GoldbergUllrich
Rechtsanwälte

Rechtliche Aspekte der Cybersicherheit

Haftungsrisiken, Pflichten, Cyberversicherung, Praxis-Checkliste

Agenda

- Warum Cybervorfälle potentielle Haftungsfälle sind
- Die wichtigsten gesetzlichen Regelungen
- Wie Haftung in der Praxis geprüft wird
- Vertrags-, Lieferketten- und Versicherungsaspekte
- Must-dos
- Checkliste
- 3 Takeaways

Mögliche Haftungsfolgen bei Cybervorfällen

Behördliche Maßnahmen
Bußgelder, Auflagen, Leitungsverantwortung

Zivilrechtliche Außenhaftung
Schadensersatz von Kunden, Betroffenen, Partnern, Vertragsstrafen, Kündigungen bei Ausfällen

Organ- und Innenhaftung
Regress gegen Geschäftsleitung bei Organisations-/Überwachungsmängeln

Versicherungsrechtliche Risiken - Später

Bsp.: Ransomware legt Betrieb lahm → Mögliche Sanktionen:

DSGVO-Bußgelder + Kundenklagen (Schadensersatz) +

Regressforderungen durch Lieferanten und Abnehmer.

DSGVO

- Art. 32 DSGVO: Risikoangemessene **T**echnische **O**rganisatorische **M**aßnahmen (TOM) („Stand der Technik“)
- Art. 33/34 DSGVO: Meldung innerhalb von 72 Stunden + ggfs. Benachrichtigung Betroffener
- Art. 82 DSGVO: Schadensersatz (materiell + immateriell)

Merksatz: Unzureichende TOM sind der Standard-Ansatzpunkt für Bußgelder und Schadensersatzklagen.

IT-Sicherheitsrecht (BSIG/NIS2)

- BSIG (neu): Pflichten für KRITIS-Betreiber und deren Zulieferer
- NIS2-Umsetzungsgesetz: In Deutschland am 6. Dezember 2025 in Kraft getreten – Neuregelung/Erweiterung des Pflichtenkataloges des BSIG
- Betroffen unter NIS2: Viele Mittelständler in Energie, Verkehr, Gesundheit, Produktion, Digitaldienste u.a.
- Pflichten: Risikomanagement, Schutzmaßnahmen, Überwachung, Schulungen, Meldepflichten, Maßnahmenkatalog inkl. Lieferkettensicherheit etc.
- Neu: Geschäftsleitung (nicht CISO) muss angemessene Cybersicherheitsmaßnahmen billigen/umsetzen, überwachen, sich selbst und Mitarbeiter schulen lassen – sonst persönliche Haftung

Cyber Resilience Act (CRA)

- Gilt für Produkte mit digitalen Elementen (Software, Hardware, IoT, Geräte mit IT-Komponenten) - Security by design / default
- Betroffen: Hersteller, Importeure und Händler, die solche Produkte in der EU anbieten
- Lifecycle-Pflicht: Schwachstellen-Management, Sicherheitsupdates, Konformität/CE-Relevanz
- Meldepflichten ab 11.09.2026, volle Anwendbarkeit ab 11.12.2027
- Haftungslogik: Sicherheitslücken oder fehlende Updates können Produktfehler sein.

Wie wird Haftung juristisch geprüft?

1. Pflichtmaßstab: Gesetz/Verordnung oder Vertrag („Stand der Technik“) – wie sollte es sein?
2. Pflichtverletzung: Negative Abweichung vom Maßstab oder fehlende Organisation/Dokumentation
3. Kausalität: Hätte ein angemessenes Schutzniveau den Schaden verhindert/verringert?
4. Zurechnung: Unternehmen außen, Geschäftsleitung innen (Organhaftung)

Vertragliche Regelungen

- Unabhängig von Spezialgesetzen gilt: IT-Sicherheit ist Nebenpflicht in fast jedem Vertrag
- Haftungshebel: vereinbarter Sicherheitsstandard (z.B. SLA, AVV) und Updatepflichten
- Vertrags- und Lieferkette: Auswahl- und Überwachungspflichten für Dienstleister bleiben beim Unternehmen
- Praxis: Ohne klare Incident-/Audit-Klauseln drohen Schadensersatzansprüche und Deckungslücken bei Versicherungen

Cyberversicherung ≠ Freifahrtschein

- Cyberversicherung = Risikotransfer, nicht Risikovermeidung
- Regulatorische Pflichten bleiben (DSGVO, NIS2, CRA,DORA, AI-Act etc.)
- Fehlannahme: „Versichert = sicher“ → Haftungs- und Deckungslücken, Bußgelder werden i.d.R. nicht übernommen
- Versicherer kalkulieren mit bestimmten Sicherheitsstandards und Obliegenheiten

Merksatz: Versicherungspolicen wirken nur, wenn die IT-Sicherheit, deren Dokumentation und die Angaben gegenüber der Versicherung fortlaufend (=immer) den Vertragsbedingungen entsprechen und zutreffend sind.

Cyberversicherung: Obliegenheiten & Leistungsfreiheit

- Typische technische Mindeststandards als Obliegenheiten:
  u.a. aktuelle IT-Sicherheit, Patch-Management und Mitarbeiterschulungen
- Wahrheitsgemäße Risikoangaben im Antrag
- Keine Gefahrerhöhung ohne Anzeige (u.a. veränderte IT-Infrastruktur, neue Software, die Nutzung externer Dienstleister, Änderungen in der Arbeitsweise (z.B. Homeoffice)
- Schaden-Obliegenheiten: sofort melden, kooperieren, IR-Dienstleister nutzen
- Mögliche Rechtsfolge bei Verletzung einer Obliegenheit:

(§ 28 VVG): grob fahrlässig → Leistungskürzung
vorsätzlich → Leistungsfreiheit

Gemeinsamer Prüfmaßstab für Haftungsfragen

1. Stand der Technik bei der IT-Sicherheit erreicht?
2. Organisation & Dokumentation vorhanden? (DSGVO, ISMS, Policies, Logs etc.)
3. Incident Response funktioniert? (Detection, Containment, Meldung)
4. Drittparteien gesteuert? (Verträge, Audits, Monitoring)

Rechtliche Must-dos

(Management/Legal):

1) Betroffenheits-Check: DSGVO immer; NIS2/BSIG/CRA/DORA je nach Branche/Produkt

2) Governance: Verantwortlichkeiten, Budget- und Leitungsbeschlüsse dokumentieren

3) Melde- und Kommunikationswege festlegen (DSGVO 72h, NIS2-Frühwarnung, Versicherer)

4) Dienstleister- und Lieferantenverträge cyberfest gestalten (Standards, Updates, Audits, IR)

5) Cyberversicherung juristisch steuern (u.a. Obliegenheiten, Risikoangaben)

Abschluss-Checkliste

Kurz-Checkliste:

- Sind Anwendungsbereich und Stichtage der gesetzlichen Regelungen geprüft und dokumentiert?
- Ist unsere IT-Sicherheit auf dem „Stand der Technik“?
- Gibt es einen nachweisbaren Beschluss der Geschäftsleitung zu Cyber-Risikomanagement?
- Sind Meldepflichten/Fristen intern und extern geregelt?
- Sind kritische Verträge inkl. Haftung/SLAs/Prüfregeln aktualisiert?
- Erfüllen wir bei bestehender Cyberversicherung die Versicherungs-obliegenheiten nachweisbar und sind unsere Dokumentationen aktuell?

3 Takeaways

IT- und Cybersicherheit sind Chefsache.

Rechtsmaßstab = Stand der Technik + Dokumentation

Versicherungsschutz besteht nur bei gelebten Obliegenheiten.

Kontakt

Michael Ullrich, LL.M. (Informationsrecht)
Rechtsanwalt | Partner
Fachanwalt für gewerblichen Rechtsschutz
Fachanwalt für Informationstechnologierecht
Lehrbeauftragter der FOM Hochschule
für Oekonomie & Management

GoldbergUllrich Rechtsanwälte PartG mbB,
Friedrichstraße 51, 42105 Wuppertal
Tel.: +49 (0) 202 9422900
E-Mail: info@goldberg.de

LinkedIn

www.goldberg.de