Quelle: VPales/shutterstock.com

KRITIS oder nicht? Was für eine Frage!

Die Versorgung mit Trinkwasser ist für die Bevölkerung lebensnotwendig und von zentraler Bedeutung, sodass die entsprechenden Anlagen und Einrichtungen der Wasserversorgungsunternehmen in Deutschland zur sogenannten kritischen Infrastruktur zählen. In den letzten Jahren ist zu beobachten gewesen, dass sich neben physischen Bedrohungen insbesondere die Gefährungslage durch Cyberangriffe stetig verschärft hat. Der Fachbeitrag erläutert in diesem Zusammenhang konkrete Schutzmaßnahmen für die Wasserwirtschaft und geht auf verschiedene Sicherheitsindikatoren ein.

von: Manfred Godek (Monheim)

Ein Großteil der deutschen Wasserwerke würde nur geringen Sicherheitsstandards unterliegen – so berichtete eine große Wirtschaftszeitung Ende September 2020. Sie bezog sich auf einen Bericht des Bundesinnenministeriums, nach dem von den insgesamt 5.748 Wasserversorgern in Deutschland nur 47 als sogenannte kritische Infrastruktur gelten, weil sie den Schwellenwert von 22 Mio. Kubikmetern verteilter Wassermenge pro Tag überschreiten [1]. Auf diese Weise entstand der Eindruck, dass nur 0,8 Prozent der deutschen Wasserversorger geschützt sind und alle anderen diese Aufgabe sträflich vernachlässigen. In der Folge entbrannte ein regelrechter Shitstorm, vor allem in den sozialen Medien.

Bekanntlich ist eine gute Kommunikation keine Stärke der Berliner Ministerialbürokratie und Nachrichten verbreiten sich im Netz meistens ungeprüft. Der genannte Schwellenwert steht in der KRITIS-Verordnung des Bundesamts für Sicherheit in der Informationstechnik und legt damit nur fest, für welche KRITIS-Betreiber gesetzliche Anforderungen in Bezug auf die IT-Sicherheit der IT-Infrastruktur vorgegeben werden. Der Bevölkerungsschutz reicht aber über den eng gesetzten Rahmen des IT-Sicherheitsgesetzes weit hinaus. Notfallsysteme in der Gefahrenabwehr, dem Bevölkerungsschutz

oder im Bereich der Infrastrukturen auf der regionalen und lokalen Ebene seien von ihm genauso wenig erfasst wie die Sektoren Öffentliche Verwaltung sowie Kultur und Medien, betont das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK). „Der umfassende Schutz von KRITIS ist eine gemeinschaftliche Aufgabe von Bund, Ländern, Kommunen und privaten Unternehmen. Aber auch die kreisangehörigen Gemeinden haben die Aufgabe, den Schutz kritischer Infrastrukturen zu gewährleisten, wenn diese in ihren Zuständigkeitsbereich fallen“, betont Wolfram Geier, Leiter der Abteilung Risikomanagement beim BKK [2].

Konkrete Maßnahmen

Das BBK hilft Kreisen und Kommunen dabei, kritische Infrastrukturen zu identifizieren und Notfallpläne aufzustellen bzw. zu optimieren. Für den Sektor Wasser bieten u. a. die Leitfäden „Schutz Kritischer Infrastrukturen – Identifizierung in sieben Schritten“ (BBK, März 2019) und „Sicherheit der Trinkwasserversorgung“ (BBK, September 2019) Arbeitshilfen. Speziell zur IT-Sicherheit gibt der Branchenstandard „IT-Sicherheit Wasser/Abwasser“ (B3S WA) konkrete organisatorische und technische Empfehlungen. Ein Blick in die Praxis zeige, dass sich mittlerweile immer mehr Wasserversorgungsunternehmen, die unter den in der BSI-KritisV festgelegten Schwellenwerten liegen, intensiv mit den Inhalten des Leitfadens auseinandersetzten oder alternative Wege zur Verbesserung der Sicherheit beschritten, so Alexander Faulhaber, Partner des internationalen Beratungs- und Wirtschaftsprüfungsunternehmens Rödl & Partner, Mitautor verschiedener Benchmark-Studien. Anhaltspunkte hierfür ließen sich zumindest mit Blick auf die Entwicklung der IT-Kosten von Wasserversorgungsunternehmen finden, die sich regelmäßig an landesweiten Kennzahlenvergleichen der Branche beteiligen.

„Wir unterziehen sämtliche Standorte und Wasseranlagen einer Risikobetrachtung, also nicht nur diejenigen, die den gesetzlichen Schwellenwert erreichen“, sagt auch Nora Weinhold, Presse- und Mediensprecherin der Sachsen Energie AG. Es erfolgten regelmäßig externe Sicherheits-Audits, um diese Anlagen, die Informations- und Fernwirktechnik sowie Schnittstellen und Dienstleistungen optimal schützen zu können. Dazu gehörten die physische Sicherheit durch eine Zutrittsüberwachung/-kontrolle (beispielsweise durch Kamera, Pförtner oder fernwirktechnische Überwachung), Notfallplanungen, IT-Sicherheit und die regelmäßige Kontrolle der Netzstrukturpläne.

Auch wenn alle Welt zurzeit vor allem über Cyber-Sicherheit spricht: Objektsicherung hat höchste Priorität. Netzwerke können durch Einbrecher oder Innentäter beispielsweise mittels infizierter USB-Sticks lahmgelegt werden und Wasser lässt sich bekanntlich auch von Hand vergiften. Nicht ohne Grund werden in den Fachschriften und Leitfäden des DVGW Objektsicherungen von Brunnen als exemplarische Beispiele herausgestellt, und auch für die technischen Schutzmaßnahmen gibt es konkrete und praxisorientierte Handlungsempfehlungen wie z. B. das DVGW-Merkblatt W 1001 und die DVGW-Information WASSER Nr. 80.

Vernetzte Systeme

„Was den öffentlichen Sektor angeht, sind Versorgungsunternehmen in puncto Sicherheitsarchitektur in letzter Zeit sehr aktiv. Vermutlich hat auch die Pandemie dazu beigetragen, denn sie hat das Bewusstsein dafür geschärft, wie lebenswichtig kritische Infrastrukturen sind“, so Dr. Urban Brauer, Geschäftsführer des BHE Bundesverband Sicherheitstechnik e. V. Ihr Schutz werde als Daueraufgabe erkannt. Beim Cyber-Schutz änderten sich die Anforderungen ohnehin geradezu im Stundentakt. Mechanische und elektronische Sicherheitstechnik wird dagegen langfristig geplant, etwa im Jahresrhythmus überprüft und angepasst. Das richtige Konzept, so banal das auch klingt, ist entscheidend für die Effektivität auf Dauer.

INFORMATIONEN

Übersicht: Schutzmaßnahmen vor Vandalismus, Sabotage und Angriff

- mechanisch: Einzäunung des Geländes, einbruchhemmende Ausführung aller Einstiege und Zugänge, Sicherung des Zugangs durch Schließanlage
- elektronisch: Perimetersicherheit zur Grundstücksüberwachung, Videosicherheit, Einbruchmeldeanlagen mit Öffnungskontakten an Türen und Fenstern sowie Bewegungsmeldern, Zutrittssteuerung, Überwachung von Sensoren, Aktoren und Übertragungsleitungen hinsichtlich Manipulation
- personell: personelle Zugangsbeschränkung, Begehungen, Plausibilitätsprüfungen von Messsignalen und Aktionen der automatischen Prozesssteuerung
- organisatorisch: Festlegung der Weiterschaltung von Alarmmeldungen, Festlegung von automatischen oder manuellen Handlungen im Alarmfall, Erstellen von Verfahrens- und Arbeitsanweisungen

INTERVIEW

»Das Risikomanagement sollte bei der Geschäftsführung aufgehängt sein.«

Im Gespräch mit Ellen Frings, Leiterin Unternehmenskommunikation bei der Stadtwerke Heidelberg GmbH

Frau Frings, wie sind Sie im Bereich Objektschutz aufgestellt?

Ellen Frings: Organisatorisch gehört diese Aufgabe zu der Abteilung, die für den Bau und die Instandhaltung von Gebäuden zuständig ist. Aspekte des Objektschutzes werden dort in den anstehenden Planungen und Maßnahmen gleich integriert. Ein besonderes Budget gibt es aufgrund dieses integrierten Ansatzes nicht. Zudem hat die technische Gesellschaft des Stadtwerke Heidelberg-Konzerns, die Stadtwerke Heidelberg Netze, in den vergangenen Jahren das Konzept für Schließanlagen – Organisation, Technik und Berechtigungen – neu aufgestellt. Für diese Aufgabe, aber auch für das Thema Videoüberwachung haben wir externe Expertise eingebunden. Wichtig dabei ist: Das Konzept wurde von höchster Managementebene beauftragt und auch dort verabschiedet. Ein weiterer Erfolgsfaktor: Die Mitarbeitendenvertretung war von Beginn an eingebunden. Parallel wurden selbstverständlich die Anforderungen des Datenschutzes und des Informationssicherheitsmanagements berücksichtigt.

Quelle: Stadtwerke Heidelberg GmbH

Wie ist Ihr Risikomanagement organisatorisch verankert?

Frings: Mit einer Stabsstelle mit dem Titel „Unternehmensentwicklung/Risikomanagement“ direkt unterhalb der Konzern-Geschäftsführung. Darüber hinaus gibt es Risikomanager in den einzelnen Gesellschaften, so auch bei den Stadtwerken Heidelberg Netze, die aus technischer Sicht für KRITIS zuständig ist. Ihnen arbeiten Risikobeauftragte aus den Abteilungen der jeweiligen Gesellschaft zu, denn jede Abteilung ist dafür zuständig, ihre Risiken eigenverantwortlich an den Risikomanager zu melden. Die Abteilungsleitungen haben den Auftrag, die Risiken zu steuern.

Wie ist der Prozess organisiert und welche Instrumente werden genutzt?

Frings: Der Konzern-Risikobericht wird einmal im Quartal für den Konzern aktualisiert; darin enthalten sind auch die Risiken der technischen Gesellschaft, der Stadtwerke Heidelberg Netze. Für

In diesem Punkt reklamieren die BHE-Experten Optimierungsbedarf. Sie treffen vor Ort häufig auf Installationen, die für sich genommen richtig und sinnvoll, als „Insellösungen“ aber weniger leistungsfähig sind. Weil es im Worst Case aber auf Minuten ankommt, sind vernetzte Systeme zu bevorzugen. Detektierte Anlagenzustände lösen reaktive Maßnahmen aus: Beispielsweise werden bei einem unautorisierten Öffnen von Brunnendeckeln dem Leitstellenpersonal Hinweise auf Pumpenabschaltungen gegeben. Registrieren Sensoren an Zäunen, Türen oder Fenstern einen Überstiegs- oder Einbruchversuch, so schaltet sich die Videokamera ein und es erfolgt ein Signal an die Alarmzentrale. Zutrittssteuerungssysteme stellen sicher, dass Mitarbeiterinnen und Mitarbeiter sowie Besucherinnen und Besucher nur in die Bereiche gelangen, in denen sie etwas zu suchen haben – und dies auch nur innerhalb definierter Zeiträume. Eine vernetzte Sicherheitsarchitektur integriert sämtliche Funktionen, vom Einbruch- bis hin zum Brandschutz und der sicheren Evakuierung. Hierzu Dr. Urban Brauer: „Eine solche Integration erhöht den Schutzlevel auf einer Zehner-Skala um mindestens drei bis vier.“

Sicherheitsfaktor SF > 1

Ein wichtiger Indikator für die Objektsicherheit ist der sogenannte Sicherheitsfaktor (kurz „SF“), der sich als Quotient aus der Widerstandszeit und der Reaktionszeit errechnet. Die Widerstandszeit ist die Zeit, die benötigt wird, um eine Barriere, etwa eine Umzäunung oder eine Tür, zu überwinden oder zu durchdringen. Die Reaktionszeit wiederum ist die Zeitspanne zwischen dem dadurch ausgelösten Alarm und seiner Verifizierung als „echt“ bzw. der Intervention durch Sicherheitspersonal oder Polizei vor Ort. Der Sicherheitsquotient sollte > 1 sein: Werte von „< 1“ bedeuten, dass beispielsweise nach dem Überklettern eines Zauns zwar Alarm ausgelöst wird, aber keine rechtzeitigen Interventionsmaßnahmen möglich sind. Die Eindringlinge können auf das Gelände oder in das Gebäude gelangen und das maximal mögliche an Chaos oder Stillstand auslösen. „Der errechnete Quotient liegt in einigen Fällen sogar unter 0,5“, so Dr. Urban Brauer. Diesbezüglich befänden sich viele Versorgungswerke allerdings in bester Gesellschaft mit anderen kri-

den Aufsichtsrat wird einmal im Halbjahr ein Risikobericht erstellt. Dazu werden die Risiken in den einzelnen Gesellschaften abgefragt und bestehende Risiken aktualisiert. Darüber hinaus besteht unterjährig die Pflicht, neue Risiken umgehend an den Risikomanager zu melden. Die einzelnen Risiken werden anhand des potenziellen finanziellen Schadens sowie der Eintrittswahrscheinlichkeit bewertet. Auf dieser Basis wird eine konzernweite Liste aller Risiken und eine sogenannte „Risk Map" der zehn größten Risiken erstellt. Dabei unterstützt uns ein Risikomanagementtool. Im technischen Bereich werden dabei u. a. die im Rahmen des ISMS (Information Security Management System) definierten Risiken berücksichtigt, hinzu kommen technische Risikoanalysen für einzelne Sparten, beispielsweise Trinkwasser. Die erfassten technischen Risiken werden erst ab Überschreiten einer bestimmten Schadenshöhe an das Konzern-Risikomanagement gemeldet; auf Nachfrage hat das zentrale Risikomanagement aber vollen Zugriff auf die Risikodokumentation der technischen Gesellschaft.

Existieren eine umfassende, regelmäßig aktualisierte Analyse und eine Bewertung von Risiken?

Frings: Ja, sie wird für den Konzern einmal im Quartal der Geschäftsführung vorgelegt sowie im Aufsichtsrat vorgestellt. Darin enthalten sind auch die Risiken der technischen Gesellschaft. Für die technische Gesellschaft finden die Aufsichtsratssitzungen halbjährlich statt, der zentrale Risikomanager berichtet dort dem Aufsichtsrat direkt.

Gibt es ein Risikofrüherkennungssystem?

Frings: Das Unternehmen scannt regelmäßig und kontinuierlich das Umfeld nach neuen Bedrohungen. Die dabei erkannten Risiken werden in das Risikomonitoring aufgenommen, sobald sich eine konkrete Bedrohung ergibt.

Welche Risiken definieren Sie – unabhängig von Ihrer konkreten Situation – für Versorgungswerke allgemein?

Frings: Wir orientieren uns im technischen Bereich an den folgenden sechs Kriterien; darüber hinaus sollte jedes Unternehmen seine Risikokategorien selbst definieren:

- Gefährdung für Leib und Leben (Arbeitsausfälle, Verletzte)
- Beeinträchtigung der Versorgungssicherheit
- monetäre Auswirkung
- Auswirkung auf die Umwelt
- Auswirkung auf die Reputation
- Gefährdung von Datensicherheit/Datenschutz

Welche Best-Practice-Tipps können Ihre Expertinnen und Experten anderen (kleineren) Versorgern geben, die das Thema neu in Angriff nehmen?

Frings: Das Risikomanagement sollte bei der Geschäftsführung aufgehängt sein. Zudem empfiehlt es sich, die Einführung durch eine Kommunikation zu flankieren, welche die Meldung von Risiken positiv bewertet. Das nimmt Ängste und dient somit der Früherkennung.

Inwieweit nutzen Sie für das Risikomanagement externe Expertise?

Frings: Bei der Einführung des Risikomanagementtools wurde externe Expertise eingebunden. Zudem werden die Wirtschaftsprüfer regelmäßig nach ihrer Einschätzung zu potenziellen Risiken befragt. Damit machen wir uns deren Branchenerfahrung zunutze. Informationen von den Industrieverbänden sowie einschlägige Publikationen werden ebenfalls zur Risikoerkennung herangezogen. Das Informationssicherheitssystem wird regelmäßig auditiert.

tischen Infrastrukturen wie Heizkraftwerken, U-Bahn-Schächten, Omnibus-Depots oder Bauhöfen.

Stärker im Verbund

Glücklicherweise lasse sich eine steigende Sensibilität für IT-Sicherheit auch unabhängig von Unternehmensgrößen und den zur Verfügung stehenden Budgets beobachten, so Experte Faulhaber. Bei kleineren Wasserversorgungsunternehmen ohne Ressourcen trügen vielerorts bereits Erfahrungsaustausche zur IT-Sicherheit oder die Schaffung unternehmensübergreifender Beauftragtenstrukturen zu einer Verbesserung der IT-Sicherheit bei. Bei dem Projekt „450 MHz" der 450connect nutzen bundesweit angesiedelte regionale und lokale Versorger sogar eine gemeinsame Infrastruktur, und zwar für eine Digitalisierung ihrer Verteilnetze. Damit lassen sich eine Vielzahl an digitalen Steuerungs- und Beobachtungfunktionen über sichere 450-MHz-Funknetze realisieren und bei Bedarf auch physische Sicherheitstechniken an eine Alarmzentale anschließen. „Das System gewährleistet eine höchste Verfügbarkeit der Netze und garantiert im Fall eines Falles eine sichere und schwarzfallfeste Kommunikation", so Theo Waerder, Geschäftsführer der Bonn-Netz GmbH, die sich an dem Projekt beteiligt. ■

Literatur

[1] Neuerer, D.: Cyberattacken: Großteil der Wasserversorger nur unzureichend geschützt, online unter www.handelsblatt.com/politik/deutschland/sicherheit-der-wasserversorgung-cyberattacken-grossteil-der-wasserversorger-nur-unzureichend-geschuetzt/26219428.html, abgerufen am 26. Dezember 2021.

[2] Geier, W.: So schützen Kommunen kritische Infrastrukturen, online unter www.kommunal.de/kommunen-kritischen-infrastrukturen-schuetzen, abgerufen am 26. Dezember 2021.

Der Autor

Manfred Godek ist freier Journalist für Wirtschafts- und Management-Themen.

Kontakt:
Manfred Godek
Presse- und Redaktionsbüro
Turmstr. 12
40789 Monheim
Tel.: 02173 690-611
E-Mail: godek@godek.onmicrosoft.com