IT-Sicherheit:

Neue Gesetze und Regelungen für kritische Infrastrukturen

Auswirkungen der neuen gesetzlichen Anforderung zur Informationssicherheit auf Wasser- und Gasversorgungsunternehmen

von: Frank Dietzsch (DVGW e. V.), Jan Feldhaus (DVGW CERT GmbH), Daniel Fricke (DVGW Service & Consult GmbH) & Kirsten J. Wagner (DVGW e. V.)

Eine zunehmende digitale Durchdringung unseres gesamten Lebensraumes bei gleichzeitig immer professioneller ausgeführten Cyber-Angriffen erfordert den Schutz von Infrastruktureinrichtungen, um die Lebensadern unserer Gesellschaft zu sichern. Vor diesem Hintergrund trat am 25. Juni 2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz – ITSiG) als eines der ersten konkreten Umsetzungsergebnisse der Digitalen Agenda der Bundesregierung in Kraft. Das ITSiG als Artikelgesetz ändert und ergänzt diverse Fachgesetze wie z. B. das BSI-Gesetz (BSIG, BSI = Bundesamt für Sicherheit in der Informationstechnik) und das Energiewirtschaftsgesetz (EnWG) hinsichtlich der IT-Sicherheitsanforderungen an Betreiber kritischer Infrastrukturen. Darunter fallen auch die Sektoren Energie- und Wasserversorgung. Die Gesetze enthalten umfassende Qualitätsanforderungen und Meldepflichten, die von den Betreibern kritischer Infrastrukturen gegenüber dem BSI und der Bundesnetzagentur (BNetzA) zu erfüllen sind.

Im Februar 2016 hat das Bundesministerium des Innern (BMI) den „Entwurf der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI-Kritisverordnung – BSI-KritisV) veröffentlicht. Darin enthalten sind Schwellenwerte zur Einstufung der kritischen Infrastrukturen aus den Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation. Für die Berechnung der Schwellenwerte der einzelnen Sektoren in der BSI-KritisV wurde ein sektorenübergreifender Regelschwellenwert von 500.000 versorgten Einwohnern bzw. Einwohnerwerten zugrunde gelegt. Damit werden vor allem Infrastrukturen (und deren Betreiber) in die Pflicht genommen, die aufgrund ihrer Größe eine Systemrelevanz aufweisen.

Neuer Ordnungsrahmen Informationssicherheit

Grundsätzlich müssen alle Betreiber aus den vom BMI definierten kritischen Sektoren den Grad der eigenen gesetzlichen Betroffenheit selbstständig ermitteln. Aus den durch das IT-Sicherheitsgesetz geänderten und ergänzten gesetzlichen Regelungen (z. B. BSIG und EnWG) und den jeweiligen Aufsichts- und/oder Regulierungsbehörden werden dem einzelnen Infrastrukturbetreiber Aufgaben auferlegt, um ein erhöhtes Sicherheitsniveau zum Schutze der IT-Infrastruktur zu erreichen.

Die Anforderungen an die IT-Sicherheitsstandards für die Unternehmen der Energie- und Wasserwirtschaft sind je nach Medium und Anlagenkategorie in unterschiedlichen Gesetzen geregelt. **Abbildung 1** zeigt schematisch, welche speziellen gesetzlichen Anforderungen an die IT-Sicherheitsstandards für welche Anlagenkategorie nach Erreichen oder Überschreiten des jeweiligen Schwellenwertes der BSI-KritisV festgelegt sind. Demnach sind die gesetzlichen Anforderungen bezüglich der Sicherheitsnachweispflicht für einen Teil der Anlagen, z. B. Anlagen für die Trinkwasserver- oder Abwasserentsorgung, ausschließlich in § 8 a Abs. 1 BSIG definiert **(Abb. 1)**. Dort ist festgelegt, dass spätestens zwei Jahre nach Inkrafttreten der BSI-Kritis angemessene organisatorische und technische Vorkehrungen vorzunehmen sind, um Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit der informationstechnischen Systeme zu vermeiden. Dabei ist der jeweilige für die Branche maßgebliche Stand der Technik einzuhalten.

Zur Ausgestaltung der Sicherheitsaudits, Prüfungen und Zertifizierungen kann das BSI Anforderungen an die Art und Weise der Durchführung und an die hierüber auszustellenden Nachweise festlegen. Weiterhin kann das BSI nach Anhörung von Vertretern der betroffenen Betreiber und Wirtschaftsverbände fachliche und organisatorische Anforderungen an die prüfende Stelle definieren. Für die Anlagenkategorie der Energieversorgungsnetze gilt daneben bzw. zusätzlich der IT-Sicherheitskatalog der

BNetzA nach § 11 Abs. 1 a EnWG, allerdings unabhängig von Schwellenwerten.

Anhand der im Februar 2016 als Referentenentwurf veröffentlichten BSI-KritisV und den darin enthaltenen Schwellenwerten können die Unternehmen der Sektoren Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation nunmehr prüfen, ob sie als kritische Infrastruktur im Sinne der BSI-KritisV eingestuft sind und damit unter den Regelbereich des BSI-Gesetzes fallen. Alle Infrastrukturbetreiber, die sogenannte kritische Dienstleistungen erbringen und deren Anlagen die in der BSI-KritisV genannten Schwellenwerte erreichen oder überschreiten, unterliegen den Meldepflichten gegenüber dem BSI nach § 8 b Abs. 4 BSIG. In diesem Rahmen müssen Betreiber kritischer Infrastrukturen alle erheblichen Störungen, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen informationstechnischen Systeme, Komponenten oder Prozesse führen können oder geführt haben, über eine Kontaktstelle unverzüglich an das BSI melden (eigene oder brancheneigene Sammelmeldestelle – SPOC – Single Point Of Contact).

Regelungen für Gasversorgungsunternehmen

Nach derzeitigem Stand des Verordnungsentwurfes werden ca. 80 Anlagen der Gasversorgung als kritische Infrastruktur eingestuft. Der Schwellenwert für die nach der Verordnung relevanten Anlagenkategorien der Gasversorgung beträgt nach derzeitigem Entwurf 5.190 GWh entnommene Arbeit pro Jahr. Dieser Wert wurde unter der Annahme eines Durchschnittsverbrauchs von 10.380 kWh pro versorgter Person und Jahr bei einem Regelschwellenwert von 500.000 versorgten Personen bestimmt. Als relevante Anlagentypen wurden für die Gasversorgung die vier Anlagenkategorien Gasförderanlagen, Gasspeicher, Fernleitungs- und Verteilernetze explizit benannt. Des Weiteren hat der Gesetzgeber vorsorglich allen Betreibern von leitungsgebundenen Energieversorgungsnetzen im § 11 Abs. 1 a EnWG Vorgaben bezüglich eines an-

Abb. 1: *Zuordnung von Anlagentypen der Gas- und Trinkwasserversorgung nach gesetzlichem Rahmen*

INFORMATIONEN

Branchenarbeitskreis Gas zur IT-Sicherheit gegründet

Der DVGW ist als Partner der UP KRITIS, einer Initiative des Bundes zum Schutz kritischer Infrastrukturen, schon seit 2014 intensiv im Austausch mit Behörden, Industrie und Verbänden. In den sogenannten Branchenarbeitskreisen wird der aktuelle Rechtsrahmen, derzeit z. B. das BSI-Gesetz und die BSI-Kritisverordnung, mit der Branche diskutiert. Aktuelle Debatten beschäftigen sich mit Meldefristen, dem Nachweis von Branchenstandards sowie der Bestimmung von Schwellenwerten.

Vertreter des Gas- und Stromfaches haben bisher gemeinsam in einem spartenübergreifenden Branchenarbeitskreis gearbeitet (BAK STROM/GAS). Um die Belange des Gasfaches sachgerecht bewerten und vollumfänglich diskutieren zu können, wurde nun ein eigener Branchenarbeitskreis Gas (BAK GAS) gegründet. Mitglieder des BAK Gas sind Vertreter von Infrastrukturbetreibern (FNB, VNB, Speicherbetreiber), Behörden (BBK, BNetzA, BMI, BSI) und Verbänden (DVGW, BDEW, WEG, INES).

Zu der Auftaktveranstaltung des Branchenarbeitskreises lud Wolfgang Anthes, Mitglied der Geschäftsführung der Open Grid Europe GmbH und Mitglied des Rates BMI UP Kritis, am 17. Februar 2016 nach Essen ein. In seiner Einführung kam er auf die zunehmende Bedrohung kritischer Infrastrukturen durch Cyber-Angriffe zu sprechen und hob in diesem Zusammenhang die Bedeutung des UP KRITIS als Public Private Partnership (PPP) hervor. Weiterhin stellte Timo Hauschild, Referatsleiter im Bundesamt für Sicherheit in der Informationstechnik (BSI), die Arbeitsweise im UP KRITIS und die grundsätzlichen Regelungsinhalte des BSI-Gesetzes und des IT-Sicherheitskataloges nach § 11 Abs. 1 a der BNetzA vor. Kathleen Gobel vom Bundesinnenministerium (BMI) stellte den Referentenentwurf der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) und die darin festgelegten Schwellenwerte für die einzelnen kritischen Dienstleistungen der einzelnen Sektoren vor.

Zur Sprecherin des BAK GAS wurde einstimmig Katka Walther, ONTRAS Gastransport GmbH, und als Leiter des BAK GAS, Rene Golembewski, Gascade Gastransport GmbH, für die Dauer von einem Jahr gewählt.

Quelle: Open Grid Europe GmbH

Teilnehmerkreis der Auftaktveranstaltung zum BAK Gas

gemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme gemacht, die für einen sicheren Netzbetrieb notwendig sind.

Unmittelbar nach Veröffentlichung des IT-Sicherheitsgesetzes hat die BNetzA einen eigenen Katalog von Sicherheitsanforderungen (IT-Sicherheitskatalog) veröffentlicht. Die Kernforderung des IT-Sicherheitskataloges ist die Einführung eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001 unter besonderer Berücksichtigung der DIN ISO/IEC 27002 und ISO/IEC TR 27019 sowie die Zertifizierung durch eine unabhängige hierfür zugelassene Stelle. Die Akkreditierungs-Voraussetzungen werden derzeit zwischen der BnetzA und der Deutschen Akkreditierungsstelle (DAkks) entwickelt. Mit einem Abschluss des Akkreditierungsverfahrens für befähigte Zertifizierungsstellen ist erst im Herbst 2016 zu rechnen. Die Anforderungen des Sicherheitskatalogs sind unabhängig von Größe oder Anzahl der angeschlossenen Kunden von allen Netzbetreibern zu erfüllen, soweit diese über Systeme verfügen, die für einen sicheren Netzbetrieb notwendig sind. Enthalten sind zumindest alle Telekommunikations- und elektronischen Datenverarbeitungssysteme des Netzbetreibers, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss auf die Netzfahrweise nehmen. Ebenfalls betroffen sind TK- und EDV-Systeme im Netz, die selbst zwar nicht direkt Teil der Netzsteuerung sind, aber deren Ausfall die Sicherheit des Netzbetriebs gefährden könnte.

Werden Anwendungen, Systeme und Komponenten, die den Anforderungen des Katalogs unterliegen, nicht vom Netzbetreiber selbst betrieben, sondern von Dritten, beispielsweise im Rahmen von Outsourcing, so ist die Anwendung und Umsetzung des Katalogs durch entsprechende Vereinbarungen sicherzustellen.

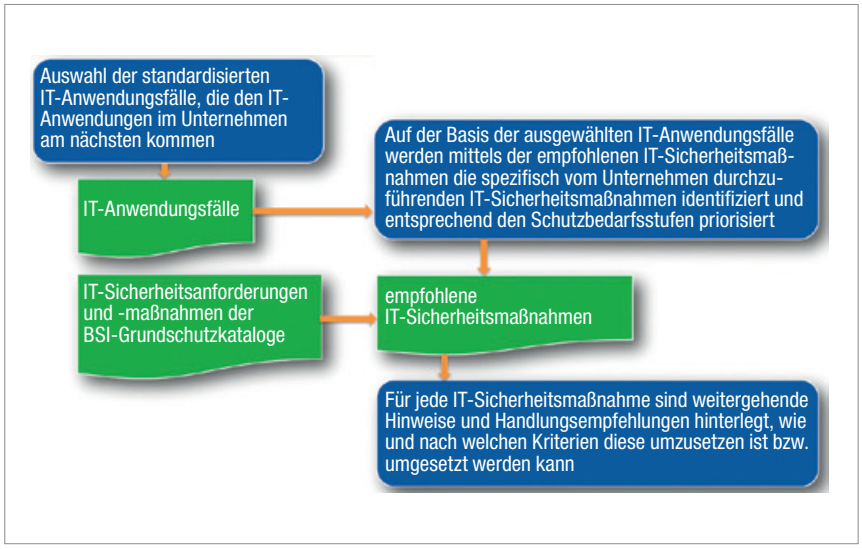
Die zuvor beschriebenen Maßnahmen wie z. B. Meldepflicht oder die Einführung eines ISMS bzw. Branchenstandards sind vom jeweiligen Betreiber zeitnah umzusetzen. Die Fristen unterscheiden sich je nach Anwendungsbereich des Gesetzes. Nach BSIG sind Branchenstandards zwei Jahre nach Inkrafttreten der BSI-KritisV einzuführen, Gasnetzbetreiber haben jedoch nur bis zum 31. Januar 2018 Zeit, ein zertifiziertes ISMS nachzuweisen. Querverbundunternehmen, deren Netzsteuerung oder IT-Systeme für verschiedene Medien im technischen Verbund geführt werden, ist zu empfehlen, sich in Bezug auf die IT-Sicherheitsstandards an den höchsten Anforderungen des Gesetzgebers, namentlich dem IT-Sicherheitskatalog der BNetzA zu orientieren.

Regelungen für die Trinkwasserversorgung

Für Wasserversorgungsunternehmen sind die gesetzlichen Rahmenbedingungen zur Sicherung der IT-Infrastruktur der als Betreiber kritischer Infrastruktur eingestuften Unternehmen im BSIG geregelt. Das gilt sowohl für die Rahmenbedingungen der zu etablierenden IT-Sicherheitsstandards als auch für die Meldepflichten. Gemäß § 8 a Abs. 2 BSIG können die Betreiber kritischer Infrastrukturen und ihre Branchenverbände branchenspezifische IT-Sicherheitsstandards definieren. Auf Antrag prüft das BSI in diesem Fall, ob der eingereichte branchenspezifische IT-Sicherheitsstandard den Anforderungen des § 8 a Abs. 1 BSIG genügt, und erkennt diesen dann gegebenenfalls als geeigneten Sicherheitsstandard an. Eine weitere Möglichkeit, den erforderlichen Nachweis nach § 8 a Abs. 3 BSIG zu erbringen, ist eine Zertifizierung nach DIN ISO/IEC 27001. Allerdings muss hierbei darauf geachtet werden, dass der Anwendungsbereich (Scope) und die gewählten Maßnahmen geeignet und alle wichtigen Schutzziele für kritische Dienstleistungen berücksichtigt sind.

In dem veröffentlichten Entwurf der BSI-KritisV ist für die Trinkwasserversorgung bezogen auf die Anlagenkategorien Gewinnungsanlage, Aufbereitungsanlage, Wasserwerk, Wasserverteilungssystem und Leitzentrale ein Schwellenwert von 21,9 Mio. m^3 Wassermenge(-aufkommen)/Jahr angegeben. Alle Unternehmen, die diesen Schwellenwert erreichen oder übertreffen, müssen spätestens zwei Jahre nach Inkrafttreten der BSI-KritisV geeignete Maßnahmen zum Schutz ihrer IT-Infrastruktur eingeführt haben und dies auch durch einen geeigneten Nachweis (z. B. Audit oder Zertifizierung) belegen können. Nach Einschätzung des DVGW werden ca. 40 Unternehmen der Wasserversorgung über dem Schwellenwert im jetzigen Referentenentwurf der BSI-KritisV liegen. Die BSI-KritisV wird nach Aussage des BMI voraussichtlich Ende April/Anfang Mai veröffentlicht.

Für die Trinkwasserversorgung wird der DVGW gemeinsam mit der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (DWA) die vom BSIG eingeräumte Möglichkeit wahrnehmen und für die Unternehmen der Wasserversorgung und Abwasserentsorgung einen branchenspezifischen IT-Sicherheitsstandard entwickeln. Die ersten Ergebnisse auf dem Weg zur Erstellung des branchenspezifischen IT-Sicherheitsstandards liegen vor. Zurzeit arbeitet eine DVGW-/DWA-übergreifende Arbeitsgruppe an einem IT-Sicherheitsleitfaden, mit dem die Wasserversorgungs- und Abwasserentsorgungsunternehmen die Möglichkeit erhalten, die sicherheitstechnischen Schwachstellen ihrer IT-Infrastruktur zu identifizieren und darauf aufbauend geeignete Schutzmaßnahmen zu ermitteln, die als Stand der Technik angesehen werden (**Abb. 2**). Ausgangspunkt sind dabei die IT-Anwendungsfälle, deren unternehmensspezifische Ausprägung bestimmt, welche Schutzbedarfsstufe (z. B. normal, hoch, sehr hoch) zutreffend ist. Auf Basis des individuellen Anwendungsfalles und der Schutzbedarfsstufe erfolgt die Verknüpfung mit den resultierenden Maßnahmen,



Quelle: DVGW

Abb. 2: *Systematik zur Bestimmung des branchenspezifischen IT-Sicherheitsstandards für die Wasserversorgung*

die sich auf den BSI-Grundschutzkatalog stützen. Um für Querverbundunternehmen die Rahmenbedingung nicht zu erschweren, wird die Widerspruchsfreiheit zwischen dem branchenspezifischen IT-Sicherheitsstandard und der DIN ISO/IEC 27001 bzw. der ISO/IEC TR 27019 gewährleistet.

Die Arbeit an diesem IT-Sicherheitsleitfaden soll im Sommer 2016 abgeschlossen werden. Das BSI und BMI wurde bereits im frühen Stadium in die Entwicklung miteinbezogen, um die Anerkennung des branchenspezifischen IT-Sicherheitsstandards nach Fertigstellung zu vereinfachen und zu beschleunigen. Anfang 2017 wird voraussichtlich das dazugehörige DVGW- und DWA-Arbeitsblatt für den branchenspezifischen IT-Sicherheitsstandard der Wasserversorgung erscheinen.

Implementierung eines ISMS

Damit ein Unternehmen die geforderte Reife in einem ISMS nachweisen kann, bedarf es einiger Vorarbeiten. Grundsätzlich erfolgt die Implementierung eines Managementsystems gemäß DIN ISO/IEC 27001 immer nach dem gleichen Schema:

- Phase 1: Initialisierung
- Phase 2: Aufbauphase
- Phase 3: Reifephase
- Phase 4: Regelbetrieb

Phase 1 – Initialisierung

In der ersten Phase werden die Weichen für die künftige Umsetzung gestellt. Mit der Leitlinie zur Informationssicherheit bestätigt die Unternehmensführung ihren Willen zur und ihre Unterstützung bei der Umsetzung eines ISMS. Ohne das Bekenntnis zur Unterstützung bei der Umsetzung und bereitzustellenden Ressourcen wird jedes ISMS-Projekt scheitern.

Die Festlegung des eigentlichen Geltungsbereiches (Scope) des ISMS ist der zweite große Schritt bei der Implementierung des ISMS. Hier muss die Abwägung zwischen Aufwand, Nutzen und gesetzlichen Vorgaben getroffen werden. Gemäß IT-Sicherheitskatalog der BNetzA sind alle zentralen und dezentralen Anwendungen sowie alle Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind, im Geltungsbereich zu erfassen. Dazu gehören nicht nur die Leitsysteme als direkt betroffene Systeme, sondern auch Systeme wie Telefonanlagen oder Geoinformationssysteme (GIS), die nur indirekt für den sicheren Netzbetrieb notwendig sind **(Abb. 3)**.

Für die Definition des Geltungsbereiches müssen also alle relevanten Systeme und Prozesse adressiert werden. Oftmals wird der Geltungsbereich sehr „dicht“ an den gesetzlichen Vorgaben definiert. Dies bedeutet aber im Nachgang oft einen erheblichen Mehraufwand, da die einzelnen Abgrenzungen und Schnittstellen dann auch betrachtet werden müssen. Der Aufwand, ein zusätzliches System zu betrachten, ist unter Umständen erheblich geringer, als permanent zu versuchen, die (künstlichen) Grenzen des ISMS-Geltungsbereiches zu beachten.

Als Nächstes gilt es, den „Informationssicherheitsbeauftragten“ (ITSB) zu benennen. Der ITSB übernimmt die Projektverantwortung für die Einführung des ISMS. Der ITSB sollte nicht in der IT-Abteilung angesiedelt sein, da er sonst im späteren Betrieb seine eigenen Arbeiten kontrollieren müsste. Der ITSB kann, analog zum „Datenschutzbeauftragten“ (DSB), auch als Stabsstelle ausgelagert werden. Wenn der DSB eine interne Stelle ist, könnte dort der ITSB, auch in Personalunion, angesiedelt werden. Der Arbeitsaufwand für einen ITSB in der Einführungsphase variiert je nach Unternehmensgröße, aber insbesondere in der Einführungsphase wird der Arbeitsaufwand die komplette Kapazität des ITSB binden.

Weitere Projektmitarbeiter müssen aus den jeweiligen Fachbereichen und gemäß dem Geltungsbereich des ISMS ausgewählt werden. Erforderlich sind Mitarbeiter aus der Büro- und Prozess-IT, da dies die direkt betroffenen Fachabteilungen sind. Die Einrichtung eines Kernteams und weiterer Teams, die bei Bedarf einberufen werden, um spezielle Aufgaben abzuarbeiten, ist zu empfehlen.

Phase 2 – Aufbau eines ISMS

In der zweiten Phase des Aufbaus eines ISMS werden alle Werte (Assets) des Unternehmens in einem Inventar erfasst. Dabei werden sowohl Hard- und Software erfasst als auch Informationswerte wie Verträge oder auch „Wissen“ von Mitarbeitern. Sind die Werte vollständig erfasst, kann im nächste Schritt die Risikoanalyse erfolgen. Für die Risikoanalyse gibt es unterschied-

Was ist denn eigentlich »virtuelles Wasser«?

Informieren Sie Ihre Kunden umfassend!

Bestellen Sie fundierte Materialien für Ihre Kundenkommunikation:

Ratgeber „Virtuelles Wasser – Weniger Wasser im Einkaufskorb“

21 x 21 cm, 40 Seiten

Preis: 3,80 €*

Paket „Virtuelles Wasser – Versteckt im Einkaufskorb“

- Broschüre „Virtuelles Wasser – Versteckt im Einkaufskorb“, 21 x 21 cm, 56 Seiten
- Poster „Wasserfußabdruck“, DIN A1

Preis: 5,50 €*

Paket „Virtuelles Wasser – Versteckt im Einkaufskorb“ (Sekundarstufe)

- Arbeitsheft „Virtuelles Wasser – Versteckt im Einkaufskorb“ für die Sekundarstufe, DIN A4, 32 Seiten
- Poster „Virtuelles Wasser in Produkten“, DIN A1

Preis: 5,50 €*

* Bitte beachten Sie den Mindestbestellwert von 15,00 € netto. Alle Preise verstehen sich zzgl. USt. und Versandkosten.

Bestellung an:
Tel.: 0228 9191-40 oder per E-Mail: info@wvgw.de

www.virtuelles-wasser.de

liche Verfahren und Ansätze, in der ISO/IEC 27005 wird ebenfalls ein entsprechendes Verfahren beschrieben. Dazu werden die Eintrittswahrscheinlichkeit, die Eintrittshäufigkeit und die Schadenshöhe des jeweiligen Ereignisses in Relation gesetzt. Im Anschluss muss die Unternehmensleitung die einzelnen Risiken bewerten. Die Bewertung entspricht einer Klassifizierung der Risiken:

- Risiko wird akzeptiert, aber
- Risiko muss durch Maßnahmen reduziert werden (z. B. Outsourcing, Versicherung, Schaffen von Redundanzen).

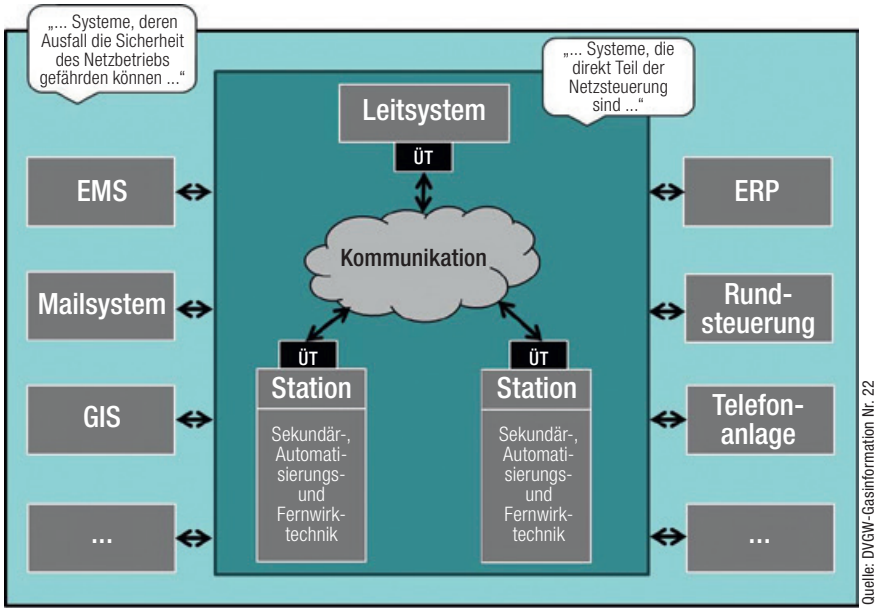
Wichtig dabei ist, dass die Unternehmensleitung, z. B. durch ein Outsourcing, nicht aus der Verantwortung für den einzelnen Teilbereich entlassen wird. Aufgaben können delegiert werden, die Verantwortung nicht.

Als nächster möglicher Schritt bietet sich die Durchführung eines internen Audits, also die Überprüfung des Ist-Stands in Bezug auf Informationssicherheit im Unternehmen, an. Anhand eines standardisierten Verfahrens, das in der Umsetzung sehr eng an das Technische Sicherheitsmanagement (TSM) des DVGW angelehnt ist, gibt es hier die Möglichkeit, Informationssicherheit zu messen.

Entscheidend für die Implementierung eines ISMS ist die Berücksichtigung des PDCA-Prozesses (Plan-Do-Check-Act). Schutzziele unterliegen immer einem kontinuierlichen Verbesserungsprozess.

Die Erkenntnisse eines solchen internen Audits werden genutzt, um erste Maßnahmen abzuleiten und damit die ISMS-Prozesse in Gang zu bringen. Der Planung der Implementierungsschritte der ISMS-Prozesse, also die gedankliche Vorwegnahme von Handlungsschritten zum Erreichen von Zielen, kommt nun eine zentrale Rolle zu. Auch hier gilt: Der ITSB ist zwar die projektverantwortliche Person, muss aber nicht alle Arbeiten selbst erledigen. Das Einsetzen von kleinen Projektteams oder die Nutzung von vorhandenen Projektmanagementkapazitäten im Unternehmen entsprechen durchaus dem „Best Practice"-Ansatz.

Eine ausführliche und schlüssige Dokumentation aller Verfahrensschritte ist zentraler Bestandteil eines ISMS. Es gibt keine Vorgaben, wie eine Dokumentation aussehen muss, in der Praxis hat es sich aber bewährt, auf Dokumentenmanagementsysteme (DMS) oder andere Werkzeuge zur Dokumentenlenkung zurückzugreifen, die im Unternehmen bereits vorhanden sind. Ebenso ist es möglich, bestehende Managementsysteme so zu erweitern, dass im Ergebnis ein integriertes Managementsystem steht.



Quelle: DVGW-Gasinformation Nr. 22

Abb. 3: *Direkt und indirekt betroffene Systeme für den sicheren Netzbetrieb (Technologiekategorien gemäß IT-Sicherheitskatalog: Leitsystem/Systembetrieb, Übertragungstechnik/Kommunikation, Sekundär-, Automatisierungs- und Fernwirktechnik, ÜT – Übertragungstechnik, EMS – Entstörmanagementsystem, GIS – Geografisches Informationssystem, Enterprise Ressource Planing)*

Phase 3 – Reifephase

Mit der Reifephase wird das ISMS im Unternehmen implementiert. Ab diesem Moment wird das ISMS auf seine Praxistauglichkeit überprüft. Das „Nachsteuern" bei einzelnen Teilschritten und Prozessen ist durchaus gewünscht und führt schon in dieser Phase zu einem gelebten kontinuierlichen Verbesserungsprozess (KVP). Zur Einführung eines ISMS sollte auch eine breite Aufklärungskampagne (Awareness) innerhalb des Unternehmens durchgeführt werden. Die Durchführung von Schulungen zur Mitarbeitersensibilisierung zum Thema Informationssicherheit und ISMS ist ebenfalls ein essenzieller Teil der ISMS-Implementierung, deren Teilnahme für die Mitarbeiter verpflichtend ist. Die Mitarbeiter sind ein zentraler Punkt in der Umsetzung von Informationssicherheit und dürfen auf keinen Fall außer Acht gelassen werden. Auch hier kann die Unternehmensleitung aktiv an der ISMS-Implementierung mitwirken, indem sie durch eigene Teilnahme mit gutem Beispiel vorangeht.

Ist das ISMS implementiert und wird es auch gelebt, bietet es sich an, vor der eigentlichen Zertifizierung ein weiteres internes Audit durchzuführen. Dabei werden alle Komponenten des ISMS auf Norm- und Zertifizierungskonformität überprüft. Hier werden das ISMS und die gelebte Praxis vom Auditor in vollem Umfang verglichen. Der Aufwand ist an dieser Stelle durchaus größer als im eigentlichen Zertifizierungsaudit. Dies ist dadurch bedingt, dass im Zertifizierungsaudit die Zeiten vorgegeben sind und der Auditor dort nur Stichproben an Betriebsstandorten durchführen kann.

Phase 4 – Regelbetrieb

Ist die Implementierung abgeschlossen und das ISMS ca. zwei bis drei Monate im Echtbetrieb, sollte das ISMS-Projekt offiziell beendet und das ISMS in den Regelbetrieb übergeben werden. Im Rahmen des KVP müssen jetzt noch Zyklen definiert werden, in denen die Wirksamkeit der Maßnahmen überprüft wird.

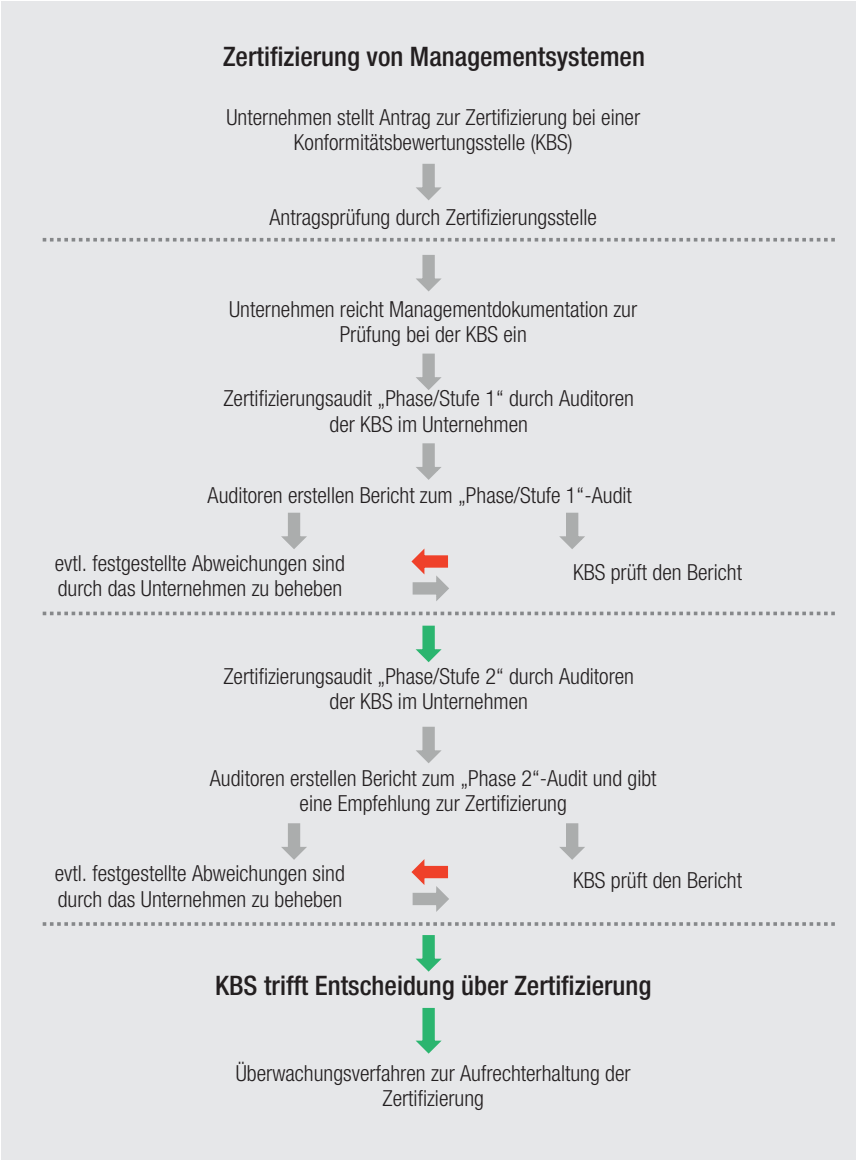
Nachweis durch Zertifizierung

Betreiber kritischer Infrastrukturen müssen entsprechend ihrer Einstufung gegenüber dem BSI einen Nachweis erbringen, dass die gesetzlichen Vorgaben eingehalten werden. Organisationen, die unter den Anwendungsbereich der BSI-KritisV fallen, müssen einen solchen Nachweis erstmalig spätestens zwei Jahre nach Veröffentlichung der Verordnung erbringen.

Nach § 8 a BSIG haben Organisationen der Trinkwasserversorgung die Möglichkeit, den Nachweis durch die Einführung des branchenspezifischen IT-Sicherheitsstandards zu erbringen. Dies beinhaltet keine Zertifizierungspflicht nach DIN ISO/IEC 27001.

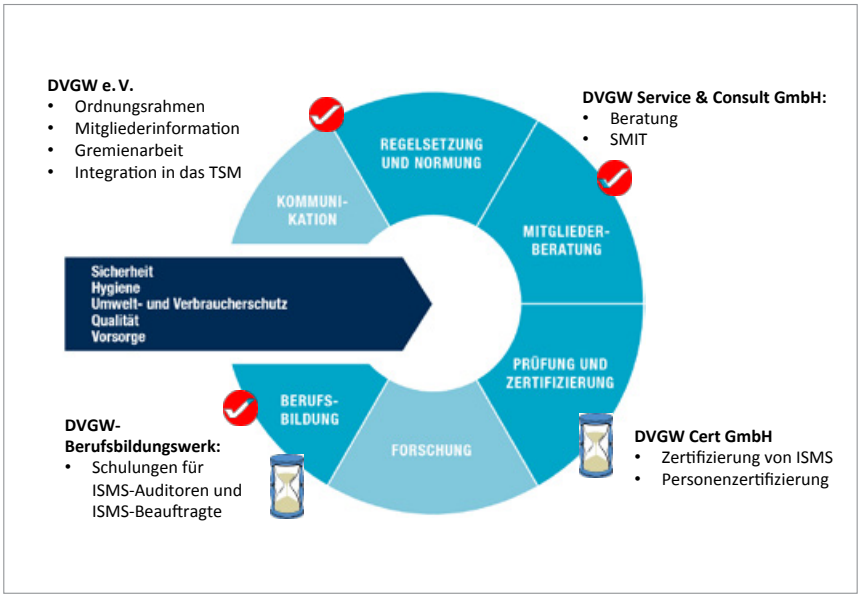
Organisationen, die unter den Anwendungsbereich des IT-Sicherheitskataloges nach § 11 Abs. 1 a EnWG fallen – zu diesen zählen die Energienetzbetreiber –, müssen bis spätestens 31. Januar 2018 einen Nachweis erbringen. Als Nachweis gilt eine Zertifizierung nach DIN ISO/IEC 27001 inkl. der zusätzlichen Anforderungen gemäß IT-Sicherheitskatalog.

Für die Aufnahme eines Zertifizierungsverfahrens müssen die betroffenen Organisationen einen Antrag bei einer akkreditierten Zertifizierungsstelle (Konformitätsbewertungsstellen = KBS) auf Zertifizierung ihres ISMS stellen. Diese betreiben unter Berücksichtigung der geltenden normativen und sonstigen Anforderungen und der entsprechenden Regeln der DAkkS ein durch die DAkkS akkreditiertes Zertifizierungssystem. Diese Organisationen haben im Zusammenhang mit der Zertifizierung und vor Aufnahme des Verfahrens organisationsspezifische und das ISMS betreffende Daten (z. B. branchenspezifische Vorgaben der BNetzA) bei der KBS einzureichen. Anhand der eingereichten Daten wird geprüft, ob die entsprechenden Voraussetzungen zur Zertifizierung erfüllt sind.



Quelle: DVGW CERT GmbH

Abb. 4: *Ablauf des Zertifizierungsverfahrens*



Quelle: DVGW

Abb. 5: *ISMS-Reflexion in der DVGW-Arbeit*

Ist dies der Fall, wird ein auf den Angaben der Organisation basierendes, individuelles Angebot erstellt.

Zur weiteren Bearbeitung des Vorgangs reicht die Organisation im Anschluss einen Antrag auf Zertifizierung des ISMS ein. Nach der Antragsprüfung beauftragt die KBS einen Auditor und/oder ggf. ein Auditorenteam mit der Auditierung des Unternehmens. Zur Prüfung und Vorbereitung der Auditierung reicht das Unternehmen vorab seine Managementsystemdokumentation ein. Die Auditierung des ISMS ist dabei in zwei Phasen unterteilt:

Phase 1 dient dazu, die Managementsystemdokumentation des Unternehmens in Bezug auf die bestehenden normativen Anforderungen zu prüfen und vor Ort im Unternehmen die Zertifizierungsfähigkeit des Managementsystems zu bewerten. Sie beinhaltet z. B.:

- die Prüfung der Vollständigkeit der Security Policies, die Risikoanalyse und -behandlung,
- die Beurteilung der Angemessenheit unter Abwägung des individuellen Schutzbedarfes.

Das Ergebnis wird in einem Bericht dokumentiert. Dabei werden Abweichungen gegenüber den Zertifizierungsgrundlagen dokumentiert, die vor einer Zertifizierung behoben werden müssen.

In Phase 2 wird die Umsetzung und Wirksamkeit des ISMS im Unternehmen bewertet. Es wird geprüft, ob den Mitarbeitern im Unternehmen die verbindlich festgelegten Regeln des ISMS bekannt sind und ob die Festlegungen in der betrieblichen Praxis konsequent angewendet werden und dies durch entsprechende Nachweise belegt werden kann. Das Audit beinhaltet z. B.:

- die Begehung der Technikräume, Büros, Kopiercenter, Ver- und Entsorgungseinrichtungen,
- Interviews mit den Mitarbeitern.

Das Ergebnis wird in einem Bericht dokumentiert. Darin werden ggf. festgestellte Abweichungen gegenüber der Zertifizierungsgrundlage oder unternehmenseigenen Festlegungen des Managementsystems aufgeführt, die vor einer erfolgreichen Zertifizierung behoben werden müssen. Der Bericht schließt mit einer Empfehlung der Auditoren an die KBS bezüglich der Erteilung des Zertifikats. Die KBS trifft die abschließende Entscheidung zur Zertifizierung.

Zwischen Phase 1 und Phase 2 des Audits sollte ein Zeitraum von mindestens zwei Wochen vorgesehen werden, um etwaig auftretende Abweichungen aus dem Audit der Phase 1 beheben zu können, die einer erfolgreichen Zertifizierung entgegenstehen.

Wurde die Erteilung der Zertifizierung entschieden, wird das entsprechende Zertifikat mit einer Gültigkeit von drei Jahren erteilt. Die Gültigkeit der Zertifizierung wird von der KBS überwacht. Dabei werden innerhalb des Gültigkeitszeitraums eines Zertifikats von drei Jahren zwei Überwachungsaudits im Unternehmen durchgeführt. Bei einer Erstzertifizierung muss das erste Überwachungsaudit nach spätestens zwölf Monaten durchgeführt werden. Bevor die Gültigkeit einer Zertifizierung endet, ist das Audit zur Re-Zertifizierung durchzuführen (**Abb. 4**).

Fazit

Das IT-Sicherheitsgesetz hat durch seine vielfältigen Eingriffe in bestehende Gesetze einigen Handlungsbedarf bei den Unternehmen der KRITIS-Sektoren notwendig gemacht. Da der Aufwand für die Umsetzung der gesetzlichen Vorgaben groß ist und die Zeit aufgrund der engen gesetzlichen Fristen drängt, müssen die Unternehmen zügig reagieren. Die zeitlichen Vorgaben zur Umsetzung der Anforderungen liegen bei mindestens zwei Jahren nach Inkrafttreten der BSI-KritisV bzw. bis zum 31. Januar 2018 für Energienetzbetreiber.

Die Einführung eines Managementsystems kostet je nach bereits erfolgter Vorarbeit Zeit und eventuell weitere Ressourcen. Das ISMS selbst sorgt aber nicht für Sicherheit. Die Mitwirkung aller Mitarbeiter, einschließlich der Unternehmensleitung, die hinter dem ISMS stehen muss, sorgt für die notwendige Sicherheit. Das Erreichen von Informationssicherheit ist kein einzelner Meilenstein, der erreicht werden kann. Vielmehr ist es ein dauerhafter Prozess, der gelebt werden muss.

Der DVGW e. V. sowie seine angegliederten Gesellschaften stehen bei der Umsetzung, Implementierung und Zertifizierung eines solchen Verfahrens gerne zur Verfügung (**Abb. 5**). ■

Die Autoren

Verm.-Ass. Dipl.-Ing. Frank Dietzsch ist Hauptreferent Gasversorgung im DVGW e. V..

Jan Feldhaus ist Referent Managementsysteme bei der DVGW CERT GmbH.

Daniel Fricke ist Leiter IT bei der DVGW Service & Consult GmbH.

Dipl.-Ing. Kirsten J. Wagner ist Referentin Benchmarking & IT-Sicherheit im DVGW e. V..

Kontakt:
Frank Dietzsch
Bereich Gasversorgung
DVGW Deutscher Verein des Gas- und Wasserfaches e. V.
Technisch-wissenschaftlicher Verein
Tel.: 0228 9188-914
E-Mail: dietzsch@dvgw.de
Internet: www.dvgw.de