Das neue IT-Sicherheitsrecht: Was jetzt auf Unternehmen zukommt

Die seit Dezember 2022 in Kraft getretene NIS-2-Richtlinie beinhaltet neue Anforderungen an Cybersicherheit im Unternehmen. Zu ihrer Umsetzung liegt inzwischen ein deutscher Referentenentwurf vor, der Unternehmen erweiterte Pflichten auferlegt. Unternehmen sollten sich angesichts des erheblichen Umsetzungsaufwandes schon früh damit beschäftigen, ob sie adressiert werden und welche Pflichten das neue Gesetz für sie bringen wird. Welche dies sind, zeigen wir Ihnen in diesem Beitrag.

Cyber-Angriffe nehmen zu, eine gute IT-Sicherheit wird immer wichtiger. Dies hat auch die EU erkannt und steuert mit verschiedenen Rechtsakten in diese Richtung. Schon zum Jahreswechsel ist dazu die NIS-2-Richtlinie verabschiedet worden, über die wir in unserer Januar Ausgabe berichteten. Als Richtlinie muss diese vom deutschen Gesetzgeber umgesetzt werden. Seit Juli 2023 liegt nunmehr ein offizieller Referentenentwurf für ein entsprechendes Umsetzungsgesetz vor. Er bringt wesentliche Neuerungen und weitreichende Pflichten für eine Vielzahl von Unternehmen, nicht nur für die bekannten KRITIS-Anlagen. Grund genug, sich schon frühzeitig mit den anstehenden Neuerungen zu beschäftigen:

Erweiterter Adressatenkreis

Wie auch schon bisher werden KRITIS-Unternehmen, also u.a. Unternehmen in der Energiewirtschaft, der Wasserversorgung oder Krankenhäuser, in Sachen IT-Sicherheit reguliert.

Die Umsetzung der NIS-2-Richtlinie wird indes deutlich mehr Unternehmen erfassen als bisher: Neu erfasst sind beispielsweise Unternehmen der chemischen Industrie, des Maschinenbaus, des produzierenden Gewerbes oder auch „digitale Dienste“. Adressiert werden dabei nicht nur große, sondern auch mittlere Unternehmen der einschlägigen Sektoren, also schon solche ab 50 Beschäftigten und einem Jahresumsatz von 10 Mio. Euro.

Welche Pflichten diese Adressaten jeweils genau treffen, ist von ihrer Bedeutung abhängig. Das Umsetzungsgesetz differenziert zwischen „besonders wichtigen“ und „wichtigen Einrichtungen“ (§ 28 BSIG-E).

Schadensprävention

Inhaltlich geht es neben erweiterten Befugnissen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) insbesondere um vielseitige Pflichten der betroffenen Unternehmen.

Insbesondere müssen die Unternehmen umfassende Risikomanagementsysteme etablieren (§ 30 BSIG-E). Dies umfasst technische und organisatorische Maßnahmen zur präventiven Vermeidung von Störungen. Durch diese Risikomanagementmaßnahmen sollen die Auswirkungen etwaiger Sicherheitsvorfälle auf die eigenen und auch auf andere Dienste verhindert bzw. möglichst gering gehalten werden. Zu den Mindestanforderungen zählen zum Beispiel Konzepte zur Risikoanalyse, zur Bewältigung von Sicherheitsvorfällen, das Back-Up Management aber auch die Sicherheit des Personals.

Verantwortung der Leitungsebene

Für die Umsetzung dieser Risikomanagementmaßnahmen soll die Leitungsebene künftig persönlich in Anspruch genommen werden: Geschäftsleiter müssen nach § 38 BSIG-E die vorgesehenen Maßnahmen überwachen und billigen, sonst droht die persönliche Haftung. Um dazu fähig zu sein, werden Schulungen der Leitungsebene, des "Cyber-Vorstands“, zwingend vorgeschrieben.

Was jetzt zu tun ist

Wichtig für Unternehmen ist es – je früher desto besser – zu prüfen, ob sie unter den Anwendungsbereich des Umsetzungsgesetzes der NIS-2-Richtlinie fallen. Wenn sie erstmals vom IT-Sicherheitsrecht erfasst sind, warten erhebliche Umsetzungsanforderungen. Auch wenn die Maßnahmen erst zum Oktober 2024 implementiert sein müssen, sollte ausreichend Zeit eingeplant werden. Mehr Informationen zum neuen IT-Sicherheitsrecht finden Sie auch auf unserem Blog unter dem #cybersecurity.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Philipp Schoel
+49(0)221 65065-200
philipp.schoel@loschelder.de

Dennis Pethke, LL.M.
+49(0)221 65065-200
dennis.pethke@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de