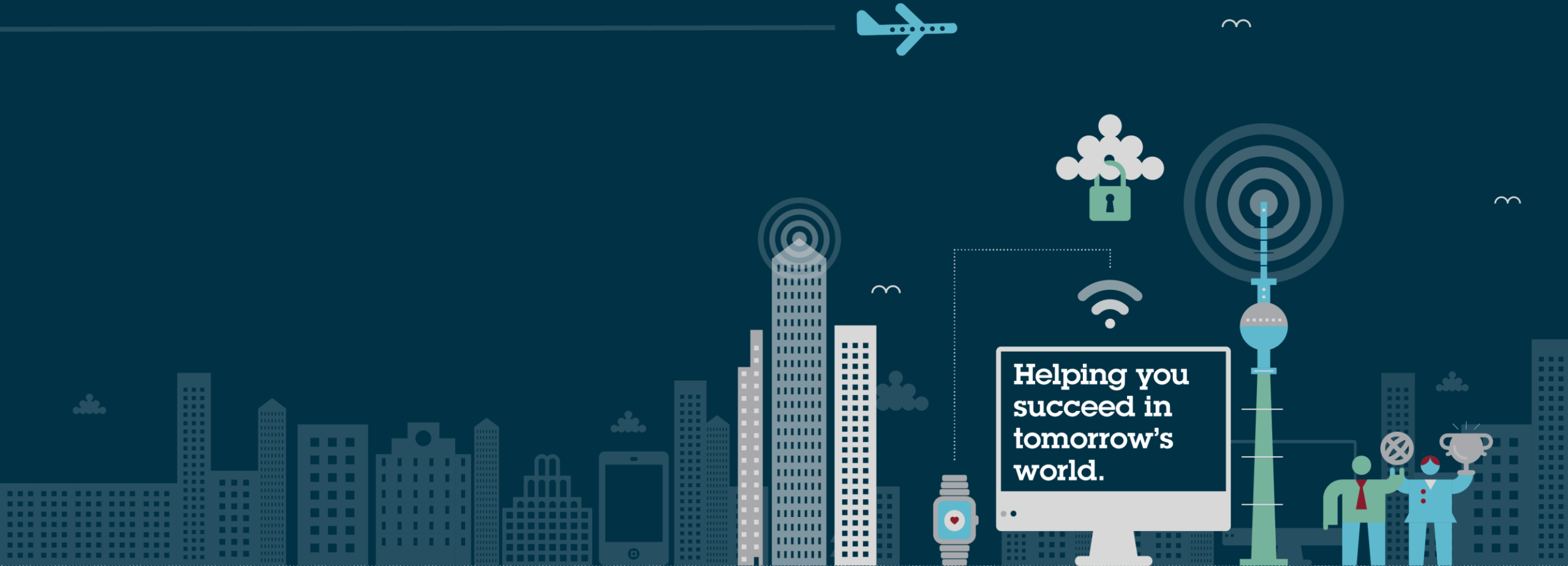


Rechts-Update: Cyber Security

Zukunftsallianz Maschinenbau e.V.

28. Oktober 2021



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 / Counsel

+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. Rechtlicher Überblick



1



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.



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



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 Produktsicherheitsrecht



Produktsicherheitsrecht: Anforderungen an Cyber-Sicherheit



Wer oder was ist geschützt?

Schutz der **Allgemeinheit** vor gefährlichen Produkten



Wer ist verpflichtet?

Unternehmen, das Produkt „auf den Markt bringt“



Was sind die Anforderungen?

Allgemein: Produkt darf bei bestimmungsgemäßer oder vorhersehbarer Verwendung die Sicherheit und **Gesundheit von Personen** nicht gefährden.

Besondere Anforderungen an bestimmte Produkte, z.B. Maschinenrichtlinie:

- Zusätzlich: Produkte dürfen Sicherheit von Haustieren, Gütern und Umwelt nicht gefährden
- Spezifische Anforderungen von EU-Richtlinien an sichere Produktgestaltung – aber nur mittelbare Anforderungen an Cyber-Sicherheit (z.B. bei Fernsteuerung)



Produktsicherheitsrecht: Anforderungen an Cyber-Sicherheit



Risiken

Zivilrechtliche Haftung
Aufsichtsbehördliche Maßnahmen
(Theoretisch) Bußgelder bis zu 100.000 EUR



Typische Herausforderungen in der Praxis

Regelungen nicht auf Cyber-Sicherheit ausgelegt – Übertragbarkeit teils schwierig.
Beispiele:

„Maßnahmen zu treffen, die eine unerlaubte Benutzung der Steuerung verhindern“
„[...] ferngesteuerte Maschine muss so konstruiert [...] sein, dass sie nur auf Steuerbefehle von dem für sie vorgesehenen Bedienungsgerät reagiert.“



Learning: Auch Sicherheitsanforderungen, die nicht spezifisch darauf ausgelegt sind, können Auswirkungen auf Anforderungen an Cyber-Sicherheit haben.



6 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.



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

