Institut für
Datenschutz und
Datensicherheit

Zusammenfassung der Haftungsrisiken eines Geschäftsführers bei unzureichenden technischen und organisatorischen Maßnahmen (TOM) zum Schutz vor Cyberrisiken und Datenschutzpannen – inkl. Rechtsgrundlagen

Ein Geschäftsführer trägt eine zentrale Verantwortung für die Einhaltung der gesetzlichen Vorgaben zum Datenschutz und der IT-Sicherheit. Unzureichende technische und organisatorische Maßnahmen (TOM) können erhebliche persönliche Haftungsrisiken auslösen. Die wichtigsten Punkte, einschließlich der relevanten Rechtsgrundlagen, sind:

---

1. Persönliche Haftung

- **§ 43 Abs. 2 GmbHG**: Geschäftsführer haften gegenüber der Gesellschaft, wenn sie ihre Sorgfaltspflichten verletzen. Dazu gehört auch die Organisation der IT-Sicherheit und des Datenschutzes.
- **§ 93 Abs. 1 AktG**: Für Vorstände in Aktiengesellschaften gilt die analoge Pflicht zur sorgfältigen Geschäftsführung.

Beispiel:

Ein Geschäftsführer, der es versäumt, geeignete Sicherheitsmaßnahmen wie Firewalls, Verschlüsselung oder Zugriffsrechte einzuführen, riskiert persönliche Schadensersatzforderungen.

---

2. Datenschutzrechtliche Verstöße

- **Art. 32 DSGVO**: Unternehmen sind verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein angemessenes Sicherheitsniveau zu gewährleisten.
- **Art. 82 DSGVO**: Betroffene haben Anspruch auf Schadensersatz bei Datenschutzverletzungen, wenn diese auf mangelnde Sicherheitsmaßnahmen zurückzuführen sind.
- **Art. 83 Abs. 4 und 5 DSGVO**: Für Verstöße gegen Datenschutzvorschriften können Bußgelder bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes verhängt werden.

Beispiel:

Falls eine Datenschutzpanne aufgrund fehlender Verschlüsselung sensibler Kundendaten auftritt, kann der Geschäftsführer verantwortlich gemacht werden, wenn er die IT-Sicherheitsstrategie nicht ausreichend überwacht hat.

---

3. Haftung bei Cyberangriffen

- **§ 823 BGB**: Schadensersatzpflicht bei Verletzung von Schutzpflichten, z. B. durch unzureichenden Schutz gegen Cyberangriffe.
- **§ 1 ProdHaftG**: Bei IT-Produkten können zusätzliche Haftungsrisiken entstehen, wenn diese Sicherheitslücken aufweisen und dadurch Schäden verursacht werden.

Beispiel:

Ein Unternehmen erleidet einen Ransomware-Angriff, weil Sicherheitsupdates für die IT-Systeme nicht rechtzeitig eingespielt wurden. Hier kann der Geschäftsführer wegen Vernachlässigung seiner Kontrollpflichten haften.

---

4. Strafrechtliche Risiken

- **§ 202a StGB**: Ausspähen von Daten durch Dritte, das durch mangelnden Schutz begünstigt wird, kann auch strafrechtliche Folgen für Geschäftsführer haben, wenn grobe Fahrlässigkeit vorliegt.
- **§ 266 StGB**: Untreue kann relevant werden, wenn durch unterlassene Sicherheitsmaßnahmen Vermögensschäden für das Unternehmen entstehen.

Beispiel:

Eine mangelnde IT-Sicherheitsstrategie kann als strafrechtlich relevante Fahrlässigkeit bewertet werden, wenn dadurch sensible Kundendaten kompromittiert werden.

---

5. Organisatorische Verantwortung

- **§ 91 Abs. 2 AktG**: Vorstände von Aktiengesellschaften müssen ein Risikomanagementsystem einrichten. Dies gilt sinngemäß auch für Geschäftsführer von GmbHs (analog zu § 43 GmbHG).
- **Art. 5 Abs. 2 DSGVO**: Nachweispflicht der Einhaltung der Grundsätze der Datenverarbeitung („Accountability“).

Beispiel:

Ein fehlendes oder unzureichendes Datenschutzmanagementsystem wird als Organisationsverschulden angesehen, was zu Bußgeldern und Haftung führen kann.

Institut für Datenschutz und Datensicherheit

6. Mögliche Sanktionen und Folgen

- **Bußgelder**: Art. 83 DSGVO (bis zu 20 Mio. € oder 4 % des Jahresumsatzes).
- **Reputationsschäden**: Durch öffentlich bekannt gewordene Datenschutzpannen kann das Unternehmen nachhaltig Schaden nehmen.
- **Versicherungsschutz**: D&O-Versicherungen (Directors & Officers) greifen oft nicht bei grober Fahrlässigkeit oder Vorsatz.

---

7. Maßnahmen zur Risikominimierung

- **Regelmäßige Sicherheitsprüfungen**: Verpflichtung zur Aktualisierung der IT-Sicherheit (Art. 32 DSGVO).
- **Schulung der Mitarbeiter**: Pflicht zur Sensibilisierung hinsichtlich Datenschutzes und Cybersicherheit.
- **Externe Beratung**: Zusammenarbeit mit Datenschutzbeauftragten und IT-Sicherheitsfirmen.

Empfehlung:

Geschäftsführer sollten ein umfassendes Compliance-System implementieren, um gesetzliche Anforderungen zu erfüllen und Haftungsrisiken zu minimieren. Ein proaktives Risikomanagement und die regelmäßige Überprüfung von TOM sind entscheidend.

Diese Zusammenfassung bietet eine rechtliche Grundlage, um die Risiken und Pflichten des Geschäftsführers in Bezug auf Cyberrisiken und Datenschutzpannen zu verstehen.

Ralko Nebelung | IT-Systemingenieur
Geschäftsführer / Gesellschafter

Institut für Datenschutz und Datensicherheit

IfDDS GmbH
Institut für Datenschutz und Datensicherheit
Dresdner Straße 58a | 01156 Dresden

Datenschutz|Datensicherheit|Managementsysteme|Arbeitssicherheit|Hinweisgeberschutz

Büro: 0351 27 57 90 57
Mobil: 0151 22 34 99 07
E-Mail: r.nebelung@ifdds.de
Besuchen Sie uns auf www.ifdds.de