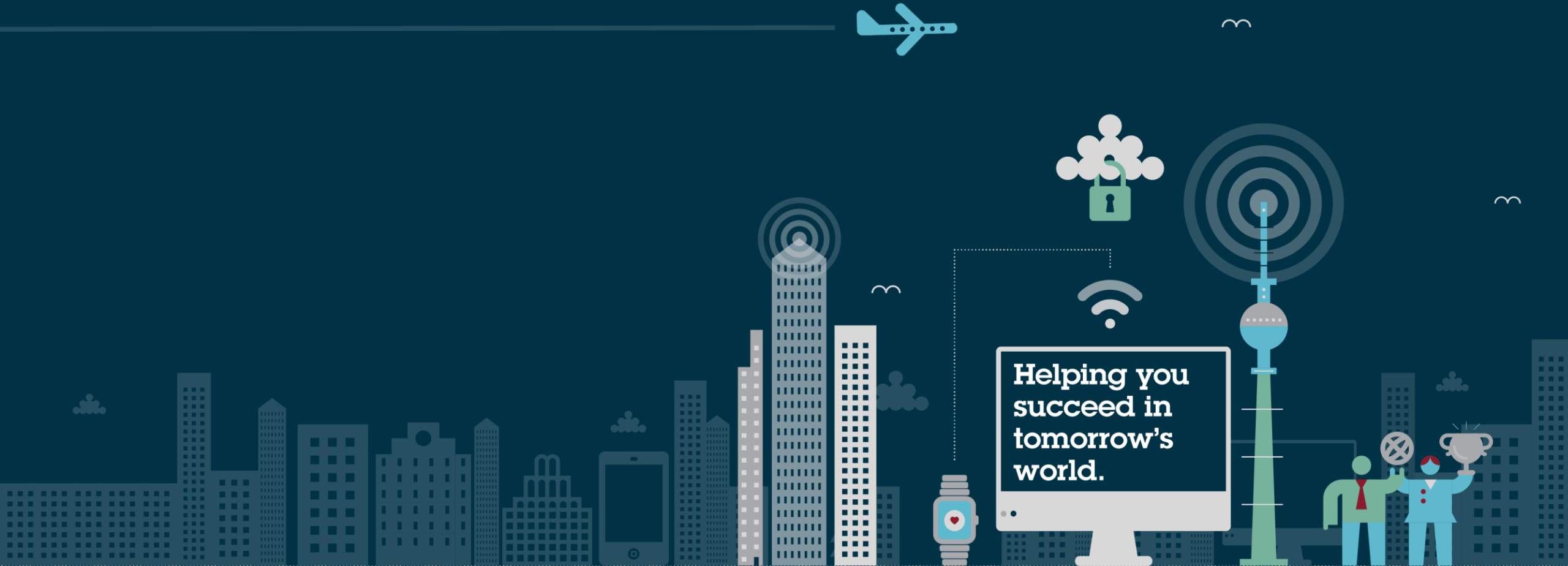


Rechts-Update: Cyber Security

Zukunftsallianz Maschinenbau e.V.

27. April 2022



Wer spricht da?

Adrian Schneider

- Rechtsanwalt bei Osborne Clarke in Köln
- Schwerpunkte:
 - IT-Recht
 - Datenschutz
 - Cyber Security
- Ehemaliger Softwareentwickler in den Bereichen Web, Mobile und Games
- Ausbildung u.a. bei Bundesamt für Sicherheit in der Informationstechnik
- Autor bei div. Fachpublikationen, u.a. Datenschutz-Berater, K&R, Telemedicus



Adrian Schneider
Rechtsanwalt / Partner

+49 (0) 221 5108 4160
adrian.schneider@osborneclarke.com

osborneclarke.com
spielerecht.de
telemedicus.info

@adrschn

Was ist Cyber Security?

Die Sicherheit der Verfügbarkeit, Integrität und Vertraulichkeit informationstechnischer Systeme, insbesondere vor Angriffen und unautorisierten Zugriffen.

Datenschutzrecht

BSI-Gesetz

Allgemeines Zivilrecht

Produkthaftungsrecht

Produktsicherheitsrecht

Telekommunikationsrecht

Energierrecht

...



1

Datenschutzrecht



Datenschutzrecht: Anforderungen an Cyber-Sicherheit



Wer oder was ist geschützt?

Schutz **personenbezogener Daten** und damit ultimativ die Rechte und Freiheiten natürlicher Personen



Wer ist verpflichtet?

Verantwortliche und Auftragsverarbeiter, d.h. in aller Regel die Betreiber von Anlagen – **Hersteller** nur mittelbar!



Was sind die Anforderungen?

Technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten unter Berücksichtigung:

1. des Stands der Technik,
2. der Implementierungskosten,
3. der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung,
4. der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos



Datenschutzrecht: Anforderungen an Cyber-Sicherheit



Risiken

- Eigene datenschutzrechtliche Haftung bei Erhebung personenbezogener Daten (z.B. Auswertung von Maschinendaten auf Anwenderebene) – Bußgelder bis 20 Mio. EUR oder 4% des Konzernumsatzes.
- Mittelbare zivilrechtliche Haftung gegenüber von Kunden bei Verkauf unsicherer Systeme
- Bußgelder gegen Kunden



Typische Herausforderungen in der Praxis

- Definition „angemessener“ Maßnahmen
- Stete Veränderung von Stand der Technik und Bedrohungslagen
- Pflichten richten sich an „Verantwortliche“ (Betreiber), tatsächliche Einflussmöglichkeit liegt aber bei Hersteller



Learning: Auch wenn Sie selbst keine personenbezogenen Daten verarbeiten können Anforderungen auf Kundenseite an Cyber Sicherheit bestehen.



Update: Aktuelle Entwicklungen

Neues Telekommunikation-Telemedien-Datenschutz-Gesetz („TTDSG“):

- **Weitgehend gleichlaufende Pflichten** wie unter altem Recht
- Neuer **Verweis auf § 7d BSI**:
BSI kann in Gefahrensituationen technische und organisatorische Maßnahmen anordnen
- Neue Regelungen zu **Lesen und Speichern von Daten auf Maschinen**:
 - Unbedingt erforderlich oder mit Einwilligung
 - Unabhängig von personenbezogenen Daten
 - Kann auch Machine-to-Machine Kommunikation betreffen
- Neue telekommunikationsrechtliche Kategorie: „**Interpersonelle Kommunikationsdienste**“
 - Messenger
 - Videokonferenzsysteme
 - Ggf. auch Fernwartungssysteme je nach Ausgestaltung

2

BSI-Gesetz



BSI-Gesetz: Anforderungen an Cyber-Sicherheit



Wer oder was ist geschützt?

Schutz von **Infrastruktur**, hauptsächlich „kritischer Infrastrukturen“ mit besonderer gesellschaftlicher Bedeutung



Wer ist verpflichtet?

Betreiber der Infrastruktur – Hersteller nur mittelbar



Was sind die Anforderungen?

Angemessene **organisatorische und technische Vorkehrungen** zur Vermeidung von **Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit** ihrer informationstechnischen **Systeme, Komponenten oder Prozesse**, die für die Funktionsfähigkeit der kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden.

► Flankiert durch technische Guidelines des BSI und anderer Organisationen und Behörden



BSI-Gesetz : Anforderungen an Cyber-Sicherheit



Risiken

- Bußgelder gegen Kunden, die kritische Infrastrukturen betreiben (bis zu 2 Mio. EUR)
- Mittelbare zivilrechtliche Haftung gegenüber von Kunden bei Verkauf unsicherer Systeme



Typische Herausforderungen in der Praxis

- Definition „angemessener“ Maßnahmen
- Schutz muss nicht nur gegen Einflüsse von außen, sondern auch interne Störungsursachen bestehen – technisch herausfordernd (z.B. „DDoS“-Attacken)
- Hohe Anforderungen an Sicherheit bei kritischen Infrastrukturen



Learning: Besonders hohe Kundenanforderungen bei kritischen Infrastrukturen



Update: Aktuelle Entwicklungen

Erweiterung der regulierten Unternehmen:

- **„Digitale Dienste“**
 - Online-Marktplätze für Verbraucher, Online-Suchmaschinen, Cloud-Computing-Dienste
 - Besondere Pflicht zu TOM über Datenschutz hinaus (z.B. Business Continuity)
 - Meldepflichten bei Sicherheitsvorfällen „mit erheblichen Auswirkungen auf die Bereitstellung des Dienstes“
- **„Unternehmen im besonderen öffentlichen Interesse“ (UBI)**
 - **UBI 1:** Hersteller von Gütern im Bereich Waffen, Munition, Rüstung oder von IT-Produkten mit Sicherheitsfunktionen zur Verarbeitung von Verschlusssachen oder wesentlichen Komponenten hierfür
 - **UBI 2:** Die nach Wertschöpfung 100 größten Unternehmen Deutschlands (konkrete Definition folgt noch durch Verordnung)
 - **UBI 2.5:** Zulieferer von UBI 2, wenn diese ein Alleinstellungsmerkmal haben und daher von wesentlicher Bedeutung von UBI 2 sind.
 - **UBI 3:** Verarbeiter von größeren Mengen gefährlicher Stoffe (Betriebsbereich der oberen Klasse im Sinne der Störfall-Verordnung)

Update: Aktuelle Entwicklungen

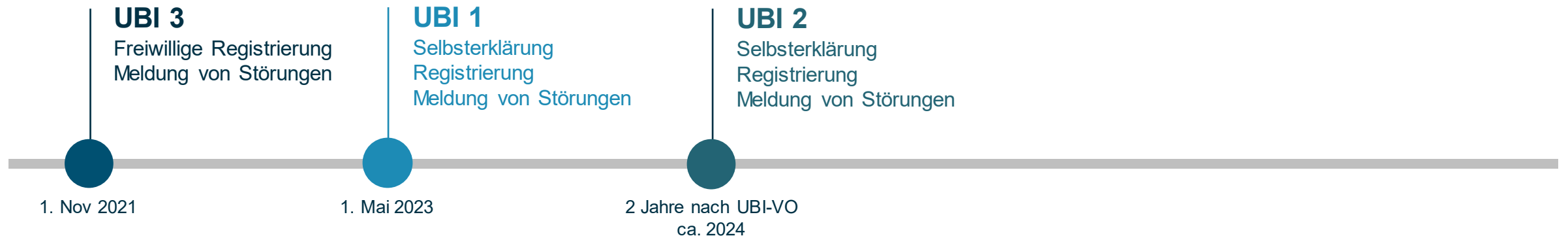
UBI 2: Voraussichtlich erfasste Unternehmen (Top 100 Hauptgutachten Monopolkommission)

Volkswagenwerk AG
 Siemens AG
 Daimler-Benz AG
 August Thyssen-Hütte AG
 VEBA AG
 BASF AG
 AEG Telefunken AG
 Hoechst AG
 Ruhrkohle AG
 Bayer AG
 Rheinisch-Westfälisches Elektrizitätswerk AG
 Adam Opel AG
 Fried. Krupp GmbH
 ESSO AG
 Gutehoffnungshütte Aktienverein
 Fordwerke AG
 Friedrich Flick KG
 Deutsche Shell AG
 Mannesmann AG
 Rheinstahl AG
 Deutsche Unilever GmbH
 Robert Bosch GmbH
 Metallgesellschaft AG
 Reemtsma Cigarettenfabriken GmbH
 IBM Deutschland GmbH
 Gelsenberg AG
 NEUE HEIMAT
 Salzgitter AG
 ESTEL NV Hoesch-Hoogovens
 Karstadt AG
 Aral AG
 Deutsche BP AG
 Kaufhof AG
 Hertie Waren- und Kaufhaus GmbH
 Gedelfi Grosseinkauf GmbH & Co. KG

Deutsche Texaco AG
 Allgemeine Deutsche Philips Industrie GmbH
 Kloeckner & Co.
 BAT Cigaretten-Fabriken GmbH
 Gustav Schickedanz KG
 Oetker-Gruppe
 Martin Brinkmann AG
 Henkel KGaA
 Kloeckner-Humboldt-Deutz AG
 Deutsche Lufthansa AG
 Alfred C. Toepfer Verwaltungs-Gesellschaft m.b.H.
 C. & A. Brennkemeyer
 BBC, Brown, Boveri & Cie AG
 Bayerische Motoren Werke AG
 COOP Zentrale AG
 SEL Standard Elektrik Lorenz AG
 Philipp Holzmann AG
 Mobil Oil AG
 Hochtief AG
 BayWa AG
 Saarbergwerke AG
 Degussa
 Kloeckner Werke AG
 Preussag AG
 Saint-Gobain-Pont-à-Mousson (Deutschland)
 Neckermann Versand KGaA
 Horten AG
 Enka Glanzstoff AG
 Nestle-Gruppe Deutschland
 Deutsche Babcock & Wilcox AG
 VEW Vereinigte Elektrizitätswerke Westfalen AG
 Vereinigte Industrie-Unternehmungen AG
 Bosch-Siemens Hausgeräte GmbH
 Otto Wolff AG
 REWE Zentral-AG

Demag AG
 Dyckerhoff & Widmann AG
 Stahlwerke Roehling-Burbach GmbH
 Ruhrgas AG
 Continental Gummi-Werke AG
 Strabag Bau-AG
 Chem. Werke Huels AG
 Stahlwerke Suedwestfalen AG
 Grundig AG
 Hapag-Lloyd AG
 Agfa-Gevaert AG
 Messerschmitt-Boelkow-Blohm GmbH
 Otto-Versand
 Marquard & Bahls GmbH & Co.
 Norddeutsche Affinerie
 Axel Springer Verlag AG
 Schering AG
 ITT Gesellschaft fuer Beteiligungen mbH
 Kugelfischer Georg Schaefer & Co.
 Eschweiler Bergwerksverein
 Deutsche Raiffeisen Warenzentrale GmbH
 Aktiengesellschaft der Dillinger Huettenwerke
 Karl Freudenberg KG
 Wilhelm Werhahn
 Papierwerke-Waldhof-Aschaffenburg AG
 Getreide-Import-Gesellschaft mbH
 Ruetgerswerke AG
 EDEKA Zentrale AG
 Carl Zeiss

Update: Aktuelle Entwicklungen



3 Allgemeines Zivilrecht



Allgemeines Zivilrecht: Anforderungen an Cyber-Sicherheit



Wer oder was ist geschützt?

Schutz der **Vertragspartner** vor Schlechtleistungen im Vertragsverhältnis
Schutz **Dritter** vor unberechtigtem Eingriff in Ihre Rechtspositionen



Wer ist verpflichtet?

Verkäufer bzw. **Betreiber** des betroffenen Systems



Was sind die Anforderungen?

Vertrag: Mangelfreie Lieferung des Systems:

- Objektive Kriterien: Was darf der Kunde erwarten?
- Subjektive Kriterien: Was ist vereinbart?

Achtung: Ab 2022 Updatepflicht für Sachen mit digitalen Elementen ggü. Verbrauchern, in einzelnen Staaten auch Kleinunternehmer (Warenkaufrichtlinie)

Delikt: Verkehrssicherungspflichten – von Produkt darf keine Gefahr ausgehen

► „Im Verkehr erforderliche Sorgfalt“



Allgemeines Zivilrecht : Anforderungen an Cyber-Sicherheit



Risiken

- Zivilrechtliche Ansprüche von Kunden (oder Dritten) auf Schadensersatz aus Vertrag oder Delikt
- Zivilrechtliche Gewährleistungsansprüche (Nacherfüllung, Rücktritt, Minderung)



Typische Herausforderungen in der Praxis

- Was ist ein **Mangel**? Was dürfen Kunden erwarten? Was ist versprochen?
- Bei Kauf nur Mängel bei **Gefahrübergang** relevant – Umgang mit **später** bekannt werdenden Sicherheitslücken (Marktbeobachtung)
- Schadensersatz setzt **Verschulden** voraus: Welche Sorgfalt ist geschuldet? (Beweis!)
- **Updatepflichten**: Technische Möglichkeiten bei Geräten (Schnittstellen)
- Abgrenzung **Miete/Pflege/Wartung**
- Haftung für **Komponenten Dritter**
- Definition von **Verkehrspflichten**



Learning: Die zivilrechtlichen Fragen sind komplex und betreffen sowohl die eigene Haftung als auch von Kunden – starkes Eigeninteresse an Sicherheit der Produkte



4 Produkthaftungsrecht



Produkthaftungsrecht: Anforderungen an Cyber-Sicherheit



Wer oder was ist geschützt?

Schutz der **Allgemeinheit** vor gefährlichen Produkten



Wer ist verpflichtet?

Hersteller, ggf. auch Importeur des betroffenen Produkts (inkl. Embedded Software)



Was sind die Anforderungen?

Sicherheit des Produktes nach dem Stand der Technik

- ▶ Gesetz sieht verschuldensunabhängige Haftung vor, d.h. es kommt nicht darauf an, ob „angemessene“ Maßnahmen zur Verhinderung getroffen wurden



Produkthaftungsrecht : Anforderungen an Cyber-Sicherheit



Risiken

Schadensersatzpflicht im Fall von Schäden durch Sicherheitslücken



Typische Herausforderungen in der Praxis

- „Produkt“ – inwiefern fällt Software darunter?
- „Fehler“ – inwiefern sind Sicherheitslücken erfasst?
- „Stand der Technik“ – inwiefern waren Fehler bei Inverkehrbringen erkennbar (Zero-Day-Lücken)? Wie umgehen mit später erkannten Sicherheitslücken?
- Serienfehler – Umgang mit bekannt gewordenen Sicherheitslücken in Serienproduktion
- Behebbarkeit von Fehlern, insbesondere bei individuellen Kundenlösungen



Learning: Hohes Eigeninteresse, bei „Inverkehrbringen“ des Produktes bekannte Sicherheitslücken zu vermeiden



5 Sektorspezifische Gesetze



Sektorspezifische Gesetze: Anforderungen an Cyber-Sicherheit

Besondere Anforderungen für Anlagen und Produkte in bestimmten Sektoren (Auswahl):

Telekommunikationsrecht

- ggf. relevant bei vernetzten Maschinen
- Spezifische technische Anforderungen an Sicherheit von Telekommunikationsanlagen

Energierecht

- ggf. relevant bei Komponenten für Energienetze oder -anlagen
- Besondere Absicherungspflichten für Betreiber von Energienetzen und -anlagen

Straßenverkehrsrecht

- ggf. relevant bei Fahrzeugen oder Bauteilen
- Besondere Regelungen für KFZ mit autonomer Fahrfunktion

Medizinprodukte

- ggf. relevant bei Bauteilen oder Maschinen zur Produktion von Medizinprodukten
- Besondere Regelungen zur Sicherheit für Gesundheit von Personen, Haustieren, Gütern und Umwelt



Learning: Je nach Branche des Kunden und Anwendungsbereich des Produktes können zusätzliche Anforderungen an Cyber-Sicherheit bestehen. Branchenspezifische Pflichten sind in der Regel deutlich konkreter als allgemeine Anforderungen.

2. Empfehlungen für die Praxis



Empfehlungen für die Praxis

Bestandsaufnahme	Rechtliche Analyse	Technische Analyse	Technischer Prüfprozess	Reaktionsplan	Mitigieren rechtlicher Risiken
Für welche Produkte können überhaupt Cyber-Risiken bestehen?	Welche allgemeinen oder konkreten rechtlichen Anforderungen bestehen für Cyber-Security bei diesen Produkten?	Welche Angriffsvektoren bestehen? Wie können Fehler behoben werden (Updatewege)? Welche Auswirkungen ergeben sich auf Umsysteme?	Wie können Cyber-Risiken in der Produktion identifiziert und adressiert werden?	Wer reagiert wie auf Bekanntwerden von Sicherheitslücken? Welche Pflichten bestehen? Was muss passieren?	ggf. Anpassung von Vertragswerken, Produktbeschreibungen oder Marketing-Material

 **Learning:** Entscheidend ist es, seine Risiken zu kennen und rechtzeitig Prozesse zu etablieren, um Risiken idealerweise von Anfang an zu vermeiden und im Ernstfall reagieren zu können.

Vielen Dank

Osborne Clarke ist der Firmenname für ein internationales Rechtsanwaltsbüro und die damit verbundenen Abteilungen. Alle Einzelheiten dazu hier: osborneclarke.com/verein

Diese Materialien werden nur zu allgemeinen Informationszwecken geschrieben und bereitgestellt. Sie sind nicht vorgesehen und sollten nicht als Ersatz für Rechtsberatung verwendet werden. Bevor Sie sich mit einem der folgenden Themen befassen, sollten Sie sich rechtlich beraten lassen.

© Osborne Clarke Rechtsanwälte Steuerberater Partnerschaft mbB

