Compliance/Digitalisierung »DK1480087

Aktuelles zu Anwendbarkeit, Pflichten und Haftung nach der NIS-2-Richtlinie

Die NIS-2-Richtlinie formuliert einheitliche Mindestanforderungen an die IT-Sicherheit. Der Anwendungsbereich wird – im Vergleich zu den bisherigen KRITIS-Regelungen nach der NIS-1-Richtlinie – deutlich erweitert. Rechtsunsicherheiten bestehen noch mit Blick auf die die Anwendbarkeit (insb. die Zurechnung von Schwellenwerten) sowie die Pflichten.

RA Dr. Patrick Grosmann, M.A, ist Rechtsanwalt für IT- und Datenschutzrecht bei FPS Rechtsanwälte in Frankfurt/M.
Kontakt: autor@der-konzern.de

I. Die NIS-2-Richtlinie und ihre nationale Umsetzung

Von dem Ziel eines einheitlichen IT-Sicherheitsniveaus ist die NIS-2-Richtlinie (kurz „NIS-2-RL“) in der Praxis noch recht weit entfernt – aktuell haben erst 9 Mitgliedstaaten diese in nationales Recht umgesetzt. Auch in Deutschland kann die Umsetzung der NIS-2-RL getrost als Odyssee bezeichnet werden. Die letzte Bundesre- gierung scheiterte mit der Umsetzung in nationales Recht. Ein Vertragsverletzungsverfahren ist bereits eingeleitet. Nun liegt ein RegE der aktuellen Regierung vor – wann das nationale Umsetzungsgesetz in Kraft treten wird, ist noch unklar.

II. DieAnwendbarkeitderNIS-2-RL

Die Anwendbarkeit der NIS-2-RL ist für die meisten Einrichtungsarten in folgendem Zweierschritt zu prüfen: Zugehörigkeit zu einer erfassten Einrichtungsart (I.) und Überschreitung der relevanten Schwellenwerte (II.), § 28 Abs. 1, 2 BSIG_E (das „BSIG_E“ bezieht sich auf den RegE zum NIS2UmsuCG vom 25.07.2025 [kurz „NIS2UmsuCG“]. Zur Vereinfachung werden lediglich die geplanten Regelungen des BSIG_E und bspw. nicht des EnWG_E dargestellt). Insbesondere die Betreiber kritischer Infrastrukturen fallen dagegen schwellenwertunab- hängig in den Anwendungsbereich. Abhängig von der Einrich- tungsart und den Schwellenwerten kommt eine Einordnung als besonders wichtige Einrichtung (§ 28 Abs. 1 BSIG_E, kurz „bwE“) oder wichtige Einrichtung (§ 28 Abs. 2 BSIG_E, kurz „wE“) in Betracht. Bereits die Bestimmung der Einrichtungsart wirft in der Praxis aufgrund komplizierter Regelungen und Verweisungen teils komplexe Rechtsfragen auf.

1. AusschlussbeivernachlässigbarerNebentätigkeit

Eine anteilige Berücksichtigung von Schwellenwerten sieht der aktuelle Entwurf nicht mehr vor (eine anteilige Berücksichti- gung von Schwellenwerten war in den Entwürfen der letzten Bundesregierung enthalten – es sollten nur die Schwellen- werte, die der konkreten Einrichtungsart zuzuordnen sind, berücksichtigt werden). Stattdessen ergibt sich aus § 28 Abs. 3 BSIG_E, dass „solche Geschäftstätigkeiten unberücksichtigt bleiben [können], die im Hinblick auf die gesamte Geschäfts- tätigkeit der Einrichtung vernachlässigbar sind.“. Wann eine solche vernachlässigbare (Neben-)Tätigkeit vorliegt, wird nicht näher definiert. Als Indiz wird lediglich die Nennung in dem Gesellschaftervertrag, einer Satzung oder ähnlichen Gründungsdokumenten genannt – ob dies in der Praxis zur Bestimmung dienlich ist, bleibt bspw. mit Blick auf IT-Services, die neben der Haupttätigkeit erbracht werden, zweifelhaft. Ebenso berücksichtigt werden sollen lt. Gesetzesbegründung die mit der Tätigkeit verbundenen Umsätze und Mitarbeiter- zahlen (NIS2UmsuCG, S. 162). Im Ergebnis erforderlich ist daher weiterhin eine Gesamtbetrachtung im Einzelfall – dies verbunden mit relevanten Rechtsunsicherheiten.

III. Pflichten nach der NIS-2-RL

Voranzustellen ist: Die Unterscheidung zwischen wE und bwE wirkt sich nicht auf die Pflichten, sondern lediglich auf die Aufsichtsbefugnisse des BSI aus: Kontrollen des BSI gegenüber wE sind nur bei einem begründeten Verdacht möglich, wohingegen Kontrollen gegenüber bwE verdachtsunabhängig erfolgen können. Die folgenden Kernpflichten gelten dagegen für alle Einrichtungen:

1. Risikomanagementmaßnahmen

Die Einrichtung muss geeignete Risikomanagementmaßnahmen ergreifen. Wie aus dem Datenschutzrecht hinsichtlich der technischen und organisatorischen Maßnahmen (TOM) bekannt, sind die Maßnahmen risikobasiert zu bestimmen. Welche Mindestmaßnahme umzusetzen sind, ergibt sich aus § 30 Abs. 2 BSIG_E. In der Praxis stellt sich insb. die Frage, wie der Nachweis geeigneter Risikomanagementmaßnah- men geführt werden kann und welche Maßnahmen konkret umzusetzen sind. Nähere Informationen der Aufsichtsbehörden hierzu fehlen weiterhin. Lediglich in einem FAQ hat das BSI angegeben, dass eine Unternehmenszertifizierung nach der ISO 27001 oder dem BSI-Grundschutz einen *Baustein* der Maßnahmen bilden kann (das FAQ ist mittlerweile archiviert, abrufbar unter https://fmos.link/13465 [Abruf am 21.08.2025]). Welche zusätzliche Maßnahmen ggf. zu ergreifen sind, lässt das BSI ausdrücklich offen. Besond re Anforderungen an die Risikomanagementmaß- nahmen gelten für Betreiber kritischer Infrastrukturen (§ 31 BSIG _ E).

2. Meldepflicht

Bei einem *erheblichen Sicherheitsvorfall* ist eine Meldung gegenüber dem BSI vorzunehmen. Das Meldeverfahren ist drei- bzw. vierstufig ausgestaltet, § 32 BSIG_E. Die Qualifizie- rung als erheblicher Sicherheitsvorfall ist stets im Einzelfall vorzunehmen. Grundsätzliche Indikatoren sind eine schwer- wiegende Betriebsstörung der Dienste oder (zukünftige) finanzielle Verluste für die betreffende Einrichtung oder wenn andere Personen (Unternehmen oder natürliche Personen) durch den Vorfall materielle oder immaterielle Schäden erlei- den könnten. Für bestimmte Anlagen legt die Durchführungsverordnung (EU) 2024/2690 der Kommission die Anforderungen an einen erheblichen Sicherheitsvorfall genauer fest. Die frühe Erstmeldung muss innerhalb von 24 Stunden ab Kenntnis des Vorfalls erfolgen. Die Folgemeldung schließt nach 72 Stunden sowie eine Abschlussmeldung einen Monat nach Kenntnis des Vorfalls an. Dauert der Vorfall über einen Monat an, ist die Abschlussmeldung durch eine Fortschrittsmeldung zu ersetzen und eine Abschlussmeldung anzuschließen. Eine gemeinsame Meldestelle der NIS-2-Aufsichtsbehörde und der Datenschutz-Aufsichtsbehörden ist nicht vorgesehen. Bei Cyberangriffen ist daher in der Praxis regelmäßig jew. eine

gesonderte Meldung gegenüber der NIS-2- und Datenschutz-Aufsichtsbehörde vorzunehmen.

3. Registrierungspflicht
Jede Einrichtung muss sich gegenüber dem BSI registrieren (§ 33 BSIG_E) – nähere Informationen zum Registrierungs-prozess liegen noch nicht vor.

IV. Pflichten und Haftung der Geschäftsleitung

Die Geschäftsleitungsmitglieder müssen nach § 38 Abs. 1 BSIG_E die Risikomanagementmaßnahmen umsetzen und die Einhaltung der darin beschriebenen Maßnahmen bspw. durch regelmäßige Audits überwachen. Durch den für das deutsche Gesellschaftsrecht ungewöhnlichen Begriff des *Geschäfts- leitungsmitglieds* bleibt der konkret erfasste Personenkreis unklar. Der Wortlaut der NIS-2-RL (*Leitungsorgane*) spricht für eine enge Auslegung, für eine Organstellung der Personen und gegen eine Ausweitung auf weitere Leitungsebenen. Zudem besteht eine Schulungspflicht im Bereich der Sicherheit der Informationstechnik, deren konkreter inhaltlicher und zeitlicher Umfang unklar ist. Der RegE nimmt einen jährlichen Schulungsaufwand von 4 Stunden an – die Inhalte werden nicht näher spezifiziert (NIS2UmsuCG, S. 126). Aus der NIS-2-RL ergibt sich zudem eine Erweiterung des Haftungsrisikos für Mitglieder der Geschäftsleitung, da es bei schuldhafter Pflichtverletzung zu einer Haftung der organ- schaftlichen Vertreter gegenüber der Gesellschaft kommen kann. Hintergrund des erweiterten Haftungsrisikos ist die Konkretisierung der IT-Sicherheitspflichten durch die NIS- 2-RL – die legalen Handlungsmöglichkeiten werden dadurch eingeschränkt (im Detail zu den Haftungsregelungen der NIS- 2-RL *Grosmann/Michel*, ZD 2025 S. 250).

V. Ausblick

Aus Unternehmenssicht lässt die Umsetzung der NIS-2-RL noch einige praxisrelevante Fragen – insb. zu der Zurechnung und den Pflichten – offen. Eine belastbare *Guidance* durch die Aufsichtsbehörden bleibt abzuwarten und wünschenswert. Trotz schleppender nationaler Umsetzung sollten Unter- nehmen umgehend die Anwendbarkeit der NIS-2-RL prüfen und die erforderlichen Umsetzungsmaßnahmen in den Blick neh men .