NIS 2: Meilenstein für Cybersicherheit als „Haftungsfalle“ für die Chefetage?

Mit zunehmender Digitalisierung und Vernetzung steigt die Bedrohung durch Cyberangriffe stetig an. Laut dem aktuellen Global Risks Report zählen Cyber-Spionage bzw. Cyberangriffe zu den fünf größten globalen Bedrohungsrisiken. Als Reaktion auf die steigende Anzahl und zunehmende Komplexität von Cyberangriffen wurde vom europäischen Gesetzgeber die NIS2-Richtline „über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“ erlassen, die mit 16.01.2023 in Kraft getreten ist und von den Mitgliedstaaten bis 17.10.2024 in nationales Recht umzusetzen war. In Österreich erfolgte die Umsetzung – reichlich verspätet – durch das neue NISG 2026 (Netz- und Informationssystemsicherheitsgesetz 2026), das im Dezember 2025 im Nationalrat beschlossen wurde.

Obwohl das NISG 2026 erst am 1. Oktober 2026 in Kraft treten wird, steht fest, dass die technischen und rechtlichen Anforderungen an (betroffene) Unternehmen im Bereich der Cybersicherheit in absehbarer Zeit sprunghaft ansteigen: Durch die Aufnahme neuer Branchen bzw. „Sektoren“ und die Festlegung von neuen Schwellenwerten wurde der **Anwendungsbereich der ursprünglichen NIS-Richtlinie erheblich ausgeweitet,** sodass künftig deutlich mehr Unternehmen von den Regelungen erfasst sind. Zudem sieht die NIS2-Richtlinie bzw. das NISG 2026 **strengere Anforderungen und Sanktionen für betroffene Unternehmen** vor.

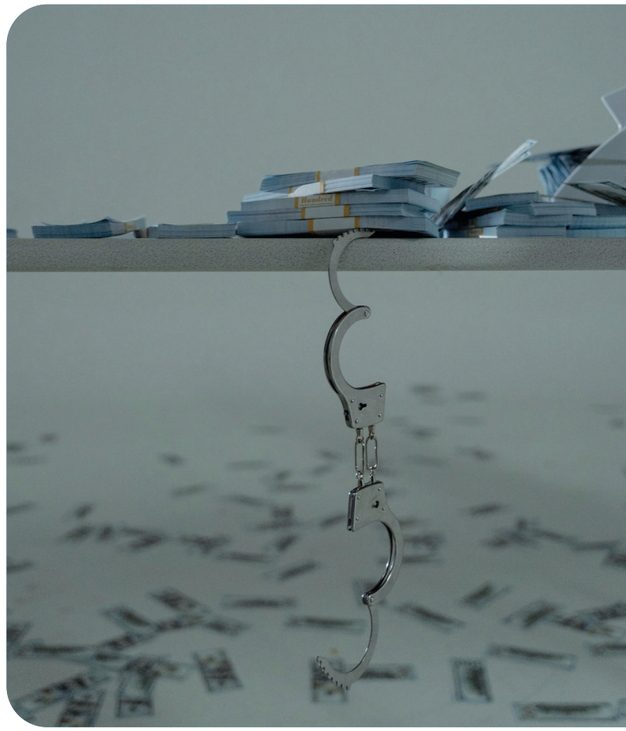
Dr. Raphael Höfer
Partner
SAXINGER Rechtsanwalts GmbH
Kontakt: r.hoefer@saxinger.com

Kernelement der NIS2-Richtlinie bzw. des NISG 2026 ist die Implementierung eines **Cybersecurity-Risikomanagements,** das entsprechend der jeweiligen Geschäftstätigkeit mit geeigneten technischen, operativen und organisatorischen Maßnahmen umzusetzen ist und auch für die Lieferkette sichergestellt werden soll. Die Umsetzung bzw. Einhaltung des Risikomanagements soll künftig durch unabhängige Stellen überprüft werden. Hinzu kommen strenge Berichtspflichten über wesentliche Sicherheitsvorfälle (Cyberangriffe), die eine Erstmeldung binnen 24 Stunden, eine Folgemeldung innerhalb von 72 Stunden und einen Abschlussbericht innerhalb eines Monats nach Kenntnis vom Sicherheitsvorfall vorsehen.

Die drohenden Sanktionen bei Nichteinhaltung sind scharf und reichen von hohen **Geldbußen** (bis zu EUR 10.000.000 oder bis zu 2% des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die betroffene Einrichtung angehört) gegen Unternehmen bis hin zu **Verboten** für Geschäftsleiter, in den betroffenen Einrichtungen Leitungsaufgaben wahrzunehmen. Die **zivilrechtliche Haftung von Leitungsorganen** wird in der NIS2-Richtlinie bzw. im NISG 2026 jedoch ausgespart und richtet sich daher nach den bestehenden nationalen Haftungsbestimmungen:
Allgemein gilt, dass Geschäftsleiter bei der Geschäftsführung die **„Sorgfalt eines ordentlichen Geschäftsmannes bzw. Geschäftsleiters“** anzuwenden haben (§ 25 GmbHG; § 84 AktG). Ein Geschäftsleiter erfüllt diesen Sorgfaltsmaßstab jedenfalls dann, wenn er sich bei unternehmerischen Entscheidungen nicht von sachfremden Interessen leiten lässt und auf der Grundlage angemessener Informationen annehmen darf, zum Wohle der Gesellschaft zu handeln („Business-Judgement-Rule“).

Demgegenüber gilt, dass die Nichteinhaltung der NISG 2026-Vorgaben durch die Geschäftsleitung einen Sorgfaltsverstoß darstellt und eine Haftung des jeweiligen Leitungsorgans gegenüber der "eigenen" Gesellschaft begründet (**„Innenhaftung“**).

Anhand eines Beispiels: Im Unternehmen kommt es zu einem Hackerangriff, der bei Einhaltung der NISG 2026-Vorgaben nicht stattgefunden hätte. Dadurch kommt es zu einem Betriebsausfall und folglich auch zu einem finanziellen Schaden für die Gesellschaft. Zusätzlich wird über die Gesellschaft wegen mangelnder Umsetzung der NISG 2026-Vorgaben eine Geldbuße verhängt, die sie bezahlt. Die Gesellschaft kann sich für die Schäden infolge des Betriebsausfalles (zB Umsatzverlust) sowie die Geldbuße – bei Vorliegen eines Verschuldens – beim Geschäftsleiter regressieren. **Wichtig:** Der Beweis, nicht schuldhaft gehandelt zu haben, ist dabei vom jeweiligen Leitungsorgan zu erbringen.



Abgesehen von der arbeits- und kostenintensiven Umsetzung eines Cybersecurity-Risikomanagements hat die Geschäftsleitung künftig also auch **persönlich für die Einhaltung der NISG 2026-Vorgaben zu sorgen.** Im Hinblick auf die sich daraus ergebenden Haftungsrisiken für Leitungsorgane (insbesondere der „eigenen“ Gesellschaft gegenüber) ist daher von einem reinen Outsourcing der NISG 2026-Compliance an die interne IT-Abteilung oder an einen externen Dienstleister abzuraten. Zudem empfiehlt es sich interne Abläufe und Verantwortungen innerhalb des Unternehmens bzw. der Unternehmensgruppe frühzeitig festzulegen und vertraglich abzusichern, damit das Thema Cybersicherheit nicht zur (vermeidbaren) „Haftungsfalle“ wird.