Einleitung:

Die Verabschiedung des NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG), das mit der Umsetzung des Entwurfs des sogenannten KRITIS-Dachgesetzes einhergeht, steht unmittelbar bevor. In diesem Zusammenhang wird das BSI-Gesetz (BSIG) umfangreiche Anpassungen erfahren. Dabei adressiert der Gesetzgeber nicht nur eine Verpflichtung gegenüber den betroffenen Unternehmen, in Sachen IT-Sicherheit erheblich aufzurüsten, sondern verbindet diese Verpflichtungen zugleich mit einem Auftrag an die Geschäftsleitung, für die Umsetzung des gesetzlichen Auftrags originär verantwortlich zu sein. Nachstehend werden die wesentlichen Aufgaben des Geschäftsleiters in Bezug auf die Umsetzung der vorstehende Gesetze dargestellt. Hierauf haben sich die Geschäftsleiter **zeitnah** einzustellen und die diesbezüglich getroffenen Maßnahmen zum Zwecke der Haftung Vermeidung zu dokumentieren.

Im Einzelnen:

1. Überwachung und Billigung von Cybersicherheitsmaßnahmen:

Der Geschäftsführer muss die im Bereich der Cybersicherheit ergriffenen Risikomanagementmaßnahmen nicht nur billigen, sondern auch deren Umsetzung überwachen. Diese Verantwortung kann nicht auf Dritte delegiert werden, allerdings sind vertikale Delegationen innerhalb des Unternehmens oder an externe Vertragspartner unter Beibehaltung der Letztverantwortung zulässig.

2. Einbindung der Geschäftsleitung in IT-Sicherheitsaufgaben:

Auch bei einer mehrköpfigen Geschäftsleitung ist jedes Mitglied des Leitungsorgans in die Pflichten zur IT-Sicherheit einbezogen, selbst wenn spezifische Ressortregelungen existieren. Eine reine Überwachungspflicht besteht für die übrigen Mitglieder des Leitungsorgans, es sei denn, es bestehen konkrete Verdachtsmomente einer fehlerhaften Compliance.

3. Teilnahme an Schulungen:

Um den Anforderungen gerecht zu werden und das Haftungsrisiko zu minimieren, müssen Geschäftsleiter regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung, Bewertung von Risiken und Risikomanagementpraktiken im Bereich der IT-Sicherheit zu erwerben.

RA Prof. Dr. Martin Spaetgens
Fachanwalt für Medizin, Arbeits- und Handels- und Gesellschaftsrecht
Health Care Compliance Officer (zertifiziert HCO)

4. Verknüpfung von Unternehmensstrukturen:

Die Geschäftsleitung muss Prozesse initiieren, die eine ausreichende Verknüpfung zwischen verschiedenen Abteilungen wie der Geschäftsleitung, Compliance-Abteilung, IT-Abteilung, dem Krisenstab sowie der Abteilung für das Business-Continuity-Management sicherstellen.

5. Compliance-Management:

Es müssen Maßnahmen innerhalb der Organisation ergriffen werden, um Compliance-Risiken, die sich aus dem BSIG ergeben, zu minimieren. Dies umfasst auch die Einhaltung der IT-Sicherheitsvorgaben durch die Leitungsebene und die Verabschiedung bzw. Anpassung von IT-Sicherheitsrichtlinien im Unternehmen.

6. Umgang mit Warnungen vor Schwachstellen

Die Geschäftsleitung sollte für Warnungen vor technischen und personellen Schwachstellen zugänglich sein. Die Etablierung eines Hinweisgeber- und Warnsystems, das auch für anonyme Hinweise geöffnet ist, ist hierbei essenziell.

7. Überwachungsbeauftragter

Es wird empfohlen, Überwachungsbeauftragte einzusetzen, die die Einhaltung der rechtlichen Vorgaben überwachen. Es ist sinnvoll, Zertifizierungen für diese Beauftragten zu etablieren, um deren Vertrauenswürdigkeit und juristische Expertise zu gewährleisten.

Empfehlung:

Um die mit der Umsetzung der Gesetzesvorhaben einhergehenden Aufgaben zu erfüllen, bietet sich beispielsweise der Erlass einer IT-Sicherheitsrichtlinie als unternehmensintern verabschiede Verhaltensanweisung adressiert an Geschäftsleitung und die sonstigen mit der Umsetzung des Gesetzes beschäftigten Mitarbeiter an. Im Rahmen einer mehrgliedrigen Geschäftsführung sollte die Ressortverantwortlichkeit durch eine Ergänzung der bestehenden Geschäftsordnung ergänzt bzw. klargestellt werden.

Alle durch die Geschäftsleitung getroffenen Maßnahmen sind zu dokumentieren.

SPAETGENS COMPLIANCE

RA Prof. Dr. Martin Spaetgens
Fachanwalt für Medizin, Arbeits- und Handels- und Gesellschaftsrecht
Health Care Compliance Officer (zertifiziert HCO)