Cybersicherheit kritischer Infrastrukturen – Die NIS2-Richtlinie – Neue Pflichten

Kernstück der NIS2-Richtlinie (EU 2022/2555) sind umfangreiche Pflichten zur IT-Sicherheit, die von den erfassten Unternehmen umgesetzt und nachgewiesen werden müssen. In der Juni-Ausgabe von Compliance hat Dr. Dr. Fabian Teichmann einen Überblick über Inhalt und Umsetzung der NIS2-Richtlinie gegeben. Im vorliegenden Beitrag beleuchtet er nun neue Pflichten – etwa zum Risikomanagement und zur 24-Stunden-Meldung von Sicherheitsvorfällen.

Pflichten und Fristen: NIS2 stellt Unternehmen vor einige organisatorische Herausforderungen.

Im Zentrum der Pflichten zur IT-Sicherheit steht ein ganzheitliches Risikomanagement im Cybersecurity-Bereich (Art. 21 NIS2-RL). Unternehmen haben geeignete und verhältnismäßige technische, organisatorische und operative Sicherheitsmaßnahmen zu ergreifen, um Risiken für die Netz- und Informationssysteme, die sie für ihre Dienste nutzen, zu beherrschen. Die Richtlinie nennt zehn Elemente, die mindestens abgedeckt werden müssen, darunter insbesondere: regelmäßige Risikoanalysen, Konzepte zur Bewältigung von Sicherheitsvorfällen (Incident Response), Notfall- und Business-Continuity-Pläne (Aufrechterhaltung des Betriebs, Backups, Wiederanlauf), Maßnahmen zur Sicherheit in der Lieferkette (Supply-Chain-Security) sowie Verfahren für Verschlüsselung/Kryptografie und Zugangskontrollen. Diese Anforderungen gehen über die bisherigen Pflichten nach dem BSIG (etwa § 8a BSIG a.F.) deutlich hinaus. Unternehmen müssen die Umsetzung ihres Informationssicherheits-Risikomanagements zudem dokumentieren und regelmäßig einen Nachweis gegenüber der Behörde führen.

Neben präventiven Maßnahmen etabliert NIS2 ein strenges Meldewesen für IT-Sicherheitsvorfälle. Bei einem erheblichen IT-Sicherheitsvorfall (Definition in Art. 6 Nr. 40 NIS2-RL) gilt ein gestuftes Meldesystem: Innerhalb von 24 Stunden nach Kenntnis des Vorfalls ist eine erste Frühwarnmeldung an die zuständige Behörde (in Deutschland: BSI) abzusetzen. Spätestens nach 72 Stunden muss ein ausführlicherer Incident-Bericht mit einer ersten Einschätzung von Ursache und Schwere des Vorfalls folgen. Spätestens einen Monat nach der 72h-Meldung ist ein Abschlussbericht mit detaillierter Analyse und Angabe ergriffener Gegenmaßnahmen zu erstatten. Die Behörde ihrerseits muss den Eingang der Frühwarnung binnen 24 Stunden bestätigen und im Bedarfsfall operative Hilfestellung anbieten. Dieses eng getaktete Meldesystem soll Transparenz und eine rasche Reaktion auf Cybervorfälle gewährleisten, stellt Unternehmen aber vor organisatorische Herausforderungen.

Schließlich begründet NIS2 weitere Verpflichtungen: So müssen relevante Unternehmen sich bzw. ihre Betriebsstätten registrieren und einen zuständigen Ansprechpartner benennen. Für wesentliche und wichtige Einrichtungen werden zudem Mitwirkungspflichten bei Aufsichtsmaßnahmen statuiert (Duldung von Prüfungen, Herausgabe von Informationen etc., vgl. Art. 32, 33 NIS2-RL). In bestimmten Fällen können Unternehmen verpflichtet werden, die Nutzer bzw. Kunden ihrer Dienste über erhebliche Cyberbedrohungen oder Vorfälle zu informieren.

RA Dr. Dr. Fabian Teichmann, LL.M.

RA Dr. Dr. Fabian Teichmann, LL.M., ist Managing Partner der Teichmann International (Schweiz) AG sowie Verwaltungsrat der Teichmann International (IT Solutions) AG. Seine Schwerpunkte liegen im Strafrecht, der Cybersecurity und der Unternehmenscompliance. Er ist zudem als Dozent an mehreren europäischen Hochschulen tätig.

Übersicht zentraler Pflichten und Fristen

Pflichtbereich	Inhalt der Vorgabe	Wichtige Fristen
Risikomanagement (Art. 21 NIS2)	Implementierung angemessener *technischer und organisatorischer* Maßnahmen der IT-Sicherheit in zehn definierten Bereichen (u.a. Risikoanalyse, Incident Response, Business Continuity, Lieferkettensicherheit, Zugriffs- und Zugriffskontrollkonzepte, Kryptografie) und regelmäßiger Nachweis gegenüber der Behörde.	*kontinuierlich*
Meldung von Vorfällen (Art. 23 NIS2)	*Stufenmodell* bei erheblichen Sicherheitsvorfällen: Frühwarnung binnen 24 h; Folgemeldung binnen 72 h; Abschlussbericht binnen eines Monats. Behördliche Bestätigung/Rückmeldung innerhalb 24 h.	24 Stunden (Erstmeldung); 72 Stunden; ein Monat
Registrierung & Kontaktstelle	Meldung an die Behörde als (neu) betroffene Einrichtung; Benennung verantwortlicher Kontaktpersonen (z.B. IT-Sicherheitsbeauftragter).	*unverzüglich* nach Einstufung
Information Betroffener		*situationsabhängig* (bei erheblichem Vorfall auf Anordnung / bei überwiegendem Schutzinteresse der Empfänger)
Kooperation mit Behörden	Mitwirkungs- und Duldungspflichten bei Prüfungen: Ermöglichung von Vor-Ort-Kontrollen, Herausgabe angeforderter Unterlagen, Umsetzung behördlicher Anordnungen (z.B. Abstellen von Sicherheitsmängeln) – bei Zuwiderhandlung ggf. Zwangsgelder.	*anlassbezogen* (auf Anordnung der Behörde; laufend einzuhalten)