GoldbergUllrich
Rechtsanwälte

Rechtliche Aspekte der Cybersicherheit

Haftungsrisiken, Pflichten, Cyberversicherung, Praxis-Checkliste

Rechtsanwalt Michael Ullrich, LL.M. (Informationsrecht)
Fachanwalt für gewerblichen Rechtsschutz
Fachanwalt für Informationstechnologierecht
Lehrbeauftragter für IT-,KI-, IP- und Datenschutzrecht an der
FOM Hochschule für Oekonomie und Management

GoldbergUllrich
Rechtsanwälte

Agenda

1. Warum Cybervorfälle potentielle Haftungsfälle sind
2. Die wichtigsten gesetzlichen Regelungen
3. Wie Haftung in der Praxis geprüft wird
4. Vertrags-, Lieferketten- und Versicherungsaspekte
5. Must-dos
6. Checkliste
7. 3 Takeaways

Mögliche Folgen von Cybervorfällen

1. **Behördliche Folgen**: Auflagen und Bußgelder bei Vorliegen der gesetzlichen Voraussetzungen
2. **Außenhaftung**: Ansprüche von Kunden, Betroffenen und Partnern, ggf. Vertragsstrafen oder Kündigungen
3. **Innenhaftung**: Regress gegen die Geschäftsleitung bei schuldhaften Pflichtverletzungen (z.B. Organisations-/Überwachungsmängel) mit Schaden
4. **Versicherung**: Deckungssumme nicht ausreichend. Pflichtverletzungen nach Police und VVG führen zu Kürzungen oder Leistungsfreiheit der Versicherung

Merke: Ein Cyberangriff allein begründet noch keine Haftung oder Sanktion.

DSGVO: Sicherheit, Meldung und Haftung

1. Art. 32: Risikoangemessene **t**echnische und **o**rganisatorische **M**aßnahmen (TOM) unter Berücksichtigung des Stands der Technik
2. Art. 33: Behörde unverzüglich, möglichst binnen 72 h ab Kenntnis informieren, außer bei voraussichtlich fehlendem Risiko
3. Art. 34: Betroffene bei voraussichtlich hohem Risiko unverzüglich benachrichtigen, gesetzliche Ausnahmen beachten
4. Art. 82: Schadensersatz setzt Verstoß, Schaden und Kausalität voraus

Merke: Ein erfolgreicher Cyberangriff beweist allein keine unzureichenden Schutzmaßnahmen. Aber: Unzureichende TOM sind ein Ansatzpunkt für Bußgelder und Schadensersatzklagen

IT-Sicherheitsrecht (BSIG/NIS2)

1. Das deutsche NIS2-Umsetzungsgesetz ist in Kraft. Jetzt betroffen: viele Mittelständler in Energie, Verkehr, Gesundheit, Produktion, Digitaldienste u.a.
2. Erfasst: besonders wichtige und wichtige Einrichtungen nach § 28 BSIG, KRITIS-Betreiber
3. Zulieferer: Eigene Betroffenheit prüfen. Zusätzlich können Kunden vertragliche Sicherheitsanforderungen stellen.
4. Pflichten: Risikomanagement, Lieferkettensicherheit, Schulungen sowie Registrierung und Vorfallmeldungen
5. Geschäftsleitung (nicht CISO): Maßnahmen umsetzen, Umsetzung überwachen und regelmäßig selbst an Schulungen teilnehmen
6. Innenhaftung bei schuldhaft verursachtem Schaden (§ 38 BSIG)

Cyber Resilience Act (CRA)

1. Gilt für Produkte mit digitalen Elementen (Software, Hardware, IoT, Geräte mit IT-Komponenten) und vorgesehener oder vorhersehbarer Datenverbindung
2. Meldepflichten (Art. 14 CRA) seit 11.09.2026: Hersteller melden aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle
3. Frühwarnung binnen 24 h, weitere Meldung binnen 72 h ab Kenntnis, danach Abschlussbericht
4. Hauptpflichten ab 11.12.2027 (volle Anwendbarkeit): sichere Produkte, Schwachstellenmanagement, Updates und Konformität/CE
5. Unterschiedliche Pflichten nach Rolle. Übergangs- und Haftungsregeln prüfen. Haftungslogik: Sicherheitslücken oder fehlende Updates können Produktfehler sein.

Prüfung zivilrechtlicher Haftung

1. Anspruchsgrundlage und Beteiligte: Wer verlangt von wem Ersatz?
2. Pflicht und Pflichtverletzung: Welche gesetzlichen oder vertraglichen Anforderungen gelten? Wie sollte es sein? Gibt es eine negative Abweichung?
3. Schaden und Kausalität: Welcher Schaden beruht auf der Pflichtverletzung?
4. Verantwortlichkeit: Verschulden, Zurechnung und mögliche Entlastung nach der jeweiligen Haftungsregel
5. Beweislast und Einwendungen: Nachweise, Haftungsgrenzen und Mitverantwortung prüfen
6. Außenhaftung und Organhaftung jeweils gesondert prüfen

Vertragliche Regelungen

1. IT-Sicherheit kann Hauptleistungspflicht oder Nebenpflicht sein. Inhalt und Umfang hängen vom Vertrag und seinen Risiken ab.
2. Sicherheitsstandards, Updates und Verfügbarkeit eindeutig vereinbaren (z. B. SLA und Auftragsverarbeitung)
3. Dienstleister risikogerecht auswählen und kontrollieren. Eigene gesetzliche Pflichten bleiben zu beachten.
4. Vorfallmeldungen, Mitwirkung, Prüfungsrechte und Verantwortlichkeiten konkret regeln
5. Haftungsklauseln und Versicherungsdeckung aufeinander abstimmen. Fehlende Klauseln begründen nicht automatisch Ansprüche.

Cyberversicherung: Umfang und Grenzen

1. Die Versicherung übernimmt vereinbarte finanzielle Risiken und ggf. Unterstützungsleistungen im Schadensfall
2. Gesetzliche Sicherheits- und Meldepflichten bleiben bestehen, soweit das Unternehmen ihnen unterliegt
3. Deckungsumfang, Ausschlüsse und Selbstbehalte der Versicherung bestimmen den Schutz
4. Eine Erstattung von Bußgeldern ist nach h.M. nicht versicherbar und in marktüblichen Policen ausgeschlossen. Rechtsverteidigungskosten prüfen.
5. Pflichtverletzungen können den Versicherungsschutz gefährden. Die Folgen richten sich nach Police und VVG, insbesondere nach Verschulden und Ursächlichkeit. Es drohen Leistungskürzungen oder Leistungsfreiheit.

Cyberversicherung: Pflichten und Rechtsfolgen

1. Antrag (§§ 19–22 VVG): bekannte erhebliche Risiken richtig und vollständig angeben
2. Gefahrerhöhung (§§ 23–27): bei erheblichen Änderungen in der IT oder der Arbeitsweise vorherige Einwilligung einholen oder unverzüglich anzeigen
3. Vertragliche Obliegenheiten (§ 28): Sicherheitsvorgaben und Pflichten im Schadensfall gemäß Police beachten
4. Mögliche Rechtsfolge bei Verletzung einer Obliegenheit:
grobe Fahrlässigkeit kann Kürzung, Vorsatz Leistungsfreiheit begründen
5. Nachweis fehlender Ursächlichkeit kann den Anspruch erhalten, außer bei Arglist. Weitere Voraussetzungen beachten.

Prüffragen zu Sicherheit und Organisation

1. Welche gesetzlichen und vertraglichen Anforderungen gelten für das Unternehmen?
2. Sind die Schutzmaßnahmen risikoangemessen und wirksam, unter Beachtung des maßgeblichen Stands der Technik?
3. Sind Zuständigkeiten, Entscheidungen und die Umsetzung nachvollziehbar dokumentiert?
4. Funktionieren Erkennung, Eindämmung, Wiederanlauf und fristgerechte Vorfallmeldungen?
5. Sind Dienstleister und Lieferanten risikogerecht eingebunden und kontrolliert?

Rechtliche Must-dos

1. Betroffenheit prüfen und beachten: DSGVO bei personenbezogenen Daten im Anwendungsbereich, NIS2/BSIG/CRA/DORA nach Tätigkeit und Produkt
2. Governance: Zuständigkeiten, Ressourcen, Leitungsentscheidungen und erforderliche Schulungen prüfen, festlegen und dokumentieren
3. Registrierungspflichten beachten: z.B. BSIG grundsätzlich binnen drei Monaten nach Eintritt der betreffenden Eigenschaft
4. Meldewege beachten: DSGVO unverzüglich, möglichst 72 h. BSIG und CRA mit 24-/72-h-Stufen bei jeweiligem Meldeauslöser
5. Verträge und Police: Standards, Vorfallmitwirkung, Haftung und Versicherungsanforderungen regelmäßig prüfen

Abschluss-Checkliste

1. Sind Betroffenheit, Stichtage und Registrierungen geklärt und dokumentiert?
2. Sind Schutzmaßnahmen wirksam und rechtskonform? Z.B.: Ist unsere IT-Sicherheit auf dem „Stand der Technik“?
3. Sind Leitungsentscheidungen und Schulungen belegt? Gibt es einen nachweisbaren Beschluss der Geschäftsleitung zu Cyber-Risikomanagement?
4. Sind Meldefristen, Adressaten und Verantwortlichkeiten geregelt?
5. Sind Sicherheits-, Haftungs- und Prüfregeln in Dienstleisterverträgen aktuell?
6. Sind Versicherungsumfang, Risikoangaben, Änderungen und Obliegenheiten bei der Cyberversicherung geprüft und dokumentiert?

GoldbergUllrich
Rechtsanwälte

3 Takeaways

1. IT- und Cybersicherheit ist Leitungsaufgabe. Umsetzung, Überwachung und erforderliche Schulungen gehören zusammen.

2. Maßgeblich sind Gesetz und Vertrag, risikoangemessene Sicherheit und belastbare Nachweise

3. Versicherungsschutz hängt von Versicherungspolice und VVG ab. Pflichtverletzungen können zur Kürzung oder Leistungsfreiheit führen

GoldbergUllrich
Rechtsanwälte

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