Unter Dauerbeschuss

Aktuelle Herausforderungen für Cybersecurity und Datenschutz

Dr. Sebastian Brüggemann

06.11.2025

ADV Rechtstag 2025

Über mich

Dr. Sebastian Brüggemann, M.A.

Director & Counsel

Global Cybersecurity & Data Governance Legal @ kyndryl

Lehrbeauftragter & Dozent

Tübingen, Winterthur, Ludwigsburg, Kehl, Stuttgart

Autor diverser Fachbeiträge

Mitglied der Redaktion der Fachzeitschrift Privacy in Germany (PinG)

War Ihr Unternehmen bereits Ziel eines Cyberangriffs?

Cybersecurity im Jahr 2025

Laut Bitkom Wirtschaftsschutz-Studie sind Cyberattacken im Unternehmensalltag angekommen...

- 87% der Unternehmen in Deutschland betroffen
- 73% berichten von einer Zunahme von Cyberattacken
- Geschätzter Gesamtschaden von ca. 200 Mrd. EUR
- 2/3 der betroffenen Unternehmen berichten von Datenverlust
- 1/3 Ransomware-Angriffe (P: Lösegeldzahlungen, Double Extortion)

Quelle: Bitkom

Aktuelle Herausforderungen

01

Gesteigerte Bedrohungslage

02

Zunehmende Komplexität

03

(Global) Zunehmende Regulierungsdichte

Jeder kann zum Ziel eines Angriffs werden!

Gesteigerte Bedrohungslage

- Weitestgehend automatisiertes Ausspähen möglicher Ziele / vorhandener Sicherheitslücken (einschl. Malware Deployment)
- Drastische Zunahme der Angriffe
- Professionalisierung der beteiligten Akteuere (Cybercrime is a Business)
- Staatliche Akteure
- Vermehrte Aufmerksamkeit auf Sicherheitslücken
- Faktor Mensch (Phishing als Hauptangriffsvektor)
- Beschleunigung des Wettrüstens durch KI
- Trittbrettfahrer

Zunehmende Komplexität

- Vielzahl von Dienstleistern (Lieferkette)
- Gesteigerte Abhängigkeiten
- Fehlende Transparenz
- Unklare Zuständig- / Verantwortlichkeiten
- Mangelnde Koordination
- Komplexere IT-Architekturen
- Faktor Mensch

(Global) Zunehmende Regulierungsdichte

Zunehmende Regulierungsdichte (EU)

DSGVO	DORA	NIS2-Richtlinie
Cyber Resilience Act (CRA)	Cybersecurity Act (CSA)	EU-Cybersolidaritäts-verordnung

Meldepflichten (Auszug)

01

Datenschutz

(Kunden, Aufsicht, Betroffene)

72 Stunden (DSGVO)

02

Cybersecurity

24 Stunden (NIS 2)

6 Stunden (Cert-In)

72 Stunden (USA)

24 Stunden bei Lösegeldzahlungen (USA)

03

Branchenspezifische Aufsicht

(z.B. Bafin, BNetzA, etc.)

24 Stunden (DORA)

04

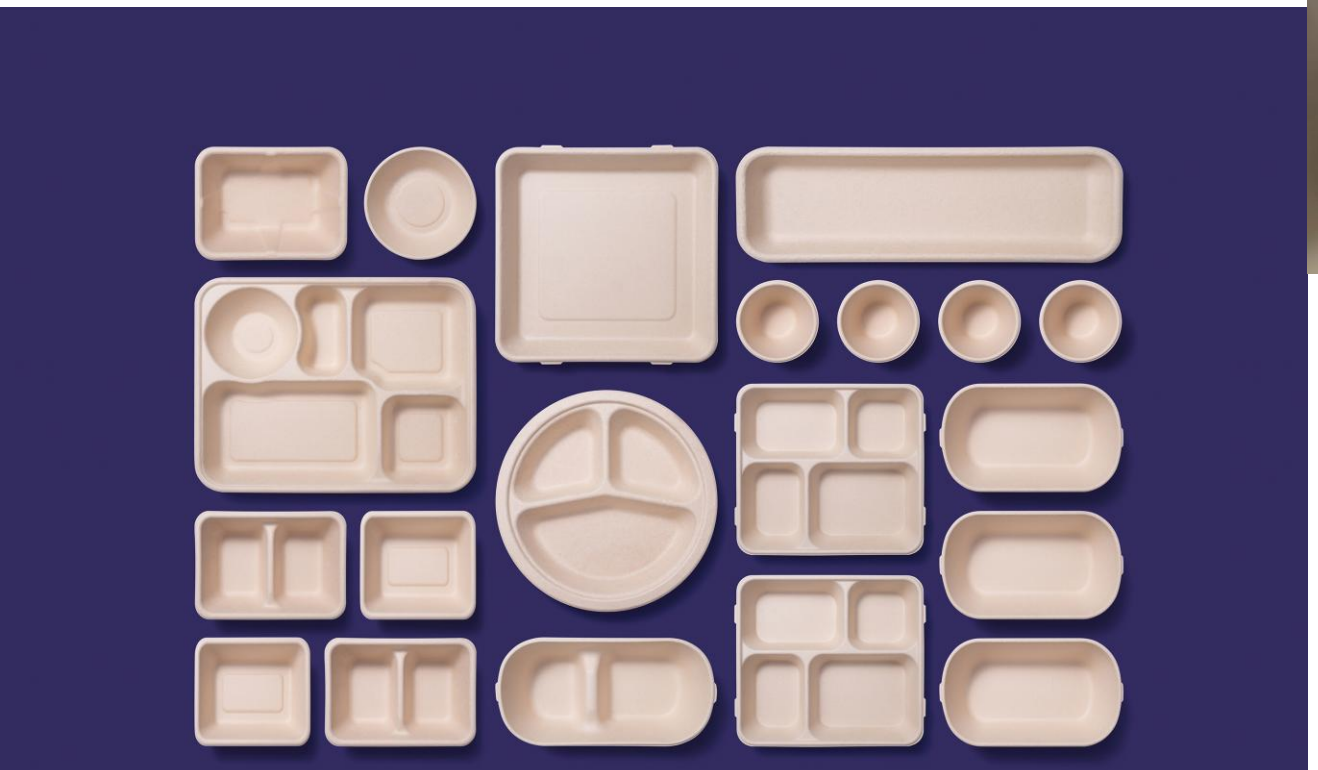
Finanz- / Börsenaufsicht

(z.B. SEC in den U.S.)

4 Tage (SEC)


Können Sie (mir) noch folgen?

Stop Thinking in Silos!



Start Managing Risk Wholistically!

Maßnahmen zur Risikominimierung

Maßnahmen zur Risikominimierung

- Cyberattacken sind im Unternehmensalltag angekommen → Betriebsrisiko, Haftung
- Datenschutz und Cybersecurity = Business Continuity
- Interne Meldeprozesse
- Geschultes Personal
- Notfallplan/-strukturen
  - Wer übernimmt die Koordination?
  - Steht mir im Notfall die erforderliche Expertise zur Verfügung? (CSIRT / Legal)
  - Welchen Regularien unterliegt mein Unternehmen?
  - Welche Aufsichtsbehörden sind zuständig? Wann melde ich, wie und wo?

Maßnahmen zur Risikominimierung

- Transparenz
  - Wer verarbeitet, welche Daten, wo? (Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO))
- Datensparsamkeit
- Vertragsgestaltung (Lieferkette)
  - Sicherheit ist vorallem (auch) Sache des Verantwortlichen (Art. 32 DSGVO) (s. Bußgeldfälle)
  - Klare Sicherheitsmaßnahmen (TOMs)
  - Klare Verantwortlichkeits-/Zuständigkeitsregelungen
  - Potenzielle Mehrkosten / Mehrarbeit regeln

Maßnahmen zur Risikominimierung

- Sicherheitsmaßnahmen vs. Datenschutz
  - Mitarbeiterdatenschutz/-überwachung
  - Rechtsgrundlagen
    - Berechtigtes Interesse (Art. 6 Abs. 1 f) DSGVO)
    - Starkes gesetzliches Mandat (Art. 32 DSGVO)

Geschafft!

Kontakt

Dr. Sebastian Brüggemann, M.A.

Director & Counsel
Global Cybersecurity & Data Governance Legal
Kyndryl Deutschland GmbH
sebastian.brueggemann@kyndryl.com