CYBERSECURITY & RESILIENCE

CII WHITE PAPER

NIS-2 Richtlinie: Umsetzung im Gesundheitswesen

Ein Leitfaden für Führungskräfte in Gesundheitsunternehmen

Rechtsanwalt Dr. Tilmann Dittrich, LL.M.

CYBER|INTELLIGENCE
.Institute

Inhalt

Autor der Studie

Dr. Tilmann Dittrich, LL.M.

Dr. Tilmann Dittrich, LL.M. Medizinrecht, war Doktorand an der Heinrich-Heine-Universität Düsseldorf und hat dort zu Compliance-Herausforderungen im Non-Profit-Bereich geforscht. Er ist außerdem Rechtsanwalt in Düsseldorf.

Im Jahr 2024 hat er zwei juristische Fachbücher zur Krisenresilienz und Cybersicherheit im Gesundheitswesen mitherausgegeben, außerdem ist er Autor zahlreicher Publikationen zu den Themen Cybersecurity, Compliance und Strafrecht.

Foto: Wessing & Partner RAe mbB Düsseldorf

Das NIS-2-Umsetzungsgesetz ist am 6. Dezember 2025 in Kraft getreten. Damit gehen umfangreiche Schulungspflichten für Leitungsorgane von betroffenen Unternehmen einher. Dieser Leitfaden soll die Geschäftsleitungen jeglicher betroffener Gesundheitsunternehmen befähigen, sich dieser **Leitungsverantwortung selbstbewusst stellen** zu können. Mit ihm kann die Umsetzung der Schulungspflicht intern und extern begleitet werden. Anders als die allgemeine Handreichung des BSI zur Schulungspflicht, zeigt der Leitfaden direkt auf, wo im Gesundheitswesen im Bereich Cybersicherheit „über den Tellerrand hinausgeschaut“ werden muss. Der Leitfaden vermittelt Zuversicht, dass mit einem gezielten Angehen der NIS-2-Umsetzung die Gesundheitsunternehmen ihrer gesamtgesellschaftlichen Verantwortung nachkommen und unangenehme Rechtsfolgen vermeiden.

Mit dem Inkrafttreten des NIS-2-Umsetzungsgesetzes am 6. Dezember 2025 sind Unternehmen mit neuen und verbindlichen Anforderungen an ihre Cybersicherheit konfrontiert. Dazu gehört eine zentrale Neuerung: **die Pflicht zur regelmäßigen Schulung von Leitungsorganen**. Geschäftsführungen, Vorstände und andere Führungskräfte tragen künftig eine deutlich erweiterte Verantwortung, Cybersicherheitsrisiken rechtzeitig zu kennen, zu steuern und geeignete Maßnahmen zu ergreifen.

Dieser Leitfaden unterstützt Entscheidungsträgerinnen und Entscheidungsträger im Gesundheitswesen dabei, dieser Verantwortung gerecht zu werden. Er vermittelt praxisnah, was Schulungspflichten konkret bedeuten, wie sich diese effizient erfüllen lassen und wie die Umsetzung im eigenen Unternehmen begleitet werden kann, intern wie extern. Ferner zeigt dieser Leitfaden gezielt auf, welche Besonderheiten und Risiken im Gesundheitssektor bestehen und wo über etablierte Standards hinausgedacht werden sollte. Mit diesem Bewusstsein und dem richtigen Wissen können Führungskräfte die NIS-2-Anforderungen und ihr Unternehmen oder ihre Einrichtung langfristig sicher und resilient aufstellen.

Kapitel 1

Zum Umgang mit diesem Leitfaden

Die Diskussionen um Krisen jeglicher Art beschäftigen seit vielen Jahren das Gesundheitswesen, von finanziellen Krisen, der Corona-Pandemie 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. Deshalb müssen viele Gesundheitseinrichtungen künftig die **NIS-2-Richtlinie** (RL (EU) 2022/2555) umsetzen. Die Besonderheit dieser Richtlinie

> **Die Besonderheit dieser Richtlinie liegt darin, dass sie die Leitungsverantwortung für den Risikobereich Cybersicherheit deutlich hervorhebt und die Geschäftsleitungen zu Schulungen verpflichtet, damit sie dieser Leitungsverantwortung nachkommen können.**

liegt darin, dass sie die Leitungsverantwortung für den Risikobereich Cybersicherheit deutlich hervorhebt und die Geschäftsleitungen zu Schulungen verpflichtet, damit sie dieser Leitungsverantwortung nachkommen können. Diese Schulungen sind nicht gleichzusetzen mit den regulären Schulungen, die Mitarbeitende zur Cyberawareness absolvieren müssen, sondern es handelt sich um spezielle Leitungsschulungen.

Dieser Leitfaden soll die Geschäftsleitungen jeglicher betroffener Gesundheitsunternehmen befähigen, sich dieser **Leitungsverantwortung selbstbewusst stellen** zu können. Mit ihm kann die Umsetzung der Schulungspflicht intern und extern begleitet werden. Er versetzt auch die Aufsichtsorgane der Einrichtungen in die Lage, die Umsetzung der Schulungspflicht zu kontrollieren, da die Schulungspflicht der Aufhänger für viele Aufsichtsmaßnahmen des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist und insgesamt die Grundlage nachteiliger Rechtsfolgen sein kann. Anders als die allgemeine Handreichung des BSI zur Schulungspflicht zeigt der Leitfaden direkt auch auf, wo im Gesundheitswesen im Bereich Cybersicherheit „über den Tellerrand hinausgeschaut“ werden muss.

Außerdem vermittelt er **Zuversicht**, dass mit einem gezielten Angehen der NIS-2-Umsetzung die Gesundheitsunternehmen ihrer gesamtgesellschaftlichen Verantwortung nachkommen und unangenehme Rechtsfolgen vermeiden.

Der Leitfaden greift die neue Fassung des BSIG auf, die am 6. Dezember 2025 in Kraft getreten ist. Das Gesetz sieht keine Übergangsfristen vor.

Kapitel 2
Einleitung zur NIS-2-Richtlinie

Ende 2020 entschied die EU-Kommission, dass der europäische Binnenmarkt nicht ausreichend vor Gefahren aus dem Cyberraum geschützt ist. Sie erarbeitete daher die **EU Cybersecurity Strategy**, um zwei Richtlinienvorhaben auf den Weg zu bringen. Ende 2022 wurden die Zweite Netzwerk- und Informationssicherheitsrichtlinie (NIS-2-Richtlinie) und die Resilienz-Richtlinie (Critical Entities Resilience Directive = CER-RL/RL (EU) 2022/2557) auf den Weg gebracht, sie traten Anfang 2023 in Kraft. Ihr Ziel ist es, dass künftig Unternehmen und öffentliche Einrichtungen, die für die Gesellschaft besonders sensible Dienste erbringen, vor Gefahren aus dem cyber- und nicht-cyberbezogenen Risikobereich geschützt werden. Den Cyberbereich übernimmt die NIS-2-Richtlinie, während die CER-RL den nicht-cyberbezogenen Risikobereich abdeckt. Das betrifft insbesondere physische Gefahren.

Beide Richtlinien sollen nach ihrer Umsetzung in nationales Recht „Hand in Hand greifen“, um möglichst alle Gefahren einer **hybriden Gefährdungslage** zu erfassen. Hybrid bedeutet, dass sich eine Gefahr nicht mehr eindeutig dem einen oder dem anderen Risikobereich zuordnen lässt – sichtbar am (fiktiven) Beispiel von physischen Sabotageakten auf eine Einrichtung eines Krankenhauses, was zum Erliegen der Stromversorgung und mithin der IT-Strukturen in diesem Bereich führen kann.

Umzusetzen gewesen wären die Richtlinien jeweils bis zum 17. Oktober 2024, das verzögerte sich in Deutschland aber u.a. wegen des Koalitionsbruchs. Die Umsetzung der NIS-2-Richtlinie erfolgt im BSIG. Die CER-RL soll in einem neuen KRITIS-Dachgesetz umgesetzt werden, hierzu läuft das Gesetzgebungsverfahren noch.

Kapitel 3
Gefährdungslage im Gesundheitswesen

a) Cyberangriffe

Es gibt zwei wichtige Cyberangriffsarten, die sich unmittelbar auf die Betriebsfähigkeit einer Einrichtung auswirken und daher für das Gesetzesziel des BSIG von herausragender Bedeutung sind. Die umgangssprachlich als Verschlüsselungstrojaner bekannten **Ransomware-Angriffe** erzielen die größten Schadwirkungen. „Ransom“ bedeutet, aus dem Englischen übersetzt, die Erpressung, und die Endung „-ware“ erfasst die Softwarekomponente. Ransomware-Angreifer identifizieren Schutzlücken in den Systemen, um beim Auffinden über diese ins System zu gelangen. Gängig hierfür sind etwa infizierte Mail-Anhänge, unsichere Webseiten oder kompromittierte Fernwartungszugänge. Die Angreifer verschlüsseln nach und nach Dateien und greifen diese in der Regel zudem auch ab. Gerade im Gesundheitswesen sind hiervon sensible Gesundheitsdaten betroffen. Durch die Verschlüsselung können die IT-Systeme nicht mehr wie gewohnt arbeiten und sind in ihrer Funktionsfähigkeit beeinträchtigt. Je nach Bedeutung für den digitalisierten Prozess fallen die Auswirkungen größer oder kleiner aus. Einen plakativen Kontrast bietet das Beispiel des Ausfalls von versorgungsnahen IT-Prozessen auf der Intensivstation im Vergleich zum Ausfall eines digitalen Auswahlprozesses für die Essensbestellung von Patientinnen und Patienten.

Die zweite Angriffsmethode stellen **DDoS-Angriffe** dar. Die Abkürzung steht für „Distributed Denial of Service“. Über „gekaperte“ Botnetze finden systemüberlastende Angriffe auf internetbasierte Lösungen statt, wodurch reguläre Dienste nicht mehr funktionieren können. Ransomware- und DDoS-Angriffe können auch kombiniert werden, um die Auswirkungen des Angriffs zu verstärken.

Die nachfolgenden Beispiele dienen nicht der Bloßstellung, sie hätten an jedem anderen Ort in Deutschland auch auftreten können. Wichtig ist aber, dass Einrichtungen aus den Vorfällen anderer lernen und sie zur Vermittlung der Gefährdungslage beherzigen:

Praxisbeispiel 1:

Universitätsklinikum Düsseldorf 2020

Vermutlich russischen Angreifern gelang es, über eine Sicherheitslücke in die Systeme des Universitätsklinikums Düsseldorf zu gelangen. Durch die Ransomware-Attacke fielen nach und nach Systeme aus. Das Klinikum sagte elektive Eingriffe ab und führte die Abmeldung von der Notfallversorgung durch. Dadurch musste eine Patientin in einem Rettungswagen in ein entfernteres Krankenhaus transportiert werden. Sie verstarb beim verlängerten Transport, weshalb die Presse vom ersten „Cybertoten“ in Deutschland sprach. Allerdings konnte dieser Ursachenzusammenhang nicht mit an Sicherheit grenzender Wahrscheinlichkeit festgestellt werden, weshalb die eingeschaltete Staatsanwaltschaft das eingeleitete Todesermittlungsverfahren gegen die unbekannten Täter wieder einstellte.

Durch die ebenfalls hinzugezogenen Beamten des Landeskriminalamts Nordrhein-Westfalen konnte Kontakt zu den Tätern aufgenommen werden. Dadurch wurde klar, dass diese nicht das Klinikum, sondern die Universität selbst attackieren wollten. Sie gaben einen funktionierenden Wiederherstellungsschlüssel heraus und die Folgen des Angriffs konnten nach und nach beseitigt werden. Im Nachgang konnten Ermittlungsbehörden auch internationale Haftbefehle gegen die Täter erwirken.

Praxisbeispiel 2:

Universitätsklinikum Frankfurt 2023

Im Rahmen einer Routinekontrolle fiel im Oktober 2023 eine Infiltration der IT-Systeme des Universitätsklinikums Frankfurt auf. Umgehend wurde das Klinikum vom Internet getrennt, um das Risiko eines Datenabflusses zu vermeiden. Rückblickend traten weder ein Datenverlust noch eine Patientengefährdung ein. Die Auswirkungen des Angriffs zeigten sich vor allem im Verwaltungsbereich. Monatelang wurden Abrechnungen per Fax verschickt und die Online-Terminbuchung war nicht möglich. Trotz des frühen Entdeckens des Angriffs entstand nach Angaben des Klinikums ein Schaden im siebenstelligen Bereich.

Praxisbeispiel 3:

National Health Service (NHS) 2024

Der große britische Gesundheitsdienstleister NHS gab 2024 bekannt, dass ein Patient infolge eines Cyberangriffs auf einen Pathologiedienstleister gestorben sei. Der Angriff führte zu einer Verzögerung bei der Bereitstellung von Blutergebnissen, auf die das Krankenhaus angewiesen war. Der Patient verstarb, die Verzögerung stellte laut NHS eine Hauptursache unter mehreren Todesfaktoren im konkreten Einzelfall dar. Gerade für multimorbide, intensivpflichtige Patienten sind solche Verzögerungen eine große Bedrohung. Es handelt sich um den ersten bestätigten Todesfall in Europa aufgrund eines Cyberangriffs, der hier die Lieferkette des Krankenhauses betraf.

Praxisbeispiel 4:

MVZ Nordoberpfalz 2025

Im November 2025 waren zwei Standorte einer MVZ-Gruppe in Bayern durch einen Cyberangriff teilweise außer Betrieb gesetzt. Ein dritter Standort sowie das Klinikum als Gesellschafter des MVZ waren nicht betroffen. In der Folge mussten Operationen in den MVZ-Standorten abgesagt werden. Das Unternehmen informierte umgehend die Presse sowie die Patienten per Internet. Die MVZ-Gruppe

schaltete einen externen Dienstleister ein und stand in engem Kontakt mit der Kriminalpolizei. Ob Daten abgeflossen waren, war zu Beginn des Angriffs noch nicht bekannt.

Praxisbeispiel 5:
Auswirkungen des Angriffs auf Kommune in NRW 2023
Im Oktober 2023 wurde ein Ransomware-Angriff auf einen kommunalen IT-Dienstleister in Nordrhein-Westfalen entdeckt. Zum Angriffszeitpunkt erbrachte dieser Dienste für 72 Kommunen. Das führte zum temporären Ausfall von Rettungswagen in Olpe und Siegen, weil die GPS-Tracker der Fahrzeuge nicht mehr funktionierten. Dadurch konnte die Leitstelle keine Disposition der Fahrzeuge vornehmen.

Praxisbeispiel 6:
Cyberattacke auf Pharmagroßhändler 2024
Im Oktober 2024 wurde ein bayerischer Pharmagroßhändler Opfer einer Ransomware-Attacke. Die Verbindungen „zur Außenwelt" wurden gekappt, externe Dienstleister zur Krisenbewältigung herangezogen. Bestellungen einzelner Apotheken konnten nicht abgearbeitet werden.

> **Doch die Gefahren für die Cybersicherheit dürfen nicht einseitig auf Cyberangriffe durch Dritte beschränkt werden. Denn zum einen lauert die Gefahr auch im Unternehmen selbst, man spricht von „Innentätern".**

b) Cybervorfälle außerhalb krimineller Strukturen

Doch die Gefahren für die Cybersicherheit dürfen nicht einseitig auf Cyberangriffe durch Dritte beschränkt werden. Denn zum einen lauert die Gefahr auch im Unternehmen selbst, man spricht von **„Innentätern"**. Ein typisches Beispiel hierfür ist ein Mitarbeiter mit IT-Zugriffsrechten, der das Unternehmen verlassen will. Meist handelt es sich um für den Arbeitnehmer unfreiwillige Kündigungsfälle, aber auch der bewusste Wechsel zu einem Konkurrenten kann relevant sein. In solchen Fällen schaden Innentäter dem Unternehmen, indem sie ihre Zugriffsrechte ausnutzen und sensible Informationen abfließen lassen. Das ist gerade im Bereich der Forschung denkbar. Möglich ist auch das Versenden von sensiblen Informationen zu Pflichtverstößen an Presse oder Behörden, hierfür sind auch keine besonderen Zugriffsrechte notwendig.

> **Zum anderen lauert die Gefahr allgemein in der Digitalisierung, weil Prozesse und Produkte erneuert werden müssen, also ohne ein vorsätzliches Handeln.**

Zum anderen lauert die Gefahr allgemein in der Digitalisierung, weil Prozesse und Produkte erneuert werden müssen, also **ohne ein vorsätzliches Handeln**. IT-Vorfälle können typischerweise auch beim Rollout einer neuen Software oder einer Update-Variante geschehen. Besonders sichtbar wurde das bei einem fehlerhaften Update eines Virenscanner-Produktes im Jahr 2024, das weltweite Auswirkungen hatte. Flüge mussten annulliert werden, Geldautomaten gaben kein Geld mehr aus. Auch das Gesundheitswesen war betroffen. In Schleswig-Holstein musste das Universitätsklinikum mit den Standorten Kiel und Lübeck elektive Eingriffe absagen. Eine weitere größere Panne folgte im Herbst 2025, als Dienste eines global tätigen Infrastruktur- und Sicherheitsanbieters für Websites und Internetdienste ausfielen. Das führte zu Funktionseinschränkungen u.a. beim Dienst ChatGPT. Wäre der Einsatz Künstlicher Intelligenz im Gesundheitswesen schon weiter fortgeschritten gewesen, hätte der Vorfall auch für das Gesundheitswesen eine deutlich größere Bedeutung haben können.

> **Auch physische Vorfälle können IT-Störungen auslösen.**

c) Physische Vorfälle mit Cyberbezug

Auch **physische Vorfälle** können IT-Störungen auslösen. Gerade das ist der Grund, warum künftig auch das KRITIS-Dachgesetz greifen soll. Eines der häufigsten Risiken für Betriebseinschränkungen in Krankenhäusern stellen Brandereignisse dar. Laut der Statistik des Bundesverbands Technischer Brandschutz e.V. kam es bspw. im Jahr 2024 in deutschen Krankenhäusern zu 114 Bränden mit 148 Verletzten und sieben Toten. Neben der unmittelbaren Gefahr für Leib und Leben

gefährden diese Ereignisse sowohl durch den Brand selbst als auch durch Löschmaßnahmen IT-Systeme in den Krankenhäusern. In Aschaffenburg gab es 2025 einen Brand bei einem Akku der Notstromversorgung eines Krankenhauses, wodurch IT-Systeme beschädigt wurden. Durch die aktivierten Notfallpläne konnte die Patientenversorgung aufrechterhalten werden, Patientendaten gingen nicht verloren.

Aufgrund des **Klimawandels** kommt es häufiger zu Extremwetterlagen, die Einflüsse auf die Gesundheitsversorgung haben können. Neben Massenanfällen von Verletzten aufgrund von Hochwasser betrifft das vor allem auch unmittelbar die bauliche Einrichtung „Krankenhaus“. Das Extrembeispiel der jüngeren Vergangenheit stellt mit Sicherheit die Flutkatastrophe im Ahrtal dar, die sowohl zu einem Extremanstieg von Patienten als auch zu einer unmittelbaren Beschädigung von Gesundheitseinrichtungen geführt hat. Häufiger sind Umweltereignisse lokaler begrenzt. So führte im Jahr 2024 ein Unwetter in Hessen zu Wassereintritten in zwei Krankenhäusern. Aus Sanitäreinrichtungen floss Wasser in die Intensivstationen, die dann durch die Feuerwehr freigepumpt werden mussten. Die Patientenversorgung war nicht gefährdet.

Auch im physischen Bereich sind kriminelle Handlungen möglich. Kritische Einrichtungen stehen im Fokus von **Sabotageakten**, sie müssen nicht immer politisch motiviert sein. In Berlin wurde 2025 ein Klinikum aufgrund der Detonation von Feuerwerkskörpern beschädigt. Solche Ereignisse können sich auch gegen IT-Systeme richten oder sich zumindest auf deren Funktionsfähigkeit auswirken.

d) Überblick zu den Auswirkungen von Cybervorfällen im Gesundheitswesen

Vielfach kommt es bei Cybervorfällen im Gesundheitswesen zum **Verlust von Gesundheitsdaten** bzw. der Zugriff hierauf ist zumindest temporär nicht mehr möglich. Nach aktuellen BSI-Zahlen sind in 18 Prozent der untersuchten Datenleaks Gesundheitsdaten betroffen.

Außerdem können **Behandlungsabläufe gestört** werden – typische Erstmaßnahmen im Krankenhaus sind die Abmeldung der Notaufnahme und die Absage elektiver Eingriffe, um den Patientenfluss zur Einrichtung zu minimieren, weil Ressourcen eingeschränkt sind. Die Patientensicherheit ist also massiv gefährdet. Eine Studie aus den USA, die 2022 veröffentlicht wurde, spricht von einer Steigerung der Sterbewahrscheinlichkeit bei Patienten von 20 bis 35 Prozent, wenn sie sich (mit Komorbiditäten) zum Zeitpunkt eines Ransomware-Angriffs im Krankenhaus befinden.

Wie das Frankfurter Beispiel zeigt, kann auch die **Störung von Verwaltungsabläufen** zur großen Herausforderung werden. Die Bandbreite ist hier groß. Bei der üblicherweise digital stattfindenden Abrechnung muss eine Vielzahl an Dokumenten mit eingereicht werden (man denke bspw. an die Dokumentation des OPS zur Intensivmedizinischen Komplexbehandlung), auf die ggf. kein Zugriff mehr möglich ist. Aber auch schon der Nachweis durchgeführter Transporte von Rettungsdiensten kann eingeschränkt sein und sich dadurch herausfordernd auswirken. Weitere Bereiche der Verwaltung mit großem Bedrohungspotenzial für die Betriebsfähigkeit sind die Einkaufsabteilung und die Personalabteilung, wenn bspw. kein Zugriff mehr auf Dienstpläne möglich ist.

Bei Cyberangriffen stellen die Täter typischerweise **Lösegeldforderungen**, die oft in den Systemen des Opfers hinterlegt werden. Die Bezahlung findet über Kryptowährungen statt. Der Median der Lösegeldforderungen in Deutschland lag 2025 im mittleren sechsstelligen Bereich. Allerdings lassen sich die Forderungen oft noch verhandeln, zugleich steigt aber das Risiko eines erneuten Angriffs, wenn eine Zahlungsbereitschaft bekannt wurde. Die Sicherheitsbehörden raten grundsätzlich von der Bezahlung ab.

Weitere Kostenpositionen sind **Folgekosten** nach einem Unfall zur Härtung der Einrichtung. Das umfasst u.a. die Aufklärung des Angriffs, Rechtsverfolgungskosten, Kosten für die Verbesserung von IT-Strukturen und Personalmaßnahmen. Außerdem wird stets das **Reputationsrisiko** bei Cybervorfällen betont, was im Gesundheitswesen besonders relevant ist, weil aufgrund der Sensibilität der verarbeiteten Daten und der Dienstleistung eine hohe Erwartungshaltung der Bevölkerung in die Funktionsfähigkeit besteht.

e) Geopolitische Einordnung der Gefährdungslage

Neben intern verursachten Gefahren spielen eine Reihe äußerer Faktoren eine wichtige Rolle in der Gefähr-

dungslage. Diese verändert sich auch immer wieder. Die wirtschaftlich intendierten Cyberangriffe werden durch hochprofessionelle Strukturen durchgeführt, man bezeichnet das als **„Cybercrime-as-a-Service“**, weil Cyberkriminelle Schadsoftware als eine Art Leihmodell zur Verfügung stellen. Dadurch können auch technisch weniger befähigte Kriminelle Cyberangriffe fahren. Bei diesen Modellen gibt es strenge Absprachen, etwa über den Rabatt, der beim Lösegeld gewährt werden darf. Einige Strukturen verfügen auch über Ehrenkodizes, in denen u.a. der Angriff auf Gesundheitseinrichtungen mit unmittelbaren Lebensgefahren als kritisch angesehen wird. Allerdings ist die „Compliance“ in diesem Bereich nicht besonders streng. Die kriminellen Gruppen sitzen vor allem im Ausland. Das erschwert auch die Strafverfolgung.

Oftmals stecken aber hinter Angriffen auch **staatliche Akteure**. Sie unterstützten die kriminellen Strukturen. Ziel ist die Destabilisierung anderer Länder, indem das Vertrauen der Bevölkerung in wichtige Einrichtungen geschwächt wird und Desinformation betrieben werden kann.

Kapitel 4
Lerninhalte der NIS-2-Schulungspflicht

Der neue § 38 Abs. 3 BSIG schreibt vor, dass sich Geschäftsleitungen der betroffenen Einrichtungen regelmäßig im Bereich Risikomanagement schulen müssen. Das BSI hat hierzu im September 2025 eine **vorläufige Handreichung** veröffentlicht, aus der sich herauslesen lässt, welche Anforderungen die Aufsichtsbehörde an die Schulungen und insbesondere an die Lerninhalte stellt.

Die Handreichung folgt einer „Soll“- und einer „Kann“-Einstufung. Die „Soll“-Empfehlungen werden dringlich empfohlen, da sie zentrale Kenntnisse vermitteln, während die „Kann“-Empfehlungen ergänzende Kenntnisse erfassen. Die Handreichung trennt außerdem zwischen „Vorbereitender Inhalte“ als Grundlage für die **„Kerninhalte“ der Schulungen** (ausdrücklich genannte Vorgaben in § 38 Abs. 3 BSIG) sowie „Ergänzender Inhalte“ zu sektor- und einrichtungsspezifischen Anforderungen sowie Übungsszenarien.

Vorbereitende Inhalte:

- → Überblick zur NIS-2-Richtlinie
- → Umsetzung und Dokumentation von Risikomanagementmaßnahmen
- → Melde- und Unterrichtungspflichten
- → Registrierungspflichten
- → Pflichten für Geschäftsleitungen

Kerninhalte:

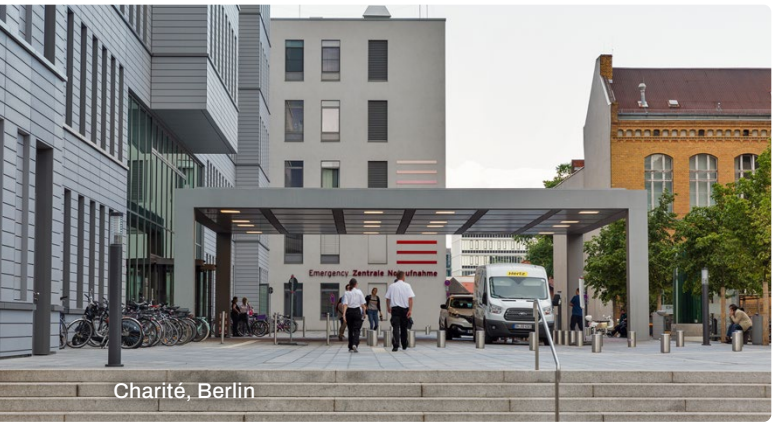
- → Risikoanalyse (Erkennung und Bewertung von Risiken)
- → Risikomanagementmaßnahmen (im Einzelnen)
- → Auswirkungen von Risiken und Risikomanagementmaßnahmen

Kapitel 5
Betroffenheit nach der NIS-2-Richtlinie

Als erster Schritt bei der NIS-2-Umsetzung erfolgt die Betroffenheitsprüfung der Einrichtung und ihrer Dienste. Bereits dieser Schritt kann herausfordernd sein, wie einige Feinheiten der nachfolgenden Ausführungen zeigen.

a) Anwendungsbereich des BSIG unter der alten NIS-Richtlinie

Bislang legte die Vorgängerrichtlinie (NIS-Richtlinie) für das BSIG nur die „Leitplanken" fest, wer betroffen sein sollte. Die Sektoren waren vorgegeben, die Größenangaben legten die Mitgliedstaaten fest, in Deutschland über die BSI-Kritis-Verordnung anhand von Schwellenwerten.



Charité, Berlin

Den größten Anteil Kritischer Infrastrukturen im Sektor Gesundheit stellten die **Großkrankenhäuser** dar, die 30.000 oder mehr vollstationäre Fälle im Jahr behandelten. Diese machten insgesamt rund 15 bis 20 Prozent der deutschen Krankenhäuser aus. Hinzu kamen noch bestimmte Hersteller von Arzneimitteln, Medizinprodukten sowie Großlabore. Über den Sektor „Finanz- und Versicherungswesen" waren zudem Kranken- und Pflegeversicherungen vom BSIG erfasst. Insgesamt fielen knapp 5.000 Unternehmen aus allen Sektoren in den Anwendungsbereich des früheren BSIG.

b) Betroffenheitsbereich nach NIS-2

Der Anwendungsbereich des BSIG wird mit der Umsetzung der NIS-2-Richtlinie **deutlich vergrößert**, der Gesetzgeber ging von 30.000 betroffenen Einrichtungen aus. Als Sonderform ist die Bundesverwaltung betroffen, ansonsten erfolgt eine Dreiteilung der Einrichtungen nach Größenvorgaben und der Voraussetzung einer Sektorzugehörigkeit nach den Anlagen I und II des BSIG.

Die Mitgliedstaaten können die Größenordnungen für die betroffenen Einrichtungen nicht mehr selbst festlegen, weil dies unter der Vorgängerrichtlinie zu deutlichen Unterschieden in Europa geführt hat und das für die Resilienz des Europäischen Binnenmarktes nicht förderlich war. Daher hat sich der europäische Normgeber für die Anwendung der KMU-Kriterien (Kleine und Mittlere Unternehmen) entschieden. Der EU-Normgeber schreibt **zwei Einrichtungskategorien** vor, der deutsche Gesetzgeber hat sich für einen Sonderweg entschieden.

Wichtige Einrichtung nach § 28 Abs. 2 BSIG
Beschäftigung von mindestens 50 Mitarbeitern oder Aufweisen eines Jahresumsatzes und einer Jahresbilanzsumme von 10 Millionen Euro

Besonders wichtige Einrichtung nach § 28 Abs. 1 BSIG
Beschäftigung von mindestens 250 Mitarbeitern oder Aufweisen eines Jahresumsatzes von über 50 Millionen Euro und einer Jahresbilanzsumme von über 43 Millionen Euro

Betreiber kritischer Anlagen nach § 2 Nr. 22 BSIG
Bestimmung anhand von Schwellenwerten der BSI-Kritis-Verordnung

Die **Betreiber kritischer Anlagen** stellen eine Sonderform der besonders wichtigen Einrichtungen dar und decken das ab, was bislang als Kritische Infrastruktur galt. Sprich: Alle Regeln für die besonders wichtigen Einrichtungen sind anwendbar, sofern nicht die Vorgaben für die Betreiber kritischer Anlagen etwas Zusätzliches regeln. Insgesamt geht der Gesetzgeber von einer Betroffenheit von 8.250 Unternehmen als besonders wichtige Einrichtungen und 21.600 Unternehmen als wichtige Einrichtungen aus (BT-Drs. 21/1501, S. 110).

c) Betroffene Teilsektoren im Gesundheitswesen

Die Betroffenheit der Einrichtungen, die die Größenvorgaben erfüllen, folgt dann aus Anlage I des BSIG, die beide Einrichtungsgrößen betrifft, und aus Anlage II des BSIG, welche die wichtigen Einrichtungen adressiert.

(1) Einrichtungen aus dem Sektor Gesundheit in Anlage I

Die meisten Anwendungsfälle im Sektor Gesundheit der Anlage I wird es über die **Gesundheitsdienstleister** geben. Das Gesetz greift dafür auf den Begriff aus der Patientenmobilitäts-Richtlinie (RL 2011/24/EU) zurück. Die Betroffenheit muss man sich in der Richtlinie über eine Normkette herleiten.

- Art. 3 lit. g der RL → **„Gesundheitsdienstleister“**: jede natürliche oder juristische Person oder sonstige Einrichtung, die im Hoheitsgebiet eines Mitgliedstaats rechtmäßig Gesundheitsdienstleistungen erbringt.
- Art. 3 lit. a der RL → **„Gesundheitsversorgung“**: Gesundheitsdienstleistungen, die von Angehörigen der Gesundheitsberufe gegenüber Patienten erbracht werden, um deren Gesundheitszustand zu beurteilen, zu erhalten oder wiederherzustellen, einschließlich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten.
- Art. 3 lit. f der RL → **„Angehöriger der Gesundheitsberufe“**: ein Arzt, eine Krankenschwester oder ein Krankenpfleger für allgemeine Pflege, ein Zahnarzt, eine Hebamme oder ein Apotheker im Sinne der Richtlinie 2005/36/EG oder eine andere Fachkraft, die im Gesundheitsbereich Tätigkeiten ausübt, die einem reglementierten Beruf im Sinne von Artikel 3 Absatz 1 Buchstabe a der Richtlinie 2005/36/EG vorbehalten sind, oder eine Person, die nach den Rechtsvorschriften des Behandlungsmitgliedstaats als Angehöriger der Gesundheitsberufe gilt.

Entscheidend ist also, dass einer der genannten Berufe eine Dienstleistung gegenüber einem Patienten erbringt, die darin liegt, seinen Gesundheitszustand zu beurteilen, zu erhalten oder wiederherzustellen, einschließlich der Verschreibung, Abgabe und Bereitstellung von Arzneimitteln und Medizinprodukten. Hauptanwendungsfälle des Teilsektors sind:

- Krankenhäuser,
- Medizinische Versorgungszentren (MVZ),
- Rettungsdienste,
- Apotheken.

Die Quote der „BSIG-Krankenhäuser“ steigt dadurch deutlich an. Die Auffangvorschrift des § 391 SGB V wird zur Ausnahme. Neu ist die Betroffenheit des ambulanten Sektors, erste Schätzungen gehen von bis zu 1.000 vom BSIG erfassten MVZ aus. Eine Herausforderung gilt bei Klinik-MVZ, da sowohl Krankenhaus als auch MVZ als eigene Einrichtungen vom BSIG erfasst sein können, dann je nach Größe unterschiedliche Anforderungen gelten können. Die Betroffenheit muss im Einzelfall begutachtet werden, ob bspw. bei MVZ-Gesellschaften die Mitarbeiter- bzw. Umsatz- und Jahresbilanzsummenzahlen kumuliert oder MVZ zur Klinik-Gesellschaft zugerechnet oder einzeln betrachtet werden. Unabhängig vom Ausgang der Frage ist es wichtig, ein gemeinsames Konzept für die **sektorenübergreifende Versorgung** zu erstellen, das auch den Notfall erfasst sowie Streitfragen zwischen Krankenhaus- und MVZ-Leitung über IT-Sicherheitsfragen klärt.

Auch für **Rettungsdienste** ist die Betroffenheit vom BSIG neu. Das BSI hatte 2024 noch eine Befragung zur Digitalisierung im Rettungsdienst durchgeführt, die zum Ergebnis kam, dass IT-Sicherheits-Managementprozesse im Rettungsdienst noch unterdurchschnittlich entwickelt sind. Ein Großteil der Leistungserbringer

hat dies aber erkannt und die Vorbereitungen auf die NIS-2-Richtlinie frühzeitig begonnen. Lediglich bei den Berufsfeuerwehren stellt sich die Frage der Betroffenheit, da diese funktional Teil der kommunalen Verwaltung sind, die in Deutschland, basierend auf Art. 2 Abs. 5 NIS-2-RL, nicht vom BSIG erfasst ist. Die Anhänge der NIS-2-RL und mithin des BSIG sind aber tätigkeitsfokussiert geregelt, was unter Berücksichtigung der Rechtsprechung des EuGH (C-529/21) zur engen Auslegung des Begriffs der öffentlichen Sicherheit gemäß Art. 2 Abs. 7 NIS-2-RL für eine Betroffenheit auch der Berufsfeuerwehren im Rettungsdienst spricht. Kommunale Eigenbetriebe nennt der Gesetzgeber ausdrücklich als Betroffene vom BSIG (BT-Drs. 21/1501, S. 110), was die anderen kommunalen Rettungsdienst-Leistungserbringer adressiert.

Weitere Einrichtungen aus dem Sektor Gesundheit in Anlage I sind:

- EU-Referenzlaboratorien (Art. 15 VO (EU) 2022/2371),
- Arzneimittelforschung und -entwicklung nach § 2 AMG,
- Hersteller pharmazeutischer Erzeugnisse nach Abschnitt C Abteilung 21 NACE Rev. 2,
- Hersteller von kritischen Medizinprodukten für Notlagen (Art. 22 VO (EU) 2022/123).

Über die BSI-Kritis-Verordnung werden Großlabore ebenfalls weiterhin vom BSIG erfasst sein, sofern sie nicht als Krankenhauslabore der Krankenhausdienstleistung zuzurechnen sind.

(2) Weitere betroffene Einrichtungen aus dem Gesundheitswesen

In Anlage II sind im Sektor „Verarbeitendes Gewerbe/ Herstellung von Waren“ die **Hersteller von Medizinprodukten** nach Art. 2 Nr. 1 der Medizinprodukte-Verordnung (VO (EU) 2017/745), sofern sie nicht bereits unter die Anlage I fallen, erfasst. Im „Sektor Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitssuchende“ der geänderten BSI-Kritis-Verordnung, die für die Betreiber kritischer Anlagen gilt, können **Kranken- und Pflegeversicherungen** wie schon bisher vom BSIG betroffen sein. Die Telematikinfrastruktur wird weiterhin über das SGB V reguliert.

a) Die Nebentätigkeitsklausel im Gesundheitswesen

Für die Zuordnung zu den Einrichtungsarten der Anlagen I und II sind nach § 28 Abs. 3 BSIG solche Tätigkeiten nicht zu berücksichtigen, die eine **Nebentätigkeit** darstellen. Konkret bedeutet das, dass die in einem solchen Nebentätigkeitsgebiet eingesetzten Mitarbeiter sowie der dort erzielte Jahresumsatz und die Jahresbilanzsumme nicht einberechnet werden müssen. Ein mögliches Beispiel für eine solche Nebentätigkeit stellt der Betrieb einer Kindertagesstätte für das Personal eines Krankenhauses dar.

Kapitel 6
Risikomanagement nach der NIS-2-Richtlinie

Der Kern des Pflichtenkatalogs des BSIG stellt das **Risikomanagement** nach § 30 BSIG dar. Durch die Vorschrift wird klargestellt, dass all das Bestreben der Regulierung dadurch erreicht werden soll, dass die Einrichtungen technische und organisatorische Maßnahmen – kurz TOM genannt – ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Die Einhaltung der Risikomanagement-Pflicht ist zu dokumentieren.

> **Bei Verfügbarkeit, Integrität und Vertraulichkeit handelt es sich um die drei klassischen Schutzziele eines Informationssicherheits-Managementsystems.**

1. Schutzziele des BSIG

Bei Verfügbarkeit, Integrität und Vertraulichkeit handelt es sich um die **drei klassischen Schutzziele** eines Informationssicherheits-Managementsystems (ISMS). Der Branchenspezifische Sicherheitsstandard (B3S) für die medizinische Versorgung, also für den Krankenhausbereich, definiert sie wie folgt (B3S, v1.3, S. 9 f.):

- **Verfügbarkeit** von Dienstleistungen und Funktionen eines Informationssystems, IT-Systems, der IT-Netzinfrastruktur oder auch von Informationen ist dann gegeben, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
- **Integrität** bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Informationen und der korrekten Funktionsweise von Systemen.
- **Vertraulichkeit** stellt den Schutz vor unbefugter Preisgabe von Informationen sicher. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.

> **Der B3S nennt außerdem weitere Schutzziele, die Authentizität ist ein gängiges ISMS-Schutzziel, die Patientensicherheit und die Behandlungseffektivität sind Besonderheiten des Gesundheitswesens.**

Der B3S nennt außerdem **weitere Schutzziele**, die Authentizität ist ein gängiges ISMS-Schutzziel, die Patientensicherheit und die Behandlungseffektivität sind Besonderheiten des Gesundheitswesens:

- **Authentizität** der Informationen ist sichergestellt, wenn sie von der angegebenen Quelle erstellt wurden.
- **Patientensicherheit** wird definiert als die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.
- **Behandlungseffektivität** stellt das zielgerichtete Zusammenwirken der beteiligten Prozesse und Informationen zur medizinischen Behandlung des Patienten, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten, sicher.

Es geht also darum, schädliche Auswirkungen durch Ausfälle, Manipulation, unberechtigte Zugriffe oder Datenverluste zu verhindern. Die Schutzziele sind bei der Auswahl, Umsetzung und Prüfung von IT-Sicherheitsmaßnahmen im gesamten Geltungsbereich der betroffenen Einrichtungen zu berücksichtigen. Die Relevanz und das Gewicht der einzelnen Schutzziele können abhängig vom jeweiligen Schutzobjekt und dessen Bedeutung für die erbrachte Dienstleistung unterschiedlich sein.

2. Stellgrößen der TOM

Stellgrößen der TOM aus § 30 BSIG

- Geeignetheit
- Verhältnismäßigkeit
  - Ausmaß der Risikoexposition
  - Größe der Einrichtung
  - Umsetzungskosten
  - Eintrittswahrscheinlichkeit
  - Schwere von Sicherheitsvorfall
  - Gesellschaftliche und wirtschaftliche Auswirkungen eines Vorfalls
- Stand der Technik
- Gefahrübergreifender Ansatz

> **Beim Stand der Technik handelt es sich nach § 30 Abs. 2 BSIG um eine „Soll-Vorgabe“, Abweichungen können ein Sicherheitsrisiko darstellen.**

Beim Stand der Technik handelt es sich nach § 30 Abs. 2 BSIG um eine „Soll-Vorgabe“, Abweichungen hiervon unterhalb dieses Standards sind in der Praxis aber selten und können ein Sicherheitsrisiko darstellen. Sie müssen gut begründet und ausreichend dokumentiert sein, da es sich um eine Risikoentscheidung handelt.

> **Für die Funktionsweise des Risikomanagements kann man sich an den Branchenspezifischen Sicherheitsstandards – kurz B3S – orientieren.**

a) Funktionsweise des Risikomanagements

Für die Funktionsweise des Risikomanagements kann man sich an den **Branchenspezifischen Sicherheitsstandards** – kurz B3S – orientieren. Sowohl das alte als auch das neue BSIG sehen dieses Instrument vor, es ist jetzt in § 30 Abs. 8 BSIG geregelt. Danach können Branchenverbände, wie die Deutsche Krankenhausgesellschaft, B3S erarbeiten und dem BSI zur Eignungsfeststellung vorlegen. Das ist u.a. für den Krankenhausbereich mit dem „B3S für die Medizinische Versorgung“ nun zum dritten Mal geschehen. Im November 2025 hat das BSI die Version 1.3 für geeignet erklärt und diese Feststellung auf drei Jahre befristet. Das bedeutet: Wer als betroffene Einrichtung sowohl aus dem BSIG als auch als „SGB-V-Krankenhaus“ den B3S sorgfältig umsetzt, für den gilt die rechtliche Vermutung, dass alle Vorgaben an das Risikomanagement erfüllt sind. Für die neuen Anwendungsbereiche des BSIG im Gesundheitswesen sollten solche Standards zeitnah durch Branchenverbände erarbeitet werden.

> **Der B3S beschreibt den Risikomanagementprozess und zieht hierfür die gängigen ISO-Standards aus der Normenfamilie 27000 zu Informationssicherheits-Managementprozessen sowie den ISO 27799 speziell für das Gesundheitswesen heran.**

Der B3S beschreibt den Risikomanagementprozess und zieht hierfür die gängigen **ISO-Standards aus der Normenfamilie 27000** zu Informationssicherheits-Managementprozessen sowie den ISO 27799 speziell für das Gesundheitswesen heran, verweist zugleich aber auch auf die BSI-Standards, die sich an den ISO-Normen orientieren. Die Funktionsweise des Risikomanagements ist dort gleich.

Als **Teilprozesse des Risikomanagements** nennt der B3S für die medizinische Versorgung, was sich auch auf die anderen Gesundheitseinrichtungen übertragen lässt (B3S, v1.3, S. 43):

Teilprozesse eines Risikomanagements

1. Informationswerte (Risikoobjekte) und Verantwortliche (Risikoeigentümer) ermitteln
2. Kritikalität der Informationswerte festlegen
3. Risikokriterien festlegen
4. Bedrohungen und Schwachstellen identifizieren (potenzielle und vorhandene)
5. Risiken bewerten (Eintrittswahrscheinlichkeit und Schadenspotenzial)
6. Risiken behandeln (akzeptieren, vermeiden, transferieren oder reduzieren)
7. Risiken kommunizieren und überwachen

Für die Implementierung des Risikomanagements kommen folgende **organisatorische Pflichten** auf die Einrichtung zu (B3S, v1.3, S. 43 f.):

Muss-Vorgaben für das Management

- Die Geschäftsleitung muss die mit dem ISMS-Risikomanagement verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege definieren und aufeinander abstimmen sowie hierfür angemessene Risikosteuerungs- und Risikocontrollingprozesse einrichten und diesbezügliche Berichtspflichten definieren.
- Die Rahmenbedingungen zum ISMS-Risikomanagement müssen in einer Richtlinie zum ISMS-Risikomanagement festgelegt werden.
- Die Informations-Risikorichtlinie muss explizit in Kraft gesetzt und allen Beschäftigten und ggf. relevanten Geschäftspartnern bekannt gegeben werden.
- Eine standardisierte Risikomethodik muss zur Ermittlung der Risikobewertungen insbesondere im Hinblick auf die Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit festgelegt werden, um die Konsistenz der Bewertung der Risiken nachvollziehbar sicherzustellen.
- Es muss festgelegt werden, wer die Ergebnisse der Risikobewertung und -behandlung dokumentiert sowie alle nachfolgenden Überprüfungen zur Risikobewertung und -behandlung durchführt.
- Zum Betrieb von als kritisch bewerteten Systemen (vernetzt, nicht vernetzt) aus den Bereichen Medizingeräte, IT-Systeme, IT-Netzwerke, IT-Anwendungen muss eine Freigabe auf Basis einer nachprüfbaren Risikobewertung vorliegen.

> **Selbstverständlich ist das Fundament jedes Risikomanagement-Systems eine Risikoanalyse, um überhaupt die Prozesse ausrichten und kontrollieren zu können.**

b) Risikoanalyse

Selbstverständlich ist das Fundament jedes Risikomanagement-Systems eine **Risikoanalyse**, um überhaupt die Prozesse ausrichten und kontrollieren zu können. Eine Risikoanalyse lässt sich wie folgt skizzieren (B3S, v1.3, S. 45 ff.):

Schritt 1:
Ermittlung der Risikoobjekte und Risikoeigentümer
Risikoobjekte (auch Informationswerte genannt) müssen ermittelt, dokumentiert und verwaltet werden. Sie müssen einem Risikoeigentümer zugeordnet werden, der für das Risikomanagement die Ergebnisse der Risikoanalyse verantwortet und alle nachfolgenden Risikoanalysen durchführt.

Schritt 2:
Festlegung der Kritikalität
Für alle kritischen Informationswerte müssen die wesentlichen Anforderungen (Eigenschaften) an die Schutzziele der Informationssicherheit erhoben werden. Hierfür muss definiert werden, welche Risiken nicht mehr akzeptabel sind, weil sie etwa zur Gefährdung von Menschenleben oder hohen wirtschaftlichen Schäden führen können. Für diese Risiken muss sichergestellt sein, dass der risikobehaftete Prozess nicht in Betrieb genommen wird.

Schritt 3:
Risikoidentifikation
Zur Identifizierung von Bedrohungen und Schwachstellen sollen Bedrohungsprofile nach einem All-Gefahren-Ansatz, der also die elementaren Gefahren nach dem IT-Grundschutz-Kompendium des BSI berücksichtigt, erhoben werden.

Schritt 4:

Risikobewertung

Für alle Risikoobjekte sind die Eintrittswahrscheinlichkeiten und Schadenspotenziale so zu bewerten, als würde das ausgemachte Risiko eintreten. Hierbei ist zu prüfen, welche Auswirkungen der Verlust eines Schutzziels für das betrachtete Informationssystem in Hinblick auf Schäden aller Art, Folgekosten und Wiederherstellungsaufwand herbeiführen könnte.

Die Geschäftsleitung muss die Kriterien zur Bewertung von Risiken auf Basis einer qualitativen Abschätzung von Eintrittswahrscheinlichkeiten und Schadenspotenzialen vorgeben.

Schritt 5:

Risikobehandlung

Die jeweiligen Risikoeigentümer legen für die Risikoobjekte einen formalen Prozess in Form eines Risikobehandlungsplans fest, wie mit den festgestellten Risiken umgegangen wird. Hierfür muss die Geschäftsleitung die zulässigen Kriterien für die Risikobehandlung und Akzeptanzkriterien für Restrisiken auf Basis von Risikoklassen vorgeben. Die Geschäftsleitung trägt die Verantwortung über die Entscheidung zur Strategie des Risikoumgangs, wobei auch eine Kombination möglich ist aus

- Risikominderung,
- Risikovermeidung,
- Risikoakzeptanz.

Schritt 6:

Risikokommunikation und -überwachung

Die Geschäftsleitung muss in den Prozess der Risikokommunikation innerhalb der Einrichtung einbezogen werden. Sie muss sich in angemessenen Abständen über die Risikosituation berichten lassen, damit sie ihrer Überwachungsverantwortung nachkommen kann. Die Kenntnisnahme der Geschäftsleitung von Risikoberichten muss dokumentiert werden.

> **Die Geschäftsleitung einer Einrichtung muss für ihre Leitungsverantwortung die Auswirkungen des Risikomanagements kennen.**

c) Auswirkungen des Risikomanagements

Die Geschäftsleitung einer Einrichtung muss für ihre Leitungsverantwortung die **Auswirkungen des Risikomanagements kennen**. Zunächst gilt das Credo: „Es gibt keine einhundertprozentige Sicherheit." Die Geschäftsleitung muss sich also, auch wenn sie die Risikomanagement-Pflichten bestmöglich einhalten will, darauf einstellen, dass es zu einem Vorfall kommen wird. Das Ziel liegt vielmehr darin, neben der Vermeidung von Vorfällen vor allem den Umgang mit Vorfällen zu professionalisieren, um Auswirkungen gering zu halten. Selbstverständlich müssen nicht akzeptable Risiken mit größter Anstrengung vermieden werden. Die eingangs genannten Beispiele zeigen die unterschiedlichsten Auswirkungen von Vorfällen auf. Anhand der Strategieentscheidungen zum Risikoumgang wird deutlich, wie das Risikomanagement sich auswirkt und wie aus den Entscheidungen eine angemessene Balance gefunden werden muss.

d) Risikomanagementmaßnahmen im Einzelnen

Der neue § 30 Abs. 2 BSIG listet Mindestvorgaben für das Risikomanagement auf, was ein Vorteil gegenüber der Vorgängerregelung ist. Die Geschäftsleitung muss ein Grundverständnis für diese Vorgaben haben, um ihrer Überwachungspflicht nachkommen zu können.

Vorgabe	Hinweise
Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik	s.o.
Maßnahmen zur Bewältigung von Sicherheitsvorfällen	Der Gesetzgeber nennt das auch Incident Response (BT-Drs. 21/1501, S. 148). Ausgewählte Profis innerhalb und außerhalb der Einrichtung folgen einem Krisenplan und geben anschließend Hinweise zum Nachschärfen der Risikomanagementmaßnahmen nach einem „Lessons-Learned-Prinzip“.
Maßnahmen zur Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	Aufgrund des Restrisikos eines Vorfalls trotz bester Sicherungsmaßnahmen müssen die bestmögliche Aufrechterhaltung sowie das schnelle „Hochfahren“ von Systemen vorbereitet sein, man bezeichnet diesen Prozess als Business Continuity Management, der selbst auch ISO-standardisiert ist (ISO 22301), außerdem gibt es den BSI-Standard 200-4.
Maßnahmen für die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Dienstleistern	Wie in den Beispielen gezeigt, muss die Ursache für einen Vorfall nicht immer bei der Einrichtung selbst liegen. Mögliche Maßnahmen sind vertragliche Vereinbarungen mit Zulieferern und Dienstleistern zu Risikomanagementmaßnahmen, zur Bewältigung von Cybersicherheitsvorfällen, zum Patchmanagement sowie zur Verpflichtung der Zulieferer und Dienstleister zur Beachtung von grundsätzlichen Prinzipien wie Security by Design oder Security by Default (BT-Drs. 21/1501, S. 148).
Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen	Durchgehend müssen Sicherheitsgefahren innerhalb der Einrichtung einem Monitoring unterzogen werden. Updates müssen vertraglich zugesichert sein und durch die Einrichtung durchgeführt werden. Unternehmensabteilungen sind zu vernetzen, um Risiken bei geplanten IT-Lösungen zu überwachen.

Vorgabe	Hinweise
Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik	Nachweisfähige, standardisierte Mechanismen, mit denen die Einrichtungen fortlaufend prüfen, ob ihre Sicherheitsmaßnahmen tatsächlich wirken, und dies durch Berichte, Tests, Audits und Kennzahlen belegen.
Grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik	Zu unterscheiden von der Leitungsschulung sind Awareness-Maßnahmen gegenüber den Mitarbeitenden, die in regelmäßigen Abständen und risikobasiert je nach Einsatzfeld ergriffen werden müssen. Zudem ist beim Onboarding eine Sensibilisierung vorzunehmen.
Konzepte und Prozesse für den Einsatz von kryptografischen Verfahren	Mit Kryptografie werden Daten anhand von Algorithmen geschützt und „verschleiert“. Das Konzept legt fest, in welchen Anwendungsbereichen Verschlüsselungstechnik verbindlich einzusetzen ist und welche Art, Stärke und Qualität die Verschlüsselung haben muss (B3S, v1.3, S. 75 f.).
Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und die Verwaltung von IKT-Systemen, -Produkten und -Prozessen	Hiermit ist ein Identitäts- und Rechtemanagement (B3S, v1.3, S. 73 f.) gemeint, sodass Zugriffe auf das Mindestmaß beschränkt werden und bspw. auch beim Offboarding-Prozess sensibler Mitarbeitender sofort beschränkend reagiert wird.

Betreiber kritischer Infrastrukturen müssen außerdem nach § 31 Abs. 2 BSIG Angriffserkennungssysteme als TOM vorhalten. Hierfür gibt es eine Orientierungshilfe des BSI, die in der seit November 2025 gültigen dritten Version des Krankenhaus-B3S vollständig integriert wurde.

Kapitel 7

Melde- und Unterrichtungspflicht nach dem BSIG

Sämtliche Einrichtungen im Anwendungsbereich des BSIG müssen nach **§ 32 BSIG erhebliche Sicherheitsvorfälle an das BSI melden**. Hierfür wird eine gemeinsame Stelle von BSI und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) eingerichtet. Ein Sicherheitsvorfall (§ 2 Nr. 40 BSIG) ist ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt. Er ist dann erheblich (§ 2 Nr. 11 BSIG), wenn er

- schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder
- andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Gerade die zweite Variante ist im Gesundheitswesen dann relevant, wenn **Gesundheitsgefahren** aufgrund der Unterbrechung oder Beeinträchtigung der medizinischen Versorgung zu befürchten sind. Das neue BSIG sieht eine gestufte Meldepflicht vor, bei der strenge zeitliche Vorgaben gelten. Das macht die **Etablierung eines Meldewesens** in der Einrichtung notwendig, sodass relevante Informationen stets weitergegeben und von der empfangenden Stelle bewertet werden, um eine Meldung anzustoßen. Die Stufen lauten wie folgt:

Frühe Erstmeldung nach § 32 Abs. 1 Nr. 1 BSIG
Die Einrichtung muss unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung über den Vorfall und darüber, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte, abgeben.

Meldung nach § 32 Abs. 1 Nr. 2 BSIG
Die Einrichtung muss unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung abgeben über diesen Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie ggf. die Kompromittierungsindikatoren angegeben werden.

Abschlussmeldung nach § 32 Abs. 1 Nr. 4 BSIG
Spätestens einen Monat nach Übermittlung der Meldung (§ 32 Abs. 1 Nr. 2 BSIG) des Sicherheitsvorfalls muss eine Abschlussmeldung abgegeben werden, die Folgendes enthält:

a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

b) Angaben zur Art der Bedrohung bzw. ihrer zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

d) ggf. die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

Weitere Meldepflichten nach § 32 BSIG
Auf Ersuchen des BSI muss eine **Zwischenmeldung** über relevante Statusaktualisierungen stattfinden. Ist nach einem Monat der Vorfall noch nicht abgeschlossen, muss nach einem Monat eine **Fortschrittsmeldung** an das BSI abgegeben werden. Die Abschlussmeldung muss dann nachgeholt werden, sobald der Vorfall mit seinen Auswirkungen beseitigt ist.

Die **Betreiber einer kritischen Anlage** müssen zudem Angaben zur Art der betroffenen Anlage und der kritischen Dienstleistung sowie zu den Auswirkungen des Sicherheitsvorfalls auf diese Dienstleistung übermitteln, wenn ein erheblicher Sicherheitsvorfall Auswirkungen auf die von ihnen betriebene kritische Anlage hat oder haben könnte.

Außerdem besteht nach § 35 Abs. 1 BSIG künftig auch die Möglichkeit einer **Unterrichtungspflicht**. Das bedeutet, dass das BSI einer Einrichtung anordnen kann, die Empfänger ihrer Dienste – also im Gesundheitswesen die Patientinnen und Patienten – unverzüglich über diesen erheblichen Sicherheitsvorfall zu unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte.

Das BSI gibt nach § 36 BSIG eine **Rückmeldung** auf die Meldung der Einrichtung. Nach § 36 Abs. 2 BSIG kann es die Einrichtung zur Offenlegung des Sicherheitsvorfalls verpflichten, wenn eine Sensibilisierung der Öffentlichkeit erforderlich ist. Ob das ein praktischer Anwendungsfall für das Gesundheitswesen ist, ist noch unklar.

Kapitel 8
Weitere Rechtspflichten im neuen BSIG

Jede Einrichtung aus dem Anwendungsbereich des BSIG muss sich nach § 33 BSIG spätestens drei Monate, nachdem sie erstmalig vom Anwendungsbereich betroffen war, bei der gemeinsamen Stelle von BSI und BBK registrieren.

Jede Einrichtung aus dem Anwendungsbereich des BSIG muss sich nach § 33 BSIG spätestens drei Monate, nachdem sie erstmalig vom Anwendungsbereich betroffen war, bei der gemeinsamen Stelle von BSI und BBK **registrieren**. Die inhaltlichen Anforderungen hierfür sind in § 33 Abs. 1 BSIG genannt.

Die Betreiber kritischer Anlagen müssen im Drei-Jahres-Turnus mittels Audits/Prüfungen/Zertifizierungen nach § 39 Abs. 1 BSIG **nachweisen**, dass sie die Risikomanagementmaßnahmen umgesetzt haben. In diesem Zusammenhang kann das BSI auch die Beseitigung von Sicherheitsmängeln verlangen. Besonders wichtige Einrichtungen können durch das BSI ebenfalls zur Vorlage von Nachweisen nach § 61 Abs. 3 BSIG verpflichtet werden, bei wichtigen Einrichtungen ist dies nach § 62 BSIG nur möglich, wenn der Verdacht vorliegt, dass die Einrichtung die Vorgaben nicht ausreichend umsetzt. Für die Krankenhäuser nach § 108 SGB V ist nach § 61 Abs. 3 S. 5 BSIG eine Anordnung erst fünf Jahre nach Inkrafttreten des überarbeiteten BSIG möglich.

Kapitel 9
Rolle der Geschäftsleitung im BSIG

Die Geschäftsleitung spielt im neuen BSIG eine zentrale Rolle.

Die Geschäftsleitung spielt im neuen BSIG eine zentrale Rolle. Dies liegt an der neuen Compliance-Vorschrift des § 38 BSIG:

1. Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.

2. Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

3. Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Um diese Vorschrift gab es seit den ersten Entwürfen zur Umsetzung von NIS-2 große Aufregung, die im Kern nicht berechtigt ist. Denn die Vorschrift stellt nur klar, was bislang auch schon als anerkannte Compliance-Grundsätze galt.

a) Geschäftsleitungsverantwortung

Nach § 2 Nr. 13 BSIG ist die **„Geschäftsleitung“** eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist. Erfasst sind also Vorstände, Geschäftsführer sowie besondere Vertreter der Einrichtungen.

Die Letztverantwortung für die Umsetzung der Vorgaben trägt die Geschäftsleitung.

§ 38 Abs. 1 BSIG stellt klar, was auch den gängigen Grundsätzen der Compliance und anderer Managementsysteme entspricht: Die **Letztverantwortung** für die Umsetzung der Vorgaben trägt die Geschäftsleitung. Der Gesetzgeber geht selbst davon aus, dass Aufgaben aber delegiert werden. Diese dürfen nicht den Kern des Sicherheitsmanagements betreffen. Die „Muss-Vorgaben“ des B3S, die unmittelbar die Geschäftsleitung adressieren, sollten immer selbst durchgeführt werden. Der „Krankenhaus-B3S“ nennt hierzu (B3S, v1.3, S. 55 f.):

- Bekanntgabe und Durchsetzung der **Ziele der Informationssicherheit** (z.B. durch Veröffentlichung einer Informationssicherheitsleitlinie und Festlegung des B3S-Geltungsbereichs etc.) und Initiierung des Informationssicherheitsprozesses;
- Definition und Sicherstellung von **Rollen und Verantwortlichkeiten** sowie die Bereitstellung von notwendigen organisatorischen, personellen und finanziellen Ressourcen zur Umsetzung des Informationssicherheitsmanagements im Krankenhaus;
- Sicherstellung der glaubhaften und nachhaltigen **Vermittlung der Bedeutung der Informationssicherheit** gegenüber Mitarbeitern, Patienten und Dritten (z.B. Aufsichtsbehörden etc.) durch die Beauftragung von Awareness- und Kommunikationsmaßnahmen;

- **Sicherstellung der Wirksamkeit des ISMS** und zeitnaher Mängelbeseitigung durch Vorgabe von überprüfbaren Zielen und fortlaufender Kontrolle;
- Sicherstellung eines **angemessenen Qualifikationsniveaus der Mitarbeiter** entsprechend ihrer Aufgaben, Kompetenzen und Verantwortlichkeiten durch Schulungs- und Weiterbildungsmaßnahmen;
- **Minimierung von Interessenkonflikten** durch eine sinnvolle Aufteilung von Aufgaben und Verantwortungsbereichen auf organisatorischer Ebene (Funktionstrennung) (Beispiel: Informationssicherheitsbeauftragter und IT-Leiter in einer Person birgt Interessenskonflikte);
- eindeutige Zuweisung der Verantwortlichkeit für die **Kontrolle der Zielerreichung** des Informationssicherheitsmanagements sowie für die Umsetzung der im IT-Sicherheitsprozess abgestimmten Maßnahmen.

> **Sofern delegiert wird, muss die ausführende Person fachlich kompetent, finanziell ausreichend ausgestattet und sorgfältig überwacht sein, damit es sich um eine rechtssichere Delegation handelt.**

Sofern delegiert wird, muss die ausführende Person fachlich kompetent, finanziell ausreichend ausgestattet und sorgfältig überwacht sein, damit es sich um eine rechtssichere Delegation handelt. Bei **Ressortaufteilungen** innerhalb der Geschäftsleitungsebene verlagert sich die Überwachungspflicht zum Ressortverantwortlichen. Allerdings müssen die anderen Geschäftsleitungsangehörigen zumindest bei drohenden Verstößen und Unzulänglichkeiten im anderen Ressort mit einschreiten.

Der B3S für die Krankenhäuser sieht zwingend vor, dass ein **Informationssicherheitsbeauftragter (ISB)/ Chief Information Security Officer (CISO)** benannt wird, der den Informationssicherheitsmanagement-Prozess initiiert und seine Weiterentwicklung koordiniert. Es ist zu empfehlen, dass der CISO der Geschäftsleitung direkt unterstellt ist. Der CISO unterstützt die Geschäftsleitung bei zentralen Fragen der Informationssicherheit und koordiniert die Untersuchung informationssicherheitsrelevanter Ereignisse. Er initiiert die Awareness-Maßnahmen für die Mitarbeitenden und berichtet regelmäßig der Geschäftsleitung über den aktuellen Stand der Informationssicherheit und über relevante Ereignisse (B3S, v1.3, S. 58).

b) Regresspflicht der Geschäftsleitung

Nach § 38 Abs. 2 BSIG kann die Geschäftsleitung für Schäden aufgrund von Verstößen gegen das BSIG haften. Der **Regress** erfolgt im Regelfall über die Leitungsvorschriften des Gesellschaftsrechts. Auch hier handelt es sich also um keine komplette Neuheit. Risikoentscheidungen müssen sorgfältig dokumentiert werden, um Haftungsrisiken zu minimieren. Eine abgeschlossene D&O-Versicherung muss ggf. an das nun konkretisierte Haftungsrisiko angepasst werden.

> **Die Schulungspflicht dient dem Umstand, dass die Geschäftsleitung nur mit ausreichenden Fachkenntnissen ihrer Letztverantwortung sorgfältig nachkommen kann, um einen persönlichen Regress zu vermeiden.**

c) Schulungspflicht der Geschäftsleitung

Die **Schulungspflicht** dient dem Umstand, dass die Geschäftsleitung nur mit ausreichenden Fachkenntnissen ihrer Letztverantwortung sorgfältig nachkommen kann, um einen persönlichen Regress zu vermeiden. Die Schulungen können intern und extern erfolgen, die Ableistung ist zwingend zu dokumentieren, da das BSI dies überprüfen kann. Das BSI hält es in seiner Handreichung (ausdrücklich als Empfehlung) für sinnvoll, neben der Geschäftsleitung auch diejenigen Personen besonders zu schulen, die in „quasi-äquivalenten Positionen im Unternehmen arbeiten oder den Geschäftsleitungen zuarbeiten." (Handreichung des BSI, S. 6)

Der Gesetzgeber ging im Entwurf von einem Mindestturnus von drei Jahren für die Schulungen aus (BT-Drs. 21/1501, S. 154). Das Bundesministerium des Innern und für Heimat schätzt den Schulungsaufwand auf vier Stunden je Schulung. Das BSI betont die Angemessenheit des Umfangs und der Regelmäßigkeit und nennt Konstellationen, bei denen vom Mindest-Intervall abgewichen werden sollte (Handreichung des BSI, S. 7):

- 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 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.

d) Compliance-Verantwortung des Aufsichtsorgans

Auch wenn das BSIG die Aufsichtsorgane nicht in die Compliance-Vorschrift aufgenommen hat, befreit sie dies nicht von ihrer Compliance-Verantwortung, die sie selbst haftbar macht. Aufsichtsräte und andere Aufsichtsgremien sind verpflichtet, die Erfüllung der Compliance-Pflichten durch die Leitungsorgane zu kontrollieren. Hierfür sind Berichtswege sinnvoll. Der Aufsichtsrat sollte bei größeren Cyber Incidents informiert werden, um die Effektivität des etablierten Compliance-Managements kontrollieren zu können. Dafür sind ausreichende Kenntnisse in Bezug auf das Risikomanagement erforderlich. Besteht der Verdacht eines Organisationsverschuldens bei einem Cyber Incident, kann eine durch den Aufsichtsrat beauftragte interne Untersuchung sinnvoll sein.

Kapitel 10
Aufsichtsmaßnahmen nach dem neuen BSIG

Das neue BSIG kennt eine Reihe an Aufsichtsmaßnahmen des BSI. Wie erwähnt betreffen diese alle Einrichtungsarten. Bei den wichtigen Einrichtungsarten gilt dies nur beim Verdacht von Verstößen. Im Kern geht es für die Aufsichtsmaßnahmen um drei Vorschriften des BSIG, deren Umsetzung beaufsichtigt werden soll:

- Risikomanagement nach § 30 BSIG,
- Meldepflicht nach § 32 BSIG,
- Schulungspflicht nach § 38 Abs. 3 BSIG.

Die betroffenen Einrichtungen müssen bei den Aufsichtsmaßnahmen mit dem BSI kooperieren. Verstöße bei der Mitwirkung können sanktioniert werden. Als Ultima-Ratio-Aufsichtsmaßnahmen sieht das BSI die temporäre Aussetzung einer erteilten Genehmigung für die Einrichtung vor, die diese für die Dienstleistung benötigt, sowie eine vorübergehende Untersagung der Geschäftsleitungstätigkeiten.

Kapitel 11
Sanktionen nach der NIS-2-Richtlinie

Schon das bisherige BSIG hatte einen Bußgeldkatalog, allerdings war dieser von geringer praktischer Bedeutung. Die EU-Kommission hat die zurückhaltende Bußgeldpraxis der Mitgliedstaaten kritisiert. Das Stufenkonzept des Bußgeldkatalogs wurde zur Umsetzung von NIS-2 übernommen und um einzelne Bußgeldtatbestände erweitert. Abgestuft bedeutet, dass es für bestimmte Verstöße unterschiedliche Bußgeldrahmen gibt. Eine wichtige Neuerung ist die Möglichkeit der Konzernbemessung des Bußgelds. Konkret bedeutet das in § 65 BSIG:

- Die Höchstgeldbuße bei besonders wichtigen Einrichtungen liegt bei bis zu zehn Millionen Euro bzw. ab einem Gesamtumsatz von mehr als 500 Millionen Euro bei bis zu zwei Prozent des Gesamtumsatzes, der konzernweit anhand des weltweiten Umsatzes berechnet werden kann.
- Die Höchstgeldbuße bei wichtigen Einrichtungen liegt bei bis zu sieben Millionen Euro bzw. ab einem Gesamtumsatz von mehr als 500 Millionen Euro bei bis zu 1,4 Prozent des Gesamtumsatzes, der konzernweit anhand des weltweiten Umsatzes berechnet werden kann.

Für die Bemessung der Sanktionen sind folgende Kriterien von Bedeutung:

- Schwere des Verstoßes, wofür etwa die Wiederholung des Verstoßes, eine unterlassene Meldung oder Behebung von Sicherheitsmängeln sprechen,
- Dauer des Verstoßes,
- einschlägige frühere Verstöße der Einrichtung,
- verursachter materieller und immaterieller Schaden,
- Vorsatz oder Fahrlässigkeit des Urhebers des Verstoßes,
- ergriffene Schadensminderungsmaßnahmen,
- Umfang der Zusammenarbeit mit den zuständigen Behörden.

Kapitel 12
Zusammenspiel mit dem KRITIS-DachG

Die Umsetzung der CER-Richtlinie für physische Sicherheit lässt noch auf sich warten. Das künftige KRITIS-DachG befindet sich im Gesetzgebungsverfahren und tritt vermutlich 2026 in Kraft. Es wird ähnlich aufgebaut sein wie das BSIG. Federführende Behörde wird das BBK sein. Nach Risikoanalysen werden die Einrichtungen dann verpflichtet werden, Risikomanagementmaßnahmen zu etablieren, um physische Gefahren mit Auswirkung auf die Betriebsfähigkeit der Einrichtung zu vermeiden. Auch Meldepflichten bei Sicherheitsvorfällen werden eingeführt. Anvisiert ist ein Gleichlauf der Gesetze – in den bisherigen Entwürfen gab es feine Unterschiede, die zu Rechtsunsicherheit führen können. Der Anwendungsbereich ist noch nicht klar vorherzusagen. Gerade aber die Einrichtungen, die schon vom bisherigen BSIG erfasst waren, sollten sich zwingend mit den künftigen Vorgaben auseinandersetzen. Möglicherweise wird der Anwendungsbereich aber auch direkt deutlich größer, wenn sich der Bundesrat mit seiner Forderung durchsetzt. Dieser will den Schwellenwert für die Einrichtungen von 500.000 versorgten Einwohnern, wie er bisher auch in der BSI-Kritis-Verordnung für das BSIG galt, auf 150.000 versorgte Einwohner herabsetzen (BR-Drs. 558/25, S. 15).

Kapitel 13
BSIG und SGB V

Die Handreichung des BSI für die Schulungspflicht empfiehlt auch die Vermittlung von sektorspezifischem Wissen zum Risikomanagement. Im Gesundheitswesen betrifft das zum einen besondere Cybersicherheitsvorschriften im SGB V:

Norm	Erklärung
§ 390 – IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung	Über die „KBV-Richtlinie“ werden Sicherheitsvorgaben für die vertragsärztliche Versorgung gemacht. Klinik-MVZ müssen diese berücksichtigen. Leider sieht § 390 keine Ausnahmeregelung vor, wenn die Einrichtung vom neuen BSIG erfasst ist, was zu einer Doppelregulierung führt. Die „KBV-Richtlinie“ ist anders als der „Krankenhaus-B3S“ aufgebaut und leichter umzusetzen. Allerdings liegt ihre Schwäche darin, dass sie keinen Informationssicherheits-Prozess vorsieht.
§ 391 – IT-Sicherheit in Krankenhäusern	Die Auffangvorschrift für Krankenhäuser, die beim vergrößerten Anwendungsbereich des BSIG an Bedeutung verlieren wird. Wer vom BSIG erfasst ist, muss die Vorschrift nicht umsetzen. Die Vorgaben sind ähnlich aufgebaut, die Einhaltung des „Krankenhaus-B3S“ wird nahegelegt. Es gibt weder Registrierungs-, Nachweis- noch Meldepflicht und auch keine Sanktion.
§ 392 – IT-Sicherheit der gesetzlichen Krankenkassen	Das Pendant zu § 391 als Auffangvorschrift. Krankenkassen, die vom BSIG erfasst sind, sind von der Vorschrift ausgenommen. Eine Besonderheit liegt darin, dass ausdrücklich darauf Wert gelegt wird, dass beim Einsatz von IT-Dienstleistern Sicherheitsmaßnahmen ergriffen werden. Das müssen aber ohnehin alle Einrichtungen für ihr ISMS berücksichtigen, weil die NIS-2-Richtlinie ausdrücklich Risikomanagementmaßnahmen für die Lieferkette vorsieht.
§ 393 – Cloud-Einsatz im Gesundheitswesen	Wenn Gesundheits- und Sozialdaten durch Leistungserbringer des SGB V und Kranken- und Pflegekassen im Wege des Cloud-Computings verarbeitet werden, müssen Sicherheitsvorkehrungen getroffen werden. Das umfasst u.a. ein sog. C5-Typ2-Testat des BSI für den Cloud-Anbieter („datenverarbeitende Stelle“).

Kapitel 14

Wechselwirkung zur Krankenhausalarm- und Einsatzplanung

Die sogenannte Krankenhausalarm- und Einsatzplanung (KAEP) wird seit vielen Jahren durch verschiedene Landesvorschriften vorgeschrieben. Für Leitungspersonen in Krankenhäusern sind die Vorgaben ebenfalls notwendiges sektorspezifisches Wissen. Die KAEP wird oft an Großschadenslagen angeknüpft und verlangt Vorkehrungen, sodass die ordnungsgemäße Versorgung auch bei Massenanfällen von Verletzten und Erkrankten gewährleistet wird (vgl. bspw. § 28 Abs. 2 KHG BW). Dies darf aber nicht darüber hinwegtäuschen, dass es sich lediglich um externe Schadensereignisse handelt, die für die KAEP eine Rolle spielen. Auch durch Cybervorfälle im Krankenhaus kann eine solche Großschadenslage ausgelöst werden. Das BSIG und die KAEP beabsichtigen beide die möglichst ungestörte Betriebsfähigkeit der Ressource Krankenhaus. Damit muss, gerade im Hinblick auf etablierte Prozesse und im Unternehmen vorhandenes Know-how, unbedingt effektiv und ressourcenschonend vorgegangen werden. Zugleich müssen die Unternehmen aber auch die Besonderheiten der Regulierungen kennen – die KAEP sieht etwa keine Bußgeldsanktionen bei Verstößen vor. Auch ist sie bei Weitem nicht so detailliert gesetzlich ausgestaltet wie die Risikomanagement-Vorgaben der NIS-2-Richtlinie, gilt allerdings für alle Gefahrentypen der hybriden Gefährdungslage.

Kapitel 15

Patientenschäden aufgrund eines Cybervorfalls

Des Weiteren gehört es zu den sektorspezifischen Besonderheiten, dass es im Gesundheitswesen zu Patientengefährdungen kommen kann. Das ruft zivil- und strafrechtliche Risiken hervor. Gerade im Zivilrecht sind die Rahmenbedingungen der Arzthaftung beim Cybervorfall noch weitgehend ungeklärt.

Sowohl im Straf- als auch im Zivilrecht ist der Sorgfaltsmaßstab von entscheidender Bedeutung. Bei der Verletzung drohen Strafbarkeiten wegen der Fahrlässigkeitsdelikte im Strafrecht (§ 222 StGB: Fahrlässige Tötung; § 229 StGB: Fahrlässige Körperverletzung), im Zivilrecht Schadensersatzansprüche. Zur Ausformung des Sorgfaltsmaßstabs kann der „Krankenhaus-B3S“ herangezogen werden, da dieser auch auf die Patientensicherheit abzielt und dadurch einen individualschützenden Charakter aufweist.

Kapitel 16
NIS-2-Richtlinie und Datenschutz

Ein weiteres wichtiges Schnittstellenthema für das BSIG ist der Datenschutz. Bei der Verarbeitung personenbezogener Daten muss nach Art. 5 Abs. 1 lit. f und Art. 32 DSGVO durch TOM ein angemessenes Schutzniveau eingehalten werden, wobei im Gesundheitswesen gerade auf die Sensibilität von Gesundheitsdaten (Art. 9 DSGVO) zu achten ist. Diese Datensicherheit kann in ihrer Umsetzung mit der IT-Sicherheit zusammenfallen bzw. sich überschneiden, aufgrund der unterschiedlichen Zielrichtungen der Vorgaben muss aber präzise vorgegangen werden, ohne alles vorschnell „in einen Topf zu werfen“. Gerade im Anwendungsbereich der DSGVO sind Bußgeldverfahren in erheblicher Höhe mittlerweile bekannt. Dieses Risiko wird durch das BSIG erhöht, da es das BSI verpflichtet, wenn es bei seinen Aufsichtsmaßnahmen einen potenziellen DSGVO-Verstoß erkennt, diesen unverzüglich an die zuständige Datenschutzaufsichtsbehörde weiterzugeben.

Außerdem sieht die DSGVO ebenfalls eine Meldepflicht in Art. 33 DSGVO und eine Benachrichtigungspflicht in Art. 34 DSGVO vor. Diese Pflichten können beim Cybersicherheitsvorfall mit den Pflichten des BSIG zusammentreffen, sie weisen aber Unterschiede auf. Die Meldeprozesse müssen also auf beide Regularien abgestimmt sein.

Kapitel 17
Cyberversicherung unter NIS-2

Es besteht die Möglichkeit, eine Cyberversicherung abzuschließen, um Schäden bei einem Cybersicherheitsvorfall abzudecken. Außerdem können weitere Versicherungsprodukte (Vertrauensschadensversicherung, Strafrechtsversicherung, D&O-Versicherung) sinnvoll sein. Bei der Cyberversicherung muss darauf geachtet werden, dass Cybersicherheitsvorfälle zeitnah der Versicherung angezeigt werden, um nicht den Deckungsschutz zu verlieren. Außerdem sind die Versicherer im Notfall ein kompetenter Unterstützer, da sie natürlich ein Interesse daran haben, Schäden möglichst gering zu halten. Dadurch erhalten sie zugleich aber auch einen tiefen Einblick in das Unternehmen mit denkbaren Risiken für die Deckung eines Vorfalls.

Kapitel 18
Best Practices zum Umgang mit der Krise

Wie das BSIG auch betont, ist es wichtig, sich ein Krisenkonzept zu erarbeiten.

Wie das BSIG auch betont, ist es wichtig, sich ein Krisenkonzept zu erarbeiten. Es beginnt bestmöglich vor der Krise und ist ausreichend eingeübt. Nachfolgend werden Impulse für ein Krisenkonzept dargestellt:

Schritt 1:
Krisenvermeidung durch Prävention
Die Sicherheitsvorgaben des BSIG zielen darauf ab, Sicherheitsvorfälle zu vermeiden und die Unternehmen zugleich auf solche vorzubereiten. Es ist daher elementar, die Präventionsvorgaben sorgfältig umzusetzen. Da es sich um rechtliche Vorgaben handelt, ist eine Verzahnung mit dem Compliance-Management existenziell. IT-Sicherheit muss zum Rechtsthema gemacht werden. Da es sich sowohl beim Risikomanagement für die IT-Sicherheit als auch beim Compliance-Management um standardisierte Management-Prozesse handelt, ist eine Abstimmung jeweils auch gut möglich. Elementar ist der „Tone from the top"-Gedanke, wonach die Geschäftsleitung die Bedeutung der Integration des IT-Sicherheitsmanagements nach dem BSIG in das Compliance-Management betonen muss.

Mögliche praktische Anwendungsfälle des Compliance-Managements für mehr Cybersicherheit sind:

- Onboarding-Prozess: Sensibilisierung neuer Mitarbeitender und Absicherung der Bedeutung von IT-Sicherheit im Arbeitsvertrag.
- Offboarding-Prozess: Vermeidung „digitaler Rache" durch einen Mitarbeitenden mit Zugriffsrechten, der das Unternehmen verlassen wird.
- Einkaufsprozess: Vernetzung von Unternehmensstrukturen (Einkauf, HR, Compliance, IT etc.), um die Risiken bei der Implementierung neuer IT-Produkte überwachen und vermeiden zu können.
- Internal Investigation: Aufarbeitung eines Sicherheitsvorfalls zur Verbesserung des Systems („Lessons Learned"), da dies den Aufsichtsbehörden besonders wichtig ist.

Schritt 2:
Vermeidung von zusätzlichen Rechtsrisiken
Kommt es zum Sicherheitsvorfall, sind Rechtsrisiken für die betroffene Einrichtung möglich. Zugleich löst der Sicherheitsvorfall auch neue Rechtspflichten aus, insbesondere die Meldepflichten aus DSGVO und BSIG sowie die Anzeigepflicht gegenüber der Versicherung. Auf die Einhaltung der Vorgaben, die zeitlich streng reglementiert sind, muss besonders geachtet werden. Das verlangt gute Informationsprozesse innerhalb des Unternehmens und strukturierte Meldeprozesse, ggf. unter Heranziehung der Rechtsabteilung oder externer Rechtsberatung.

Die Zahlung von Lösegeldforderungen muss vorbereitet sein. Behörden raten von der Zahlung der Lösegelder u.a. zur Eindämmung des Kriminalitätsphänomens Cyberkriminalität ab. Zudem besteht das Risiko, dass ein Wiederherstellungsschlüssel nach einer Lösegeldzahlung nicht funktioniert oder man mit einer zu frühen Zahlung eine Zahlungsbereitschaft vorschnell suggeriert und sich noch weiter erpressbar macht. Weiterhin gibt es eine juristische Diskussion über die Strafbarkeit von Lösegeldzahlungen, wobei praktische Fälle zu Ermittlungsverfahren oder Verurteilungen hierzu nicht bekannt sind. Weiterhin ist zu bedenken, wie die Kryptowährungen konkret bezahlt werden können und ob möglicherweise die Cyberversicherung eine Zahlung abdeckt und unterstützt.

Schritt 3:

Erstellung des Krisenkonzepts als Teamaufgabe

In den verschiedenen Abteilungen der Gesundheitseinrichtungen steckt viel Know-how. Beispielsweise in Krankenhäusern durch die landesrechtlich vorgeschriebene Krankenhausalarm- und Einsatzplanung (KAEP), die seit vielen Jahren umgesetzt wird, um auf Großereignisse reagieren zu können. Diese „Krisenprofis“ und Krisenstrukturen können Unternehmen aufgreifen und unterschiedliche Risikomanagementprozesse aufeinander abstimmen.

Deshalb ist es besonders wichtig, für den Krisenfall zu wissen, wer die internen und externen Partner sind **(Know Your Partners)**, was sie leisten können und wo aber auch keine Hilfe zu erwarten ist.

- Beispiele für interne Partner: IT-Abteilung, Krisenstab, Rechtsabteilung, Kommunikationsabteilung, Betriebsfeuerwehr ...
- Beispiele für externe Partner: IT-Notfalldienstleister, Cyberversicherung, BSI, Landeskriminalämter, Datenschutzaufsichtsbehörden, Rechtsberatung, Kommunikationsberatung ...

Damit Strafverfolgungsbehörden die Chance haben, Vorfälle strafrechtlich zu verfolgen, und da es in seltenen Fällen auch gelingt, gezahlte Lösegelder wieder abzugreifen, ist es sinnvoll, eine Strafanzeige gegen unbekannt zu erstatten. In vielen Bundesländern gibt es Schwerpunkt-Staatsanwaltschaften in Zusammenarbeit mit den Landeskriminalämtern, die im Krisenfall Unterstützung bieten können.

Bei der Vorfallsbewältigung müssen Maßnahmen und Feststellungen dokumentiert werden. Es lohnt sich bei schwerwiegenden Fällen die Durchführung einer internen Untersuchung zur Klärung von Verantwortlichkeiten und möglichem Fehlverhalten im Unternehmen. Außerdem kann sie helfen, festgestellte Missstände abzustellen. Das „Lessons Learned“-Prinzip bzw. die sog. Remediation sind wichtige Bestandteile von Risiko- und Compliance-Management und können nachteilige Rechtsfolgen abmildern.

Hinweise zum Leitfaden

Der Leitfaden wurde erstellt durch Dr. Tilmann Dittrich, LL.M. (Medizinrecht), Mitglied des Scientific Advisory Board des cyberintelligence.institute mit Sitz in Frankfurt am Main und Rechtsanwalt der Kanzlei Wessing & Partner Rechtsanwälte mbB in Düsseldorf. Der Leitfaden stellt eine allgemeine Information dar und ersetzt keine individuelle Rechtsberatung. Für die Lösung konkreter Sachverhalte wenden Sie sich bitte an einen Rechtsanwalt oder eine andere qualifizierte Person.

Hinweise, Verbesserungsvorschläge und Kritik nimmt der Autor gern entgegen über LinkedIn (https://www.linkedin.com/in/dr-tilmann-dittrich-ll-m-61bb521a7/) sowie die Kontaktadresse des CII (info@cyberintelligence.institute).

Der Leitfaden ist auf dem Stand vom 30.11.2025 und berücksichtigt, wie eingangs erwähnt, die verabschiedete Fassung des BSIG. Er liegt in der Version 1.0 vor.

Über das CII

Neue Zeiten brauchen eine neue Form der Forschung: das cyberintelligence.institute (CII) – ein Ort, an dem sich Innovation, Technologie, Strategie und Resilienz treffen. An der Schnittstelle von Wirtschaft und Wissenschaft, NGO und Start-up entwickelt das CII in Frankfurt am Main neue Lösungen für eine sichere digitale Zukunft. Kerngedanken sind die Kooperation, der Dialog und der interdisziplinäre und globale Informations- und Wissensaustausch, um Staat, Wirtschaft und Gesellschaft resilienter zu machen. Gefragt sind dabei ganzheitliche Konzepte, die Cybersicherheit nicht nur als abstrakte technisch-organisatorische Gewährleistungsverantwortung, sondern als gesamtgesellschaftliche Aufgabe zum Schutz gemeinsamer europäischer Werte verstehen. Damit tritt das cyberintelligence.institute aktiv für mehr digitale Sicherheit in einem Zeitalter neuer digitaler Herausforderungen ein.

Weitere Informationen gibt es auf der Website des CII unter www.cyberintelligence.institute.

CYBERINTELLIGENCE
.Institute

cyberintelligence.institute
MesseTurm
Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

www.cyberintelligence.institute
info@cyberintelligence.institute

+49 69 505034602

Date of Publication: 12/2025