Talsperren als kritische Infrastrukturen aus dem Blickwinkel der Cybersicherheit

Vivian Mommert
Ruhrverband, Essen, Deutschland

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. In dem Beitrag werden die Methodik und Erfahrungen des Ruhrverbands bei der Vorbereitung auf die Anforderungserfüllung, sowie ein Ausblick auf die gesetzlichen Änderungen geben.

Anpassungen an den Klimawandel fordern die Wasserwirtschaft zu einer klimaresilienteren Aufstellung und sind damit wesentlicher Treiber der Digitalisierung. Dabei nimmt die Cybersicherheit eine immer größere Rolle ein. 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. Mit der Definition des Bundesministeriums für Inneres und 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. Gemäß § 2 Absatz 10 BSI-Gesetz sind Kritische Infrastrukturen im Sinne dieses Gesetzes Einrichtungen, Anlagen oder Teile davon, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 BSIG (BSI-Kritisverordnung) näher bestimmt. Der Sektor Wasser ist mit der Trinkwasserversorgung und Abwasserbehandlung einer der regulierten Bereiche aus der Definition der kritischen Dienstleistungen. Welche Einrichtungen, Anlagen oder Teile als Kritische Infrastrukturen im Sinne des BSI-Gesetzes gelten, wird durch die BSI-Kritisverordnung definiert. Ob ein bedeutender Versorgungsgrad vorliegt, ist vom Erreichen oder Überschreiten von in der BSI-Kritisverordnung aufgeführten Schwellenwerten abhängig. Werden diese Schwellenwerte erreicht oder überschritten, gelten für KRITIS-Betreiber die gesetzlichen Melde- und Nachweispflichten des BSI-Gesetzes.

Der Ruhrverband ist als Betreiber kritische Infrastrukturen beim Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet und verpflichtet alle zwei Jahre einen Nachweis über die Einhaltung des Standes der Technik zum Schutz der kritischen Dienstleistung vor Ausfällen einzureichen. Für kritische Dienstleistungen, die unter die regulatorischen Anforderungen fallen, muss der Ruhrverband nachweisen, dass ein angemessener Stand der Informationssicherheit eingehalten und die Dienstleistungen ausreichend geschützt sind. Für die Wassermenge, aber auch für den gesamten Ruhrverband sind daher einige Sicherheitsmaßnahmen erforderlich. Die Vorbereitung auf den Nachweis und die Umsetzung von Maßnahmen lässt sich nicht durch den normalen Betrieb stemmen, zumal die Vorbereitung abteilungsübergreifend erfolgt. Aus diesem Grund gibt es ein Projekt, in dem das erste Audit vorbereitet wird. Informationssicherheit hat das Ziel, zu schützen, was für den Ruhrverband von Wert ist, indem alle Informationen, Daten und Werte (unabhängig davon, ob sie IT-gestützt oder manuell verarbeitet im Unternehmen vorhanden sind) in ihrer Verfügbarkeit gesichert werden. Um dieses Ziel zu erreichen, wird ein Informationssicherheitsmanagement-System (ISMS) aufgebaut. Bei der Methodik wendet der Ruhrverband die Standards und den IT-Grundschutz des BSI an. In den regulierten Unternehmensbereichen werden zunächst Geschäftsprozesse beschrieben, deren Schutzbedarf ermittelt und Risiken identifiziert. Im Rahmen des Risikomanagements erfolgt im Anschluss die Behandlung der Risiken durch angemessene Maßnahmen.

Durch die Auditierung und bei der anschließenden Nachweisprüfung durch das BSI erfolgt keine Zertifizierung. Es ist demnach nicht möglich die Prüfung nicht zu bestehen. Dennoch werden die Mängel und Abweichungen aus dem Audit dem BSI gemeldet und müssen vom Betreiber in einem Maßnahmenplan behandelt werden.

Die derzeitigen gesetzlichen Rahmenbedingungen werden im Jahr 2024 durch zusätzliche und angepasste Gesetze ergänzt. Auf europäischer Ebene sind mit der Verabschiedung der NIS2-Richlinie und der CER-Richtlinie bereits Regelungen erlassen, die bis Oktober 2024 in nationales Recht überführt werden müssen. Für die Umsetzung der NIS2-Richtlinie ist in Deutschland das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz geplant. Darin werden Anforderungen an die IT- und Informationssicherheit gestellt. Die Umsetzung der CER-Richtlinie erfolgt über das KRITIS-Dachgesetz, welches Anforderungen an die Resilienz und den physischen Schutz von Anlagen stellt.