

1 Zum Umgang mit dem Leitfaden

Die Diskussionen um Krisen jeglicher Art beschäftigen seit vielen Jahren das Gesundheitswesen, von finanziellen Krisen, der Coronapandemie über Cybersicherheitsereignisse bis zu Kriegsfolgen. Der Gesetzgeber schärft in einigen Bereichen erheblich nach. Das gilt aktuell insbesondere für die Vermeidung von Cybersicherheitsvorfällen in einer angespannten und auch geopolitisch beeinflussten Sicherheitslage. Zur Umsetzung der sog. NIS-2-RL wurde das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG) Ende 2025 novelliert. Hiervon ist eine Vielzahl von Gesundheitseinrichtungen betroffen, die umfassende Risikomanagementmaßnahmen zur Gewährleistung ihrer IT-Sicherheit treffen müssen, begleitet von weiteren Rechtspflichten.

Die Geschäftsleitung der Einrichtungen wird vom Gesetzgeber ausdrücklich angesprochen, indem ihre Verantwortung für die Umsetzung des Risikomanagements klargestellt wird. Die Haftungsmöglichkeit bei der Verletzung dieser Leitungssorgfaltspflicht wird ebenfalls betont. Abgerundet wird die Compliance-Pflicht mit der Pflicht für die Geschäftsleitungen, durch Schulungen ausreichende Fachkenntnisse zu erlangen bzw. aufrechtzuerhalten, um dieser Pflicht angemessen nachkommen zu können.

An dieser Schulungspflicht knüpft der vorliegende Leitfaden an und zeigt die Einschätzung der Autoren, welche Inhalte in diesen Schulungen behandelt werden sollten. Er kann also begleitend zu Schulungen eingesetzt werden, zur Nachbereitung dienen oder die Vorbereitung von Schulungen (inhouse/extern) erleichtern.

Die Schulungen sollten stets auf die betroffenen Einrichtungen zugeschnitten sein, denn die Schulungen müssen auch sektorspezifische Besonderheiten vermitteln. Das betrifft etwa die konkrete Art der relevanten Dienstleistungen. Die Schulung für die Leitung eines

Krankenhauses muss andere Besonderheiten vermitteln als die für die Leitung eines Rettungsdienstes.

Der Leitfaden soll außerdem motivieren, die Schulungen nicht nur als lästige Pflicht zu verstehen. Denn über diese Rechtspflicht hinaus bietet ein gutes Risikomanagement in einer Gesundheitseinrichtung die Möglichkeit, die immer weiter ansteigenden Anforderungen an das Risikomanagement mit unterschiedlichen Zielrichtungen zu bündeln, effizient umzusetzen und das in den Einrichtungen bereits vorhandene Know-how und die Strukturen aufzugreifen.

2 Lerninhalte der NIS-2-Schulungspflicht

Der Gesetzgeber ging im Gesetzentwurf von einem Mindestturnus von drei Jahren für die Schulungen aus (BT-Drs. 21/1501, S. 154). Das Bundesministerium des Innern und für Heimat schätzte den Schulungsaufwand auf vier Stunden je Schulung. Das BSI hat zur Orientierung eine »Handreichung für die Empfehlung zur Schulungspflicht für Geschäftsleitungen wichtiger Einrichtungen und besonders wichtiger Einrichtungen nach dem BSI-Gesetz sowie für freiwillige Schulungen von Geschäftsleitungen nicht-regulierter Unternehmen« entwickelt.¹ Diese geht nicht mehr ausdrücklich von einem Umfang von vier Stunden aus, die Umfangseinschätzung dient in der Praxis aber weiterhin als Orientierungswert.

In der Handreichung betont es die Angemessenheit des Umfangs und der Regelmäßigkeit und nennt Konstellationen, bei denen vom Mindestintervall abgewichen werden sollte:

- Wechsel in der Geschäftsleitung,
- signifikante Änderungen in den Geschäftsprozessen,
- signifikante Änderungen der Risikoexposition,
- signifikante Änderungen bei implementierten oder geplanten Risikomanagementmaßnahmen.

Solche Ereignisse können neben dem genannten Wechsel in der Geschäftsleitung etwa die Aufnahme eines neuen Fachgebiets mit

1 Die Handreichung ist abrufbar unter: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Geschaeftsleitungsschulung/NIS-2-Geschaeftsleitungsschulung_node.html.

den dazugehörigen IT-Prozessen und medizinischen Geräten, die Zusammenlegung von Einrichtungen oder neue Kooperationen mit anderen Gesundheitseinrichtungen sein, wie etwa auch die Neueröffnung eines MVZ, das der Klinik angehört und mit ihr über gemeinsame IT-Prozesse verbunden ist.

Grundsätzlich bieten sich daher folgende Lerninhalte an, die regelmäßig je nach Bedarf der Geschäftsleitung entsprechend intensiv besprochen werden sollten, um das methodische Verständnis zu vermitteln:

- Einführung in das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (»NIS-2-Umsetzungsgesetz«)
- Erklärung der Einrichtungskategorien im BSIG
- Pflichten der Geschäftsleitungen, Haftungs- und Bußgeldvorschriften
- Einführung in das Informationssicherheits-Risikomanagement
- Identifikation von Informationssicherheitsrisiken
- Analyse von Informationssicherheitsrisiken
- Bewertung von Informationssicherheitsrisiken
- Behandlung von Informationssicherheitsrisiken
- Überwachung des Informationssicherheits-Risikomanagements
- Umzusetzende Maßnahmen zur Behandlung von Informationssicherheitsrisiken im Kontext von § 30 BSIG
- Darüber hinaus umzusetzende Maßnahmen zur Behandlung von Informationssicherheitsrisiken im Kontext von § 31 BSIG für Betreiber kritischer Anlagen
- Gesprächsgeführtes Üben von mehreren Fallbeispielen, Szenarien und Übungen zum Risikomanagement

Die Schulungsinhalte sollten sektor- und einrichtungsspezifische Inhalte berücksichtigen, um die Auswirkungen des Risikomanagements auf die eigenen Dienstleistungen abzubilden.

Aus der Erfahrung in den Schulungen sollte immer auch ausreichend Platz für Diskussionen sowohl zu inhaltlichen Fragen als auch zum Abgleich von Erwartungen und Verständnis zu Risikomanagement-themen innerhalb der Geschäftsleitung verbleiben.

3

Einführung in das NIS-2-Umsetzungsgesetz

Die EU hatte am 27. Dezember 2022 die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2-Richtlinie) 2022/2555 veröffentlicht, welche die EU-Mitgliedsstaaten in nationales Recht umsetzen mussten. Sie stellt die Weiterentwicklung der (ersten) NIS-Richtlinie von 2016 dar, in der kritische Infrastrukturen adressiert wurden.

In Deutschland wurde das Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung am 5. Dezember 2025 verabschiedet, so dass es am 6. Dezember 2025 in Kraft getreten ist. Es hat im Schwerpunkt das BSIG novelliert.

Aus den Erwägungsgründen der NIS-2-Richtlinie geht hervor, dass sowohl eine *»Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden«*, als auch *»die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen«*, wesentlich ist. Daher wurde die Stärkung der Cyberresilienz der Union vorangetrieben.

Die EU hat insofern frühzeitig erkannt, dass Vorfälle bei Netz- und Informationssystemen *»die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanziellen Verlust verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft der Union großen Schaden zufügen«* können.

Cybersicherheit – und damit auch die geeignete Vorsorge und Wirksamkeit – sind daher wichtiger denn je für ein reibungsloses Funktionieren des europäischen Binnenmarkts. Die Cybersicherheit ist darüber hinaus in kritischen Sektoren eine wesentliche Voraus-

setzung, um einen erfolgreichen digitalen Wandel zu vollziehen und von den wirtschaftlichen wie auch sozialen Vorteilen der Digitalisierung zu profitieren.

Allerdings könnte sich eine Fragmentierung des Binnenmarkts – insbesondere auf die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz – nachteilig auswirken, wenn diese Vorgehensweisen nicht einheitlich geregelt werden.

Wesentliches Ziel war daher, mit dieser Richtlinie die Mindestvorschriften für Cybersicherheit in allen EU-Mitgliedsstaaten zu vereinheitlichen. Dadurch sollten die Cyberresilienz und das Cybersicherheitsniveau innerhalb der EU weiter verbessert werden.

Die Vorgaben der EU NIS-2 lassen sich im Wesentlichen auf fünf Punkte zusammenfassen:

3.1 Geschäftsleitungspflichten

Die Geschäftsleitung ist verpflichtet, das Informationssicherheits-Risikomanagement zu steuern, zu überwachen und zu kontrollieren, auch wenn operative Tätigkeiten z.B. an einen Chief Information Security Officer (CISO) oder Informationssicherheitsbeauftragten (ISB) delegiert werden können. Die Letztverantwortung für die Umsetzung rechtlicher Vorgaben liegt stets bei der Geschäftsleitung. Sie haftet dabei auch für schuldhaft verursachte Schäden.

Um diese Verantwortung wahrnehmen zu können, ist die Geschäftsleitung verpflichtet, regelmäßig an Schulungen teilzunehmen, um

- ♦ Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen und

- ♦ die Auswirkungen von Risiken und Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Es geht also um Methodikwissen und das Verständnis zu Auswirkungen von Risiken oder Maßnahmen, die diese Risiken reduzieren sollen.

3.2 Risikomanagement

Eine der Kernvorschriften betrifft das Risikomanagement. Die betroffenen Einrichtungen müssen geeignete, verhältnismäßige, wirksame, auf dem Stand der Technik entsprechend ihrer Risikoexposition basierende technische und organisatorische Maßnahmen (TOM) ergreifen. Zur besseren Übersicht sind die Maßnahmen in der nachfolgenden Abbildung thematisch in Kategorien strukturiert aufgeführt (► Abb. 1).



Abb. 1: Technische und organisatorische NIS-2-Anforderungskategorien

Zusätzliche Anforderungen treffen die Betreiber kritischer Anlagen (KRITIS), welche die Schwellenwerte der BSI-Kritisverordnung² (künftig: Verordnung zur Bestimmung kritischer Anlagen nach dem KRITISDachgesetz (Kritisverordnung – KritisV)) überschreiten. Beispielsweise sind dann verpflichtend Systeme zur Angriffserkennung einzusetzen. KRITIS-Einrichtungen müssen auch über das allgemeine Schutzniveau hinausgehende Maßnahmen als verhältnismäßig ansehen und umsetzen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht (§ 39 BSIg) (zur Betroffenheitsprüfung ausführlich in ► Kap. 5).

3.3 Registrierungspflicht

Die Einrichtungen müssen selbst ihre Betroffenheit prüfen und sich dann fristgemäß bei der zuständigen Behörde registrieren. Dies ist in der Regel das Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Registrierung erfolgt über das BSI-Portal.³ Das BSI stellt hierzu auch eine Schritt-für-Schritt-Anleitung⁴ bereit. Zur Betroffenheitsanalyse stellt das BSI einen »Entscheidungsbaum der NIS-2-Betroffenheitsprüfung«⁵ auf der Hilfeseite zur NIS-2-Betroffen-

2 BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 9 des Gesetzes vom 11. März 2026 (BGBl. 2026 I Nr. 66) geändert worden ist. Sie ist abrufbar unter: <https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html>.

3 Das BSI-Portal ist abrufbar unter: <https://portal.bsi.bund.de/>.

4 Die Anleitung ist abrufbar unter: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Anleitung-Registrierung/Anleitung-Registrierung_node.html.

5 Der Entscheidungsbaum ist abrufbar unter: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-betroffenheit-entscheidungsbaum.htm?nn=1116326>.

heitsprüfung bereit. Es empfiehlt sich aus der Praxis dabei immer, nach erfolgter Analyse eine juristische Bewertung vorzunehmen, da viele Ausnahmen und Spezialfälle zu beachten sind (zur Betroffenheitsprüfung ausführlich in ► Kap. 5).

3.4 Meldemechanismen inkl. Unterrichtungspflicht

Das Vorgehen im Krisenfall ist vorzubereiten, eine Identifikation von internen und externen Ansprechpartnern vorzunehmen und eine interne Sicherheitsvorfalldefinition und -behandlung umzusetzen. Bei einem erheblichen Sicherheitsvorfall ist dieser nach einem dreistufigen Melderegime zu melden (zur Meldepflicht ausführlich in ► Kap. 7).

3.5 Nachweispflicht

Auf Anfrage kann die Aufsichtsbehörde die Vorlage von Nachweisen über die Erfüllung der Vorgaben – bei einem Betreiber kritischer Anlagen auch durch alle drei Jahre durchzuführende Audits zur Nachweiserbringung der Einhaltung des Gesetzes – zum Risikomanagement, den umgesetzten Maßnahmen und der Einhaltung der Meldepflichten (und bei KRITIS auch die Systeme zur Angriffserkennung) einfordern.