Kolumne von Mag. Nevena M. Shotekova-Zöchling
Rechtsanwältin – spezialisiert auf Unternehmensrecht,
Vertragsrecht und Gesellschaftsrecht
E-Mail: shotekova@advokat-wien.at, www.advokat-wien.at

Hohe Anforderungen durch die NIS-2-Richtlinie

Die Cybersicherheits-Richtlinie (Richtlinie-EU 2022/2555) bzw. die sogenannte NIS-2-Richtlinie wurde am 27. Dezember 2022 im Amtsblatt der EU veröffentlicht und ist am 16. Jänner 2023 in Kraft getreten. Durch ihren Erlass wurden zahlreiche neue Anforderungen an die Cyber- und Informationssicherheit von Unternehmen und Institutionen im Bereich der kritischen Infrastruktur definiert. Das Ziel der Richtlinie besteht im unionsweiten Aufbau von Cybersicherheitskapazitäten, der Eindämmung von Bedrohungen für Netz- und Informationsdienste in Schlüsselsektoren und der Sicherstellung der Kontinuität solcher Dienste bei Vorfällen.

Die EU-Mitgliedsstaaten müssen die Vorschriften der Richtlinie bis Oktober 2024 in das nationale Recht umsetzen, insbesondere die Verpflichtung zum Erlass nationaler Cybersicherheitsstrategien sowie die Ernennung und Einrichtung der nationalen Behörden für das Cyberkrisenmanagement sowie der zentralen Anlaufstellen für Cybersicherheit und der Computer-Notfallteams.

Unternehmen und Organisationen sollten sich daher rechtzeitig mit den neuen Anforderungen an das bestehende Cyber-Risikomanagement, Kontrolle und Überwachung sowie Umgang mit Zwischenfällen befassen. Insbesondere soll der Schutz vor Cyberangriffen auf kritische Unternehmen und Institutionen, die Einhaltung von zahlreichen Sicherheitsstandards und die Verpflichtung, Systeme stets auf dem neuesten Stand zu halten, implementiert werden.

Für die Geschäftsleitung der betroffenen Organisationen werden strengere Haftungsregeln für den Fall der Nichtbefolgung gelten. Mit der NIS-2 Richtlinie will die EU Unternehmen dazu verpflichten, ihre Widerstandsfähigkeit gegenüber Cyberbedrohungen zu erhöhen. Zu den Verpflichtungen in der NIS-2-Richtlinie zählen Maßnahmen zur Erhöhung des Schutzes vor Cyberangriffen, die Einhaltung von Sicherheitsstandards und die Verpflichtung, Systeme stets auf dem neuesten Stand zu halten. Ferner müssen die betroffenen Unternehmen regelmäßig sogenannte Penetrationstests an ihren Systemen durchführen um herauszufinden, wie leicht das eigene System für einen Angreifer zugänglich ist. Darüber hinaus müssen die Unternehmen und Institutionen diverse Systeme zur Meldung von Cybervorfällen einrichten und eine umfassende Risikobewertung über die potenziellen Schwachstellen bzw. Unsicherheiten im eigenen IT-System durchführen und die Schwachstellen entsprechend beheben.

Angesichts der Verschärfung und der zunehmenden Komplexität von Cyberbedrohungen sollten die kritischen Unternehmen bestrebt sein, dafür zu sorgen, dass die Umsetzung der vorgeschriebenen Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit auch ausreichend sind, um die zunehmenden Cyberangriffe abzuwehren. Die Unternehmen müssen dementsprechend auch ein eigenes Risikomanagement einrichten.

Die NIS-2-Richtlinie sieht ferner auch extra Bestimmungen zum Schutz von wichtigen Lieferketten vor sowie Meldepflichten für die betroffenen Unternehmen gegenüber den Behörden dahingehend, Schwachstellen und aufgetretene Angriffe unverzüglich zu melden.

Obwohl die NIS-2-Richtlinie primär nur für Unternehmen und Institutionen der kritischen Infrastruktur bzw. von bedeutsamen Lieferketten gilt, wird sich dennoch jedes Unternehmen, welches als Lieferant derartiger Unternehmen tätig ist, ebenfalls damit auseinandersetzen müssen. Denn die Praxis zeigt, dass die eigenen Vorgaben gerne auch an die Lieferanten weitergereicht werden. Die Unternehmen, die von den neuen Bestimmungen unmittelbar betroffen sind, sind im Anhang I und II der Richtlinie aufgelistet.

Es bleibt abzuwarten, wie der nationale Gesetzgeber die betreffenden Unternehmen (Größe, Arbeitnehmeranzahl, sonstige Kriterien) exakt definieren wird. Jedenfalls empfehle ich, sich rechtzeitig mit den Anforderungen der Richtlinie und vor allem mit der Frage der eigenen Betroffenheit auseinanderzusetzen.