



Cybersicherheit: Neue Richtlinie "NIS2" verpflichtet auch kleinere und mittlere Unternehmen

Die überarbeitete EU-Richtlinie für Network and Information Security (NIS 2) läutet eine Zeitenwende in der Bekämpfung von Cyberangriffen ein. Die aktualisierte Richtlinie nimmt nun auch kleine und mittlere Unternehmen (KMU) in die Pflicht. Damit soll die Cybersicherheit in Unternehmen europaweit gestärkt und die allgemeine Bedrohungslage reduziert werden.

Der Blick auf die Zahlen der von Cyber-Angriffen bedrohten Unternehmen erklärt, warum: 2022 waren bereits 84 Prozent aller Firmen in Deutschland Opfer eines Angriffs auf ihre IT-Systeme. Die Zahlen steigen stetig. Zu beachten ist zudem die neu eingeführte Haftung und persönliche Verantwortung von Leitungsorganen.

Cyber-Angriffe bedrohen Unternehmen aller Größen und Branchen. Deshalb wurde in der NIS2-Richtlinie der Kreis der Unternehmen, die von der Umsetzung betroffen sind, ausgeweitet. Letztlich gibt es kaum eine Branche, die nicht betroffen ist. Mit Inkrafttreten der neuen Richtlinie, deren Umsetzung in deutsches Recht im Herbst 2023 erfolgen muss, sind dann alle Unternehmen ab 50 Mitarbeitenden und einem Umsatz von mehr als zehn Millionen Euro betroffen.

NIS 2 fordert die Unternehmensleitung

NIS 2 ist deshalb mehr als nur ein Regelwerk. Die Richtlinie markiert einen Meilenstein auf dem Weg zu einer sichereren digitalen Welt. Insbesondere für kleine und mittlere Unternehmen bringt NIS 2 neue Anforderungen

und Herausforderungen mit sich: Von der Einführung von Richtlinien und Standards für Informationssicherheit bis hin zur Entwicklung von Präventionsmaßnahmen, der Erkennung und Abwehr von Cyberangriffen sowie dem Aufbau eines robusten Incident Managements reichen die Maßnahmen, die die Unternehmensleitung zu beachten hat.

Sie müssen ferner die Geschäftskontinuität sicherstellen und Lieferketten schützen. Schon der funktionale Anforderungskatalog ist umfangreich. Gleichzeitig werden die neu geforderten technologischen und prozessualen Standards von strengen Vorgaben für das Meldewesen begleitet.

Mit NIS 2 rückt auch die persönliche Haftung von Geschäftsleitern in den Fokus. In einer Zeit, in der Unternehmen vermehrt von Cyberangriffen betroffen sind, erhöht sich somit der Druck auf Entscheider, sich aktiv mit Cybersicherheit auseinanderzusetzen. Die Organhaftung gilt übrigens auch bei Delegation! Hier müssen dann Kontrollpflichten eingehalten werden. Die Delegation

schützt also nicht vor einer möglichen persönlichen Inanspruchnahme.

Cyberisiken haben eine hohe Relevanz im Risk-Management. Zusammen mit Inflation („Chart-Stürmer“), Klimarisiken („Dauerbrenner“) und der Furcht vor einer neuen Finanzkrise ist Cyber als tägliches Risiko präsent. Deshalb muss auch die Herangehensweise in der Unternehmensführung und im Risikomanagement überdacht werden.

Drohen Regressforderungen gegen die Unternehmensleitung?

Die Rechtsprechung zu Haftungsfragen des Managements, gerade im Rahmen der Bußgeldregresse, ist noch uneinheitlich. So lehnt zum Beispiel eine jüngste Entscheidung des OLG Düsseldorf (Urteil vom 27.7.2023 – VI-6 U 1/22 (Kart)) zum Thema Kartellrechtsbußen und Kartellrechtsschadenersatz die Regressfähigkeit von Kartellunternehmensgeldbußen ab. Im Gegensatz dazu bestätigt das Gericht eine persönliche Haftung von Vorständen und Geschäftsführern dem Grunde nach für Schäden, die ihrem Unternehmen durch Schadensersatzzahlungen an Kartellgeschädigte entstanden sind.

Die höchstrichterliche Entscheidung durch den BGH bleibt noch abzuwarten. Es ist fraglich, ob der BGH zwischen Kartellunternehmensgeldbußen und Kartellschadenersatz unterscheiden wird. Die Frage nach der Regressfähigkeit von Unternehmensgeldbußen stellt sich auch im Datenschutzrecht, Lieferkettensorgfaltspflichtgesetz und Kapitalmarktrecht.

Es zeigt sich, dass im Rahmen des Compliance Managements gerade auch das Thema Cyber auf der Agenda der Geschäftsleitung stehen muss. Je mehr unsere Abhängigkeit von digitalen Systemen zunimmt, ist es unsere Pflicht, die Cybersicherheit auf allen Ebenen zu stärken.

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4927497/cybersicherheit-neue-richtlinie-nis2-verpflichtet-auch-kleinere-und-mittlere-unternehmen/>