Energie. Wasser. Leben.

Die Wasserwirtschaft im BDEW

Berlin, 20. Mai 2026

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Anwendungshilfe

Sicherheit und Resilienz in der Wasserwirtschaft

Hinweise und Empfehlungen zum Umgang mit dem NIS2-Umsetzungsgesetz und dem KRITIS-Dachgesetz

Versionsnummer: 1

Inhalt

Hinweise zur Verwendung

Die nachfolgende Anwendungshilfe soll den Unternehmen der Wasserwirtschaft einen möglichst schnellen und einfachen Einstieg sowie Orientierung bieten, um die Pflichten aus dem KRITIS-Dachgesetz (nachfolgend: KRITISDachG) und dem NIS2-Umsetzungsgesetz (nachfolgend NIS2-UG) umzusetzen. Gleichzeitig besteht damit die Chance, die betriebliche Sicherheit und Resilienz der Unternehmen generell weiter zu verbessern. Die einzelnen Kapitel geben praktische Hinweise und Empfehlungen zur Umsetzung, nützliche Verweise auf weiterführende Quellen sowie Erläuterungen zu einzelnen Aufgaben.

Die dargestellten Empfehlungen im Vorgehen beziehen sich auf die Rechtslage im Mai 2026. Sie ersetzen weder Einzelfallprüfungen, eine individuelle Rechtsberatung noch vollumfängliche und zertifizierbare Managementsysteme.

Einleitung

Liebe Kolleginnen und Kollegen der Wasserwirtschaft,

Sicherheit und Resilienz, die in der politischen und öffentlichen Diskussion deutlich an Bedeutung gewonnen haben, sind für uns als Unternehmen der Trink- und Abwasserwirtschaft in Deutschland schon seit langem Verpflichtung. Ohne unsere grundlegenden Dienstleistungen der Daseinsvorsorge können das Zusammenleben in unseren Städten und Gemeinden, aber auch die Wirtschaft, nicht funktionieren.

Damit Trinkwasser und Abwasser auch weiterhin 24/7 x 365 Tage im Jahr zuverlässig laufen können, müssen wir über den Rand unserer Versorgungsgebiete hinaus auch globale Veränderungen im Blick behalten und vorausschauend Prävention und unsere Reaktionsfähigkeit in unterschiedlichsten krisenhaften Situationen stärken sowie unsere Prozesse und Strukturen anpassen.

Wie wichtig das ist, erleben wir beim fortschreitenden Klimawandel, der gerade in unserem Sektor mit wachsenden Extremwetterereignissen ganz erhebliche Anstrengungen sowohl im Hinblick auf präventive Anpassungsmaßnahmen als auch im Hinblick auf Bewältigung und Krisenstrategien im Ereignisfall notwendig macht.

Spätestens mit der Corona-Pandemie haben wir zudem lernen müssen, dass auch unsere Lieferketten, beispielsweise bei den für uns so notwendigen Fällmitteln, extrem brüchig waren.

Hinzugekommen sind mit inzwischen weit ausgereifter Digitalisierung unserer technischen, kaufmännischen, personellen oder kommunikativen Prozesse auch Abhängigkeiten von zum Teil marktbeherrschenden Anbietern und deren Produkten. Gleichzeitig vergrößern sich mit wachsender Digitalisierung, darunter auch zunehmende KI-Anwendungen, generell auch die Risiken für Daten- und Informationssicherheit.
Allein schon vor diesem Hintergrund lohnt es sich, Schutzbedürfnisse neu zu überdenken.

Die Steuerung über gut durchdachte Systeme vom Risiko-, über das Krisen-, das Datenschutz- und Informationssicherheitsmanagement bis hin zum auditierten technischen Sicherheitsmanagement, bilden bisher eine sehr gute Basis dafür, unsere Dienstleistungen versorgungssicher und in der gesetzlich geforderten Qualität zu liefern.

Neu ist jedoch eine sich deutlich verändernde Sicherheitslage. Seit einigen Jahren, mit sowohl stetig steigenden Angriffszahlen als auch stetig steigender Professionalität, stellt Cyberkriminalität - ganz gleich, ob monetär oder politisch motiviert - eine wachsende Bedrohung dar. Häufig

stehen dabei Unternehmen der Daseinsvorsorge, darunter auch die Wasserwirtschaft, im Fokus.

Der anhaltende Krieg Russlands gegen die Ukraine, die Spannungen und auch militärischen Auseinandersetzungen im Nahen Osten, die wachsende globale Instabilität, wirtschaftliche wie militärische Abhängigkeiten und eine ganze Reihe bedrohlicher wie leider auch denkbarer Szenarien, die uns ganz unmittelbar betreffen können, markieren eine Zäsur. Hybride Bedrohungsszenarien, die neben konkreten Schäden auch Unruhe und Angst in unserem Land verbreiten sollen, lassen sich nicht wegdiskutieren, sondern erfordern kluges Handeln.

Im Ringen um tragfähige Lösungen für Europa und für unser Land kommen Sicherheit und Resilienz, insbesondere in der Wasserver- und Abwasserentsorgung, eine besondere Bedeutung zu. Dies spiegeln auch die reformierten Rechtsrahmen wider, die mit dem KRITISDachG[1] sowie dem NIS2-Umsetzungsgesetz[2] für viele Unternehmen der Wasserwirtschaft Gültigkeit haben.

Ziel beider sich ergänzender Gesetze ist es, die Sicherheit und Resilienz sowohl für die Netzwerk- und Informationstechnologien in zentralen Prozessen sowie für die physischen Anlagen und Infrastrukturen zu verbessern. Auf Basis eines „All-Gefahren-Ansatzes“ sind bei der physischen Sicherheit Szenarien wie Naturkatastrophen, Spionage, Sabotage, Terroranschläge, aber auch massives menschliches Versagen im Rahmen einer Risikoanalyse in den Blick zu nehmen und hierauf aufbauend, bestmögliche Maßnahmen zu etablieren, konkret einen Resilienzplan aufzustellen. Hiermit sollen Schäden bestmöglich vorgebeugt, abgewehrt oder nach Schadenseintritt möglichst rasch beseitigt werden, um die Versorgungssicherheit wieder herzustellen.

Das KRITISDachG nimmt aktuell die Betreiber kritischer Ver- und Entsorgungsstrukturen ab 500.000 zu versorgenden Personen in den Blick. Das NIS2-UG verpflichtet Betreiber bereits ab einer Unternehmensgröße von mind. 50 Mitarbeitenden oder einem Jahresumsatz und einer Jahresbilanzsumme von jeweils mindestens 10 Mio. Euro. Damit sind viele Unternehmen nach NIS2 verpflichtet, die bisher nicht im Anwendungsbereich der KRITIS-Regulierungen waren.

Gerade weil unseren Dienstleistungen eine besondere Bedeutung zukommt, ist es sinnvoll und geboten, dass nicht nur formal auf eine Gesetzeserfüllung geblickt wird. Unternehmen der Trink- und Abwasserbranche sollten auch ohne unmittelbare gesetzgeberische Betroffenheit

[1] https://www.recht.bund.de/bgbl/1/2026/66/regelungstext.pdf?__blob=publicationFile&v=1
[2] https://www.recht.bund.de/bgbl/1/2025/301/VO.html

Sicherheit und Resilienz unter den aktuellen Entwicklungen hybrider Bedrohungen neu denken oder Bestehendes überdenken. Das gebietet unsere Verantwortung vor Ort!

Aufbauend auf den guten Grundlagen, die wir schon haben, auf Erfahrungswissen und partnerschaftlichen Austausch, soll diese Anwendungshilfe dabei unterstützen, zunächst einen guten Einstieg in die gesetzlichen Erfordernisse zu finden. Ebenfalls nützlich sind auch die Anregungen, Hinweise und Empfehlungen aus der Praxis, die Sicherheit und Resilienz aus konkreter wasserwirtschaftlicher Perspektive verbessern helfen können. Darüber hinaus wird es voraussichtlich in Kürze weitere Rechtsverordnungen bzw. Anpassungen von rechtlichen Rahmen geben, welche dann zu gegebener Zeit in einer überarbeiteten Version dieser Anwendungshilfe über den BDEW zur Verfügung gestellt werden.

Nicht zuletzt geht es auch um den politischen Dialog, den wir auf zentraler Verbandsebene intensiv führen, etwa zu Fragen der Finanzierung oder der Abgrenzung zur staatlich definierten Schutzpflicht, wie sie bereits im Grundgesetz angelegt ist.

Wir müssen handeln und wir werden handeln. Die Anwendungshilfe soll eine gute Unterstützung dabei bieten.

Ihre Gunda Röstel

(Vizepräsidentin Wasser/Abwasser BDEW, Kaufmännische Geschäftsführerin Stadtentwässerung Dresden GmbH/ Prokuristin GELSENWASSER AG)

1 Prüfung Betroffenheit und Anwendungsbereich

Jedes Unternehmen muss selbstständig prüfen, ob es in den Scope des NIS2-Umsetzungsgesetzes (NIS2-UG) und des KRITIS-Dachgesetzes (KRITISDachG) fällt. Das Ergebnis ist zu dokumentieren. Es empfiehlt sich, eine frühzeitige Abstimmung mit den jeweiligen Aufsichtsbehörden, der Verwaltung, Aufsichtsräten, Stakeholdern wie auch möglichen Vertragspartnern bei operativen Aufgabenübertragungen vorzunehmen.

Hinweis:
Nach aktueller Rechtslage definiert das KRITISDachG die Betreiber kritischer Anlagen noch anders als das NIS2-UG. Aktuell gilt nach dem KRITISDachG ein Unternehmen der Wasserwirtschaft dann als KRITIS-Betreiber und damit betroffen, sofern es mind. 500.000 Einwohner wasserbezogen ver- oder entsorgt. Das NIS2-UG, welches das BSI-Gesetz erweitert, bezieht sich auf die Definitionen der KRITIS-Betreiber in der BSI-KRITIS-Verordnung. Hier werden neben bestimmten Anlagenkategorien die Schwellenwerte von 500.000 Einwohnerwerten im Abwasserbereich sowie 22 Mio. m³/Jahr Trinkwasseraufbereitung und -verteilung für die Wasserversorger genannt. Das NIS2-UG weitet diesen Kreis der betroffenen Unternehmen jedoch auf deutlich kleinere Ver- und Entsorger aus.

Konkret sind aktuell Unternehmen mit mehr als 50 Mitarbeitenden oder einem Jahresumsatz und einer Jahresbilanzsumme von jeweils 10 Mio. EUR von NIS2 betroffen. Vom KRITISDachG sind nur solche Unternehmen betroffen, die einen Versorgungsgrad von mind. 500.000 Einwohnern haben.

Die nachfolgenden Ausführungen sollen, orientiert an der aktuellen Rechtslage, die Einordnung erleichtern und grundlegende Fragen beantworten.

KRITISDachG:

Eine erste Einschätzung zum Adressatenkreis ist über die nachfolgende Grafik möglich:

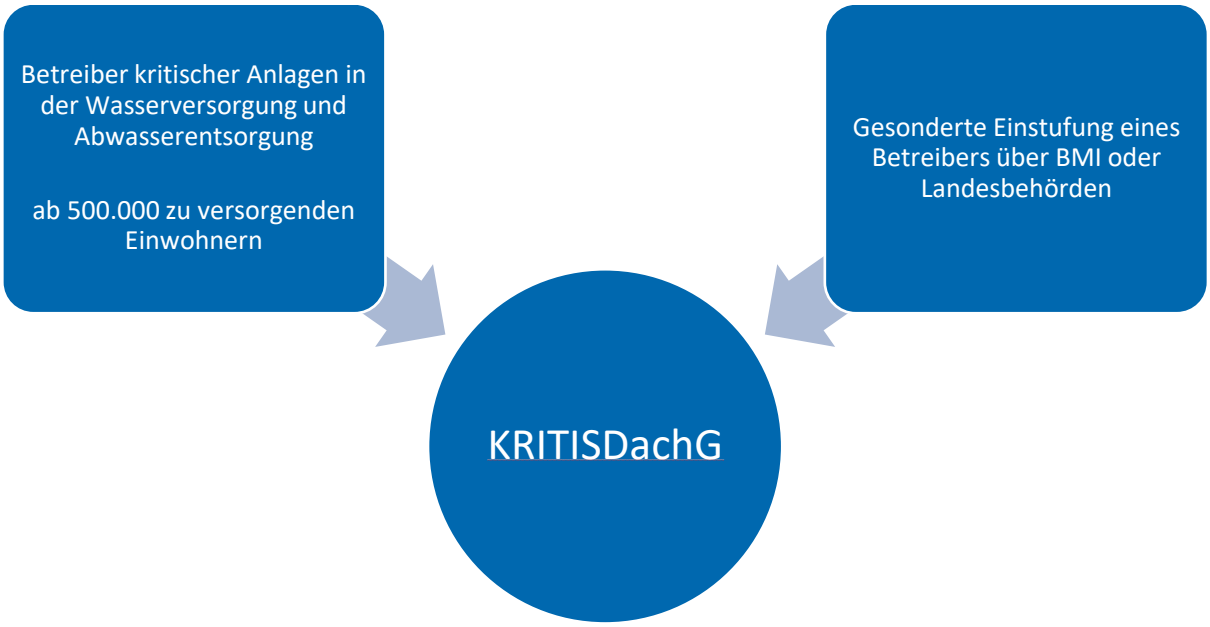


Abbildung 1: Betroffenheit der Sektors Wasser nach dem KRITISDachG

Trink- und Abwasser sind über die Nennung des Sektors „Wasser“ explizit in § 4 Abs. 1 Nr. 6 vom Geltungsbereich des KRITISDachG erfasst. Darüber hinaus liegt der Schwellenwert aktuell bei 500.000 Einwohnern, die wasserbezogen ver- oder entsorgt werden. Dies soll nach § 5 durch eine ergänzende Rechtsverordnung konkretisiert werden, die sektor-, branchen-, und anlagespezifische Schwellenwerte festlegen wird.

Daneben kann nach § 5 Abs. 1 Nr. 4 sowie § 5 Abs. 7 eine gesonderte Einstufung eines Betreibers auch über das Bundesministerium des Innern sowie über die jeweils zuständigen Landesbehörden erfolgen. Dies geschieht in der Regel durch die Innenministerien der Länder, die trotz Unterschreitens der geltenden Schwellenwerte eine Anlage dem Anwendungsbereich des KRITISDachG zuordnen, weil sie von strategischer oder sonstiger wichtiger Bedeutung ist. Gegen diese Entscheidung kann zwar Widerspruch eingelegt werden, allerdings hat der Widerspruch keine aufschiebende Bedeutung und die Landesbehörden haben einen weiten Ermessensspielraum, der rechtlich schwer überprüfbar ist.

NIS2-Umsetzungsgesetz

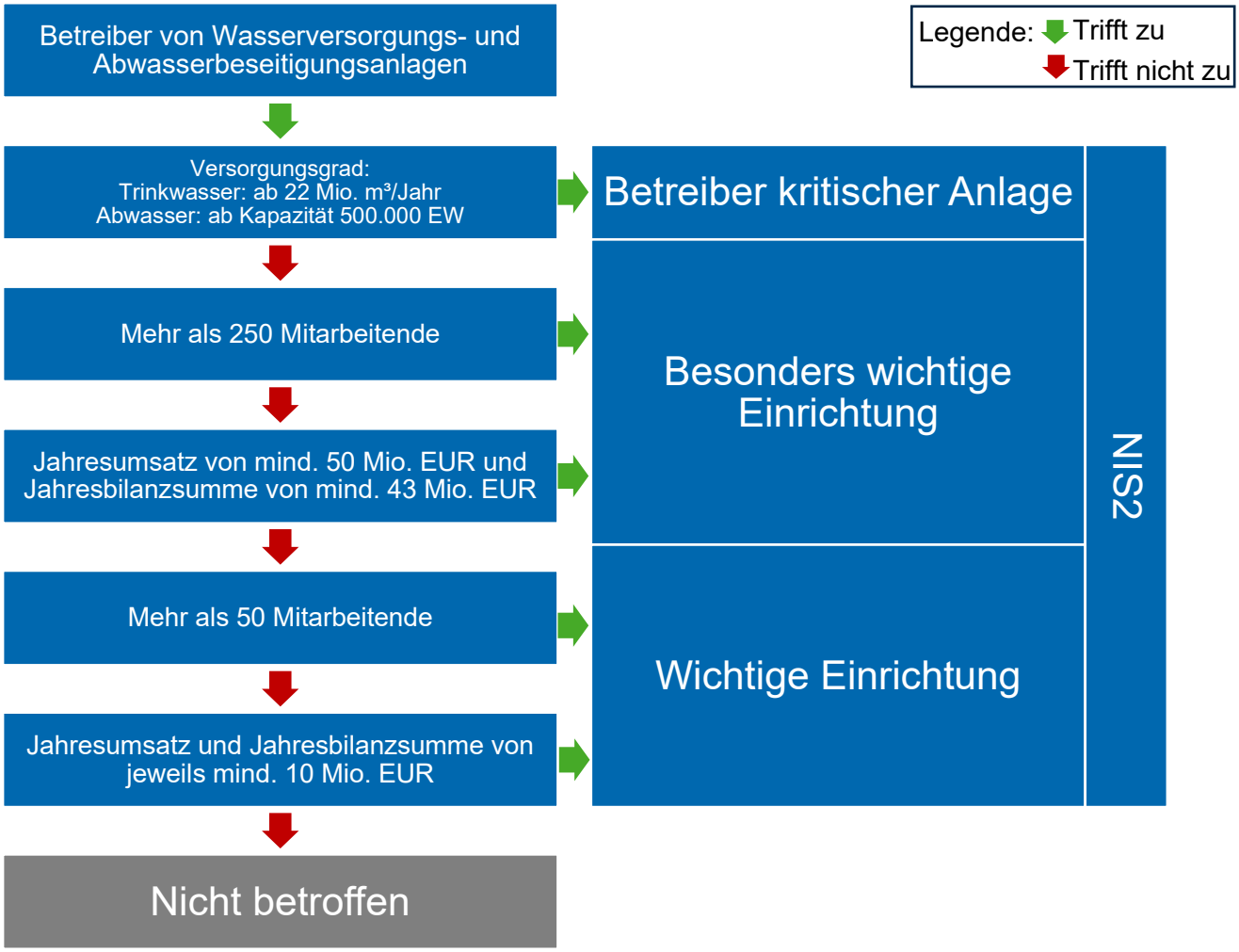


Abbildung 2: Prüfschema NIS2-Betroffenheit im Sektor Wasser

Das NIS2-UG erweitert den Anwendungsbereich des bisherigen BSI-Gesetzes (BSIG) erheblich. Dadurch sind künftig nicht mehr nur die Betreiber der kritischen Anlagen (KRITIS) in der Wasserwirtschaft betroffen, diese bleiben unverändert im Adressatenkreis, sondern auch viele kleinere und mittlere Betreiber von Wasserversorgungsanlagen und Abwasserbeseitigungsanlagen.

Die Schwellenwerte für die Betreiber, die als KRITIS gelten und damit von NIS2 betroffen sind, ergeben sich wie bisher aus der BSI-KRITIS-Verordnung[3], welche am BSI-Gesetz aufgehangen ist. Ob Betreiber, die unterhalb dieser KRITIS-Schwellenwerte liegen, von NIS2 betroffen sind, hängt hingegen von der Unternehmensgröße, also Anzahl der Mitarbeitenden oder einem bestimmten Jahresumsatz und einer bestimmten Jahresbilanzsumme ab.

Betreiber kritischer Anlagen (KRITIS):

Ob ein Unternehmen als Betreiber einer kritischen Anlage gilt, ist wie bisher anhand der BSI-KRITIS-Verordnung zu prüfen. Dabei gelten die betriebene Anlagenkategorie und jeweilige Schwellenwerte in der Ver- bzw. Entsorgung als maßgebliche Kriterien:

Trinkwasserversorgung		
Anlagenkategorie	Bemessungskriterium	Schwellenwert
Gewinnungsanlage	Gewonnene Wassermenge in Millionen m^3/Jahr	22
Aufbereitungsanlage (Wasserwerk)	Aufbereitete Trinkwassermenge in Millionen m^3/Jahr	22
Wasserverteilungssystem	Verteilte Wassermenge in Millionen m^3/Jahr	22
Leitzentrale	Von den gesteuerten/überwachten Anlagen gewonnene, transportierte oder aufbereitete Wassermenge in Millionen m^3/Jahr	22

Abwasserbeseitigung		
Anlagenkategorie	Bemessungskriterium	Schwellenwert
Kanalisation	Angeschlossene Einwohner	500.000
Kläranlage	Ausbaugröße in Einwohnerwerten	500.000

[3] https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html

Leitzentrale	Ausbaugrößen der Anlagen in Einwohnerwerten oder angeschlossene Einwohner der gesteuerten oder überwachten Anlagen	500.000

Hinweis:
Hier kann es in der Festlegung der KRITIS-Betreiber zu einer Diskrepanz zwischen Trink- und Abwasser kommen. Der Schwellenwert im Trinkwasserbereich von 22 Mio. m³/Jahr beruht auf dem Bundesdurchschnitt des täglichen Wasserverbrauchs pro Person/pro Tag von 121 Litern, hochgerechnet auf 500.000 Personen. Da die Trinkwasserverbräuche jedoch regional variieren können, kann es sein, dass ein Trinkwasserversorger in einer Stadt mit 500.000 Einwohnern noch nicht als KRITIS gilt, da die Wasserverbräuche der zu versorgenden Einwohner unter dem Bundesdurchschnitt liegen. Gleichzeitig kann in derselben Stadt der zuständige Abwasserentsorger aufgrund seiner Ausbaukapazität als KRITIS gelten. Der BDEW wirbt dafür, dass diese Diskrepanz durch eine Novelle der BSI-KRITIS-Verordnung aufgelöst wird.

Besonders wichtige und wichtige Einrichtungen:

Liegt ein Betreiber von Wasserversorgungs- oder Abwasserbeseitigungsanlagen unterhalb der Versorgungsgrade, die die BSI-KRITIS-Verordnung definiert, kann man dennoch als besonders wichtige oder wichtige Einrichtung im Sinne des NIS2-UG adressiert sein. Dies ist durch § 28 Abs. 1 Nr. 4 sowie § 28 Abs. 2 Nr. 3 geregelt.

Entscheidend ist hier zunächst, ob die Anlagen, die betrieben werden, in die Kategorien der Anlage 1 des NIS2-UG fallen:

Trinkwasserversorgung	Betreiber von Wasserversorgungsanlagen im Sinne von § 2 Nummer 3 TrinkwV, jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist
Abwasserbeseitigung	Unternehmen, die Abwasser nach § 54 Absatz 1 WHG sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung oder die Behandlung solchen

	Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist

Werden demnach Wasserversorgungs- oder Abwasserbeseitigungsanlagen betrieben, gilt die Unternehmensgröße als entscheidendes Kriterium zur Festlegung der Betroffenheit.

Als **besonders wichtige Einrichtung** nach dem NIS2-UG gelten Betreiber, wenn sie:

- mehr als 250 Mitarbeitende beschäftigen **oder**
- einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen

Ist das Unternehmen kleiner und liegt unterhalb der Schwellenwerte der besonders wichtigen Einrichtungen, kann es dennoch in die Kategorie der **wichtigen Einrichtungen** fallen und wäre dann ebenfalls von NIS2 betroffen. Als wichtige Einrichtung nach dem NIS2-UG gelten Betreiber, wenn sie:

- mehr als 50 Mitarbeitende beschäftigen **oder**
- einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen

Im NIS2-UG sind die Unternehmen der Kategorien besonders wichtige und wichtige Einrichtungen im § 28 Abs. 1 Nr. 4 sowie § 28 Abs. 2 Nr. 3 nicht explizit als kleinere Betreiber benannt. Vielmehr findet sich dort die Formulierung:

> *„sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind“*

Bei der Ausdeutung ist der Verweis auf die Einrichtungsarten in der Anlage 1 entscheidend. Hieraus geht hervor, dass es sich bei den Organisationseinheiten, die Waren und Dienstleistungen anbieten, um Ver- und Entsorger der Wasserwirtschaft im Sinne der TrinkwV bzw. des WHG handelt.

Wenn der Betrieb solcher Anlagen der Trink- und Abwasserwirtschaft nur einen geringen Teil einer ansonsten anderweitigen Geschäftstätigkeit eines Unternehmens ausmacht, ist es möglich, für diesen Anteil nicht nach NIS2 reguliert zu sein. Dies ist gemäß § 28 Abs. 3 festgelegt. Damit wird im Einzelfall vermieden, dass eine nur geringfügige Nebentätigkeit zu einer

unverhältnismäßigen Identifizierung als wichtige oder besonders wichtige Einrichtung führt. Auch wenn die Abgrenzung hierzu nicht einfach abzuleiten ist, können mögliche Anhaltspunkte für diese Bewertung etwa die Anzahl der in diesem Bereich tätigen Mitarbeitenden oder der durch diese Geschäftstätigkeit erwirtschaftete Umsatz bzw. die Bilanzsumme für diesen Bereich sein. Ein Indiz, dass es sich nicht um eine vernachlässigbare Geschäftstätigkeit handelt, kann auch eine Nennung des Unternehmens in einem Gesellschaftervertrag, einer Satzung oder einem vergleichbaren Gründungsdokument der Einrichtung sein[4].

Eine weitere Orientierungshilfe zur NIS2-Betroffenheitsprüfung bietet zudem das BSI mit einem Online-Prüfungstool[5] an. Obgleich hiermit in wenigen Schritten anhand konkreter Fragen überprüft werden kann, ob ein Unternehmen in den Anwendungsbereich des Gesetzes fällt, ist weder das Ergebnis rechtlich bindend noch besteht ein Anspruch auf Vollständigkeit und Richtigkeit der Inhalte.

Empfehlungen für Unternehmen der Wasserwirtschaft in unterschiedlichen Kooperationsformen

Wer selbst als Betreiber wasserwirtschaftlicher Anlagen in den Anwendungsbereich des KRITISDachG und NIS2-UG fällt und als Kooperationspartner für andere Aufgabenträger der Wasserwirtschaft Verantwortung übernommen hat, sollte in Abstimmung mit den jeweiligen Kooperationspartnern die Frage einer weitergehenden Betroffenheit sorgfältig prüfen. Aus beiden Gesetzlichkeiten lassen sich keine klaren Ableitungen für im Wassersektor spezifische Formen der Zusammenarbeit ableiten. Wir empfehlen daher zunächst prinzipiell eine individuelle vertragsrechtliche Prüfung. Nachfolgend finden sich spezifische Hinweise zu einzelnen Kooperationsformen:

- Konzessionen und Betriebsführungen:
  Wenn ein Unternehmen operative Aufgaben über Konzessionen oder Betriebsführungsverträge an Dritte überträgt, sind die jeweilige Betroffenheit und die Verantwortlichkeiten für Sicherheits- und Meldepflichten klar zu regeln. Dies ist auch für jene Fälle zu empfehlen, in denen ein Unternehmen durch die Summe seiner Dienstleistungstätigkeit für andere Unternehmen in den Anwendungsbereich beider Gesetzlichkeiten kommen könnte. Verträge sollten daher überprüft und gegebenenfalls angepasst werden. Üblicherweise enthalten Verträge salvatorische Klauseln, die eine

[4] Vgl. Begr. RegE zu Art. 1 (Änderung des BSIG) zu § 28 (Besonders wichtige Einrichtungen und wichtige Einrichtungen), zu Abs. 3, BT-Drs. 21/1501, S. 144.

[5] https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung.html

Vertragsanpassung an geänderte gesetzliche Rahmenbedingungen ermöglichen. Dies schließt auch den Umgang mit möglichen Finanzierungsthemen für notwendig werdende Maßnahmen mit ein.

- Beteiligungen und Querverbundunternehmen:
  Bei Beteiligungen und Querverbundunternehmen hängt die Frage der Betroffenheit davon ab, inwieweit das beteiligte Unternehmen bzw. durch die Konstruktion des Querverbundes Einfluss auf kritische Anlagen der Wasserwirtschaft ausgeübt wird, vor allem aber, wie oben schon beschrieben, welcher Anteil der Gesamtgeschäftstätigkeit dem Betrieb wasserwirtschaftlicher Anlagen zuzurechnen wäre.

- Interkommunale Zusammenarbeit:
  Bei Zweckverbänden oder öffentlich-rechtlichen Kooperationen empfiehlt es sich ebenfalls bei möglicher Betroffenheit durch beide Gesetzlichkeiten, die zugrunde liegenden Verträge oder Satzungen zu überprüfen und gegebenenfalls anzupassen. Ziel ist es auch hier, die regulatorischen Pflichten, Zuständigkeiten und Meldewege eindeutig festzulegen. Anpassungen der Verbandsbeiträge können notwendig werden, wenn zusätzliche Ressourcen für die Umsetzung der regulatorischen Anforderungen erforderlich sind.

Hinweis: In beiden gesetzlichen Regelungen, spielen die verschiedenen Kooperationsformen, die im Wassersektor etabliert sind, keine gesonderte Rolle, weshalb es auch keine entsprechenden Festlegungen gibt. Der aktuell reformierte Gesetzesstand mit dem KRITISDachG und dem NIS2-UG ist jedoch Ausdruck erhöhter Sicherheitsrisiken und -bedürfnisse für die Branche: Versorgungsinfrastruktur muss zuverlässig geschützt werden, und dafür muss klar eine verantwortliche Stelle bestimmt sein. Die empfohlenen vertraglichen Regelungen dienen genau dazu, mögliche Verantwortlichkeiten praktisch zuzuordnen und das Sicherheitsniveau zu gewährleisten.

2 Pflichten der Geschäftsführung

Bei Betroffenheit durch das KRITISDachG und dem NIS2-UG ist es essenziell, dass die Geschäftsführung die formale Gesamtverantwortung für die Umsetzung im Unternehmen übernimmt und notwendige Prozesse initiiert. Sie haftet persönlich für die Einhaltung der Vorgaben. Zudem müssen Verantwortliche im Unternehmen benannt werden, auch gegenüber den zuständigen Behörden, die die Umsetzung operativ steuern und als Ansprechpartner der Behörden fungieren.

Sowohl in Bezug auf das KRITISDachG wie auch beim NIS2-UG obliegt die Gesamtverantwortung für das Einhalten aller Pflichten der Geschäftsführung. Sie haftet persönlich für die physische, die Informations- und Cybersicherheit sowie generell für die Resilienz des jeweiligen Unternehmens. Sie muss entsprechend für angemessene präventive wie reaktive Schutz- und Steuerungssysteme sorgen, welche Schadensereignisse bestmöglich verhindern oder minimieren, im Schadensfall ein rasches Wiederherstellen des operativen Betriebes ermöglichen sowie den Erfordernissen in der gesetzgeberisch gebotenen Meldepflicht nachkommen.

Um die technischen und organisatorischen Prozesse zur Sicherheit der Informationstechnik mit ausreichend fundierten Kenntnissen anleiten und überwachen zu können, wurde im NIS2-UG festgeschrieben, dass die Geschäftsführung entsprechende Schulungen nachweisen muss. Ein vorläufiger Leitfaden[6] zu den Schulungspflichten der Geschäftsführung wurde bereits vom BSI veröffentlicht. Die Schulungen müssen bei Betroffenheit durch das NIS2-UG gegenüber dem BSI nachgewiesen werden können, umfassen mindestens 4 Stunden und mindestens alle 3 Jahre zu wiederholen. VBEW[7] sowie EW-Medien[8] bieten regelmäßig entsprechende Schulungsformate an.

Ein weiterer wichtiger Punkt, der durch die Geschäftsführung initiiert und umgesetzt werden muss, ist die Benennung mindestens einer Person im Unternehmen, die die Umsetzung der Pflichten operativ steuert und gegenüber den Behörden als zentraler Ansprechpartner fungiert. Diese Person sollte i.d.R. dann auch die Funktion der verpflichtenden Schadensmeldung bei den zuständigen Meldestellen übernehmen und eine entsprechende 24/7-Erreichbarkeit sicherstellen. Es empfiehlt sich hierfür, eine Stellvertretung zu benennen.

---

6 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-geschaeftsleitungsschulung.pdf?__blob=publicationFile&v=

7 https://www.vbew-gmbh.de/seminare/alle-seminare/

8 https://www.essociation.de/

3 Registrierung des Unternehmens / Meldung im Schadensfall

Bei Betroffenheit durch das NIS2-UG muss sich das Unternehmen gemäß § 33 Abs. 1 bis zum 05. März 2026 beim BSI-Portal registriert haben. Bei Betroffenheit durch das KRITISDachG muss sich das Unternehmen gemäß § 8 Abs. 1 drei Monate nach Feststellung einer kritischen Anlage beim BSI-Portal registriert haben. In beiden Fällen ist ein ELSTER-Organisationszertifikat für die Registrierung notwendig. Treten Schadensereignisse ein, müssen diese unter Beachtung zeitlicher Fristen in den entsprechenden Portalen gemeldet werden. Eine Schadensereignismeldung ist auch ohne vorhergehende Registrierung möglich.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) haben für den Registrierungsprozess eine gemeinsame Stelle geschaffen, welche formal beim BSI angesiedelt ist. In diesem Portal[9] müssen sich die Unternehmen in einem zweistufigen Prozess registrieren. Zunächst erfolgt die Erstellung eines Unternehmenskontos („Mein Unternehmenskonto“) im BSI-Portal. Im nächsten Schritt erfolgt dann die eigentliche Registrierung des Unternehmens. Hierfür muss zuvor ein ELSTER-Unternehmenskonto[10] eingerichtet werden, sofern noch keines vorliegt.

Tritt ein Schaden ein, muss das Unternehmen schnellstmöglich diesen Schaden bei der zuständigen Stelle melden. In Bezug auf Vorfälle im Zusammenhang mit Informationstechnik ist eine entsprechende Meldung beim BSI[11] zu machen. Sollte zu diesem Zeitpunkt noch keine vorhergehende Unternehmensregistrierung erfolgt sein, kann auch ohne Registrierung eine Schadensmeldung gemacht werden. Wichtig ist, dass die Meldung binnen 24 Stunden nach Erkennen des Schadensereignis erfolgt.

In Bezug auf jegliche anderen betriebsgefährdenden Ereignisse, muss eine Meldung bei einer vom BSI und BBK gemeinsam eingerichteten Meldestelle erfolgen. Auch hier ist innerhalb von 24 Stunden nach Kenntnis des Vorfalls eine Meldung zu machen. Nach den Vorgaben in § 18 Abs. 2 KRITISDachG müssen folgende Informationen angegeben werden:

- Art, Ursache und mögliche Folgen
- Anzahl der vom Vorfall Betroffenen
- Das betroffene geografische Gebiet – Achtung: Wegen Abstimmung mit Bundeswehr neben Straßennamen und Nr. auch GIS-Daten übermitteln
- Weitere Einzelheiten durch BBK

[9] https://portal.bsi.bund.de/
[10] https://info.mein-unternehmenskonto.de/
[11] https://mip2.bsi.bund.de/de/

4 Übersicht zentraler Pflichten für Anwender

Die nachfolgende Übersicht stellt die wesentlichen Pflichten aus beiden Gesetzesakten für die Anwender zur Verfügung. Eine ausführliche Erläuterung erfolgt in den Anlagen 3 und 4.

Pflicht	KRITISDachG[12]	NIS2-UG[13]
	Betreiber kritischer Anlagen	**Betreiber kritische Anlagen / Besonders wichtige Einrichtungen & wichtige Einrichtungen im Wassersektor**
Betroffenheitsprüfung	§ 4 Abs. 1 Nr. 6 & § 5 Abs. 1 Ab 500.000 zu versorgenden Einwohnern oder durch behördliche Festlegung <u>Hinweis:</u> Spezifischere Festlegungen sind über eine gesonderte Rechtsverordnung zu erwarten	§ 28 Betreiber einer für die Versorgung kritischen Anlage = besonders wichtige Einrichtung: • Trinkwasserversorger ab 22 Mio. m³/Jahr • Abwasserentsorger ab 500.000 EW/Personen Betreiber einer Wasserversorgungs- oder Abwasserbeseitigungsanlage (nach Anlage 1 NIS2-UG): Besonders wichtige Einrichtung: • Ab 250 Mitarbeitende oder Jahresumsatz von mind. 50 Mio. EUR und

[12] https://www.gesetze-im-internet.de/kritisdachg/BJNR0420B0026.html
[13] https://www.recht.bund.de/bgbl/1/2025/301/VO.html

		Jahresbilanzsumme von mind. 43 Mio. EUR Wichtige Einrichtung: • Ab 50 Mitarbeitende oder Jahresumsatz und Jahresbilanzsumme von jeweils über 10 Mio. EUR Tool zur Betroffenheitsprüfung[14] beim BSI nutzbar
Registrierungspflicht	§ 8 Abs. 1 Registrierung beim BSI-Portal[15]: innerhalb 3 Monate nach Feststellung als KRITIS-Betreiber	§ 33 Registrierung beim BSI-Portal: innerhalb 3 Monate nach Inkrafttreten = Bis zum 05. März 2026
Meldepflicht im Schadensfall	§ 18 Abs. 1 Meldung erfolgt beim BSI[16]: Innerhalb von 24 h Erstmeldung, Aktualisierungsmeldung mit Schadensbewertung, innerhalb von einem Monat Abschlussmeldung	§ 32 Meldung erfolgt beim BSI: Innerhalb von 24 h Erstmeldung, innerhalb von 72 h Aktualisierungsmeldung mit Schadensbewertung, innerhalb von einem Monat Abschlussmeldung
Absicherung der betriebskritischen Systeme und	§ 13 Abs. 2 Nr. b – c	§ 31 Abs. 2

14 https://betroffenheitspruefung-nis-2.bsi.de/
15 https://portal.bsi.bund.de/
16 https://mip2.bsi.bund.de/de/

Anlagen / Angriffserkennung	Absicherung und Angriffserkennung insb. Liegenschaftsabsicherung, bspw. durch Überwachungs- und Detektionssysteme	Systeme zur Angriffserkennung nach dem Stand der Technik[17] - Empfehlung: Anwendung B3S Wasser/Abwasser[18]
Benennung 24/7-Kontaktstelle ggü. BBK / BSI	§ 8 Abs. 1 Nr. 6 Kontaktstelle setzt dies voraus	§ 33 Abs. 2 Angabe von Kontaktdaten setzt dies voraus
Risikomanagement/ Risikoanalyse/ Risikobewertung	§ 12 Risikoanalyse und Risikobewertung mind. alle 4 Jahre, methodische Vorgaben können durch das BMI durch Rechtsverordnung erlassen werden Empfehlung: Anwendung eines BCMS Hinweis: Eine ausführliche Beschreibung zur Beantwortung dieser Anforderungen angelehnt an das BCMS findet sich in Kapitel 5	§§ 30 f. Risikomanagement für Sicherheit in der Informationstechnik Empfehlung: Anwendung eines ISMS und Risikomanagementsystems (RMS) Hinweis: Aspekte des ISMS sind in Kapitel 5 integriert
Resilienzpflichten/ Resilienzplan	§ 13	§§ 30 f.

[17] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=8
[18] https://www.dvgw.de/medien/dvgw/leistungen/publikationen/b3swa-edition-2023-2402.pdf

	Gewährleistung der Resilienz – Verhinderung von Vorfällen, angemessener physischer Schutz nach dem Stand der Technik, Vorfälle wirksam begrenzen und zügige Wiederherstellung Empfehlung: Anwendung eines BCMS Hinweis: Eine ausführliche Beschreibung zur Beantwortung dieser Anforderungen findet sich in Kapitel 5.	Siehe oben
Unterrichtungspflicht ggü. Kunden/Öffentlichkeit bei Vorfällen	§ 18 Abs. 8 BBK entscheidet über Information der Öffentlichkeit, Vollzug entweder durch das BBK oder den Betreiber auf Anweisung des BBK	§§ 35 f. BSI entscheidet über Information an Empfänger der Dienstleistung (Kunden) oder der Öffentlichkeit
Haftung und Schulung der Geschäftsleitung	§ 20 Persönliche Haftung der Geschäftsleitung für Umsetzung von Resilienzmaßnahmen	§ 38 Persönliche Haftung der Geschäftsleitung für Umsetzung Risikomanagement Verpflichtende regelmäßige Schulung zu Risikomanagementpraktiken im Bereich Sicherheit in der Informationstechnik
Nachweispflicht/ Dokumentation	§ 16	§ 39

ggü. Zuständiger Behörde	BBK kann über BSI Nachweise einholen oder Betreiber direkt zur Vorlage entsprechender Nachweise insb. eines Resilienzplanes auffordern <u>Empfehlung:</u> Die Anwendung eines BCMS kann als fundierte Grundlage für die Nachweise dienen <u>Hinweis:</u> Eine nachgeordnete Rechtsverordnung zu ergänzenden methodischen Vorgaben zum Aufbau eines Resilienzplanes bleibt abzuwarten	Nachweise über Risikomanagementmaßnahmen müssen gegenüber BSI mind. alle 3 Jahre nachgewiesen werden <u>Empfehlung:</u> Die Anwendung eines ISMS und des Branchenstandards B3S kann als fundierte Grundlage für die Nachweise dienen

5 Aufbau eines Resilienzplanes

Nach dem KRITIS-Dachgesetz und dem NIS2-UG sind die betroffenen Unternehmen verpflichtet, auf Grundlage einer individuellen Risikobewertung entsprechende Maßnahmen zur Verbesserung ihrer Sicherheit und Resilienz umzusetzen (siehe auch Übersichtstabelle oben).

Im KRITISDachG finden sich diese Anforderung in § 12 „Risikoanalyse und Risikobewertung“ sowie in § 13 „Resilienzplan“. Im NIS2-UG findet sich dies im § 30 „Risikomanagementmaßnahmen“ wieder. In beiden Fällen geht es darum, auf Basis einer individuellen Risikobewertung Schwachstellen im Unternehmen im Hinblick auf die physische wie Informations- und Cybersicherheit zu ermitteln und diese mit entsprechenden Maßnahmen und Plänen auszustatten.

Auf Unternehmensebene kann dies durch die Entwicklung eines ganzheitlichen Resilienzplanes[19] beantwortet werden. Einen Überblick hierzu vermittelt folgende Grafik:

[19] Im KRITISDachG ist unter § 13 Abs. 5 angekündigt, dass über das BBK noch entsprechende Vorlagen und Muster für die Erstellung von Resilienzplänen veröffentlicht werden. Zum Zeitpunkt der Veröffentlichung dieser Anwendungshilfe liegen diese jedoch noch nicht vor, daher kann diese Systematik im Nachhinein Abweichungen aufweisen.

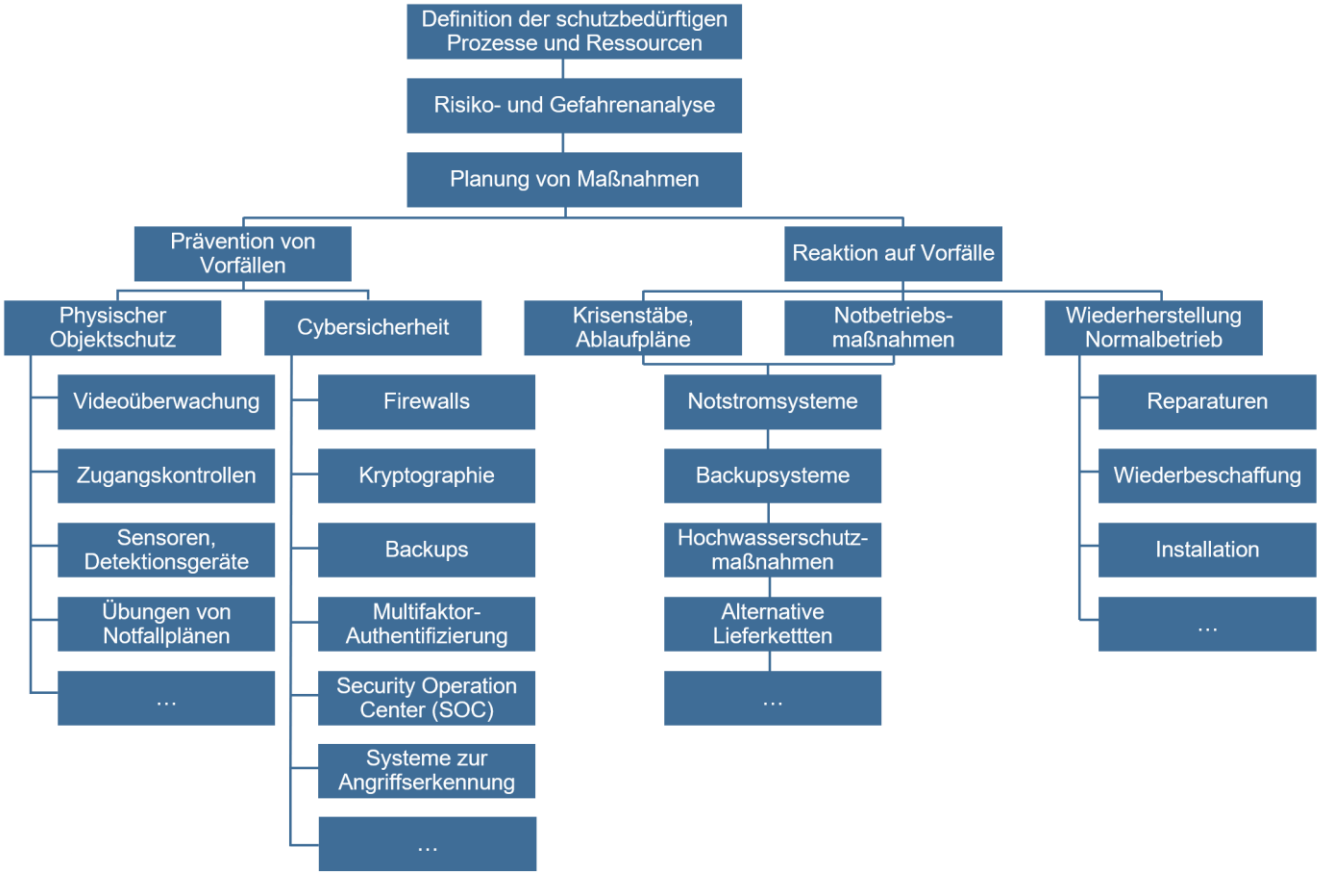


Abbildung 3: Mögliches Schema eines Resilienzplanes

Die in diesem Kapitel beschriebenen Schritte zur Entwicklung eines Resilienzplanes bauen auf bestehenden Managementsystemen auf, darunter vor allem auf dem Business Continuity Managementsystem (BCMS). Ein BCMS eignet sich, um systematisch zu ermitteln, was im Unternehmen geschützt werden muss, welche Risiken relevant sind (Risikoanalyse), wo vorsorgende Schutzmaßnahmen ansetzen sollten, was im Falle einer signifikanten Betriebsstörung oder -unterbrechung zu tun ist und wie ein schneller Wiederhochlauf des Betriebs gewährleistet werden kann. Bereits im Unternehmen vorhandene Risikomanagementsysteme und Krisenmanagementpläne können hier integriert werden. Mit diesem Managementsystem lassen sich demnach die wesentlichen Anforderungen des KRITISDachG unter § 12 beantworten.

In Bezug auf die Anforderungen des NIS2-UG lassen sich einige der in § 30 formulierten Anforderungen wie die Risikoanalyse, die Bewältigung von Sicherheitsvorfällen oder das Aufrechterhalten des Betriebs ebenfalls mit dem BCMS beantworten, sofern hier Risiken der Informationssicherheit mitbetrachtet werden.

Die nachfolgenden Unterkapitel geben einen Überblick und Orientierung über die Anforderungen eines BCMS, welche um Aspekte der Informationssicherheit ergänzt wurden. Die Ausführungen ersetzen jedoch keine vollumfänglichen und zertifizierbaren Managementsysteme, sondern erleichtern lediglich das Verständnis für deren Aufbau. Insbesondere beim NIS2-UG sollte darüber hinaus auch ein Informationssicherheitsmanagementsystem (ISMS) bzw. auch branchenspezifische Sicherheitsanforderungen in Bezug auf die Informationssicherheit im Unternehmen umgesetzt werden.

Relevante Managementsysteme zur Beantwortung der Anforderungen aus dem KRITISDachG und NIS2-UG aus aktueller Sicht:

- Business Continuity Managementsystem (BCMS)
  - BSI-Standard 200-4[20] oder ISO/IEC 22313[21]
- Risikomanagementsystem (RMS)
  - BSI-Standard 200-3[22] oder ISO/IEC 27005[23]
- Informationssicherheitsmanagementsystem (ISMS)
  - BSI-Standard 200-1[24] und 200-2[25] oder ISO/IEC 27001[26]
- B3S Wasser/Abwasser[27]
  - Von DVGW und DWA erarbeitet, auf Abfrage erhältlich
- Technisches Sicherheitsmanagement (TSM)

Ergänzend können auch weitere Grundlagen konsultiert werden wie die Leitlinien zum Krisenmanagement der DIN[28] oder die kürzlich veröffentlichte DIN SPEC 14027 zur Corporate Security[29].

5.1 Identifikation wesentlicher Prozesse

[20] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8
[21] https://www.iso.org/standard/75107.html
[22] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2
[23] https://www.iso.org/standard/80585.html
[24] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2
[25] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2
[26] https://www.iso.org/standard/27001
[27] https://www.bsi.bund.de/SharedDocs/Textbausteine/DE/KRITIS/B3S/Wasser/b3s-wasser-abwasser.html
[28] https://www.din.de/resource/blob/851282/e2530905512b05975549b3547151a698/inhalte-von-e-din-en-iso-22361-2021-12-data.pdf
[29] https://www.dinmedia.de/de/technische-regel/din-spec-14027/400565136

Zunächst sollten die betriebskritischen Prozesse im Unternehmen identifiziert werden, die bei einer Beeinträchtigung oder Unterbrechung ein hohes Schadenspotenzial ausbilden können. Hierbei ist es wichtig, die richtige Granularität zu finden und nicht jeden Einzel- oder Unterstützungsprozess als betriebskritisch zu definieren.

Hinweis:
Hier geht es noch nicht um mögliche Ursachen für Ausfälle, sondern nur darum festzulegen, welche Prozesse besonders schützenswert sind und nicht unterbrochen werden sollten.

Um die Schutzziele im Unternehmen festzulegen, sollte zunächst damit begonnen werden, die Hauptprozesse zu identifizieren, die möglichst störungsfrei funktionieren sollten. Hierbei empfiehlt es sich, nicht jeden Unterstützungs- und Unterprozess als eigenständiges Schutzziel mitaufzunehmen, sondern für die Haupttätigkeiten eine angemessene Granularität der Prozesse zu finden.

Beispiele für die Prozessdefinition:

Wasserversorgung	**Abwasserentsorgung**
Rohwasserförderung	Abwassersammlung
Rohwasseraufbereitung	Abwasseraufbereitung
Trinkwasserverteilung	Abwassereinleitung
Personalmanagement	Klärschlammmanagement
Energieversorgung	Personalmanagement
IT-Management	Energieversorgung
	IT-Management

Für die unternehmensindividuell festgelegten betriebskritischen Prozesse sollte je Prozess ein Prozesseigner festgelegt werden, welcher die Prozesse verantwortlich steuert und über alle notwendigen Ressourcen und Abhängigkeiten Auskunft geben kann. In der Praxis ist dies oft eine entsprechende Führungskraft. Bedient ein Betreiber beide Versorgungssparten, so sind die Prozesse immer ganzheitlich d. h. in KRITIS-Verbünden und damit auch in ihren Abhängigkeiten zueinander zu betrachten.

5.2 Ermittlung zeitkritischer Prozesse und Schadenskategorien

Für die zuvor festgelegten wesentlichen Prozesse muss ermittelt werden, ab welchem Zeitraum der Ausfall der jeweiligen Prozesse signifikante oder sogar untragbare Schäden hervorruft. Hierbei muss das Schadensausmaß in Bezug auf verschiedene Schadenskategorien betrachtet und bewertet werden. Mögliche Prozess- und Ressourcenabhängigkeiten werden ebenfalls ermittelt. Bereits vorhandene Schutzmaßnahmen spielen hier noch keine Rolle, die Betrachtung bezieht sich immer auf den „worst case“, also einen kompletten Prozessausfall.

Hinweis:
Dieser wichtige Schritt entspricht der sog. Business Impact Analysis (BIA), die Teil des Business Continuity Managements (BCM) ist.

Die Zeitkritikalität eines Prozesses sagt aus, wie lange ein Prozess ausfallen kann, bis ein untragbarer Schaden entsteht. Dies ist später wichtig, da für diesen Zeitraum entsprechende Notbetriebsmaßnahmen festgelegt werden sollen, die verhindern, dass ein Prozessausfall eskaliert. Innerhalb dieses Zeitraumes sollten auch die Maßnahmen zum Wiederanlauf des Normalbetriebes umgesetzt werden können.

Bei der Ermittlung der Zeitkritikalität geht es im Wesentlichen darum, die folgenden Fragen zu beantworten:

- Wann wird ein Ausfall eines Prozesses untragbar?
- Welche Art von Schäden können bei einem Ausfall entstehen?

Vorab festzulegen:

Bevor die Zeitkritikalität der einzelnen Prozesse bewertet werden kann, müssen vorab verschiedene Betrachtungsparameter festgelegt werden, die für jede Prozessbetrachtung gleichbleibend sind.

Zunächst gilt es, verschiedene Schadenskategorien festzulegen, auf die ein Prozessausfall hin betrachtet werden kann. Neben finanziellen Schäden können auch andere Aspekte eine Rolle spielen, die sich nur schlecht finanziell beziffern lassen, beispielsweise eine Gefahr für Leib und Leben oder ein Reputationsschaden.

Beispiele für wesentliche Schadenskategorien:

- Massive Beeinträchtigung der Aufgabenerfüllung / Versorgungssicherheit
- Erhebliche finanzielle Auswirkungen
- Rechtliche Verstöße mit erheblichem Strafmaß (gegen Gesetze, Vorschriften, Verträge)
- Persönliche Unversehrtheit (Personal, Kunden)
- Dauerhafte Reputationsschäden

Als nächstes sollten Schadensklassen definiert werden, die aussagen, wie hoch ein Schaden innerhalb einer Schadenskategorie wäre.

Beispiel für die Definition von Schadensklassen:

- Sehr gering
- Gering
- Mittel
- Hoch

Ebenfalls sollten vorab Betrachtungszeiträume für mögliche Prozessausfälle definiert werden, also Zeitintervalle, die den Verlauf eines Prozessausfalls darstellen können.

Beispieldefinition eines Betrachtungszeitraumes für mögliche Prozessausfälle:

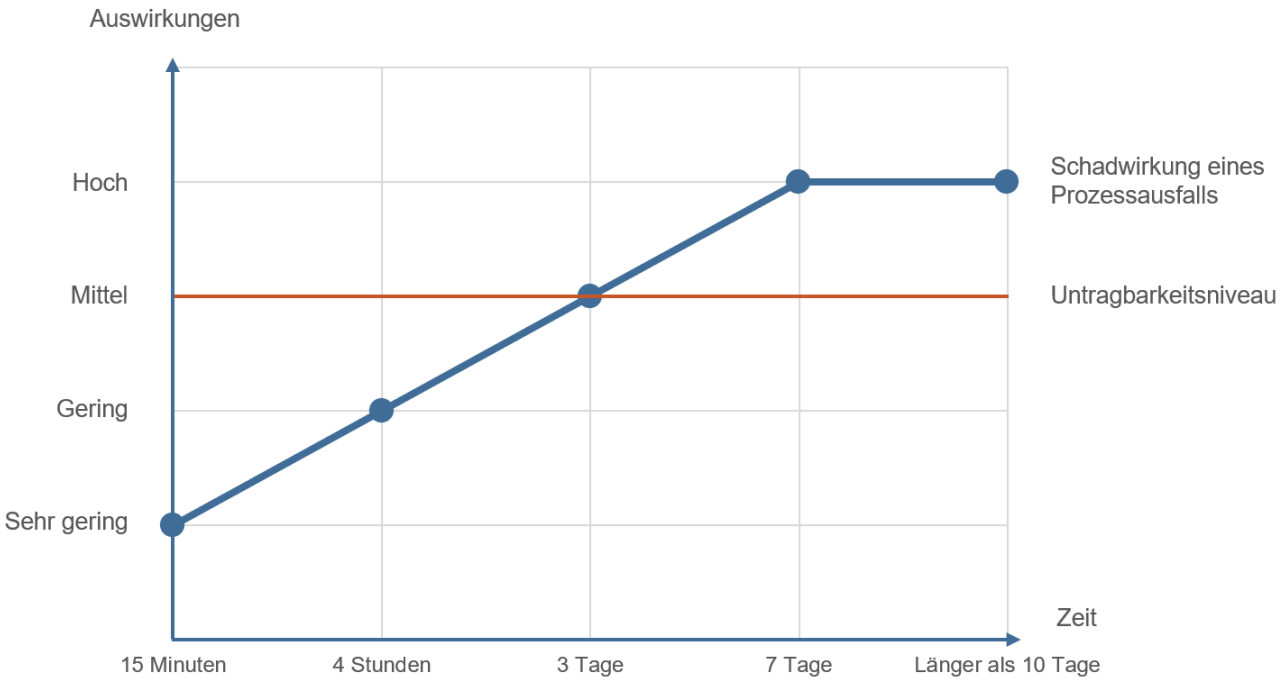
- 15 Minuten
- 4 Stunden
- 3 Tage
- 7 Tage
- 14 Tage
- 30 Tage (ermöglicht Periodenwechsel wie z. B. Lohnfortzahlungen, Monatsabschlüsse etc. in den Blick zu nehmen)

Hinweis: Da die Wasserwirtschaft zur Daseinsvorsorge und kritischen Infrastruktur zählt, sollten die zeitlichen Betrachtungspunkte nicht erst nach Tagen beginnen.

Bewertungsprozess:

Nachdem die Parameter entsprechend definiert wurden, startet der Bewertungsprozess der einzelnen betriebskritischen Prozesse. Dies sollte in Form von Einzelinterviews oder gemeinsamen Workshops mit den jeweiligen Prozesseignern stattfinden. Je Prozess sollte je Schadenskategorie die Zeitkritikalität eingeschätzt werden. Maßgeblich geht es dabei um die Beantwortung zweier Fragen:

1. Welche Auswirkung (Schadensklasse) in Bezug auf Schadenskategorie X ergibt sich durch einen Ausfall des Prozesses Y ab einer bestimmten Zeit? Ab welchem Zeitpunkt wird ein Ausfall untragbar?



Darüber hinaus sollte eingeschätzt werden, welche Einflüsse der betrachtete Prozess zu anderen Prozessen hat und welche Ressourcen für die Funktionalität des betrachteten Prozesses unabdingbar sind, also:

2. Welche grundsätzlichen Einflüsse auf oder Abhängigkeiten von anderen Prozessen bestehen und welche Ressourcen sind für den Wiederanlauf des Prozesses kritisch?

Hierbei ist es wichtig, sowohl die vorgelagerten als auch die nachgelagerten Prozesse einzubeziehen, um einen genauen Abhängigkeitsplan aller betriebskritischen Prozesse aufzustellen. Externe Lieferketten werden dabei als Ressourcen betrachtet.

Beispiel für eine mögliche Ressourcenliste:

- IT/OT (Technik, Systeme, Steuerung etc.)
- Informationen/Daten (z. B. in Prozessleitsystemen zu Mengen, Frachten, Parametern etc.)
- Infrastruktur (z. B. Gebäude, Becken, Leitungen etc.)
- Personal
- Energie
- Betriebsmittel
- Dienstleister
- Finanzmittel

Tabelle 1 Beispiel Bewertung Prozess- und Ressourcenabhängigkeiten

Betrachteter Prozess	**Vorgelagerte Prozesse**	**Nachgelagerte Prozesse**	**Notwendige Ressourcen (für den betrachteten Prozess)**
Beispiel Trinkwasserprozess: **Trinkwasseraufbereitung**	Rohwassergewinnung	Trinkwassertransport und Verteilung	OT: Anlagen, Pumpen etc. Infrastruktur IT Informationen/Daten Betriebsmittel Energie Personal
Beispiel Abwasserprozess: **Abwasseraufbereitung**	Abwassersammlung	Abwassereinleitung	OT: Anlagen, Pumpen etc. Infrastruktur IT

		Schlammbehandlung	Informationen/Daten Betriebsmittel Energie Personal

Ergebnis:

- Zeitkritikalität:
  Die Auswertung der Zeitkritikalität der Prozesse gibt Auskunft über die Schutzbedürftigkeit einzelner Prozesse gegenüber Ausfällen.

- Prozessabhängigkeiten:
  Verkettungen einzelner Prozesse geben Auskunft darüber, wie sich Ausfälle im Unternehmen auswirken können, dies muss bei Notfallplänen beachtet werden.

- Ressourcen:
  Die ermittelten Ressourcen, die zum Wiederanlauf eines zeitkritischen Prozesses benötigt werden, sind die Schutzgüter, auf die sich die zu entwickelnden Resilienzmaßnahmen und -pläne konzentrieren sollten.

Hinweis: Auch Informationen und Daten sind wichtige Ressourcen, die bei fast allen zeitkritischen Prozessen eine wichtige Rolle spielen. Daher sollten auch mögliche Informations- und Datenverluste mit einer maximal tolerierbaren Zeit bewertet werden. Hiernach können sich künftig die Intervalle von Backups richten bzw. auch geklärt werden, an welchen Stellen generell weiterführende Maßnahmen zur Informationssicherheit ansetzen sollten.

5.3 Durchführen einer strukturierten Risikoanalyse

Nachdem die Schutzbedürftigkeit der einzelnen Prozesse im Unternehmen und ihrer Ressourcen ermittelt wurde, geht es nun in der Risikoanalyse um die Ermittlung von Ursachen, die sich prozessgefährdend auswirken könnten. Hierbei muss zunächst eine Liste der möglichen Gefährdungsszenarien aufgestellt werden. Dazu wird das Verhältnis von Bedrohung und Schwachstellen ermittelt. Dann wird ermittelt, wie hoch jeweils die Eintrittswahrscheinlichkeit eingeschätzt wird und wie groß das Schadensausmaß sein kann. Die Betrachtung bezieht sich auf die Gefährdung der Verfügbarkeit der kritischen Ressourcen als Schutzgüter.

Hierbei sollte auf bereits vorhandene Risikomanagementsysteme aufgebaut werden. Dies gilt auch für bereits vorhandene Schutzmaßnahmen und Krisenpläne, welche in die Bewertung der Risiken einbezogen werden und sich risikomindernd auswirken.

Im Ergebnis erhält man mit dieser Risikoanalyse eine Aussage darüber, welche Ressourcen und auch Prozesse gegen welche Gefährdungen mit weiteren präventiven wie reaktiven Maßnahmen hinterlegt werden sollten.

Leitfrage: Welche Gefahren können die Verfügbarkeit der kritischen Ressourcen beeinträchtigen?

Erstellung einer Gefährdungsliste

Zunächst sollte eine Liste aller möglichen Gefährdungen erstellt werden, die das Potenzial haben, betriebskritische Prozesse zu gefährden. Hierzu kann neben der nachfolgenden Grafik auch der BSI-Standard 200-3[30] genutzt werden. Im Kapitel 4 des BSI-Standards werden zahlreiche Gefährdungen mit Fokus auf Informationssicherheitsrisiken gelistet. Darüber hinaus sollten weitere Gefährdungen aus anderen Bereichen ebenfalls erfasst werden, dazu verpflichtet der „All-Gefahren-Ansatz“ aus dem KRITISDachG.

[30] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2

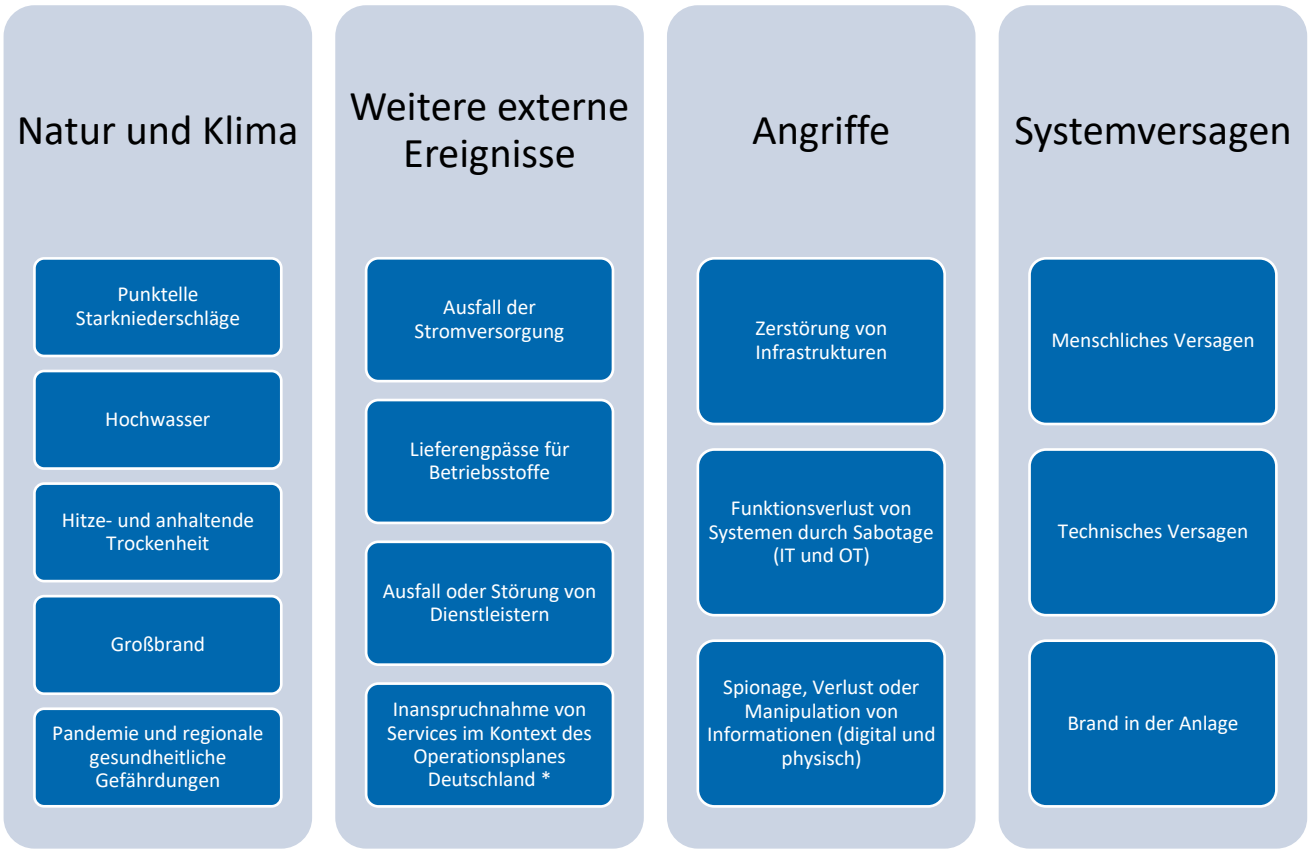


Abbildung 4: Mögliche Gefährdungen in der Wasserwirtschaft

** Operationsplan Deutschland: Definiert konkrete Maßnahmen für den Verteidigungsfall und umfasst militärische und zivile Akteure, um Deutschland als logistische Drehscheibe für die NATO zu sichern. Dies bezieht auch die wasserwirtschaftlichen Unternehmen als wichtige Versorger bei NATO-Truppenverlegungen mit ein.*

Auswirkungen auf kritische Ressourcen

Nach der Erstellung der Gefährdungsliste sollte zunächst ermittelt werden, ob sich die jeweiligen Gefährdungen auf die kritischen Ressourcen (Schutzgüter) auswirken können. Dieser Schritt kann die darauffolgende Risikoanalyse verkürzen, wenn hier bereits festgestellt wird, dass bestimmte Risiken keine oder nur geringe Auswirkungen auf die Ressourcen haben.

Hinweis: In Bezug auf Informationen und Daten als Ressource sollte hier nicht nur der Verlust der Verfügbarkeit als prozesskritisches Risiko angesehen werden, sondern auch der Verlust der Integrität sowie Vertraulichkeit, da hierdurch ebenfalls Unterbrechungen kritischer Prozesse ausgelöst werden können.

	IT/OT	Infrastruktur	Personal	Energie	Betriebsmittel	Informationen		
						Verfügbarkeit	Integrität	Vertraulichkeit
Hochwasser	Relevant	Relevant	Weniger relevant	Relevant	Relevant	Relevant	Weniger relevant	Weniger relevant
Hitze- und anhaltende Trockenheit	Weniger relevant	Weniger relevant	Weniger relevant	Weniger relevant	Weniger relevant	Weniger relevant	Weniger relevant	Weniger relevant
Pandemie	Weniger relevant	Weniger relevant	Relevant	Weniger relevant	Relevant	Weniger relevant	Weniger relevant	Weniger relevant
Brand in Anlage	Relevant	Relevant	Relevant	Relevant	Weniger relevant	Weniger relevant	Weniger relevant	Weniger relevant
Terrorismus/ Anschlag	Relevant	Relevant	Weniger relevant	Relevant	Weniger relevant	Relevant	Weniger relevant	Weniger relevant
Cyberangriff	Relevant	Weniger relevant	Weniger relevant	Relevant	Weniger relevant	Relevant	Relevant	Relevant
…								

Tabelle 2: Beispiel Beurteilung Gefährdungen je zeitkritischer Ressource – In diesem Beispiel wäre die Gefährdung „Hitze und anhaltende Trockenheit“ nicht relevant für die weitere Risikoanalyse

Die Gefährdungsübersicht gibt Auskunft, welche Gefährdungen in der Risikoanalyse genauer auf ihr Schadenspotenzial und Eintrittswahrscheinlichkeiten hin bewertet werden sollten. Die Ermittlung der relevanten Ressourcen je nach Risikokategorie ist zudem die Grundlage für die spätere Entscheidung, wo Maßnahmen im Unternehmen ansetzen müssen.

Risikobewertung:

Im nächsten Schritt muss ermittelt werden, wie hoch die Eintrittswahrscheinlichkeit jeder Gefährdung ist und wie hoch das Schadenspotenzial bei Eintritt in Bezug auf die wesentlichen Ressourcen im Unternehmen eingeschätzt wird.

Die Eintrittswahrscheinlichkeit einer Gefährdung kann anhand konkreter Erfahrungswerte, wissenschaftlicher Statistiken und Prognosen oder sonstiger fundierter Erkenntnisse eingeschätzt werden.

Beispielkategorisierung für die Eintrittswahrscheinlichkeit:

- Selten
  (Ereignis könnte höchstens alle 5 Jahre eintreten)
- Mittel
  (Ereignis könnte alle 5 Jahre bis einmal im Jahr eintreten)
- Häufig
  (Ereignis könnte einmal im Jahr bis einmal pro Monat eintreten)
- Sehr häufig
  (Ereignis könnte mehrmals im Monat eintreten)

Jede Gefährdung muss auch im Hinblick auf ihr potenzielles Schadensausmaß auf die kritischen Ressourcen betrachtet werden. Der Maßstab für das Schadensausmaß ist sowohl quantitativ (Anzahl der gefährdeten Ressourcen, siehe oben) wie auch qualitativ bewertbar. In der Praxis empfiehlt es sich, beide Betrachtungsdimensionen einzubeziehen.

Für die qualitative Bewertung ist zwischen direkten Schäden (Wiederbeschaffungskosten, Wiederherstellungs- und Reparaturkosten) und Folgeschäden (Kosten durch Stillstand, Imageverlust, Transaktionskosten, Schadenszahlungen durch mögliche Grenzwertverletzungen, potenzielle Inanspruchnahme durch Dritte, welche durch Ausfall von Dienstleistungen zu Schaden kamen) zu unterscheiden. Die Summe der direkten Schäden und der Folgeschäden ergibt die gesamte Schadensauswirkung.

Hinweis: Bereits etablierte Schutzmaßnahmen wie ein vorhandenes Hochwasserschutzkonzept, Übungspläne, Sicherheitselemente in der IT-Infrastruktur, Ausweichsysteme etc. können das Netto-Risiko in der Einschätzung mindern.

Beispielkategorisierung Schadensausmaß (jeweils auf Grundlage der quantitativen und qualitativen Einschätzung):

- Vernachlässigbar
- Begrenzt
- Beträchtlich
- Existenzbedrohend

Schadensausmaß				
Existenzbedrohend	Mittel	Hoch	Hoch	Sehr hoch
Beträchtlich	Mittel	Mittel	Hoch	Hoch
Begrenzt	Gering	Gering	Mittel	Mittel
Vernachlässigbar	Gering	Gering	Gering	Gering
	Selten	Mittel	Häufig	Sehr häufig

Eintrittswahrscheinlichkeit

Tabelle 3: Beispiel Risikomatrix

Ergebnis:

Die Risikoanalyse gibt Auskunft über den Grad der Exponiertheit der kritischen Ressourcen. Je höher das Risiko eingeschätzt wird, umso dringender sollten vorhandene Maßnahmen aktuell gehalten und ggf. auch neue Maßnahmen entwickelt werden, die das Netto-Risiko im Hinblick auf die jeweilige Gefährdung senken.

Hinweis: Zu ermittelnde Maßnahmen auf Grundlage der Risikoanalyse müssen auch wirtschaftlich angemessen sein. Nicht jedes ermittelte Risiko kann im Hinblick auf die Verhältnismäßigkeit der Kosten mit Maßnahmen hundertprozentig abgesichert werden. Diese Entscheidung zur Akzeptanz eines verbleibenden Restrisikos ist von der Geschäftsleitung zu treffen und muss dokumentiert werden sowie bei künftigen Evaluierungen der Risikoanalyse erneut überprüft werden.

5.4 Erstellung einer strategischen Maßnahmenplanung

Nach der Ermittlung der betriebskritischen Ressourcen und Prozesse sowie der jeweiligen Risiken und Schwachstellen muss nun eine übergreifende Strategie entwickelt und durch die Geschäftsführung beschlossen werden. Diese legt fest, an welchen Stellen präventive Maßnahmen zur Verbesserung des Schutzniveaus umgesetzt werden sollten und für welche

Gefährdungen Krisenpläne, Notbetriebslösungen und Wiederherstellungspläne erstellt werden müssen.

Nachdem die Schutzziele übergreifend festgelegt wurden, müssen auf Ebene der zeitkritischen Prozesse Notfallpläne und -maßnahmen entwickelt sowie präventive Schutzmaßnahmen identifiziert und umgesetzt werden. Bereits bestehende Schutzmaßnahmen und Krisenpläne werden hier integriert.

Hinweis: Im Business Continuity Management entspricht dieser Schritt den Business-Continuity-Strategien und -Lösungen, dem Geschäftsfortführungsplan sowie dem Wiederanlauf- und Wiederherstellungsplan. Ergänzt wird dies um präventive Schutzmaßnahmen, um einen ganzheitlichen Resilienzplan zu entwickeln.

Übergeordnete strategische Planung

Nachdem die Schutzgüter (betriebskritischen Ressourcen) sowie die Schwachstellen (Risikobewertung) ermittelt wurden, sollte durch die Geschäftsleitung beschlossen werden, welche Schutzziele mit einem Resilienzplan verfolgt werden. Das heißt, es muss entschieden werden, welche ermittelten Risiken mit Maßnahmen ausgerüstet werden, um das Schutzniveau des Unternehmens weiter zu verbessern.

Die Schutzziele entsprechen den zu schützenden betriebskritischen Ressourcen, die den jeweiligen zeitkritischen Prozessen im Unternehmen zugeordnet sind. Dementsprechend muss nun je Ressourcenkategorie bzw. je Prozess eine Strategie entwickelt werden, mit der sowohl das Schutzniveau verbessert werden kann (präventive Maßnahmen) als auch die Geschäftsfortführung im Schadensfall schnellstmöglich wieder anlaufen kann (reaktive Maßnahmen). Hierbei werden bereits vorhandene Schutzmaßnahmen oder Krisenpläne beachtet und einbezogen.

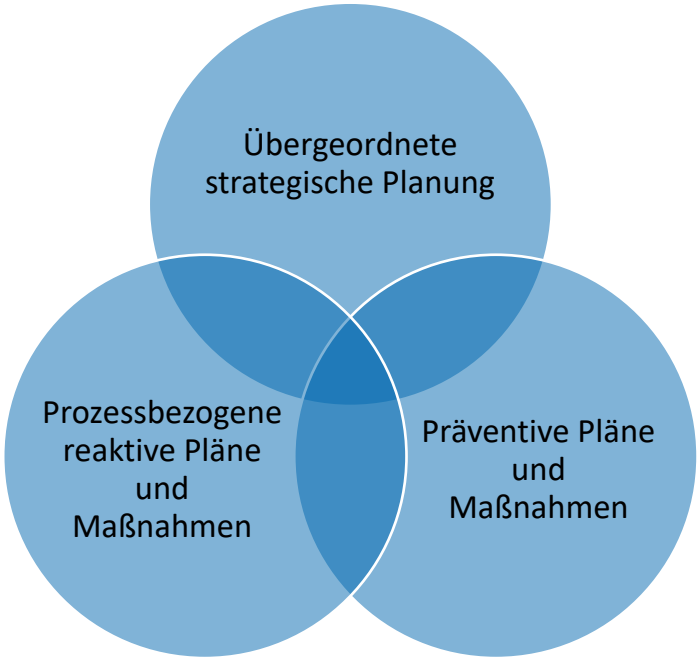


Abbildung 5: Bestandteile der Maßnahmenplanung

Prozessbezogene reaktive Pläne und Maßnahmen:

Reaktive Pläne konzentrieren sich auf den Umgang mit eingetretenen Schadensereignissen und daraus resultierenden Prozessausfällen. Sie umfassen sowohl organisatorische Verfahrensweisen wie die Bereitstellung und Koordination von Mitarbeitenden, den Einsatz von Ressourcen als auch die Wiederherstellung des Normalbetriebes und bauen auf den Erkenntnissen der Business Impact Analyse wie auf denen der Risikoanalyse auf.

Die organisatorischen Pläne und Notfallmaßnahmen sollten je zeitkritischem Prozess festgelegt und in eine übergeordnete Eskalationsplanung eingebunden werden. Ein übergeordneter Krisenstab kann bei multiplen Prozessausfällen entscheiden, wo und wie Ressourcen effektiv eingesetzt und welche Maßnahmen priorisiert werden. Er kann zudem die Kommunikation mit den Behörden und Organisationen mit Sicherheitsaufgaben (Polizei, Feuerwehr, Katastrophenschutz, BSI etc.) steuern.

Das Ziel jeder prozessbezogenen Planung sollte die Wiederherstellung des Normalbetriebs des jeweiligen Prozesses sein und sich daher auf die Wiederherstellung der notwendigen Ressourcen konzentrieren und Maßnahmen für den Übergang bzw. den Anlauf eines Notbetriebs festlegen. Diese Pläne sollten dezidiert und in Abstimmung mit der Geschäftsführung ausgearbeitet und dokumentiert werden und müssen allen relevanten Mitarbeitenden im Ernstfall sowohl digital wie auch auf Papier zugänglich sein.

Geschäftsfortführungspläne (Notfallmaßnahmen)

Durch die Ermittlung der zeitkritischen Prozesse wurden jene Zeiträume festgelegt, innerhalb derer ein Prozessausfall entweder wiederhochgefahren oder durch einen Notbetrieb aufrechterhalten werden muss. Diese Reaktionszeit gibt also vor, wie schnell Maßnahmen greifen müssen. Kann ein Prozess nicht innerhalb dieser Zeit wieder vollständig hochgefahren werden, müssen Notfallressourcen zum Einsatz kommen und Notfallpläne zum Einsatz kommen, um einen Notbetrieb zu gewährleisten, also eine zumindest eingeschränkte Fortführung des Prozesses. Für jede kritische Ressource eines Prozesses muss daher ermittelt werden:

- Welche Notfallressourcen müssen geschaffen/vorgehalten werden (z. B. Notstromaggregate, redundante Pumpensysteme, parallele IT-Systeme, Ausweichgebäude bei Gebäudeausfällen etc.), um einen Notbetrieb zu ermöglichen?
- Wie lange sollte diese Notfallressource den Notbetrieb mindestens aufrechterhalten können (Ergebnisse aus der Ermittlung zeitkritischer Prozesse entscheidend)?
- Wie kann die reguläre Ressource wiederhergestellt werden, um den Prozess in den Normalbetrieb zurückzuversetzen?

Je nach Schadenssituation können ggf. auch kurzfristig umsetzbare Brücken- oder Behelfslösungen (Quickfixes und Workarounds) zum Tragen kommen, um mind. ein Notbetriebsniveau zu erreichen. Gibt es beispielsweise durch einen Brand einen Gebäudeausfall, so kann ein zeitweises Ausweichen auf alternative Gebäude oder Homeoffice eine kostengünstige Kompensation darstellen.

In der Praxis kann es vorkommen, dass nicht alle ermittelten Risiken bzw. kritischen Ressourcen mit Notfallmaßnahmen ausgestattet werden können. Dies kann zum Beispiel daran liegen, dass die Kosten für eine Notbetriebslösung zu hoch und nicht der Eintrittswahrscheinlichkeit oder des erwarteten Schadensausmaßes angemessen sind. In diesen Fällen muss dokumentiert werden, dass diese Risiken durch die Geschäftsleitung akzeptiert werden und hierzu keine weitere Maßnahmenplanung erfolgt.

Geschäftswiederanlauf- und Wiederherstellungspläne

Neben der Herstellung eines Notbetriebes muss parallel an der Ursachenbeseitigung gearbeitet werden, um einen schnellstmöglichen Wiederanlauf einzuleiten und die vollständige Wiederherstellung des Prozesses zu gewährleisten.

Der erste Schritt ist also immer die Ursachenermittlung für einen Prozessausfall. Sobald diese gefunden wurde, startet der Wiederanlauf des Prozesses, indem die notwendigen Ressourcen zum Beispiel neubeschafft, repariert oder neukonfiguriert werden. Die hierfür jeweils notwendigen Mittel (Finanzen, Personal, Materialien etc.) müssen für jede betriebskritische Ressource definiert werden.

Im nächsten Schritt müssen Wiederanlaufpläne festgelegt werden, die ein genaues Ablauf- und Prüfschema festhalten, welches gleichzeitig sowohl als Dokumentation des Vorgangs als auch als Checkliste durch die Prozess- und Ressourcenverantwortlichen genutzt werden kann.

Diese Wiederanlaufpläne müssen von der Geschäftsführung auf Vollständigkeit, Plausibilität und Aktualität kontrolliert und anschließend freigegeben werden. Dies ist auch wichtig, um die übergeordnete strategische Planung zu ermöglichen.

Hilfestellungen für den Wiederanlauf und die Wiederherstellung der Prozesse sind in Form von Dokumentenvorlagen beim BSI erhältlich.[31]

Übungen und Tests

Die aufgestellten Pläne zur Geschäftsfortführung, zum Wiederanlauf und zur Wiederherstellung müssen regelmäßig geübt und getestet werden, die relevanten Mitarbeitenden sollten stets zu allen Belangen gut geschult und informiert sein. Durchgeführte Tests müssen dokumentiert und ausgewertet werden. Hieraus abgeleitete Verbesserungsbedarfe müssen im nächsten Planungszyklus adressiert werden.

Präventive Pläne und Maßnahmen

Die Ergebnisse der Auswertung der Zeitkritikalität der betrieblichen Prozesse sowie die Risikoanalyse geben Auskunft über den Schutzbedarf einzelner Ressourcen im Unternehmen. Neben den Plänen und Maßnahmen zur Schadensminimierung im Ernstfall, sollten auch präventive Schutzmaßnahmen umgesetzt werden, die unter Umständen Vorfälle und Schäden verhindern oder zumindest ihr Ausmaß minimieren können.

Vorsorgende Sicherheitsmaßnahmen sollten sowohl im Bereich des physischen Objektschutzes wie auch im Bereich der Cybersicherheit ansetzen. Hierbei ist zu beachten, dass die Informationssicherheit sowohl digital als auch physisch umgesetzt werden muss und damit beide Bereiche tangiert. Dabei umfassen präventive Maßnahmen nicht nur technische, sondern auch organisatorische Maßnahmen, die das Sicherheitsniveau verbessern.

Zu den technisch umsetzbaren präventiven Sicherheitsmaßnahmen zählen beispielsweise:

- Funktionierende und schwarzfallsichere (mechanische Öffnung möglich) Schließsysteme auf dem Betriebsgelände, an Gebäuden und Büros
- Effektive Zugangskontrollen (Mitarbeitende, Gäste, Vertragspartner, Fahrzeuge, etc.)

[31] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/BSI-Standard-200-4_Hilfsmittel/BSI_Standard_200_4_Hilfsmittel_node.html

- Effektiver Objektschutz (Zäune, Kamerasysteme, Sensortechnik, etc.)
- Beleuchtungskonzept
- 24/7-Überwachung OT/IT sowie Reaktionen durch qualifiziertes Personal
- Berechtigungskonzepte / Authentifizierung (IT-Systeme)
- Datensicherung / Backupsysteme* (eigene Serverstrukturen, Clouds)
- Schutz vor Schadprogrammen (Anti-Virensoftware, Sperren von bestimmten Domains)
- Verschlüsselung/Kryptografie (bei der Verarbeitung, Übertragung und Speicherung von Informationen)
- Systeme zur Angriffserkennung

* Zur Erstellung und Umsetzung eines Datensicherungskonzepts bietet das BSI Hinweise[32]. Darüber hinaus bietet das BSI auch eine generelle Handreichung[33] zur Behandlung von Sicherheitsvorfällen im Bereich der Informationssicherheit an.

Zu den organisatorischen Maßnahmen zählen beispielweise:

- Interne Richtlinien mit Festlegungen von Verantwortlichkeiten und Prozessabläufen (z. B. zu Datenschutz, Compliance, Informationssicherheit etc.)
- Schulung und Sensibilisierung von Mitarbeitenden (z. B. zur Selbstwirksamkeit in Bezug auf Sicherheitsbelange oder zum Verhalten bei Sicherheitsvorfällen)
- Sicherheitsüberprüfungen (z. B. Revision und externe Audits, Penetrationstests etc.)

[32] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_3_Datensicherungskonzept_Edition_2023.pdf?__blob=publicationFile&v=3

[33] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/05_DER_Detektion_und_Reaktion/DER_2_1_Behandlung_von_Sicherheitsvorfaellen_Edition_2023.pdf?__blob=publicationFile&v=3

6 Finanzierung von Sicherheits- und Resilienzmaßnahmen

Nicht nur für die Bürgerinnen und Bürger sowie die Wirtschaft und andere Versorgungsunternehmen ist Versorgungssicherheit im Wassersektor von höchstem Wert. Auch für die Operationsfähigkeit der Bundeswehr und ihrer Verbündeten sowie wesentlicher Teile der Behörden und Organisationen mit Sicherheitsaufgaben (BOS), darunter Feuerwehr, Katastrophenschutz oder Technisches Hilfswerk, bilden diese Dienstleistungen wichtige Voraussetzungen zur eigenen Aufgabenerfüllung im Krisen-, Katastrophen- oder Angriffsfall.

Für einen wirksamen Schutz in der Wasserver- und Abwasserentsorgung müssen deshalb die Finanzierung von Sicherheits- und Resilienzmaßnahmen, darunter eine breite Palette von Investitionen, eindeutig als betriebsnotwendige Maßnahmen anerkannt werden.
Die Refinanzierung zur Kostenanerkennung, ganz gleich, ob dies über die kartellrechtliche Preiskontrolle im Tarifbereich bei privatrechtlich organisierten Unternehmen erfolgt oder bei öffentlich-rechtlich organisierten Unternehmen über Gebührenrecht und Kommunalaufsicht, muss zeitnah und sicher gewährleistet sein.

So stellt sich allein schon im Rahmen der im BBK Merkblatt “Vorsorgemaßnahmen zur Sicherstellung der Trinkwassernotversorgung (2022)”[34] enthaltenen Empfehlungen, die öffentliche Wasserversorgung bei einem großflächigen Stromausfall mindestens 72 Stunden so funktionstüchtig zu halten, dass über diesen Zeitraum Wasser in Trinkwasserqualität bereitgestellt und Abwasser abgeführt werden kann, die Frage der kartellrechts- und gebührenrechtskonformen Kalkulation. Hierzu ist zeitnah eine rechtlich anzuerkennende Definition betriebsnotwendiger Kosten in der Tarifkalkulation und im Gebührenkontext durch Entgelte/Umlagen zu schaffen.

Der BDEW setzt sich intensiv für eine entsprechende Anpassung innerhalb der bestehenden regulierten Entgeltsysteme ein, um eine klare Rechtsgrundlage für die Refinanzierung von Kosten über Preise und Gebühren sowie aus staatlichen Mitteln zu schaffen.
Mit wachsender hybrider Bedrohungslage ist es jedoch auch dringend angezeigt, erhöhte Schutz- und Resilienzbedarfe für den Wassersektor auch über den von der Schuldenbremse ausgenommenen Verteidigungshaushalt und einen noch einzurichtenden Resilienzfonds zu finanzieren.

Darüber hinaus stehen für Wasserver- und Abwasserentsorger bislang eher kleinere Förderprogramme zur Verfügung, um Investitionen in Sicherheits- und Resilienzmaßnahmen gemäß KRITISDachG und NIS2-UG zu finanzieren. Diese reichen von zinsgünstigen KfW-Krediten über

[34] https://www.bbk.bund.de/SharedDocs/Downloads/DE/KRITIS/planungshilfe-wassersicherstellung.pdf?__blob=publicationFile&v=2

limitierte Zuschüsse für IT-Sicherheit (z. B. BAFA, MID NRW) bis hin zu limitierten EU-Förderungen (EFRE, Horizon Europe). Darüber hinaus empfehlen wir, die Fördermittelprogramme des jeweiligen Bundeslandes auf Eignung zur Finanzierungsunterstützung zu prüfen.

Staatliche Mitfinanzierung soll und muss dazu beitragen, die betriebliche Tragfähigkeit notwendig werdender Kosten zu garantieren und gleichermaßen Verzögerungen und breite öffentlichkeitswirksame Diskussionen, wie beispielsweise zu Gebührenerhöhungen, die in der Regel durch das jeweilige Gremium wie z. B. Stadtrat, Verbandsrat etc. zu diskutieren und zu beschließen sind und nicht selten längere Zeit in Anspruch nehmen, zu vermeiden.
Weil nicht erst in einer akuten Bedrohungslage oder gar im Verteidigungsfall Schutz- und Resilienzmaßnahmen geschaffen und investiert werden können, ist zeitnah auf politischer Ebene die unbürokratische Umsetzung in beiden Finanzierungssträngen zu ermöglichen.

Nicht zuletzt ist auf Bundesebene insbesondere auch dafür Sorge zu tragen, dass eine bundeseinheitliche Praxis hierfür sichergestellt wird. Eine ansonsten erforderliche Abstimmung mit 16 Landeskartellbehörden und/oder Kommunalaufsichtsbehörden wäre weder leistbar noch zielführend im Interesse von Sicherheit und Resilienz. Förderseitig in Frage kommen hierbei sowohl spezifisch deklarierte Förderprogramme der Länder, die Bundesförderung für Infrastrukturmaßnahmen sowie die Investitionsmittel, die unmittelbar der Verteidigung zugeordnet wurden.

Unternehmensseitig setzt dies jedoch voraus, dass entsprechend der Erfordernisse aus dem KRITISDachG und dem NIS2-UG sowie nach entsprechender Risikoanalyse im All-Gefahrenansatz, ein klarer Überblick zu neuen notwendigen Maßnahmen und Investitionen besteht. Hierbei können zunächst auch solche Maßnahmen und Investitionen als förderlich für die Sicherheit und Resilienz identifiziert worden sein, die deutlich über die bisherige Verantwortung eines störungsfreien Normalbetriebes hinausgehen.

Erfahrungswerte aus dem Krisenmanagement im Umgang mit Extremwetterereignissen, mehrtägigen Energieausfällen, Cyberattacken oder dem Umgang mit Pandemie bieten hierbei eine wertvolle Grundlage. Vom effektiven Objektschutz, über redundante technische Systeme bis hin zur 24/7 Überwachung im IT- und OT-Bereich ist Vieles bereits adressiert. Zu den bisher eher ungewohnten Maßnahmen können dabei unter anderem Systeme zur Detektion und Abwehr von Drohnen, die Schaffung interoperabler Kommunikationssysteme zum Austausch mit den BOS, zusätzliches, spezifisch geschultes Personal, der Ausbau von Schutzräumen, zusätzliche redundante Infrastrukturen oder auch eine umfängliche, lokal übergreifende Lagerbewirtschaftung technisch wie in wichtigen Einsatzstoffen gehören.

Neben den Abstimmungen zu den notwendigen Maßnahmen für mehr Sicherheit und Resilienz und deren Finanzierung, empfehlen wir zudem zu prüfen und in der Kostenumlage ebenfalls ansatzfähig einzustufen, im Planansatz grundsätzlich einen zweckgebundenen,

angemessenen Anteil des Aufwandes für die Finanzierung notwendig werdender Maßnahmen vorzuhalten.

7 Weiterführende Hinweise aus der Praxis

Über die unmittelbaren Verpflichtungen aus beiden Gesetzesakten hinaus empfiehlt es sich, auch die folgenden, ganz praktischen Überlegungen in den Blick zu nehmen.

In den Anlagen findet sich zudem ein Beispiel anhand eines Musterunternehmens, welches einen Cybersicherheitsvorfall verzeichnet und die notwendigen Schritte in die Wege leitet.

Vertragsgestaltungen gegenüber Auftragnehmern auf Informationssicherheit prüfen

Über den Auftrag des NIS2-UG hinaus, wonach nach § 30 Abs. 2 Nr. 4 in der vor- und nachgelagerten Lieferkette sehr sorgsam mit sensiblen Informationen aus dem eigenen Unternehmen umzugehen ist und bei notwendiger Weitergabe für die nachweisliche Einhaltung entsprechender Sicherheitsanforderungen auch vertraglich Sorge zu tragen, sind noch die folgenden 3 Punkte zu empfehlen.

1. Sollten Auftragnehmer selbst in die Situation kommen, dass Dritte Auskunftsrechte ihnen gegenüber geltend machen, die Informationen zum Betrieb kritischer Anlagen umfassen, müsste ein Umgang wie zum Beispiel die Rückverweisung an den Auftraggeber vereinbart sein.
2. Weiterhin ist darauf zu achten, dass in den Verträgen mit Dritten keine Komponenten oder Anlagen verbaut werden, die einer Fremdsteuerung unterliegen und damit missbrauchsanfällig sind. Auch hierzu empfiehlt sich die Aufnahme in einer vertraglichen Formulierung, zuzüglich zu den unter NIS2 bereits angekündigten Sicherheitsanforderungen für den Einsatz kritischer Komponenten.
3. Nicht zuletzt sollten sich Wasserwirtschaftsunternehmen im Kontext von Leitungsauskünften, wie u. a. im Zuge von Glasfaserverlegungen, auch in den Fällen, wo sie nicht selbst der Auslöser sind, über vertragliche Vereinbarungen zu Gunsten der eigenen Informationssicherheitsbedarfe mit den Auskunftssuchenden angemessen vereinbaren.

Transparenzbitten und mögliche Transparenzpflichten kritisch prüfen

Vielfach bestehen neben den gesetzgeberisch unmittelbar adressierten Transparenzpflichten u. a. aus der Trink- und Abwasserrichtlinie oder der Nachhaltigkeitsberichterstattung weitergehende Informations- und Datenabfragen von unterschiedlichen administrativen Ebenen wie von öffentlichen oder privaten Institutionen.

Unternehmen des Wassersektors sollten zunächst prüfen, ob die Notwendigkeit der Daten- und Informationsweitergabe tatsächlich erforderlich ist. Wenn dies bejaht wird, sollten analog zu Vertragsvereinbarungen mit Unternehmenspartnern vergleichbare Vereinbarungen auch mit öffentlichen Partnern getroffen werden.

Clusterung von Informationen und Daten

Für die Entscheidung welche Daten und Informationen als sensibel oder sogar besonders sensibel zu bewerten sind und damit nicht an Dritte weitergeben werden dürfen, empfiehlt sich der Aufbau einer Clusterung von verschiedenen Informations- und Datengruppen sowie unternehmensinterne Regelungen zum Umgang. Prinzipiell ist dies ohnehin Auftrag bei der Implementierung eines ISMS.
Im Zuge dessen sollte auch nachvollziehbar geregelt werden, welche überschaubare Anzahl von Mitarbeitenden überhaupt befugt sind, Informationen und Daten des Unternehmens an Dritte weiterzugeben.

Sensibilisierung der Mitarbeitenden

Die Herausforderungen, die ganz real aus der hybriden Bedrohungslage sowie den hieraus erwachsenen gesetzlichen Vorgaben zu bewältigen sind, erfordern die Sensibilisierung und Mitwirkung aller Beschäftigten. Hierzu empfiehlt sich eine unternehmensinterne Kommunikation, welche einerseits die real mögliche Betroffenheit bspw. bei Cyberangriffen oder Verletzungen des Eigentums in den Blick nimmt. Andererseits sollten Beschäftigte nicht nur für die neue Lage sensibilisiert, sondern mit ihren Ideen, im Rahmen ihrer jeweiligen Verantwortlichkeiten aktiv eingebunden werden. Vielfach lässt sich dabei an bereits bekannte und geübte Themen wie Krisenmanagement, Umgang mit Hochwasserereignissen oder Stromausfall anknüpfen.

Nicht zuletzt kann die Einbindung der Mitarbeitenden ein potenzielles Ohnmachtsempfinden in aktives, sinnvolles Handeln übersetzen. Um Sicherheit und Resilienz in den Unternehmen des Wassersektors zu verbessern, braucht es das Verständnis und die aktive Mitwirkung aller Beschäftigten sowie der Arbeitnehmervertretung.

Angemessene Einbindung der Share- und Stakeholder

Auf Seiten der Shareholder, welche deutschlandweit mehrheitlich kommunal geprägt sind, besteht bereits im Rahmen der üblichen Berichtspflichten der verbindliche Auftrag, über neue oder sich verändernde Risiken zu berichten bzw. über hieraus abzuleitende Maßnahmen. Dies gilt auch im Kontext der neuen Gesetzlichkeiten und der realen sich verändernden Sicherheitslage.

Die Anteilseigner tragen mit ihren Entscheidungen zur Planung von Investitions- oder Aufwandsmaßnahmen eine Mitverantwortung, dass Objektschutz, die Einführung oder Erweiterung von Sicherheitstechnologien oder der Aufbau von personellen Ressourcen umgesetzt werden können, was ggf. über angepasste Tarife oder auch Fördermöglichkeiten zu finanzieren ist.

Analog zu den Mitarbeitenden ist auch die Sensibilisierung und Unterstützung der jeweiligen Stakeholder sowie der entsprechenden Gremien wie Stadt-, Gemeinde- oder Verbandsräte zwingend notwendig, um eine breite Akzeptanz notwendiger Maßnahmen, die zu einer weiteren Verbesserung der Sicherheit und Resilienz der Versorgung beitragen, zu erreichen.

Institutionsübergreifende Katastrophen-, Krisen- und Notfallplanung

Nicht zuletzt lassen sich auf lokaler und ggf. auch auf regionaler Ebene mit den Share- wie mit den Stakeholdern, darunter auch weiteren Versorgungsunternehmen der Region, den BOS und ggf. auch mit lokalen Medien hilfreiche Netzwerke aufbauen, in denen die Beteiligten voneinander lernen und sich wechselseitig im Ernstfall ggf. Unterstützung leisten können. Eine gemeinsame Planung und Übung zum Umgang mit Katastrophen- und Krisenszenarien sichert zudem eine effiziente und logistisch koordiniere Nutzung von wichtigen Ressourcen bzw. lassen sich so im Vorfeld auch notwendige Lagerhaltungen organisieren. Gemeinsames Agieren und eine krisensichere Kommunikation erleichtern im Ernstfall den notwendigen Austausch aller Beteiligten untereinander ab. Das regelmäßige Üben solcher gemeinsamen Pläne sollte ebenso vorangetrieben werden, um notwendige Verbesserungen im Ablauf und ein schnelles Handeln abzusichern sowie Festlegungen immer wieder ins Gedächtnis zu rufen und auf Aktualität wie Praxistauglichkeit zu prüfen.

Externe “Auditierung” und Besicherung

Neben der eigenen Anstrengung gesetzeskonform wie praxistauglich Maßnahmen zur weiteren Verbesserung des physischen wie Cyberschutzes zu implementieren, empfiehlt es sich, auch geeignete Managementsysteme zu nutzen sowie externe Audits vorzunehmen. Eine Übersicht zu empfehlenswerten Managementsystemen findet sich im Einleitungsteil des Kapitel 5.

Auch Penetrationstests können helfen, noch vorhandene Schwachstellen zu identifizieren und zu beseitigen.

Nicht zuletzt sollte überlegt werden, inwieweit über Versicherungen, bspw. für Cybersicherheit, ergänzend mögliche eingetretene Schäden in der Bewältigung unterstützt werden könnten.

Anhang 1: Glossar

Hinweis: Das nachfolgende Glossar trägt die erläuterungsbedürftigen Begriffe zusammen, die in der vorliegenden Anwendungshilfe verwendet werden. Die Definitionen stammen entweder direkt aus den Gesetzestexten des KRITISDachG[35] und des NIS2-UG[36] oder aus Glossaren der zuständigen Bundesbehörden wie dem BSI (Glossar des BSI-Standard 200-4[37] sowie Glossar zum IT-Grundschutzkompendiums[38]) und des BBK[39].

Zu beachten ist, dass sich die Definitionen je nach Quelle unterscheiden können. Sofern dies der Fall ist, werden alle vorhandenen Definitionen genannt.

Betreiber	KRITISDachG & NIS2-UG: „Betreiber kritischer Anlagen“ [ist] eine natürliche oder juristische Person oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausübt.
Business Continuity Management (BCM)	BSI-Glossar 200-4: Steuerung sämtlicher Aktivitäten, die eine geordnete Geschäftsfortführung nach Schadensereignissen zum Ziel haben Zu unterscheiden sind zwei wichtige Bereiche: 1. Vorsorge (Geschäftsprozesse sollten möglichst nicht unterbrochen werden.) 2. Reaktion (Geschäftsprozess sollten nach einem Ausfall in angemessener Zeit wieder hergestellt werden.) BSI-Glossar IT-Grundschutzkompendium: Business Continuity Management (BCM) bezeichnet alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts einer Behörde oder eines Unternehmens nach Eintritt eines Notfalls bzw. eines

35 https://www.recht.bund.de/bgbl/1/2026/66/regelungstext.pdf?__blob=publicationFile&v=1
36 https://www.recht.bund.de/bgbl/1/2025/301/VO.html
37 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Glossar.pdf?__blob=publicationFile&v=4
38 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1
39 https://www.bbk.bund.de/DE/Infothek/Glossar/_functions/glossar

	Sicherheitsvorfalls dienen. Weiterhin unterstützt BCM die sukzessive Fortführung der Geschäftsprozesse bei länger anhaltenden Ausfällen oder Störungen.
Business Impact Analyse (BIA)	BSI-Glossar 200-4: Strukturierte Untersuchung mit dem Ziel, (zeit-)kritische Geschäftsprozesse und Ressourcen (Assets) zu identifizieren. Hierzu werden diejenigen direkten und indirekten potenziellen Folgeschäden für die Institution ermittelt, die durch den Ausfall von Geschäftsprozessen verursacht werden. Daraus werden die Anforderungen an den Wiederanlauf von Geschäftsprozessen abgeleitet. BSI-Glossar IT-Grundschutzkompendium: Eine Business Impact Analyse (Folgeschädenabschätzung) ist eine Analyse zur Ermittlung von potenziellen direkten und indirekten Folgeschäden für eine Institution, die durch das Auftreten eines Notfalls oder einer Krise und Ausfall eines oder mehrerer Geschäftsprozesse verursacht werden. Es ist ein Verfahren, um kritische Ressourcen und Wiederanlaufanforderungen sowie die Auswirkungen von ungeplanten Geschäftsunterbrechungen zu identifizieren.
Gefährdung	BBK: Möglichkeit, dass an einem konkreten Ort aus einer Gefahr ein Ereignis mit einer bestimmten Intensität erwächst, das Schaden an einem Schutzgut verursachen kann. BSI-Glossar IT-Grundschutzkompendium: Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. Sind beispielsweise Schadprogramme eine Bedrohung oder eine Gefährdung für Personen, die im Internet surfen? Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwendenden prinzipiell durch Schadprogramme im Internet bedroht sind. Die Person, die eine mit Schadprogrammen infizierte Datei herunterlädt, wird von dem Schadprogramm gefährdet, wenn das IT-System anfällig für diesen Typ des Schadprogramms ist. Für Anwendende mit einem wirksamen Virenschutz, einer Konfiguration, die das Funktionieren des Schadprogramms verhindert, oder einem Betriebssystem, das den Code des

	Schadprogramms nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.
Katastrophe	BBK: Ein Geschehen, bei dem Leben oder Gesundheit einer Vielzahl von Menschen oder die natürlichen Lebensgrundlagen oder bedeutende Sachwerte in so ungewöhnlichem Ausmaß gefährdet oder geschädigt werden, dass die Gefahr nur abgewehrt oder die Störung nur unterbunden und beseitigt werden kann, wenn die im Katastrophenschutz mitwirkenden Behörden, Organisationen und Einrichtungen unter einheitlicher Führung und Leitung durch die Katastrophenschutzbehörde zur Gefahrenabwehr tätig werden. Anmerkung des BBK: Die Definition der Katastrophen kann entsprechend landesrechtlicher Regelungen abweichend gefasst sein, s. DIN 13050:2015- 04 (Begriffe im Rettungswesen)
Krise	BBK: Vom Normalzustand abweichende Situation mit dem Potenzial für oder mit bereits eingetretenen Schäden an Schutzgütern, die mit der normalen Aufbau- und Ablauforganisation nicht mehr bewältigt werden kann, so dass eine besondere Aufbauorganisation (BAO) erforderlich ist. BSI-Glossar 200-4: Schadensereignis, das sich in massiver Weise negativ auf eine Institution auswirkt und dessen Auswirkungen nicht im Normalbetrieb bewältigt werden können Im Gegensatz zu einem Notfall liegen zur Bewältigung einer Krise jedoch keine spezifischen Notfallpläne vor. Vorhandene Notfallpläne können nicht oder nur bedingt adaptiert werden oder greifen schlicht nicht.
Krisenmanagement	BBK: Alle Maßnahmen zur Vorbereitung auf Erkennung und Bewältigung, Vermeidung weiterer Eskalationen sowie Nachbereitung von Krisen. Anmerkung des BBK: Krisenmanagement beinhaltet die Schaffung von konzeptionellen, organisatorischen und verfahrensmäßigen Voraussetzungen durch staatliche und nichtstaatliche Akteure, um eine schnellstmögliche Zurückführung der eingetretenen außergewöhnlichen Situation in den Normalzustand zu unterstützen oder eine Eskalation zu

	vermeiden. Krisenmanagement ist im Idealfall mit Risikomanagement verzahnt. BSI-Glossar 200-4: Im Rahmen des BSI-Standards 200-4 bezieht sich der Begriff lediglich auf institutionsinterne Krisen, d. h. ist enger gefasst als im Zusammenhang mit der öffentlichen Gefahrenabwehr, z. B. durch die Feuerwehr (siehe FwDV 100)
Normalbetrieb	BSI-Glossar 200-4: planmäßiger Geschäftsbetrieb einer Institution
Notfall	BBK: Situation mit dem Potenzial für oder mit bereits eingetretenen Schäden an Schutzgütern, die neben Selbsthilfemaßnahmen des Einzelnen staatlich organisierte Hilfeleistung erforderlich machen kann. BSI-Glossar 200-4: Unterbrechungen mindestens eines zeitkritischen Geschäftsprozesses, der nicht im Normalbetrieb innerhalb der maximal tolerierbaren Ausfallzeit wiederhergestellt werden kann. Im Gegensatz zu Störungen wird zur Bewältigung von Notfällen eine BAO benötigt. Im Gegensatz zur Krise ist ein Notfall ein Schadensereignis für dessen Bewältigung entweder geeignete Pläne vorliegen oder bestehende Pläne adaptiert werden können. Notfälle können auch eintreten, bevor das Schadensereignis zu einer Unterbrechung des Geschäftsbetriebs führt. Es genügt die Gefahr, dass durch das Schadensereignis der Geschäftsbetrieb unterbrochen wird.
Prozesskette	BSI-Glossar 200-4: Eine Reihe von mehreren, untereinander abhängigen Geschäftsprozessen, z. B. Auftragseingang, Herstellung, Lieferung, Abrechnung. Die Reihe als Ganzes trägt zur Wertschöpfung in einem Unternehmen oder zur Erfüllung des öffentlichen Auftrages einer Behörde bei.
Resilienz	KRITISDachG: Fähigkeit einer kritischen Anlage, einen Vorfall zu verhindern, sich vor einem Vorfall zu schützen, einen Vorfall abzuwehren, auf einen Vorfall zu reagieren, die Folgen eines Vorfalls zu

	begrenzen, einen Vorfall aufzufangen und zu bewältigen und sich von einem Vorfall zu erholen BBK: Fähigkeit von Systemen und Lebewesen, Ereignissen zu widerstehen beziehungsweise sich daran anzupassen und dabei Funktionsfähigkeiten zu erhalten und das Überleben zu sichern.
Ressource	BSI-Glossar 200-4: Alle physischen und digitalen Werte, die erforderlich sind, um Geschäftsprozesse durchführen zu können. Werte im betriebswirtschaftlichen Sinn sind z. B. Personal, IT-Systeme, Gebäude, Dienstleistungsunternehmen, Maschinen oder Betriebsmittel. BBK: Abgrenzbare Einheit von Personal, Finanzmitteln, Sachmitteln, Informationen, Hilfs- und Unterstützungsmöglichkeiten, die zur Durchführung oder Förderung eines einsatzfähigen Systems zum Schutz der Bevölkerung herangezogen werden können.
Risiko	KRITISDachG: „Risiko“ [ist] das Potenzial für Ausfälle oder Beeinträchtigungen, die durch einen Vorfall verursacht werden, das als eine Kombination des Ausmaßes eines Ausfalls oder einer Beeinträchtigung und der Wahrscheinlichkeit des Eintretens des Vorfalls zum Ausdruck gebracht wird BBK: Kombination aus der Eintrittswahrscheinlichkeit eines Ereignisses und dessen negativen Folgen (UNISDR, Terminology on Disaster Risk Reduction, Genf 2009, S. 25). BSI-Glossar IT-Grundschutzkompendium: Risiko wird häufig definiert als die Kombination (also dem Produkt) aus der Häufigkeit, mit der ein Schaden auftritt und dem Ausmaß dieses Schadens. Der Schaden wird häufig als Differenz zwischen einem geplanten und ungeplanten Ergebnis dargestellt. Risiko ist eine spezielle Form der Unsicherheit oder besser Unwägbarkeit.

	In der ISO wird Risiko auch als das Ergebnis von Unwägbarkeiten auf Zielobjekte definiert. In diesem Sinne wird daher auch von Konsequenzen statt von Schaden gesprochen, wenn Ereignisse anders eintreten als erwartet. Hierbei kann eine Konsequenz negativ (Schaden) oder positiv (Chance) sein. Die obige Definition hat sich allerdings als gängiger in der Praxis durchgesetzt. Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.
Risikoanalyse	KRITISDachG / BBK: Das systematische Verfahren zur Bestimmung eines Risikos BSI-Glossar IT-Grundschutzkompendium: Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln. Risikoanalyse bezeichnet nach den einschlägigen ISO-Normen ISO 31000 und ISO 27005 nur einen Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht: • Identifikation von Risiken (Risk Identification) • Analyse von Risiken (Risk Analysis) • Evaluation oder Bewertung von Risiken (Risk Evaluation) Im deutschen Sprachgebrauch hat sich allerdings der Begriff Risikoanalyse für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert. Daher wird auch in den Dokumenten zum IT-Grundschutz weiter der Begriff Risikoanalyse für den umfassenden Prozess benutzt.
Risikobewertung	KRITISDachG: Der Prozess, in dem Risiken in Bezug auf deren Wirkung auf die kritische Dienstleistung verglichen und priorisiert werden und entschieden wird, ob Maßnahmen zur Risikobehandlung zu ändern und zu ergänzen sind BBK: Verfahren, mit dem: 1. festgestellt wird, in welchem Ausmaß das zuvor definierte Schutzziel im Falle eines bestimmten Ereignisses erreicht wird; 2. Entschieden wird, welches verbleibende Risiko akzeptabel ist und; 3. Entschieden wird, ob

	Maßnahmen zur Minimierung ergriffen werden können/müssen.
Risikomanagement	BBK: Kontinuierlich ablaufendes, systematisches Verfahren zum zielgerichteten Umgang mit Risiken, das die Analyse und Bewertung von Risiken sowie die Planung und Umsetzung von Maßnahmen insbesondere zur Risikovermeidung/-minimierung und -akzeptanz beinhaltet. Systematischer Prozess mit dem ein Unternehmen Risiken identifiziert, bewertet, steuert und überwacht, um mögliche negative Auswirkungen auf Ziele, Prozesse oder Werte zu minimieren. BSI-Glossar IT-Grundschutzkompendium: Als Risikomanagement werden alle Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken bezeichnet, also alle Tätigkeiten, um Risiken für eine Institution zu identifizieren, zu steuern und zu kontrollieren. Das strategische Risikomanagement beschreibt die wesentlichen Rahmenbedingungen, wie die Behandlung von Risiken innerhalb einer Institution, die Kultur zum Umgang mit Risiken und die Methodik ausgestaltet sind. Diese Grundsätze für die Behandlung von Risiken innerhalb eines ISMS müssen mit den Rahmenbedingungen des organisationsweiten Risikomanagements übereinstimmen bzw. aufeinander abgestimmt sein. Die Rahmenbedingungen des operativen Risikomanagements umfassen den Regelprozess aus • Identifikation von Risiken, • Einschätzung und Bewertung von Risiken, • Behandlung von Risiken, • Überwachung von Risiken und • Risikokommunikation.
Schaden	BBK: Negativ bewertete Auswirkung eines Ereignisses auf ein Schutzgut BSI-Glossar IT-Grundschutzkompendium (Schaden / Konsequenz): Eine Abweichung von einem erwarteten Ergebnis führt zu einer Konsequenz (häufig „Schaden“ genannt). Hierbei kann es

	sich grundsätzlich um eine positive oder negative Abweichung handeln. Eine positive Konsequenz beziehungsweise positiver Schaden im Sinne der Chancen- und Risikoanalyse wird auch als Chance bezeichnet. Meistens werden in der Risikoanalyse jedoch die negativen Konsequenzen, also die Schäden, betrachtet. Das Ausmaß eines Schadens wird als Schadenshöhe definiert und kann als bezifferbar oder nicht direkt bezifferbar betitelt werden. Die bezifferbaren Schäden können in der Regel mit direkten Aufwänden (z. B. finanzieller Art) dargestellt werden. Zu den nicht direkt bezifferbaren Schäden gehören z. B. Imageschäden oder Opportunitätskosten. Bei diesen lässt sich die tatsächliche Schadenshöhe häufig nur vermuten oder schätzen. Alle Angaben werden in der Regel aufgrund von Erfahrungs- oder Branchenwerten in Kategorien klassifiziert.
Störung	BSI-Glossar 200-4: Eine Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen oder funktionieren. So bezeichnet werden Situationen, die in der Regel innerhalb des Normalbetriebs durch die Allgemeine Aufbauorganisation der Institution behoben werden können. Hierzu wird auf vorhandene Prozesse zur Störungsbeseitigung oder des Incident-Managements zurückgegriffen.
Vorfall	KRITISDachG: Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich beeinträchtigt oder beeinträchtigen könnte, mit Ausnahme von Ereignissen, die ausschließlich Sicherheitsvorfälle im Sinne des § 2 Nummer 40 des BSI-Gesetzes oder § 3 Nummer 53 des Telekommunikationsgesetzes sind NIS2-UG (Sicherheitsvorfall): 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
Zeitkritisch	BSI-Glossar 200-4: Einordnung für alle Geschäftsprozesse oder Ressourcen, deren Ausfall innerhalb eines zuvor festgelegten Zeitraums zu

	einem nicht tolerierbaren, unter Umständen existenzgefährdenden Schaden für eine Institution führen kann. Die Einordnung von Ressourcen wird dabei von der Einordnung der Geschäftsprozesse, die die jeweiligen Ressourcen benötigen, abgeleitet.

Anhang 2: Praxisbeispiel Management eines Cybervorfalls

Der „Abwasserverband Beispiel“ betreibt drei Kläranlagen und rund 150 km Kanalnetz, entsorgt 280.000 Einwohnerwerte, beschäftigt 130 Mitarbeitende und erzielt einen Jahresumsatz von 25 Mio. EUR. Damit fällt der Verband in den Anwendungsbereich des NIS2-Umsetzungsgesetzes als KRITIS-Betreiber, einer Teilmenge der besonders wichtigen Einrichtungen, ohne die Einwohnerschwelle des KRITIS-Dachgesetzes zu erreichen.

In einer Nacht wird in der zentralen Kläranlage ein Cyberangriff auf das Prozessleitsystem festgestellt: Die Leitwarte erkennt ungewöhnliche Stellgrößen in der Belüftung und drohende Grenzwertüberschreitungen im Ablauf. Als 24/7-Kontaktstelle informiert die Leitwarte umgehend den Informationssicherheitsbeauftragten als Incident Manager sowie den technischen Bereitschaftsdienst.

Gemeinsam nehmen Leitwarte, Incident Manager und Bereitschaftsdienst eine erste Bewertung vor und stufen den Vorfall als potenziell meldepflichtig ein, da die Abwasserbehandlung als kritischer Prozess betroffen ist und eine Gefährdung der Umwelt sowie der gesetzlichen Einleiteranforderungen nicht ausgeschlossen werden kann. Innerhalb weniger Stunden erfolgt eine Erstmeldung über das BSI-Portal als Sicherheitsvorfall nach NIS2, die wesentlichen Eckdaten (Art des Vorfalls, Zeitpunkt der Kenntnis, betroffene Anlage, erste Auswirkungen) werden dokumentiert.

Parallel werden gemäß Resilienzplan und BCMS die vorgesehenen Notbetriebs- und Wiederanlaufmaßnahmen umgesetzt: Rückfall auf manuelle Steuerungsmodi, Plausibilitätsprüfungen vor Ort, temporäre Reduktion der Zulaufmengen und verstärkte Probenahmen. Der BCM-Verantwortliche prüft eine Einberufung des Krisenstabs, entscheidet sich aufgrund der beherrschbaren Lage dagegen, initiiert aber eine abgestimmte Information der betroffenen Kommunen.

Innerhalb von 72 Stunden wird eine Ergänzungsmeldung an das BSI mit präzisierter Schadensbewertung und ersten Ursachenhinweisen übermittelt. Spätestens einen Monat nach dem Vorfall erstellt der Verband einen Abschlussbericht mit Ursachenanalyse (z. B. Angriffsvektor über einen unzureichend gesicherten Fernzugang), den umgesetzten und geplanten Sicherheitsmaßnahmen (u. a. zusätzliche Angriffserkennung gemäß B3S Wasser/Abwasser, Anpassung der Fernzugriffskonzepte, Schulungen) sowie dokumentierten „Lessons Learned“. Der Bericht wird im BSI-Portal hinterlegt und als interner Input für die nächste Überprüfung der Risikoanalyse und des Resilienzplans genutzt.

Checkliste Meldepflicht

1. Vorfall erfassen

1.1. Wurde ein Vorfall festgestellt, der den Betrieb einer kritischen Anlage oder eines kritischen Prozesses (v. a. Wasser-/Abwasser, Leitwarte, zentrale IT-/OT-Systeme) beeinträchtigt oder beeinträchtigen kann?

1.2. Sind Zeitpunkt der Kenntnisnahme, Ort, betroffene Anlagen/IT-Systeme und erste Beobachtungen dokumentiert?

2. Kritische Dienstleistung betroffen

2.1. Betrifft der Vorfall eine als kritisch eingestufte Dienstleistung im Sinne von NIS2/KRITISDachG?

2.2. Führt der Vorfall zu einer erheblichen Betriebsstörung oder ist eine solche plausibel zu erwarten (z. B. Unterbrechung, massive Einschränkung der Versorgung, drohende Grenzwertverletzungen)?

3. Schadenspotenzial bewerten

3.1. Können erhebliche Schäden für Gesundheit, Umwelt, Versorgungssicherheit, Vermögenswerte oder Reputation entstehen?

3.2. Sind gesetzliche oder vertragliche Pflichten (z. B. Einleitergrenzwerte, Versorgungsaufträge) gefährdet?

4. Art des Vorfalls feststellen

4.1. Liegen Anzeichen für einen IT-/OT-Sicherheitsvorfall vor (z. B. Cyberangriff, Malware, Datenmanipulation, Ausfall von Leit-/Fernwirktechnik)?

4.2. Liegt ein physischer Vorfall im Sinne des KRITISDachG vor (z. B. Brand, Explosion, Sabotage, Naturereignis, langandauernder Stromausfall mit wesentlicher Auswirkung auf eine kritische Anlage)?

4.3. Gibt es Hinweise auf rechtswidrige oder böswillige Handlungen (z. B. Erpressung, gezielter Angriff)?

5. Umfang und Dauer abschätzen

5.1. Wie viele Nutzer/Einwohner könnten betroffen sein (abschätzen)?

5.2. Überschreitet der Vorfall voraussichtlich die im BCMS definierten maximal tolerierbaren Ausfallzeiten (BIA) für die betroffenen Prozesse?

5.3. Ist absehbar, dass der Vorfall nicht kurzfristig behoben werden kann (andauernde Störung)?

6. Entscheidung zur Meldepflicht

6.1. Liegt eine erhebliche Betriebsstörung oder ein erhebliches Risiko für Menschen, Umwelt oder wesentliche Vermögenswerte vor?

6.2. Liegen Hinweise auf einen gezielten oder gravierenden IT-/OT-Sicherheitsvorfall vor?
6.3. Wenn eine dieser Fragen mit „Ja“ beantwortet wird: Vorfall als meldepflichtig einstufen und externe Meldung vorbereiten.

7. Meldung fristgerecht auslösen
7.1. Erstmeldung an das BSI-Portal bzw. die gemeinsame BSI/BBK-Meldestelle spätestens innerhalb von 24 Stunden nach Kenntniserlangung veranlassen.
7.2. Ergänzungsmeldung mit aktualisierten Informationen innerhalb von 72 Stunden erstellen.
7.3. Abschlussmeldung mit Ursachen, Auswirkungen und Maßnahmen spätestens innerhalb eines Monats übermitteln.

8. Dokumentation der Entscheidung
8.1. Entscheidung „meldepflichtig ja/nein“, Begründung und beteiligte Personen dokumentieren (z. B. im Incident- oder Krisenprotokoll).
8.2. Vorfall und Bewertung als Input für „Lessons Learned“ und die nächste Aktualisierung von Risikoanalyse, BIA und Resilienzplan nutzen.

Anhang 3: Zusammenfassung des KRITIS-Dachgesetzes

Das KRITIS-Dachgesetz, im Folgenden KRITISDachG, dient der Umsetzung der Richtlinie der EU 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen - der sogenannten „CERRichtlinie“ und soll eine hohe physischen Sicherheit von KRITIS-Anlagen bewirken. Es führt erstmals sektorenübergreifende Mindestvorgaben für den physischen Schutz kritischer Anlagen ein.

Das KRITISDachG wurde am 29. Januar 2026 vom Bundestag verabschiedet und ist seit dem 16. März 2026 in Kraft.

Übersicht Pflichten der KRITIS-Betreiber

- **Registrierungspflicht bei BBK + BSI als zentrale Anlaufstelle** im Sinne des Artikels 8 Absatz 1 des KRITISDachG - **spätestens 3 Monate nach Einstufung**, jedoch **frühestens bis einschließlich 17.07.2026**
- Benennung **24/7-Kontaktstelle** gegenüber BBK + BSI ("jederzeit erreichbar")
- Verpflichtung zum **Risikomanagement**
- Verpflichtung zur Ergreifung von Maßnahmen zur Erhöhung der Resilienz ("**Resilienzplan**") und entsprechende Nachweisverpflichtung („auf Verlangen“)
- **Meldepflichten für Vorfälle** gegenüber BBK + BSI
- **Pflichten der Geschäftsleitung** insbesondere Übernahme der Gesamtverantwortung mit persönlicher Haftung

Registrierungspflicht:

Hinsichtlich der Registrierungspflicht bei BBK und BSI wurde ein gemeinsames Registrierungsportal geschaffen, welches unter folgendem Link abrufbar ist: https://portal.bsi.bund.de/

Wichtig zu wissen: Das Unternehmen muss vor der Registrierung ein ELSTER-Unternehmenszertifikat „Mein Unternehmenskonto“ beantragen. Unter folgendem Link kann dieses beantragt werden: https://info.mein-unternehmenskonto.de/

Kontaktstelle

Die 24/7 – Kontaktstelle und verantwortliche Ansprechpartner kann in Verknüpfung mit einem Bereitschaftsdienst bzw. in Anknüpfung an Schichtpläne erfolgen.

Meldepflicht

Ereignet sich ein Vorfall, der zu einer Beeinträchtigung der Dienstleistung führt, welcher nicht mit normalen Mitteln behoben werden kann, muss innerhalb von 24 h bei der gemeinsam betriebenen Meldestelle des BBK und BSI eine Meldung erfolgen. Dauert der Vorfall länger als 24 h an, muss die Erstmeldung aktualisiert werden. Spätestens einen Monat nach Kenntnis des Vorfalls muss ein ausführlicher Bericht übermittelt werden. Die Erstmeldung muss folgende Informationen umfassen:

- die Anzahl und der Anteil der von dem Vorfall Betroffenen,
- die bisherige und voraussichtliche Dauer des Vorfalls sowie
- das betroffene geografische Gebiet des Vorfalls, unter Berücksichtigung des Umstands, ob das Gebiet geografisch isoliert ist.

Das Meldeverfahren kann noch weiter ausgestaltet werden, hierzu informiert das BBK auf dessen Internetseite.

Risikomanagement

Nach § 12 i.V.m § 11 sind die Betreiber kritischer Anlagen zu einer Risikoanalyse und Risikobewertung verpflichtet. Hierbei sind alle Risiken zu betrachten, die zu einer Unterbrechung der Versorgung führen können. Dabei ist der All-Gefahrenansatz zu beachten, das heißt es müssen naturbedingte, technische oder menschlich verursachte Risiken sowie hybride Bedrohungen, sicherheitsgefährdende oder andere feindliche Bedrohungen einschl. terroristischer Straftaten einbezogen werden.

Um dieser Pflicht entsprechend nachzukommen, muss jeder Betreiber einer kritischen Trinkwasserversorgungsanlage, eines kritischen Trinkwasserversorgungssystems sowie einer kritischen Abwasseraufbereitungsanlage ein prozessorientiertes Risikomanagement durchführen. Hierzu können die BSI-Standards 200-3 und 200-4 hinzugezogen werden. Ausgangspunkt einer jeden Risikoabschätzung ist zunächst die Identifizierung von jeweils für das zu betrachtende Unternehmen relevanten Gefährdungen bzw. Gefährdungsereignissen (Gefährdungsanalyse).

Gemäß § 12 Abs. 3 KRITISDachG wird das BMI per Rechtsverordnung weitere methodische Vorgaben machen.

Resilienzmaßnahmen

Nach § 13 Abs. 1 KRITISDachG sind die Betreiber kritischer Anlagen verpflichtet Maßnahmen zur Gewährleistung ihrer Resilienz umzusetzen. Diese sollten insbesondere einen angemessenen physischen Schutz für Liegenschaften und kritischen Anlagen gewährleisten sowie geeignet sein, um auf Vorfälle reagieren zu können, sie abzuwehren und negative Auswirkungen zu begrenzen sowie nach Vorfällen eine zügige Wiederherstellung der kritischen Dienstleistungen zu gewährleisten. Diese Maßnahmen sollen technisch, wirtschaftlich, sicherheitsbezogen und

organisatorisch verhältnismäßig sein. Der Stand der Technik ist dabei zu beachten und einzuhalten.

Explizit benannt werden Maßnahmen in folgenden Bereichen:

- Bauliche wie technische Sicherung der Liegenschaften (Objektsicherung)
- Überwachung der Umgebung
- Einsatz von Detektionsgeräte
- Zugangskontrollen
- Risiko- und Krisenmanagementverfahren und -protokolle
- Vorgegebene Abläufe im Alarmfall
- Maßnahmen zur Aufrechterhaltung des Betriebs, darunter Notstromversorgung
- Alternative Lieferketten
- Sicherheitsmanagement hinsichtlich der Mitarbeitenden, einschließlich externer Dienstleister
- Schulungen und Sensibilisierung der Mitarbeitenden sowie Übungen

Für die aufzustellenden Resilienzpläne wird das BBK voraussichtlich Vorlagen und Muster auf seiner Internetseite bereitstellen.

Eine ausführliche Beschreibung zum Aufbau eines Resilienzplanes findet sich im Kapitel 5 dieser Anwendungshilfe.

Aufgrund aktueller Ereignisse weisen wir daraufhin, dass bei einer Kollision von Überwachungsmaßnahmen mit dem Datenschutz eine Einzelfallabwägung durchzuführen ist und der Datenschutz dann in den Hintergrund tritt, wenn das Sicherheitsinteresse für eine Vielzahl von Personen höher einzustufen ist als mögliche betroffene Persönlichkeitsrechte, die durch eine Überwachung beeinträchtigt sind; siehe 10 Punkte des BDEW zu Transparenzpflichten.

Dokumentations- und Nachweispflichten

Nach § 16 müssen die Betreiber kritischer Anlagen den zuständigen Behörden nachweisen, dass sie die Resilienzpflichten umgesetzt haben. Hierzu kann das BBK beim BSI Informationen zu bereits nachgewiesenen Maßnahmen einholen und darüber hinaus von den Betreibern weitere Nachweise verlangen, insbesondere den obligatorischen Resilienzplan. Die entsprechenden Nachweise können auch über Audits nachgewiesen werden. Die zuständige Behörde kann auch eine eigene Nachprüfung anordnen, bei der sie einen qualifizierten Dritten zur Prüfung abbestellt. Die Betreiber haben dem Prüfer entsprechend Zugang zu Geschäfts- und Betriebsräumen wie zu notwendigen Dokumenten und Informationen zu gewähren und sind dementsprechend auskunftspflichtig. Aufgedeckte Mängel müssen innerhalb einer

angemessenen Frist beseitigt werden, ein entsprechender Nachweis hierüber ist bei der zuständigen Behörde einzureichen.

Pflichten der Geschäftsleitung

Die Verantwortung für die oben genannten Pflichten liegt nach § 20 KRITISDachG bei der Geschäftsleitung. Sowohl in Bezug auf das KRITISDachG wie auch beim NIS2-UG obliegt die Gesamtverantwortung für das Einhalten aller Pflichten der Geschäftsführung. Sie haftet persönlich für die physische, die Informations- und Cybersicherheit sowie generell für die Resilienz des jeweiligen Unternehmens. Sie muss entsprechend für angemessene präventive wie reaktive Schutz- und Steuerungssysteme sorgen, welche Schadensereignisse bestmöglich verhindern oder minimieren, im Schadensfall ein rasches Wiederherstellen des operativen Betriebes ermöglichen sowie den Erfordernissen in der gesetzgeberisch gebotenen Meldepflicht nachkommen.

Ein weiterer wichtiger Punkt, der durch die Geschäftsführung initiiert und umgesetzt werden muss, ist die Benennung mindestens einer Person im Unternehmen, die die Umsetzung der Pflichten operativ steuert und gegenüber den Behörden als zentraler Ansprechpartner fungiert. Diese Person sollte dann auch die Funktion der verpflichtenden Schadensmeldung bei den zuständigen Meldestellen übernehmen und eine entsprechende 24/7-Erreichbarkeit sicherstellen. Es empfiehlt sich hierfür ebenfalls, eine Stellvertretung zu benennen.

Der Begriff der Geschäftsleitung ist nach der hier vertretenen Auffassung weit zu verstehen es können damit sowohl die Geschäftsführer als auch andere operativ verantwortliche Personen gemeint sein.

Empfehlung: Austausch mit den zuständigen Behörden

Ein regelmäßiger Austausch mit den Sicherheitsbehörden wie der Polizei der Feuerwehr, dem THW und dem Ordnungsamt zu aktuellen Entwicklungen ist essenziell. Objektschutzakten der Sicherheitsbehörden können veraltet oder unvollständig sein. Eine aktive Kommunikation kann dazu beitragen, dass sich der Kenntnisstand bei den Behörden zu den Bedürfnissen und der Situation der Wasserver- und Abwasserentsorgungsunternehmen weiter verbessert und somit stärker in den Fokus rückt. Nachfolgend findet sich eine Übersicht der zuständigen Behörden.

Übersicht zu den zuständigen Behörden als Ansprechpartner für KRITIS-Unternehmen

Übersicht der Sicherheitsbehörden als Ansprechpartner für KRITIS-Unternehmen im Rahmen des KRITIS-Dachgesetzes:

- Bundesministerium des Innern und für Heimat (BMI)
  - Rolle: Strategische Koordination des Schutzes Kritischer Infrastrukturen innerhalb der Bundesregierung und Abstimmung sektorübergreifender Vorgaben und Maßnahmen.
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
  - Rolle: Zuständig für Resilienz und physischen Schutz; gemeinsam mit dem BSI künftig Betrieb eines Online-Meldeportals für Störungen und Vorfälle.
  - Im Gesetz ausdrücklich als zentrale Behörde genannt, zusammen mit weiteren zuständigen Bundes- und Landesbehörden sowie Aufsichtsbehörden.
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - Rolle: Zuständig für IT-Sicherheitsvorgaben und Meldepflichten bei IT-Sicherheitsvorfällen; gemeinsam mit dem BBK Betrieb des Online-Meldeportals.
  - Für KRITIS-Betreiber regelmäßig einer der wichtigsten Ansprechpartner in IT-Sicherheitsfragen.
- Aufsichtsbehörden des Bundes (sektorspezifisch)
  - Rolle: Aufsicht und Umsetzung der gesetzlichen Pflichten in den jeweiligen Sektoren; im KRITISDachG als Teil der zuständigen Behördenlandschaft vorgesehen.
- Zuständige Behörden der Länder
  - Rolle: Mitwirkung an Aufsicht, Umsetzung und Kontrollen nach Landeszuständigkeit; im KRITISDachG ausdrücklich erwähnt.

Für den Sektor Wasser und Abwasser ergeben sich folgende sektorspezifische Ansprechpartner und Zuständigkeiten:

- Bundesamt für Sicherheit in der Informationstechnik (BSI) – KRITIS-Büro
  - Ansprechpartner für IT-Sicherheit, Schwellenwerte/Anlageneinstufung, jährliche Prüfung/Meldung von Änderungen im Sektor Wasser.
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
  - Ansprechpartner für Resilienz und physischen Schutz; bietet sektorspezifische Informationen und Empfehlungen für die Wasserversorgung.
- Gemeinsames Meldeportal von BBK und BSI
  - Zukünftiger zentraler Meldeweg für Störungen und Vorfälle (technisch/physisch).
- Zuständige Landesbehörden
  - Trinkwasserüberwachung und Sicherstellung der Qualität nach EU-Trinkwasserrichtlinie und Infektionsschutzgesetz; konkret sind hierfür die Länder- und

Kommunalbehörden zuständig (z. B. Gesundheitsämter bzw. oberste/obere Wasserbehörden – genaue Bezeichnung variiert je Bundesland).

- Landes-Cyberbehörden (Beispiel)
  - Einige Länder unterhalten spezielle Stellen mit Beratungsangeboten für Wasser-/Abwasserbetriebe, z. B. das Landesamt für Sicherheit in der Informationstechnik (LSI) in Bayern.

Anhang 4: Zusammenfassung des NIS2 Umsetzungs- und Cybersicherheitsstärkung-Gesetzes

Das NIS2UmsG präzisiert und ergänzt die nach dem BSIG bereits bestehenden Pflichten. Es werden auch eine Reihe gänzlich neuer Pflichten eingeführt. Für besonders wichtige und wichtige Einrichtungen geht es dabei insbesondere um folgende Pflichten:

- die Registrierung;
- das Ergreifen von Risikomanagementmaßnahmen;
- die Meldung von erheblichen Sicherheitsvorfällen;
- die Umsetzungs-, Überwachungs- und Schulungspflichten für Geschäftsleitungen.

Betreiber kritischer Anlagen müssen zudem erweiterte Risikomanagementmaßnahmen ergreifen und die Erfüllung von Nachweispflichten umsetzen (vgl. §§ 31, 39 BSIG). Daneben werden bestimmte Bereiche sektorspezifisch geregelt.

Registrierungspflicht

Es obliegt jedem Unternehmen selbst, zu identifizieren, ob es unter das BSIG fällt.

Umfang der Registrierung

Die betroffenen Einrichtungen haben sich gemäß § 33 Abs. 1 BSIG spätestens innerhalb von drei Monaten zu registrieren, nachdem sie erstmals oder erneut unter eine der oben genannten Kategorien fallen oder Domain-Name-Registry-Dienste anbieten. Im Rahmen der Registrierung sind dem Bundesamt für Sicherheit in der Informationstechnik („BSI“) über eine gemeinsam vom BSI und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe („BBK“) eingerichtete Registrierungsmöglichkeit bestimmte Angaben zu übermitteln, insbesondere der Name der Einrichtung, deren Anschrift und aktuelle Kontaktdaten (§ 33 Abs. 1 BSIG). Für Betreiber kritischer Anlagen gelten erweiterte Registrierungspflichten (§ 33 Abs. 2 BSIG).

Darüber hinaus sind bestimmte, in § 60 Abs. 1 S. 1 BSIG genannte Einrichtungen - etwa Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Managed Service Provider oder Managed Security Service Provider mit Hauptniederlassung in der Europäischen Union in Deutschland-, ebenfalls innerhalb von drei Monaten, nachdem sie als eine der vorgenannten Einrichtungen gelten, zur Registrierung beim BSI verpflichtet (§ 34 BSIG).

Registrierungsverfahren

Das BSI sieht für betroffene Einrichtungen ein zweistufiges Registrierungsverfahren vor:

Im ersten Schritt muss eine Registrierung beim digitalen Dienst „Mein Unternehmenskonto“ (MUK) erfolgen. Im zweiten Schritt folgt die Registrierung im neu entwickelten BSI-Portal. Über das BSI-Portal erfolgen anschließend auch Meldungen von IT-Sicherheitsvorfällen.

Erfüllt eine besonders wichtige oder wichtige Einrichtung die Registrierungspflicht nicht, kann das BSI die Registrierung im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde auch selbst vornehmen. In diesem Falle drohen erhebliche Bußgelder, die der Höhe nach an die Datenschutzgrundverordnung angepasst worden sind. Bestehen Anhaltspunkte für eine unterlassene Registrierung, kann das BSI zudem die Vorlage relevanter Unterlagen und Auskünfte verlangen, soweit keine Geheimhaltungs- oder Sicherheitsinteressen entgegenstehen (vgl. § 33 Abs. 3, 4 BSIG).

Praxisempfehlungen

Betroffene Unternehmen sollten insbesondere:

- zeitnah prüfen und dokumentieren, ob sie dem Anwendungsbereich des BSIG unterfallen und welcher Einrichtungskategorie sie zuzuordnen sind;
- einschlägige Veröffentlichungen des BSI fortlaufend berücksichtigen;
- bei grenzüberschreitender Registrierung nationale Besonderheiten beachten.

Risikomanagement

Besonders wichtige und wichtige Einrichtungen sind gemäß § 30 Abs. 1 BSIG verpflichtet, ein angemessenes Risikomanagement umzusetzen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Vorkehrungen zur Bewältigung von Sicherheitsvorfällen zutreffen. Der Begriff der Diensterbringung ist dabei weit zu verstehen.

Zentrale Grundlage des Risikomanagements ist eine regelmäßig durchzuführende Risikoanalyse, mit der Einrichtungen systematisch Risiken für ihre Organisation bewerten und geeignete Schutzmaßnahmen ergreifen, um diese zu abzuschwächen. Bei der Wahl der Methodik sind die Einrichtungen frei. Die Risikoanalyse umfasst insbesondere die Identifikation von Bedrohungen und Schwachstellen, die Bewertung von Eintrittswahrscheinlichkeit und potenziellen Auswirkungen sowie die Überprüfung bestehender Sicherheitsmaßnahmen auf ihre Wirksamkeit. Unzureichende Maßnahmen sind anzupassen und erneut zu bewerten. Die Risikoanalyse ist kontinuierlich durchzuführen und in das Sicherheitsmanagement zu integrieren. Ihre Ergebnisse sowie die umgesetzten Maßnahmen sind nach§ 30 Abs. 1 S. 3 BSIG zu dokumentieren.

Auf Grundlage der Risikoanalyse haben Einrichtungen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen umzusetzen, § 30 Abs. 1 S. 1 BSIG. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen sind das Ausmaß der Risikoexposition,

die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen, § 30 Abs. 1 S. 2 BSIG.

Die Maßnahmen müssen gemäß § 30 Abs. 2 BSIG alle für die Diensterbringung genutzten IT-Systeme, Komponenten und Prozesse erfassen, den Stand der Technik einhalten, die einschlägigen europäischen sowie internationalen Normen berücksichtigen und auf einem gefahrenübergreifenden Ansatz beruhen.

Nach § 30 Abs. 2 S. 2 BSIG sind als Mindestanforderungen - inhaltsgleich mit Art. 21 NIS2-Richtlinie- insbesondere Maßnahmen zur Bewältigung von Sicherheitsvorfällen, zur Aufrechterhaltung des Betriebs, zur Sicherheit der Lieferkette, zur sicheren Entwicklung und Wartung von IT-Systemen, zur Wirksamkeitskontrolle von Risikomanagementmaßnahmen, zur Cyberhygiene und Schulung, zum Einsatz kryptografischer Verfahren sowie zur Nutzung von Multi-Faktor-Authentifizierung umzusetzen.

Nach § 31 Abs. 1 BSIG haben **Betreiber kritischer Anlagen** innerhalb ihrer Einrichtung für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, gegenüber wichtigen und besonders wichtigen Einrichtungen ein nochmals erhöhtes Sicherheitsniveau zu gewährleisten.

Betroffene Unternehmen sollten insbesondere:

- die für die Anpassung der Risikomanagementmaßnahmen relevanten Dienste, Geschäftsprozesse und IT-Systeme identifizieren;
- regelmäßige, dokumentierte Risikoanalysen etablieren und wirksame, verhältnismäßige Risikomanagementmaßnahmen umsetzen und fortlaufend anpassen;
- die Lieferkette in die Risikoanalyse einbeziehen, insbesondere indem Risiken bei Dienstleistern und Lieferanten durch geeignete vertragliche Regelungen zur Cybersicherheit adressiert werden;
- nationale und europäische Rechtsentwicklungen fortlaufend berücksichtigen.

Meldepflichten

Mit dem NIS2UmsG werden die Meldepflichten bei erheblichen Sicherheitsvorfällen in § 32 BSIG deutlich ausgeweitet und konkretisiert. Es wird nunmehr ein mehrstufiger Ansatz für die Meldung erheblicher Sicherheitsvorfälle festgelegt.

Begriff des erheblichen Sicherheitsvorfalls

Ein „erheblicher Sicherheitsvorfall“ liegt vor, wenn ein Sicherheitsvorfall

- 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 (§ 2 Nr. 11 BSIG).

Ein „Sicherheitsvorfall“ ist jedes 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 (§ 2 Nr. 40 BSIG). Eine Konkretisierung des erheblichen Sicherheitsvorfalls enthält die Durchführungsverordnung (EU) 2024/2690, die unionsweit unmittelbar gilt. Sie konkretisiert für bestimmte Arten von Einrichtungen, insbesondere Anbieter digitaler Infrastrukturen und digitaler Dienste, ab wann ein Sicherheitsvorfall als erheblich einzustufen ist.

Ein Sicherheitsvorfall gilt nach der Durchführungsverordnung in Bezug auf die betreffende Einrichtung als erheblich, wenn beispielsweise:

- der Vorfall der betreffenden Einrichtung einen direkten finanziellen Verlust in Höhe von mehr als 500 000 EUR oder 5 Prozent ihres jährlichen Gesamtumsatzes im vorangegangenen Geschäftsjahr - je nachdem, welcher Wert niedriger ist - verursacht hat oder einen solchen Verlust verursachen kann;
- der Vorfall den Tod einer natürlichen Person verursacht hat oder einen solchen Tod verursachen kann; oder
- der Vorfall eine schwere Schädigung der Gesundheit einer natürlichen Person verursacht hat oder eine solche Schädigung verursachen kann. Maßgeblich sind zudem sektorspezifische Kriterien wie Ausfallzeiten, Nutzerbetroffenheit und die Auswirkungen auf die Vertraulichkeit, Integrität oder Authentizität der im Zusammenhang mit der Erbringung eines Dienstes gespeicherten, übermittelten oder verarbeiteten Daten, deren Schwellenwerte je nach Art der Dienstleistung variieren können.

Inhalt und Fristen der Meldungen

§ 32 BSIG regelt ein dreistufiges Meldeverfahren. Betroffene Unternehmen sind im Falle eines erheblichen Sicherheitsvorfalls gemäß § 32 Abs. 1 BSIG verpflichtet,

- unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall eine frühe Erstmeldung einzureichen;
- unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall eine Meldung über diesen Sicherheitsvorfall einzureichen; und

- spätestens einen Monat nach Übermittlung des Sicherheitsvorfalls eine Abschlussmeldung einzureichen, die den Vorfall detailliert erläutert und die Ursachen offenlegt. Dauert der Vorfall zu diesem Zeitpunkt noch an, tritt eine Fortschrittsmeldung an die Stelle der Abschlussmeldung. Die Abschlussmeldung ist dem BSI erst nach abschließender Bearbeitung des Sicherheitsvorfalls.

Eine bereits abgegebene Meldung kann nachträglich nicht storniert oder zurückgezogen werden. Sollte sich der gemeldete Sachverhalt jedoch als unzutreffend oder unvollständig herausstellen, kann er im weiteren Verlauf durch eine Folgemeldung korrigiert oder ergänzt werden.

Darüber hinaus sind dem BSI während des gesamten Zeitraums eines Sicherheitsvorfalls auf dessen Nachfrage Zwischenmeldungen zu übermitteln. Maßgeblich für den Fristbeginn ist der Zeitpunkt der Kenntniserlangung über einen erheblichen Sicherheitsvorfall durch einen Mitarbeiter einer Einrichtung während seiner Arbeitszeit.

Meldestelle und organisatorische Umsetzung

Die Meldestelle für erhebliche Sicherheitsvorfälle ist das BSI-Portal. Meldungen können grundsätzlich durch jede Mitarbeiterin und jeden Mitarbeiter einer Einrichtung abgegeben werden; für diese Personen muss der Zugang zur Meldestelle eingerichtet werden. Alternativ können auch konzerninterne Stellen oder externe Dienstleister zur stellvertretenden Meldungsabgabe bevollmächtigt werden. Die rechtliche Verantwortung für den Sicherheitsvorfall und den Inhalt der Meldung verbleibt jedoch stets bei der betroffenen Einrichtung.

Unterrichtung der Empfänger der Dienste

Wird die Erbringung von Diensten durch besonders wichtige und wichtige Einrichtungen in Folge von aufgetretenen erheblichen Sicherheitsvorfällen beeinträchtigt, kann dies regelmäßig auch zu weiteren- auch mittelbaren - Einschränkungen bei den Empfängern dieser Dienste führen. Dies ist insbesondere dann der Fall, wenn die betroffenen Dienste von den Empfängern zur Erbringung weiterer oder anderer Leistungen für Dritte genutzt werden. Das BSI kann daher gemäß § 35 Abs. 1 S. 1 BSIG im Einzelfall betroffene Einrichtungen anweisen, die Empfänger ihrer Dienste unverzüglich über den erheblichen Sicherheitsvorfall zu unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte. Eine solche Unterrichtung kann auch durch eine Veröffentlichung auf der Internetseite der Einrichtung erfolgen, § 35 Abs. 1 S. 3 BSIG.

Ist zur Verhinderung oder Bewältigung eines erheblichen Sicherheitsvorfalls eine Sensibilisierung der Öffentlichkeit erforderlich oder liegt die Offenlegung anderweitig im öffentlichen Interesse, kann das BSI nach Anhörung der betroffenen Einrichtung diese zur Information der

Öffentlichkeit über den erheblichen Sicherheitsvorfall verpflichten oder die Öffentlichkeit auch selbst informieren (§ 36 Abs. 2 BSIG).

Praxisempfehlungen

Betroffene Unternehmen sollten insbesondere:

- interne Meldeprozesse im Lichte der erweiterten Anforderungen des BSIG anpassen;
- nationale und europäische Rechtsentwicklungen zu den Meldepflichten kontinuierlich berücksichtigen;
- klare Zuständigkeiten für die Abgabe von Meldungen und die Kommunikation mit dem BSI festlegen;
- den ausgewählten Personen einen Zugang zur Meldestelle einrichten;
- Mitarbeitende regelmäßig schulen und sensibilisieren, um meldepflichtige Sicherheitsvorfälle frühzeitig zu erkennen und ordnungsgemäß weiterzuleiten;
- eine strukturierte Dokumentation und Nachbereitung von Sicherheitsvorfällen sicherstellen.

Aufsichtsmaßnahmen und Sanktionen

Das BSI kann besonders wichtige Einrichtungen unter anderem dazu verpflichten, Audits, Prüfungen oder Zertifizierungen durch unabhängige Stellen durchführen zu lassen, um die Einhaltung der Verpflichtungen im Zusammenhang mit Risikomanagement-, Melde- sowie Schulungspflichten zu überprüfen, § 61 Abs. 1 BSIG.

Bei der Ausübung dieser Aufsichtsmaßnahmen in Bezug auf besonders wichtige Einrichtungen ist nicht erforderlich, dass dem BSI Hinweise oder Informationen vorliegen, welche die Annahme rechtfertigen, dass eine Einrichtung die Anforderungen des BSIG nicht oder nicht richtig umgesetzt hat. Die Aufsichts- und Durchsetzungsmaßnahmen sehen unter bestimmten Voraussetzungen als ultima ratio in § 61 Abs. 9 S. 2 Nr. 2 BSIG sogar vor, dass der Geschäftsleitung die Ausübung der Tätigkeit vorübergehend untersagt werden kann.

Zentrale Compliance-Pflichten nach dem BSIG:

Eine detaillierte Übersicht ist abrufbar unter https://ruw-link/2026/38

Praktische Handlungsempfehlung

Die folgenden Hinweise sollen helfen die komplexen Anforderungen weiter einzuordnen und sind als mögliche Handlungsempfehlungen zu verstehen.

Risikoanalyse

Die Risikoanalyse ist ein strukturierter Prozess zur Identifizierung, Bewertung und Behandlung von Informationssicherheitsrisiken, wobei der BSI-Standard 200-3 (IT-Grundschutz) und die ISO 27001 (Informationssicherheits-Managementsysteme, ISMS) die führenden Standards sind. Der BSI-Standard 200-3 liefert eine detaillierte Methodik, die auch für spezifische gesetzliche Anforderungen von NIS-2 relevant ist.

Link: BSI-Standard 200-3, ISO/IEC 27005:2025-01

Konzept zur Behandlung von Sicherheitsvorfällen

Um Schäden zu begrenzen und um weitere Schäden zu vermeiden, müssen erkannte Sicherheitsvorfälle schnell und effizient bearbeitet werden. Dafür ist es notwendig, ein vorgegebenes und erprobtes Verfahren zur Behandlung von Sicherheitsvorfällen zu etablieren. Eine entsprechende Handreichung zur Behandlung von Sicherheitsvorfällen bietet das BSI an.

Link: DER.2.1 Behandlung von Sicherheitsvorfällen

Datensicherungskonzepte erstellen und umsetzen

Backups sind eine der wichtigsten Maßnahmen, um Datenverlust vorzubeugen. Als besondere Herausforderung ist der Datenverlust aufgrund eines Ransomware-Angriffs zu berücksichtigen, da schon vorhandene Backups von einer Infizierung betroffen sein können.

Zur Erstellung und Umsetzung eines Datenssicherungskonzepts bietet das BSI Hinweise.

Link: CON.3 Datensicherungskonzept

Krisenmanagement und Business Continuity Management

Eine Krise im Umfeld kritischer Infrastrukturen wird definiert als eine Situation, in der der Ausfall oder die Beeinträchtigung dieser Infrastrukturen nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen verursachen könnte.

Krisenmanagement umfasst alle Maßnahmen, die ein Unternehmen ergreift, um auf unerwartete, bedrohliche Ereignisse zu reagieren, deren Auswirkungen zu begrenzen und den Normalbetrieb möglichst schnell wiederherzustellen.

Business Continuity Management ist ein ganzheitlicher Managementprozess, der sicherstellt, dass kritische Geschäftsprozesse auch während und nach Störungen funktionsfähig bleiben – durch präventive Planung, Notfallstrategien und Wiederanlaufkonzepte.

Hilfestellung zum Aufbau von Krisen- und Business Continuity Management bieten sowohl das BSI mit dem Standard BSI 200-4 als auch das DIN mit der DIN EN ISO 22361.

Link: BSI 200-4 Business Continuity Management, DIN EN ISO 22361:2021 Krisenmanagement

Risikomanagement

NIS-2 fordert einen ganzheitlichen, gefahrenübergreifenden Ansatz mit umfassenden Cybersicherheitsmaßnahmen, der auf einer regelmäßigen Risikoanalyse basiert.

Die Kernanforderungen an das Risikomanagement lassen sich wie folgt zusammenfassen:

Umfassende Risikoanalyse: Bewertung von Risiken für Netz- und Informationssysteme, unter Berücksichtigung der Größe und Risikobelastung des Unternehmens.

Risikobehandlung: Umsetzung angemessener und wirksamer Maßnahmen zur Risikominimierung.

Regelmäßige Überprüfung: Kontinuierliche Aktualisierung der Analyse und Maßnahmen, besonders bei neuen Bedrohungen oder Schwachstellen.

Dokumentation: Lückenlose Aufzeichnung der Risikoanalyse und der umgesetzten Maßnahmen.

Hinweise zur Umsetzung eines Risikomanagements finden sich wiederum beim BSI und beim DIN.

Link: #nis2know: NIS-2 Risikomanagementmaßnahmen

BSI Standard 200-3 Risikomanagement

DIN ISO 31000 Risikomanagement

Anhang 5: KI-Verordnung und Informationssicherheit

Neben KRITIS DG und NIS2 UG kommt auch der Einhaltung der EU-KI-Verordnung mit Blick auf Informations- und Datensicherheit eine besondere Bedeutung zu, Sie reguliert den sicheren Betrieb sowie die Entwicklung und Einführung von KI-Systemen auf dem europäischen Binnenmarkt. Ziel sind einerseits die Förderungen von Innovationen im europäischen Raum sowie andererseits auch die Schaffung von übergreifenden Standards zur Wahrung von Grundrechten, Gesundheit und Sicherheit in Bezug auf KI-Anwendungen. Verstöße können mit Bußgeldern bis zu 35 Mio. € oder 7 % des weltweiten Jahresumsatzes geahndet werden.

Die Verordnung ist seit dem 1. August 2024 in Kraft und gilt unmittelbar in allen Mitgliedstaaten der EU. Anzuwenden sind die Inhalte nach spätestens 24 Monaten, also ab dem 1. August 2026 mit Ausnahme der Regeln zu verbotenen KI-Praktiken sowie dem Aufbau notwendiger KI-Kompetenz, wenn KI-Systeme im Unternehmen eingesetzt werden. Hier gelten die Festlegungen bereits ab 1. Februar 2025.

Einige zentrale Pflichten sind jedoch von den Mitgliedstaaten umzusetzen, hierzu hat die Bundesregierung am 11.02.2026 das KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG) beschlossen. Hierin wurde die Bundesnetzagentur (BNetzA) als zentral verantwortliche Behörde für KI benannt.

Derzeit wird die EU-KI-Verordnung als Teil des „Digital-Omnibus“ der EU überarbeitet, ein erster Entwurf[40] sieht u.a. Verschiebungen von festgelegten Umsetzungsfristen einzelner Punkte sowie punktuelle Entlastungen von KMU vor. Die finale Verabschiedung bleibt noch abzuwarten. Im Folgenden wird sich auf die aktuell gültige Version (EU) 2024/1689 bezogen.

Risikobasierter Ansatz

Die Verordnung ist gültig für alle Anbieter und Nutzer von KI-Systemen, unabhängig vom Unternehmenssitz oder der Größe des Unternehmens, sofern die KI innerhalb der EU zum Einsatz kommt.

Wenn KI-Systeme im Unternehmen genutzt werden sollen, ist eine Risikoabschätzung des betreffenden Systems gemäß der folgenden Kategorisierung notwendig:

[40] https://cdn.netzpolitik.org/wp-upload/2025/11/EU-Kommission-Digital-Omnibus-B-KI.pdf

1. Verbotene Praktiken:
   Anwendungsfälle, bei denen KI-Systeme für manipulative, ausbeuterische und soziale Kontrollpraktiken eingesetzt werden sollen

3. Hochrisiko KI-Systeme:
   Anwendungsfälle, bei denen KI-Systeme potenziell Einfluss auf die Grundrechte, Gesundheit und Sicherheit von Personen nehmen können, z. B. Systeme, die sicherheitsrelevante Funktionen in Kritischen Infrastrukturen steuern wie digitale Zwillinge, Hochwassermanagement, Leckageerkennung etc.

3. KI-Systeme mit niedrigem Risiko:
   Anwendungsfälle, bei denen KI-Systeme keine Gefährdung von Grundrechten, Gesundheit und Sicherheit von Personen darstellen, aber ein Risiko für Täuschung, Fehlinformation oder Manipulation aufweisen kann, wie bei Chatbots, die nicht aufzeigen, ob die Interaktion mit einem Menschen oder einer Maschine stattfindet.

4. KI-Systeme ohne besonderes Risiko:
   Anwendungsfälle, bei denen KI-Systeme innerhalb sehr limitierter Regeln agieren, um bestimmte Aufgaben zu erfüllen und dabei keine weiteren Risiken aufweisen, wie Spam-Filter in E-Mailprogrammen.

Typische KI-Anwendungen in der Wasserwirtschaft und ihre Risikoeinstufung

Die meisten Unternehmen der Trink- und Abwasserwirtschaft fallen in die Rolle der Betreiber (Nutzer) von KI-Systemen. Branchentypische Anwendungsfälle von KI-Systemen können z. B. in der Überwachung, Optimierung oder Simulation von Betriebsprozessen zum Einsatz kommen (z. B. digitaler Zwilling), bei der Leckage-Erkennung, im Hochwassermanagement oder im Wartungsmanagement. Im Bereich der Office-IT können vor allem generative KI-Systeme zur Unterstützung im Büroarbeitsalltag zum Einsatz kommen.

Grundsätzlich bestimmt sich die Risikoklassifizierung von KI-Systemen anhand ihres beabsichtigten Einsatzzweckes bzw. der Einsatzmodalitäten. Typische Einsatzzwecke im Bereich der Hochrisiko-KI sind u.a. biometrische Fernidentifizierungssysteme, KI-Systeme im Personalmanagement sowie im Bereich von sicherheitsrelevanten Bauteilen oder Prozessen in der Kritischen Infrastruktur. Hierbei kommt es auch immer auf den Grad der Autonomie des betreffenden Systems an sowie auf den Zugriff auf sicherheitsrelevante/sensible Informationen.

Einen Sonderfall stellen KI-Systeme mit allgemeinem Einsatzzweck (General Purpose Artificial Intelligence – GPAI) dar. Dazu zählen die weithin bekannten Sprachmodelle wie ChatGPT, Microsoft Copilot, Google Gemini, Perplexity AI, Claude etc. – Bei der Risikoeinstufung dieser

generativen KI-Systeme kommt es vor allem auf den Zugriff der KI auf sensible Daten/Informationen an und zu welchem Zweck die KI eingesetzt werden soll.

Pflichten für Unternehmen

Die zu erfüllenden Pflichten nach der KI-Verordnung richten sich zunächst nach der jeweiligen Rolle in Bezug auf KI, die im Gesetzestext definiert sind wie z. B. Anbieter, Betreiber, Einführer, Händler oder Produkthersteller.

Sofern KI-Systeme weitestgehend unverändert zum Einsatz kommen, d. h. nicht auf das jeweilige Unternehmen hin angepasst werden oder für spezielle Aufgabe weiterentwickelt werden, ist das betreffende Unternehmen ein „Betreiber“ im Sinne der KI-Verordnung.

Die Pflichten eines Betreibers lassen sich wie folgt zusammenfassen:

- Risikoklassifizierung
  Prüfung, ob das jeweilige KI-System als hochriskant im Sinne der KI-Verordnung einzustufen ist (vgl. Art. 5, 6 & Anhang III KI-Verordnung)

Sofern das Unternehmen zu dem Schluss kommt, dass das betreffende KI-System als hochriskant einzuordnen ist, gelten folgende Pflichten (vgl. Art. 4, 26, 27 & 50 KI-Verordnung):

- Information an betroffene Arbeitnehmer und Betriebsrat:
  Vor der Inbetriebnahme des Hochrisiko-KI-Systems werden betroffene Arbeitnehmer und Arbeitnehmervertreter über den geplanten Einsatz informiert.

- Menschliche Aufsicht:
  Festlegung einer natürlichen Person mit entsprechenden Kompetenzen (Ausbildung, Befugnis), die das KI-System überwacht und Anbieter, Händler oder Marktüberwachungsbehörde bei Fehlfunktionen oder neu identifizierten Risiken informiert

- Datenschutzfolgeabschätzung:
  Gemäß geltender Datenschutzbestimmungen und anhand der Betriebsanleitung muss eine Datenschutzfolgeabschätzung zum Betrieb des KI-Systems erstellt werden

- Grundrechtefolgenabschätzung:
  Beschreibung möglicher Folgen des Einsatzes des KI-Systems auf die Grundrechte von Personen, diese kann die Datenschutzfolgeabschätzung ergänzen

- Risikomanagementsystem
  Einführung eines kontinuierlichen Risikomanagementsystems in Bezug auf das jeweilige Hochrisiko-KI-System

- Schulungen der nutzenden Mitarbeitenden und verantwortliche Fachkräfte
  Sicherstellung eines ausreichenden Maßes an KI-Kompetenz, um das System ordnungsgemäß bedienen zu können

- Ordnungsgemäßer Betrieb:
  Sicherstellung, dass das KI-System nur gemäß Betriebsanleitung betrieben wird

- Zweckmäßige Dateneingabe:
  Kontrolle, dass Eingabedaten (Prompts, Dokumente etc.) nur für den festgelegten Einsatzzweck des KI-Systems eingegeben werden

- Dokumentation:
  Aufbewahrung von Sicherheitsprotokollen von mind. 6 Monaten

- Transparenz:
  Kennzeichnung und Offenlegung, wenn KI mit Menschen interagiert oder KI-generierte Inhalte verbreitet werden

Sofern das Unternehmen zu dem Schluss kommt, dass das betreffende KI-System nicht als hochriskant einzustufen ist, gilt dennoch:

- Schulungen der nutzenden Mitarbeitenden:
  Sicherstellung eines ausreichenden Maßes an KI-Kompetenz, um das System ordnungsgemäß bedienen zu können

- Transparenz:
  Kennzeichnung und Offenlegung, wenn KI mit Menschen interagiert oder KI-generierte Inhalte verbreitet werden

Darüber hinaus empfiehlt sich auch bei nicht hochriskanten KI-Systemen:

- Ordnungsgemäßer Betrieb:
  Sicherstellung, dass das KI-System nur gemäß Betriebsanleitung betrieben wird

- Zweckmäßige Dateneingabe:
  Kontrolle, dass Eingabedaten (Prompts, Dokumente etc.) nur für den festgelegten Einsatzzweck des KI-Systems eingegeben werden

- Information an Betriebsrat/Arbeitnehmervertreter:
  Information zum Einsatzzweck des KI-Systems

Zur Überprüfung, ob ein bestimmtes KI-System als hochriskant einzustufen ist, gibt es Hilfestellungen, wie z. B. den EU AI Act Compliance Checker[41], bei dem die Risikoeinschätzung mittels Fragebogen durchgeführt werden kann:

Empfehlungen zur Nutzung von KI-Systemen aus Perspektive der Informationssicherheit und des Datenschutzes

Kommt ein KRITIS-Unternehmen zu dem Schluss, dass der angestrebte Nutzungsrahmen eines KI-Systems als nicht hochriskant einzustufen ist, da die Nutzung keinen potenziellen Ausfall oder eine signifikante Störung des Betriebs nach sich ziehen kann (siehe auch Erwägungsgrund 55, KI-Verordnung), gelten wie oben beschrieben nur sehr eingeschränkte Pflichten für die Betreiber.

Dennoch empfiehlt es sich zu prüfen, ein freiwilliges Risikomanagement im Hinblick auf Informationssicherheit und Datenschutz für die betreffenden KI-Systeme aufzubauen. Dies kann insbesondere dann sinnvoll sein, wenn GPAI-Systeme wie z. B. Microsoft Copilot in lizensierter Version im Unternehmen genutzt werden sollen und Einfluss auf eine Vielzahl von Office-Prozessen hat und unternehmensinterne Daten verarbeitet.

Hier bestehen theoretische Risiken in Bezug auf die Integrität, die Vertraulichkeit und auch der Verfügbarkeit von Informationen. Potenzielle Fehlfunktionen wie „Halluzinationen“ der KI oder Manipulation von Daten durch ein KI-System sind nicht auszuschließen und sollten daher kontinuierlich beobachtet werden. Außerdem kann nicht gänzlich ausgeschlossen werden, dass die cloudbasierte Informationsverarbeitung der KI-Systeme nicht selbst kompromittiert wird und dadurch dem Betreiberunternehmen ein Schaden entsteht.

Daher empfiehlt sich ein risikobewusster Umgang mit KI-Systemen, auch wenn keine Hochrisiko-KI im Sinne der KI-Verordnung im Einsatz ist. Jeder Einsatz eines KI-Systems sollte vorab vom zuständigen Informationssicherheitsbeauftragten des Unternehmens auf mögliche

[41] https://artificialintelligenceact.eu/de/bewertung/eu-ai-act-compliance-checker/

Risiken überprüft werden. Auch empfiehlt sich ein frühzeitiger Einbezug der Arbeitnehmervertretung/ des Betriebsrates in mögliche betriebliche Absichten der KI-Nutzung, da oftmals auch Rechte von Arbeitnehmenden tangiert sein können.

Mitwirkende der BDEW-Projektgruppe Sicherheit & Resilienz

- Althoff, Dr. Heiko (Emschergenossenschaft und Lippeverband)
- Baurschmid, Dr. Michael (Emschergenossenschaft und Lippeverband)
- Beckord, Jürgen (Rheinisch-Westfälische Wasserwerksgesellschaft)
- Behnisch, Ann-Kathrin (Verband der Bayerischen Energie und Wasserwirtschaft)
- Eichler, Jens (Stadtentwässerung Dresden)
- Exner, Sebastian (Landesverband der Energie- und Wasserwirtschaft Hessen/Rheinland-Pfalz)
- Hasche, Dr. Frank (Hessenwasser)
- Hoche, Henri (Nordwasser)
- Höck, Torsten (Verband für Energie- und Wasserwirtschaft Baden-Württemberg)
- Hüllen, Michael (Emschergenossenschaft und Lippeverband)
- Kleinschmidt, Annika (BDEW Landesgruppe NRW)
- Mattner, Florian (Verband der Bayerischen Energie und Wasserwirtschaft)
- Minor, Lisa (GELSENWASSER Dresden)
- Noll, Fabian (Rheinisch-Westfälische Wasserwerksgesellschaft)
- Putzar, Mario (Verbandswasserwerk Bad Langensalza)
- Rehberg, Dr. Jörg (BDEW)
- Reißmann, Dr. Florian (BDEW Landesgruppe Mitteldeutschland)
- Röstel, Gunda (Stadtentwässerung Dresden)
- Von Fircks, Regina (Wasserwerke Zwickau)
- Wirtz, Dr. Miriam (GELSENWASSER AG)
- Wrede, Dr. Sabine (BDEW)
- Wünsch, Jonathan (Verband für Energie- und Wasserwirtschaft Baden-Württemberg)

Ansprechpartner

Dr. Jörg Rehberg
Fachgebietsleiter
Telefonnummer: +49 30 300 199 1211
E-Mail-Adresse: joerg.rehberg@bdew.de

Dr. Sabine Wrede
Fachgebietsleiterin
Telefonnummer: +49 30 300 199 1523
E-Mail-Adresse: sabine.wrede@bdew.de