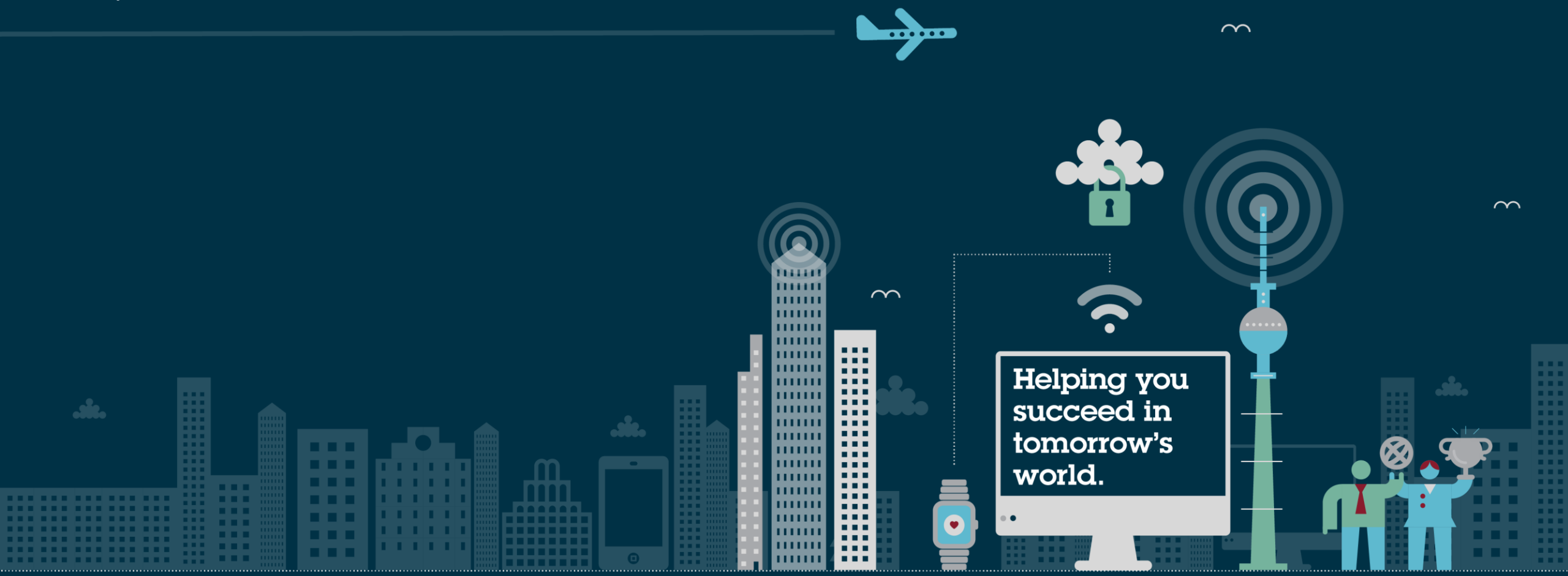
Rechts-Update: Cyber Security

Zukunftsallianz Maschinenbau e.V.

19. April 2023



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
- …

Lagebericht: Bedrohung massiv gestiegen

CYBERANGRIFFE IN DEUTSCHLAND 2023

Diese Unternehmen hat's schon erwischt

Ransomware, Brute Force, DDoS und Co: Diese deutschen Unternehmen wurden in diesem Jahr bereits von Cyberkriminellen attackiert.

IT-Sicherheitslage spitzt sich zu

Lohnlisten erbeutet?

Hacker-Gruppe Play erpresst NZZ und CH Media

17. April 2023

Ransomware-Angriff auf Lürssen Werft

18. April, 2023 07:56

18. April 2023

Ransomware-Attacke: Kassensystemhersteller NCR Opfer von Cyber-Angriff

18. April 2023

Cyberangriff auf Continental

10. Februar 2023

Deutschlands größter Rüstungskonzern

Cyberangriff auf Rheinmetall

14. April 2023

Angriff mit Ransomware

Ferrari wird nach Datendiebstahl erpresst

21. März 2023

1 Ausblick: NIS II-Richtlinie

Was bisher geschah…

1991
Inkrafttreten;
Gründung des BSI

2009
Erweiterung Aufgabenkatalog BSI & Ausweitung Befugnisse

2015
Änderungen durch IT-Sicherheitsgesetz 1.0

2016
EU erlässt NIS-1-Richtlinie
Deutschland setzt um

2021
Änderungen durch IT-Sicherheitsgesetz 2.0

2022
Veröffentlichung NIS 2 im EU-Amtsblatt
27. Dezember 2022

2023 …
Umsetzung in neues Recht

Frist: Oktober 2024

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.

Melde-, Registrierungs- und Nachweispflichten

Ab 1. Mai 2023: Pflicht zur Implementierung von **Systemen zur Angriffserkennung** (SIEM/IDS)

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

BSI-Gesetz: Anforderungen an Cyber-Sicherheit

Risiken

- Bußgelder gegen Unternehmen, 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

Was bisher geschah…

Gruppe 1: KRITIS

- Energie
- Transport und Verkehr
- Ernährung
- Finanz- und Versicherungswesen
- Gesundheit
- Wasser *(Trinkwasserversorgung und Abwasserbeseitigung)*
- Informationstechnik und Telekommunikation
- Siedlungsabfallentsorgung

+ Schwellenwerte in KRITIS-VO

Gruppe 2: Digitale Dienste

Digitale Dienste (Marktplätze, Suchmaschinen, Cloud-Computing)

Gruppe 3: UBIs

UBIs (AWV, Wertschöpfung, Störfall)

+ Ausnahmen für KMU

UBI

Erweiterung der regulierten Unternehmen:

- „**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 (**vermutlich überholt**)
  - **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)

Das kommt mit NIS 2

Sektoren mit hoher Kritikalität

- Energie
- Verkehr
- Bankwesen
- Finanzmarkt
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT
- Öffentliche Verwaltung
- Weltraum

Sonstige kritische Sektoren

- Post
- Abfallwirtschaft
- Chemie
- Lebensmittel
- Verarbeitung und Herstellung von Waren
- Digitale Dienste
- Forschung

Das kommt mit NIS 2

Sektore

Verarbeitendes Gewerbe / Herstellung von Waren

- Herstellung von Medizinprodukten und In-vitro-Diagnostika
- Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
- Herstellung von elektrischen Ausrüstungen
- **Maschinenbau**
- Herstellung von KFZ und KFZ Teilen
- Sonstiger Fahrzeugbau

Energie

Finanzmarkt

Abwasser

Digitale Infrastruktur

Verwaltung von IKT

Öffentliche Verwaltung

Weltraum

Sonstige kritische Sektoren

Post

Abfallwirtschaft

Chemie

Lebensmittel

Verarbeitung und Herstellung von Waren

Digitale Dienste

Forschung

Anwendungsbereich

Wesentliche Einrichtung

Große Unternehmen[1] aus Sektor mit hoher Kritikalität

250+ Beschäftigte und
50+ Mio. EUR Umsatz oder 43+ Mio. EUR Bilanzsumme

Wichtige Einrichtung

Mindestens mittlere Unternehmen[1] aus beiden Sektorgruppen

50+ Beschäftigte und
10+ Mio. EUR Umsatz und < 43 Mio. EUR Bilanzsumme

oder

Sonderfälle

- Anbieter von öffentlichen elektronischen Kommunikationsnetzen oder -diensten
- Vertrauensdiensteanbieter
- Domain Registries oder bestimmte DNS-Dienste
- Einziger Anbieter kritischer gesellschaftliche oder wirtschaftlich wichtiger Tätigkeiten („sole provider“)
- Störung des Dienstes hätte wesentliche Auswirkungen auf öffentliche Ordnung oder Sicherheit
- Besondere Bedeutung auf nationaler oder regionaler Ebene für den jeweiligen Sektor
- Bestimmte Einrichtungen öffentlicher Verwaltung
- Betreiber von Einrichtungen unter RCE-Richtlinie[2]

1 Nach Empfehlung 2003/361/EG
2 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen

Pflichten unter NIS2

	Wesentliche Einrichtungen	Wichtige Einrichtungen
Meldungen wesentlicher Störfälle an Behörden	Ja	Ja
Meldung wesentlicher Störfälle an Kunden	Ja	Ja
Risikomanagement	Ja	Ja
Technische und organisatorische Maßnahmen	Ja	Ja
Verpflichtung für Leitungsorgane (Geschäftsführerhaftung?)	Ja	Ja

Folgen unter NIS2

	Wesentliche Einrichtungen	Wichtige Einrichtungen
Durchführung von Sicherheitsaudits durch Behörde	Ja	Ja
Gezielte Sicherheitsprüfungen und Scans durch Behörde	Ja	Ja
Regelmäßige und Ad-hoc Sicherheitsprüfungen	Ja	Nein
Informations- und Nachweispflichten gegenüber Behörde	Ja	Ja
Warnung durch Behörde möglich	Ja	Ja
Proaktive Anweisungen durch Behörde möglich	Ja	Nein
Reaktive Anweisung durch Behörde möglich	Ja	Ja
Benennung eines Überwachungsbeauftragten	Ja	Nein
Verpflichtung, Verstöße gegen NIS2 auf Anordnung offenzulegen	Ja	Nein
Bußgeld	10 Mio EUR oder 2% des Jahresumsatzes	7 Mio. EUR oder 1,4% des Jahresumsatzes

Konkrete Vorgaben für Maßnahmen

- Risiko- und Sicherheitskonzepte
- Maßnahmen zur Bewältigung von Sicherheitsvorfällen
- Business Continuity Konzept (insbesondere Backup und Restore)
- Maßnahmen zur Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen (insbesondere Schwachstellenmanagement)
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Kryptografie
- Maßnahmen zur Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- Verwendung Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme

2 Blick an den Horizont

Cyber Resilience Act

Worum geht es?

Anforderungen an Produkte mit digitalen Elementen über den gesamten Lebenszyklus von Produkten:

- Vorschriften für Hersteller, Importeure und Händler von Soft- und Hardware
- Anforderungen an Entwicklung von Produkten (Entwicklungsstandards, Due Diligence von Drittkomponenten)
- Informations- und Dokumentationspflichten
- Konformitätsbewertung und –überwachung
- Meldepflichten
- Updatepflichten
- Gestaffelt nach Risikoklassen
- Bußgelder zwischen **5 Mio. und 15 Mio. EUR** oder zwischen **1% und 2,5%** des weltweiten Jahresumsatzes

AI Act

Worum geht es?

Regulierung von Systemen der künstlichen Intelligenz

- Generelles Verbot bestimmter KI-Systeme
- Hohe Anforderungen an bestimmte Hochrisiko-KI und „General Purpose“-KI
- Risiko- und Qualitätsmanagement
- Data-Governance
- Transparenz- und Informationspflichten
- Konformitätsbewertung und –überwachung
- Menschliche Aufsicht
- Registrierungspflicht
- Meldepflichten
- Bußgelder zwischen **10 Mio. und 30 Mio. EUR** oder zwischen **2% und 6%** des weltweiten Jahresumsatzes

Richtlinie über KI-Haftung

Worum geht es?

Regelungen zur Beweiserleichterung bei Schäden durch KI

- Verpflichtung zur Herausgabe von Beweismitteln in Haftungsfällen
- Vermutung von Sorgfaltspflichtverletzungen, wenn Beweismittel nicht herausgegeben werden
- Vermutung von haftungsbegründender Kausalität, wenn Beweismittel nicht herausgegeben werden

Produkthaftungsrichtlinie

Worum geht es?

Erweiterung der europäischen Produkthaftung – auch auf Software und Sicherheitsaspekte

- Soll nun auch (eindeutig) Software erfassen
- Auch Haftung für nachträgliche Fehler – auch in Bezug auf Updates
- Produkt gilt als fehlerhaft, wenn es nicht die Sicherheit bietet, die Öffentlichkeit erwarten darf
- Folge: **Verschuldensunabhängige Haftung**
- Nach aktuellem Diskussionsstand ohne Haftungscap und ohne Mindestschadensbetrag

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.