Infoblatt für Geschäftsführer

IT Security, gesetzliche Pflichten & Verhalten bei Sicherheitsvorfällen

Geschäftsführer tragen eine persönliche Verantwortung für eine angemessene IT-Sicherheitsorganisation und den Schutz sensibler Daten. Gesetzliche Vorgaben wie DSGVO und NIS2 verpflichten zu klaren Strukturen, wirksamen Maßnahmen und nachweisbarer Umsetzung. Im Sicherheitsvorfall zählt ein strukturiertes, dokumentiertes Vorgehen, um Schäden zu minimieren und Meldepflichten fristgerecht zu erfüllen.

It-consulting@edc.de

Inhalt

1. Warum IT-Security Chefsache ist

Cyberangriffe gehören heute zu den größten Geschäftsrisiken. Geschäftsführer tragen **persönliche Verantwortung** für die Sicherheit der Unternehmenswerte – inklusive Daten, Systeme und Prozesse. Fehlende oder unzureichende IT-Security kann zu:

- Betriebsstillstand
- Erpressung (Ransomware)
- Verlust sensibler Daten
- Bußgeldern
- persönlicher Haftung

führen. IT-Security ist damit ein **strategisches Unternehmensrisiko**.

2. Gesetzliche Pflichten für Geschäftsführer

2.1. § 43 GmbHG / § 93 AktG – Sorgfaltspflichten

Geschäftsführer müssen die „Sorgfalt eines ordentlichen Geschäftsmanns“ anwenden. Dazu gehört ausdrücklich:

- angemessene Organisation
- angemessene IT- und Informationssicherheit
- Risikomanagement

Unterlassung kann zu **persönlicher Haftung** führen.

Weiterführende Links

§43 GmbHG

§93 AktG

2.2. DSGVO (Datenschutz-Grundverordnung) – gilt branchenübergreifend

Pflichten im Normalbetrieb

- Schutz personenbezogener Daten
- technische und organisatorische Maßnahmen (TOMs)
- Datenschutz-Folgenabschätzungen

Pflichten bei einem Sicherheitsvorfall

Ein „Datenpannen-Vorfall“ liegt vor, wenn personenbezogene Daten:

- verloren gehen
- unbefugt verändert werden
- unbefugt offengelegt werden
- unbefugt zugänglich werden

Meldepflichten:

- **Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden**
- **Benachrichtigung betroffener Personen**, wenn ein hohes Risiko besteht
- Dokumentationspflicht aller Vorfälle

Bußgelder: bis zu **20 Mio. € oder 4 % des weltweiten Jahresumsatzes**.

Weiterführende Links

Datenschutz-Grundverordnung