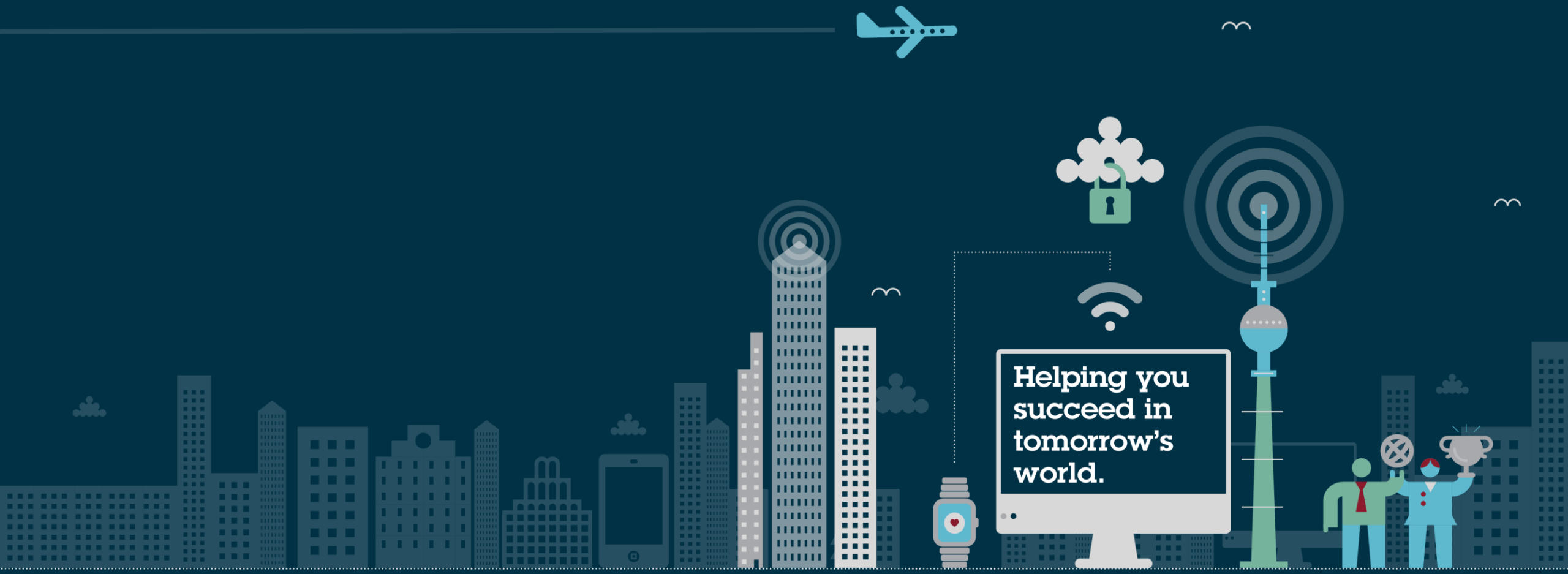
Industrial Cyber Security für den Mittelstand

Rechtliche Anforderungen an IT-Sicherheit

8. 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
- Energierecht
- …

Typische gesetzliche Anforderungen

Technisch-organisatorische Maßnahmen

- Allgemeine technische und organisatorische Maßnahmen zum Schutz von Daten, Systemen, Institutionen oder Personen
- Beispiele:
  - DSGVO
  - BSI-Gesetz
  - TTDSG
- In aller Regel technologie-neutral und flexibel formuliert
- Spezifizierung durch Normen, Behörden, Verordnungen oder Industriestandards

Spezifische Anforderungen an bestimmte Produkte

- Konkrete Gestaltungsvorgaben für bestimmte Produkte oder Maschinen
- Beispiele:
  - Maschinenrichtlinie
  - FahrzeugzulassungsVO
  - Telekommunikationsanlagen
  - Funkanlagen
  - Energieanlagen und -netze
  - Außenwirtschaftverordnung
- Häufig sektor- oder produktspezifisch

Anforderungen an Prozesse und Dokumentation

- Pflichten für Konzeption und Unternehmensorganisation
- Beispiele:
  - Dokumentationspflichten nach DSGVO
  - Sicherheitsmanagement-system und -konzept nach StörfallVO / Immissionsschutz
  - Systeme zur Angriffserkennung nach BSI-Gesetz (ab 1. Mai 2023)

Melde- und Informations-pflichten

- Pflichten zur Information von Behörden oder Betroffenen
- Beispiele:
  - Melde- und Benachrichtigungspflichten nach DSGVO
  - Meldepflichten nach BSI-Gesetz für kritische Infrastrukturen, UBÖFI und digitale Dienste
  - Meldepflichten nach StörfallVO
  - Informations- und Warnpflichten nach Produkthaftungsrecht

Top 3 Fälle aus der Praxis

1 Datenleck

Datenlecks – Rechtsfragen in der Praxis

Was ist zu tun?

- **Sachverhalt klären**: Wurden tatsächlich Daten abgezogen? Welche Daten? Wie viele? Verschlüsselt oder Klartext?
- **Mitigierende Maßnahmen** treffen: Lücken schließen, betroffene Accounts sperren, Passwörter zurücksetzen, etc.

Bestehen Meldepflichten?

Unter Umständen ja, zum Beispiel:

- Datenschutzbehörden bei Verlust personenbezogener Daten
- BSI bei erheblichen Beeinträchtigungen auf bestimmte Online Dienste
- BSI bei Störungen kritischer Infrastrukturen

Müssen Kunden informiert werden?

Unter Umständen ja, z.B.

- bei Verlust von personenbezogenen Daten über Kunden (Information an Betroffene), wenn potenziell ein hohes Risiko besteht
- bei Verlust von Daten, die für Kunden verarbeitet werden (Auftragsverarbeitung)
- Bei vertraglicher Vereinbarung

Staatsanwaltschaft einschalten?

- Tendenziell **ja**
- Spezialisierte Staatsanwaltschaften haben zahlreiche Möglichkeiten zur **Beweissicherung** und **Verfolgung**, ggf. auch zur **Wiederherstellung der Daten**
- Potenziell Faktor bei Bemessung von Bußgeldern

Bestehen Schadensersatzpflichten?

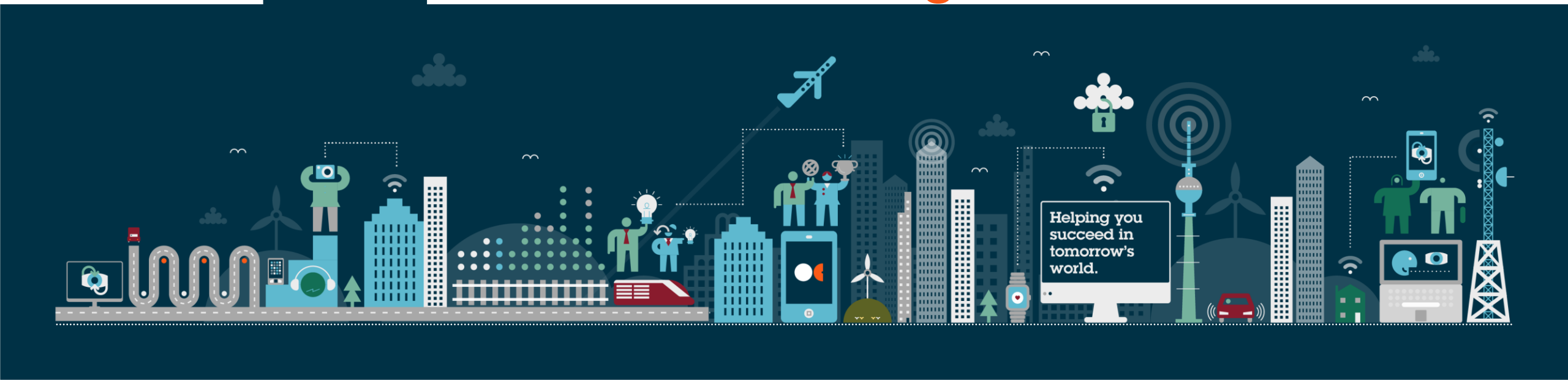
- **Unter Umständen ja**, z.B. bei Verlust von Daten, die für Kunden verarbeitet werden
- Verlust von benötigten Informationen zur **Abwehr gegen Ansprüche** (z.B. Verlust von Projektdokumentationen)

Maßgeblich: Verletzung von Pflicht zu technisch-organisatorischen Maßnahmen

Bestehen Bußgeldrisiken?

Unter Umständen ja:
Potenziell Verstoß gegen Pflicht zu technischen und organisatorischen Maßnahmen unter DSGVO und BSIG

2 Ransomware Angriffe



Ransomware Angriffe – Rechtsfragen in der Praxis

Bezahlen oder nicht bezahlen?

- Empfehlung: **Nicht vorschnell** bezahlen
- **Keinerlei Garantie**, dass Daten freigegeben werden
- Eigene **Strafbarkeit** wegen Beihilfe denkbar, insbesondere Geldwäsche

Staatsanwaltschaft einschalten?

- Tendenziell **ja**
- Spezialisierte Staatsanwaltschaften haben zahlreiche Möglichkeiten zur **Beweissicherung** und **Verfolgung**, ggf. auch zur **Wiederherstellung der Daten**
- Strafrechtliche Möglichkeiten zur **Vermögenssicherung** (z.B. Adhäsion)
- Individuelle Prüfung

Bestehen Meldepflichten?

- **Unter Umständen ja**, zum Beispiel:
  - Datenschutzbehörden bei Verlust personenbezogener Daten
  - BSI bei erheblichen Beeinträchtigungen auf bestimmte Online Dienste
  - BSI bei Störungen kritischer Infrastrukturen

Müssen Kunden informiert werden?

Unter Umständen ja, z.B.

- bei Verlust von personenbezogenen Daten über Kunden (Information an Betroffene) , wenn potenziell ein hohes Risiko besteht
- bei Verlust von Daten, die für Kunden verarbeitet werden (Auftragsverarbeitung)

Bestehen Schadensersatzpflichten?

- **Unter Umständen ja**, z.B. bei Verlust von Daten, die für Kunden verarbeitet werden
- Verlust von benötigten Informationen zur **Abwehr gegen Ansprüche** (z.B. Verlust von Projektdokumentationen)

Fehlende Backups sind Pflichtverletzung!

Bestehen Bußgeldrisiken?

- **Unter Umständen ja.**
- Fehlende Backups sind Verstoß gegen Pflicht zu technischen und organisatorischen Maßnahmen unter DSGVO und BSIG

3 Software-Sicherheitslücken

Software-Sicherheitslücken – Rechtsfragen in der Praxis

Was ist zu tun?

- **Sachverhalt klären**: Welche und wie viele Systeme sind betroffen? Welche Risiken bestehen? Welche Kunden sind potenziell betroffen?
- Mitigierende Maßnahmen einleiten: Patches einspielen (wenn verfügbar), Systeme anderweitig absichern, Umgehungsmaßnahmen

Müssen Kunden informiert werden?

Unter Umständen ja, z.B.

- wenn eigene Systeme bei Kunden **on-premise** betroffen sind (Schadensminderungspflicht)
- wenn Gewährleistungs- oder Pflegeansprüche bestehen
- Warnung bei Produkthaftung

Muss ich patchen?

- Bei eigenen Systemen: **Ja**
- Bei Kundensystemen:
  - Wenn Gewährleistung besteht
  - Wenn Wartungs-/Pflegevertragbesteht
  - Bei Miete/Leasing
  - Bei SaaS

Bestehen Schadensersatzpflichten?

Unter Umständen ja, wenn:

- Gewährleistung, Wartungs-/Pflegevertrag, Miete/Leasing oder SaaS und
- wenn Pflichtverletzung vorliegt und
- Schaden eintritt.

Bestehen Meldepflichten?

- **Unter Umständen ja**, zum Beispiel:
  - BSI bei erheblichen Beeinträchtigungen auf bestimmte Online Dienste
  - BSI bei Störungen kritischer Infrastrukturen

Bestehen Bußgeldrisiken?

Nur bei **Verletzung von Pflichten** zu technischen und organisatorischen Maßnahmen oder wenn Schadensfall eintritt.

Bei nicht ausgenutzten Lücken in der Praxis **eher nicht**.

Empfehlungen für die Praxis

Empfehlungen für die Praxis

Bestandsaufnahme	Rechtliche Analyse	Technische Analyse	Technischer Prüfprozesses	Reaktionsplan	Mitigieren rechtlicher Risiken
Für welche Produkte können überhaupt Cyber-Risiken bestehen?	Welche rechtlichen Anforderungen bestehen für Cyber-Security bei diesen Produkten? Welche vertraglichen Verpflichtungen bestehen ggü. Kunden?	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.