Talsperren als kritische Infrastrukturen aus dem Blickwinkel der Cybersicherheit

Vivian Mommert, Lars Schwätzer
Ruhrverband, Essen, Deutschland

Kurzfassung
Cybersicherheit wird für die Wasserwirtschaft mehr und mehr relevant. Durch gesetzliche Anforderungen werden Betreiber von kritischen Infrastrukturen zur Erfüllung des Stands der Technik bei der Informationssicherheit ihrer Anlagen verpflichtet. Neben Anforderungen an die IT-Sicherheit werden auch Anforderungen an die physische Absicherung von kritischen Infrastrukturen gestellt. In dem Beitrag werden Anforderungen aus dem IT-Sicherheitsgesetz 2.0 sowie zu erwartende Anforderungen aus dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz und dem KRITIS-Dachgesetz vorgestellt und eine Empfehlung zur Vorbereitung auf die Umsetzung gegeben.

1. Einleitung

Anpassungen an den Klimawandel fordern die Wasserwirtschaft zu einer klimaresilienteren Aufstellung und sind damit wesentlicher Treiber der Digitalisierung

[18]. Die zunehmende Digitalisierung umfasst auch immer Risiken, insbesondere für die Informationssicherheit. Die Vermeidung von Ausfällen durch Informationssicherheitsrisiken ist ein breites Feld und kann nicht vollständig erreicht werden. Durch die Integration von verschiedenen Sicherheitsebenen und Maßnahmen können Risiken reduziert oder vermieden werden. Vor diesem Hintergrund nimmt die Cybersicherheit eine immer größere Rolle ein [22]. Gleichzeitig wandelt sich die Gefährdungsbeurteilung für kritische Infrastrukturen. Von den vormals überwiegend internen Angreifern und Angreiferinnen auf die Sicherheit von industriellen Steuerungen werden diese immer mehr zu strategischen Zielen für staatliche Angriffe. Die strategische Ausrichtung von Unternehmen der Wasserwirtschaft als Betreiber von kritischen Infrastrukturen zum Schutz vor Cyberangriffen ist somit erforderlich [17].

2. Cybersicherheit in kritischen Infrastrukturen

Die Beschreibung wesentlicher Infrastrukturen, die von Bedeutung für die Allgemeinheit sind, mit dem Begriff der kritischen Infrastrukturen wurde bereits in den 90er Jahren in den USA vorgenommen. Präsident Clinton beschreibt diese als: „Bestimmte nationale Infrastrukturen sind so wichtig, dass ihre Unfähigkeit oder ihre Zerstörung negative Auswirkungen auf die Verteidigung oder die wirtschaftliche Sicherheit der Vereinigten Staaten haben würde.“ [9]. Mit der Definition des Bundesministeriums des Inneren und für Heimat (BMI) in Deutschland werden in der nationalen Strategie zum Schutz Kritischer Infrastrukturen, der KRITIS-Strategie, verschiedene Sektoren als besonders wichtig für das Gemeinwesen beschrieben [4]. Der Sektor Wasser ist mit den Schwerpunkten der Trinkwasserversorgung und Abwasserbehandlung einer der regulierten Bereiche aus der Definition der kritischen Dienstleistungen nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik [13].

In seinem Jahresbericht 2023 zur Lage der IT-Sicherheit in Deutschland stellt das Bundesamt für Sicherheit in der Informationstechnik fest, dass die Zahl der Cyberangriffe und Varianten sowie die dadurch verursachten Schäden zunehmen. Damit ist die Bedrohung für die Informationssicherheit so hoch wie nie zuvor. Den besten Schutz, um dieser Bedrohungslage zu begegnen bietet eine ausgeprägte Cyberresilienz. Dabei geht es darum, die Widerstandsfähigkeit zu erhöhen und Angriffen besser begegnen zu können [24].

Cyberangriffe betreffen nicht nur IT-Systeme und IT-Anwendungen, sondern auch die steuernden Infrastrukturen (englisch: Industrial Control Systems, ICS) und Anlagen. Der Einsatzschwerpunkt von ICS liegt in der Industrie und bei Betreibern von kritischen Infrastrukturen. Im Vergleich zu IT-Infrastrukturen sind die Schadensauswirkungen bei ICS in der Regel mit physischen Schäden und Gefahren für Menschenleben verbunden [3]. Unternehmen der kritischen Infrastrukturen sind damit in besonderem Maße gefordert, ihre Systeme und Anlagen und damit die Bevölkerung vor negativen Auswirkungen durch Ausfälle zu schützen.

2.1. Informationssicherheitsvorfälle bei kritischen Infrastrukturen

Angreifertypen lassen sich nach ihren Motiven, zur Verfügung stehenden Ressourcen und Zielen unterteilen. Diese reichen von wenig ausgebildeten Skript-Kiddies mit geringen finanziellen Ressourcen über Cyberkriminelle mit finanziellen Zielen bis zu staatlich-motivierten Angreifern und Angreiferinnen [1].

Zu den Cybersicherheitsbedrohungen mit der größten Relevanz für den Berichtszeitraum von Juni 2022 bis Juli 2023 zählten nach der Agentur der Europäischen Union für Cybersicherheit (ENISA) Ransomware und die

Bedrohungen gegen die Verfügbarkeit von Systemen. Mittels Ransomware werden Daten verschlüsselt und Lösegeldforderungen für die Wiederherstellung der Daten gefordert. Angriffe auf die Verfügbarkeit von Systemen werden unter dem Begriff Denial of Service (DoS) gefasst. Dieser Ausfall von Systemen kann durch Überlastung, beispielsweise aufgrund von massenhaften Anfragen oder Befehlen erfolgen. Zusätzlich wird eine Zunahme von cyberkriminellen Aktivitäten im Zusammenhang mit dem Krieg in der Ukraine und mit geopolitischem Interesse beobachtet. Dazu zählen Cyberangriffe auf wesentliche Cloud-Dienste und Supply-Chain-Angriffe, bei denen Dienstleister und Hersteller mit einem großen oder wichtigen Kundenstamm zum Ziel werden [10].

Eine Analyse von Angriffen auf kritische Infrastrukturen seit dem Jahr 1999, die einen Ausfall von industriellen Steuerungen verursachten, zeigt eine Zunahme von Angriffen durch staatliche Akteure und organisierte Kriminalität seit dem Jahr 2009. Von den 19 Cyberangriffen im Zeitraum von 2009 bis 2019 wurden 16 Angriffe diesen beiden Angreifertypen zugeordnet. Der letzte Ausfall der kritischen Infrastrukturen in dem Berichtszeitraum, der durch interne Angriffe verursacht wurde, fand im Jahr 2010 statt [20].

Der Sicherheitsvorfall Stuxnet aus dem Jahr 2011 ist ausführlich beschrieben und liefert eine Analyse des Stuxnet-Schadprogramms, welches gezielt für SCADA-Systeme der Firma Siemens entwickelt und für Angriffe auf iranische Atomanlagen genutzt wurde. Als erstes Schadprogramm, welches für die Kompromittierung von industriellen Steuerungen eingesetzt wurde, unterscheidet sich dieses Vorgehen zu den bis dato bekannten Cyberangriffen. Die Fokussierung auf industrielle Steuerungen zur strategischen Beeinflussung von Grundversorgungen und staatlich relevanten Unternehmen bildet die Grundlage für diese Schadsoftware [16].

Als Teil der kritischen Infrastrukturen sind auch Betreiber der Wasserwirtschaft Ziel von Cyberangriffen. Die überwiegende Anzahl der wissenschaftlich analysierten Angriffe bezieht sich auf Ziele in den USA. Zum einen hängt dies mit der verbreiteten Vernetzung zwischen IT- und OT-Komponenten zusammen und zum anderen sind Meldungen zu Cyberangriffen in den USA durch die Regularien der Bundesbehörde, das National Institute of Standards and Technology (NIST), weiterverbreitet als in anderen Ländern [15].

Eine Unterbrechung der Trinkwasserversorgung kann an verschieden Stationen der Wasserwirtschaft erfolgen und liefert damit ein Ziel für terroristische Angriffe [14]. Bei einem europäischen Wasserversorger nutze eine Schadsoftware Ressourcen der industriellen Steuerung, um Cryptomining zu betreiben und sorgte damit für verlangsamte Reaktionszeiten bei den betroffenen Systemen. Andere Ransomware-Vorfälle bei Wasserversorgern aus dem Jahr 2019 zeigen, dass neben IT-, auch OT-Infrastrukturen durch Verschlüsselungstrojaner infiziert wurden und damit zu einem Ausfall der kritischen Dienstleistung führen [15].

Ausfälle und Manipulationen von Steuerungen, IT-Systemen oder Datenübertragungen im Bereich von kritischen Infrastrukturen der Wasserwirtschaft werden immer relevanter und können zu Umwelt- und Personenschäden führen. Um Betreiber kritischer Infrastrukturen zu einem Risikomanagement zu verpflichten, sind auf EU-Ebene und in Deutschland regulatorische Anforderungen an die IT-Sicherheit und die physische Sicherheit festgelegt.

2.2. Regularien zur IT-Sicherheit in der EU und Deutschland

Auf europäischer Ebene werden im Rahmen der EU NIS-Regulierung Mindestanforderungen für den Schutz von Netz- und Informationssystemen in kritischen Infrastrukturen festgelegt, die dann von EU-Mitgliedsstaaten in nationales Recht überführt werden. Im Jahr 2022 ist die neue Fassung der NIS-2-Richtlinie vom europäischen Parlament und des Rates veröffentlicht worden. In der EU NIS2-Richtlinie werden Betreiber kritischer Infrastrukturen nach kritischen und wichtigen Sektoren unterteilt. Die Sektoren Trinkwasser und Abwasser zählen neben acht weiteren Sektoren zu den kritischen Sektoren von Betreibern, die als wesentliche Einrichtungen bezeichnet werden [11].

In Deutschland werden Regularien zum Schutz kritischer Infrastrukturen durch das BMI erarbeitet und durch Bundestag und Bundesrat verabschiedet. Die Überführung der EU NIS2-Richtlinie in nationales Recht ist mit Verabschiedung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, dem IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) im Jahr 2021, in Teilen erfolgt [19]. Bei dem IT-SiG 2.0 handelt es sich um ein Artikelgesetz, mit dem unter anderem das BSI-Gesetz (BSIG) sowie weitere Gesetze beeinflusst werden [23].

Das BSIG regelt die Befugnisse und Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI), um den Anforderungen aus dem europäischen Rechtsrahmen nachzukommen. Das BSI fungiert als zentrale Cybersicherheitsbehörde in Deutschland. Zu den damit verbundenen Aufgaben gehört die Unterstützung von Unternehmen der kritischen Infrastrukturen bei der Verbesserung der Informationssicherheit [13].

Die Identifikation von kritischen Infrastrukturen erfolgt im Rahmen der BSI-Kritisverordnung. Kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes haben eine besondere Bedeutung für das Funktionieren des Gemeinwesens [21].

Das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) basiert auf der EU-Richtlinie NIS2 und hat das Ziel, die Cybersicherheit in Deutschland zu stärken und die Umsetzung der NIS2-Richtlinie sicherzustellen. Derzeit befindet sich das Gesetz in der Ressort- und Verbändeabstimmung und wird bis Oktober 2024 in

Kraft treten. Einem veröffentlichten Diskussionspapier des BMI sind bereits einige Inhalte des neuen Gesetzes zu entnehmen. Unter anderem ist diesem Diskussionspapier zu entnehmen, dass eine Organisation als besonders wichtige Einrichtung zählt, sobald diese ein Betreiber kritischer Anlagen ist. Damit fällt eine Organisation als Wasserversorger oder -entsorger unter Betreiber kritischer Anlagen und die weiteren Schwellwerte sind nicht relevant [5].

2.3. Regularien zur physischen Sicherheit in der EU und Deutschland

Unter dem Begriff der physischen Sicherheit verstehen sich Maßnahmen und Strategien, die physische Assets, Einrichtungen, Personen und Informationen vor unautorisiertem Zugriff, Schäden oder Bedrohungen schützen. Regulatorische Anforderungen zur physischen Sicherheit finden sich auf europäischer Ebene in der Richtlinie (EU) 2022/2557, der EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience / CER-Richtlinie), welche im Januar 2023 in Kraft getreten ist. Um die Resilienz von kritischen Einrichtungen zu stärken, werden im Sinne des All-Gefahren-Ansatzes Naturkatastrophen oder vom Menschen verursachte, unbeabsichtigte oder vorsätzliche Gefährdungen berücksichtigt [12]. Das KRITIS-Dachgesetz (KRITIS-DachG) wird die EU-Richtlinie über die Resilienz kritischer Einrichtungen in nationales Recht überführen und bis Oktober 2024 in Kraft treten. Ziel des Gesetzes ist es bundeseinheitliche Regelungen für den physischen Schutz kritischer Infrastrukturen festzulegen und somit die Resilienz der Wirtschaft und dadurch auch die Versorgungssicherheit der Bevölkerung zu stärken. Für das KRITIS-DachG ist das das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) die zentrale Anlaufstelle [5].

Bei der Erstellung dieses Beitrags lag ein Referentenentwurf des KRITIS-DachG mit Stand vom 21.12.2023 vor, auf den hier eingegangen wird. Die Entwurfsfassung sieht vor, dass Betreiber kritischer Anlagen durch das KRITIS-DachG und seiner zugehörigen Rechtsverordnungen bestimmt werden. Eine Anlage, die dem Sektor Trinkwasser oder Abwasser zugeordnet ist und einen Schwellenwert von 500.000 zu versorgenden Einwohnern überschreitet, gilt damit als kritische Anlage [2].

2.4. gesetzliche Anforderungen an die Umsetzung und Nachweiserbringung

Derzeit legt das IT-Sicherheitsgesetz 2.0 fest, dass Betreiber von kritischen Infrastrukturen den aktuellen Stand der Technik in Bezug auf Informationssicherheit einhalten müssen. Dies beinhaltet sowohl präventive als auch reaktive Maßnahmen zur Gewährleistung von Sicherheit und Resilienz gegenüber Cyberangriffen. Betreiber müssen die Vermeidung von Störungen der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität in der Erbringung der kritischen Dienstleistung durch angemessene technische und organisatorische Maßnahmen sicherstellen. Im Fokus steht dabei der Schutz von informationstechnischen Systemen, Komponenten und Prozessen, die für die Aufrechterhaltung der kritischen Dienstleistung erforderlich sind. Beim BSI ist dazu die Umsetzung nach dem „Stand der Technik“ nachzuweisen [13].

Mit dem NIS2UmsuCG werden konkrete Maßnahmen an die Umsetzung der IT-Sicherheit gestellt. Der „Stand der Technik“ ist weiterhin gefordert und wird durch Mindestanforderungen erweitert. Darin enthalten sind Verpflichtungen zum Risikomanagement, zum Notfallmanagement, zum Einsatz von Systemen zur Angriffserkennung und weitere technische sowie organisatorische Maßnahmen. Die Umsetzung der Maßnahmen muss dem BSI durch Audits, Prüfungen oder Zertifizierungen nachgewiesen werden [5].

Die Umsetzung des KRITIS-DachG fordert von Betreibern einer kritischen Dienstleistung eine resiliente Aufstellung. Darunter wird die Fähigkeit einen Vorfall zu vermeiden und diesen zu behandeln verstanden. Betreiber sind verpflichtet einen Resilienzplan zu erstellten. In diesem sind Risikoanalysen und Risikobewertungen durchzuführen und technische, organisatorische und sicherheitsbezogene Maßnahmen umzusetzen (Diskussionspapier).

2.5. Umsetzung für Betreiber von Talsperren

Betreiber von wasserwirtschaftlichen Anlagen aus dem Sektor Trinkwasser werden ab Oktober 2024 unter das NIS2UmsuCG und, bei einer Anlagengröße über 500.000 Einwohnerwerten, zusätzlich unter das KRITIS-DachG fallen. Der Betrieb von Informationssicherheitsmanagement, Risikomanagement und Notfallmanagement sind demnach durch alle Betreiber nachzuweisen. Für den Nachweis zur Umsetzung des „Stand der Technik“ in Bezug auf die Informationssicherheit können branchenspezifische Sicherheitsstandards (B3S) oder der IT-Grundschutz des BSI genutzt werden. Der B3S Wasser/Abwasser wird alle zwei Jahre von der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V. (DWA) und vom Deutschen Verein des Gas- und Wasserfaches e. V. (DVGW) erarbeitet und durch das BSI als Prüfgrundlage zur Nachweiserbringung zugelassen. Branchenunabhängig steht der IT-Grundschutz des BSI zur Verfügung. Der IT-Grundschutz besteht aus den Grundschutz-Standards und dem Grundschutz-Kompendium. In den Standards werden Methoden und Prozesse zum Aufbau von Informationssicherheit beschrieben. Das Grundschutz-Kompendium definiert konkrete Anforderungen und technische, organisatorische und personelle Maßnahmen zur Informationssicherheit.

Mit dem Aufbau eines Informationssicherheitsmanagementsystems (ISMS) wird ein Sicherheitsprozess etabliert, um kontinuierlich die Absicherung des betrachteten Unternehmensbereichs zu verbessern. Die Methodik des IT-Grundschutzes führt zunächst eine Strukturanalyse zur Erfassung des IST-Zustandes und im

Anschluss eine Schutzbedarfsfeststellung durch. Darauf aufbauend werden Sicherheitsanforderungen an organisatorische und technische Themen mit Hilfe der zur Verfügung gestellten IT-Grundschutz Bausteine modelliert. Die Anforderungen aus den Bausteinen werden dann mit dem Umsetzungsstand abgeglichen, um Abweichungen zu identifizieren. Für Bereiche des Unternehmens, die in der Strukturanalyse als besonders schützenswert eingestuft wurden, wird eine Risikoanalyse durchgeführt. Die Ergebnisse aus dem Umsetzungsstand und der Risikoanalyse werden in einem Realisierungsplan mit Maßnahmen versehen, um Risiken zu behandeln [6].

Konkrete Maßnahmen, die bereits aus dem Diskussionspapier zum NIS2UmsuCG hervorgehen, sollten geplant und umgesetzt werden. Dazu zählt neben dem Aufbau eines ISMS und Risikomanagements auch das Notfallmanagement, Lieferketten- und Beschaffungsrichtlinien, Konzepte zur Kryptographie, Schulungen und Sicherheit von Personal, sowie technische Maßnahmen zur Authentifizierung und Absicherung der Kommunikation.

Zum Managen von Risiken bietet der BSI-Standard 200-3 eine Beschreibung der Methodik. Die Liste von elementaren Gefährdungen liefert branchenübergreifend die Ausgangslage zur Gefährdungsübersicht. Diese Liste enthält wesentliche Bedrohungen, deren Relevanz für das Unternehmen gemeinsam mit weiteren Bedrohungen ermittelt wird. Mit dieser Einschätzung erfolgt eine Gefährdungsübersicht für das Unternehmen. Im Rahmen der Risikoeinstufung werden Bewertungskriterien festgelegt, anhand derer Risiken im Folgenden bewertet werden. Eine Kenngröße für den Handlungsbedarf stellt der Risikoappetit dar. Dieser beschreibt, ab welcher Einstufung Risiken behandelt werden und welche Risiken unbehandelt akzeptiert werden. Der Risikoappetit variiert für jedes Unternehmen, je nach Risikobereitschaft der Unternehmensleitung und der -branche. Die Behandlungsoptionen von Risiken umfassen neben der Akzeptanz auch die Reduzierung, die Transferierung und die Vermeidung. Innerhalb des zugrundeliegenden Sicherheitsprozesses werden die identifizierten Risiken demnach durch Maßnahmen behandelt oder akzeptiert [7].

Für die Durchführung von Risikoanalysen kann der BSI-Standard 200-3 genutzt werden, solange durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe keine Vorlagen und Muster zur Risikoanalyse vorgegeben sind.

Konkrete Maßnahmen, die bereits im KRITIS-DachG genannt werden, sollten konsolidiert werden. Dazu zählen Maßnahmen der Notfallvorsorge und Anpassung an den Klimawandel, Maßnahmen des Objektschutzes, wie das Aufstellen von Zäunen und Sperren, Überwachung der Umgebung, Einsatz von Detektionsgeräten und Zugangskontrollen, Risiko- und Krisenmanagementverfahren und -protokolle und Alarmpläne, Notfallvorsorgemaßnahmen sowie Schulungen und Übungen.

Sowohl im NIS2UmsuCG als auch im KRITIS-DachG sind Notfallvorsorgemaßnahmen, Alarmpläne und Wiederanlaufpläne gefordert. Diese liefern die sogenannte letzte Verteidigungslinie bei Sicherheitsvorfällen. Dabei werden präventive Maßnahmen ergriffen, die bei einem Sicherheitsvorfall das Ausmaß des Schadens so gering wie möglich halten. Eine wesentliche Maßnahme sind dazu Reaktions- und Wiederherstellungspläne. Industrielle Standards und Anforderungen von Regierungen zur Informationssicherheit lassen sich zusammengefasst in vier Phasen unterteilen. Die Planung einer Notfallvorsorge umfasst die Identifizierung von kritischen Prozessen sowie Festlegung von Rollen und Verantwortlichkeiten im Schadensfall. In der Vorbereitungsphase werden Notfallübungen und Tests durchgeführt. In vielen Standards zählt auch die Erkennung von Angriffen zu dieser Phase. Während des Vorfalls steht die Information von relevanten Personen, die Eindämmung des Vorfalls und die Wiederherstellung an. In der Nachbereitung wird dann ein Lessons-learned durchgeführt [20].

Eine Orientierung zum Aufbau eines erweiterten Notfallmanagements, welches unter dem Begriff Business Continuity Managements (BCM) gefasst wird, bietet das BSI in dem Standard 200-4. Darin werden Methodiken eines Notfallmanagements und eines Notfallvorsorgekonzepts beschrieben, die reaktiv und präventiv zur Aufrechterhaltung des Geschäftsbetriebs genutzt werden können. Die Ereignisvorsorge und Ereignisreaktion als Teilprozesse eines BCM beschreiben die konzeptionelle Vorbereitung von Unternehmen auf Ausfälle und Unterbrechungen, die beispielsweise aus Cyberangriffen resultieren [8].

3. Zusammenfassung

Cybersicherheit gewinnt immer mehr Relevanz im Bereich der kritischen Infrastrukturen. Vor diesem Hintergrund sind für Oktober 2024 weitreichende gesetzliche Änderungen angekündigt, die von Betreibern kritischer Infrastrukturen umzusetzen sind. Die Diskussionspapiere und Referentenentwürfe zum NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz sowie zum KRITIS-Dachgesetz legen Vorgaben für Betreiber von kritischen Infrastrukturen fest. Dabei werden sowohl Anforderungen an IT-Sicherheit und physische Sicherheit gestellt. Diese Anforderungen umfassen technische, organisatorische und personelle Maßnahmen.

Betreiber sollten sich frühzeitig mit den neuen Anforderungen beschäftigen, eine Sicherheitsstrategie aufbauen und Vorsorgemaßnahmen treffen, um Talsperren vor IT-Sicherheits- und physischen Gefahren zu schützen und, um im Schadensfall handlungsfähig zu sein.

Die vollständige Umsetzung der Anforderungen benötigt Ressourcen und eine umfangreiche Planung. Betreiber sollten daher zyklisch vorgehen, einen kontinuierlichen Verbesserungsprozess aufbauen und ihr Sicherheitsniveau verbessern.

Literaturverzeichnis

[1] Ablon, L. (2018) Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. RAND Corporation. Verfügbar unter: https://doi.org/10.7249/CT490.

[2] AG KRITIS (2024), Stellungnahme zum Ref-E des Kritis Dachgesetz [online], https://ag.kritis.info/2024/01/24/stellungnahme-zum-ref-e-des-kritisdachgesetz/ [14.02.2024]

[3] Bhamare, D. et al. (2020) 'Cybersecurity for industrial control systems: A survey', Computers & Security, 89, p. 101677. Verfügbar unter: https://doi.org/10.1016/j.cose.2019.101677.

[4] Bundesministerium für Inneres und Heimat (BMI): Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). BMI09324. p. 20. (2009) [online] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=4 [14.02.2024].

[5] Bundesministerium des Innern und für Heimat (2023): Diskussionspapier des Bundesministeriums des Innern und für Heimat für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland, [online] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/diskussionspapier-NIS-2-umsetzung.html [14.02.2024]

[6] Bundesamt für Sicherheit in der Informationstechnik (2017) 'BSI-Standard 200-2, IT-Grundschutz-Methodik. [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2 [14.02.2024]

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI b, 2017) 'BSI-Standard 200-3, Risikoanalyse auf der Basis von IT-Grundschutz'. [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2 [14.02.2024]

[8] Bundesamt für Sicherheit in der Informationstechnik (2023) 'BSI-Standard 200-4, Business Continuity Management'. [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8, [14.02.2024]

[9] Clinton, W.J. (1996) Executive Order 13010 of July 15, 1996 'Critical Infrastructure Protection', 37347. [online] https://www.govinfo.gov/content/pkg/FR-1996-07-17/pdf/96-18351.pdf [14.02.2024].

[10] ENISA (2023) ENISA Threat Landscape 2023. European Union Agency for Cybersecurity, ENISA. [online] ENISA Threat Landscape 2023 — ENISA (europa.eu), DOI: 10.2824/782573, [14.02.2024]

[11] European parliament and the council of the European Union (2022): Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, [online] https://eur-lex.europa.eu/eli/dir/2022/2555 [14.02.2024]

[12] European parliament and the council of the European Union (2022): Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC, [online] https://eur-lex.europa.eu/eli/dir/2022/2557/oj [14.02.2024]

[13] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik - BSI-Gesetz (BSIG) (2021). [online] https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf [14.02.2024]

[14] Gleick, P.H. (2006) 'Water and terrorism', Water Policy, 8(6), pp. 481–503. Verfügbar unter: https://doi.org/10.2166/wp.2006.035.

[15] Hassanzadeh, A. et al. (2020) 'A Review of Cybersecurity Incidents in the Water Sector', Journal of Environmental Engineering, 146(5), p. 03120003. Verfügbar unter: https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686.

[16] Langner, R. (2011) 'Stuxnet: Dissecting a Cyberwarfare Weapon', IEEE Security & Privacy Magazine, 9(3), pp. 49–51. Verfügbar unter: https://doi.org/10.1109/MSP.2011.67.

[17] Miller, T. et al. (2021) 'Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems', International Journal of Critical Infrastructure Protection, 35, p. 100464. Verfügbar unter: https://doi.org/10.1016/j.ijcip.2021.100464.

[18] Müller-Czygan, G. et al. (2022) 'Die deutschsprachige Wasserwirtschaft im Jahr 2020/21 – Metastudie „WaterExe4.0" zeigt Erfolgsfaktoren und Erwartungen für die digitale Zukunft auf', Österreichische Wasser- und Abfallwirtschaft [Preprint]. Verfügbar unter: https://doi.org/10.1007/s00506-022-00850-z.

[19] Schmitz-Berndt, S., Chiara, P. G., (2022). One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. Verfügbar unter: https://doi.org/10.1365/s43439-022-00058-7

[20] Staves, A. et al. (2022) 'A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems', International Journal of Critical Infrastructure Protection, 37, p. 100505. Verfügbar unter: https://doi.org/10.1016/j.ijcip.2021.100505.

[21] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) (2023). [online] https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html, [14.02.2024]

[22] Zimmermann, M., Schramm, E. and Ebert, B. (2020) 'Siedlungswasserwirtschaft im Zeitalter der Digitalisierung: Cybersicherheit als Achillesferse', TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, 29(1), pp. 37–43. Verfügbar unter: https://doi.org/10.14512/tatup.29.1.37.

[23] Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – IT-Sicherheitsgesetz2.0 (IT-SiG 2.0) (2021). [online], http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf, [14.02.2024]

[24] 2023: Bundesamt für Sicherheit in der Informationstechnik (BSI) (2023), Die Lage der IT-Sicherheit in Deutschland 2023, [online], https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7 [14.02.2024]