Deutscher Verein des
Gas- und Wasserfaches e.V.

www.dvgw.de

STELLUNGNAHME

vom 10. Dezember 2020 zum

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 9. Dezember 2020
(Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

DVGW Deutscher Verein des Gas- und Wasserfaches e.V.

Ansprechpartner
Dipl.-Ing. Kirsten Wagner
Josef-Wirmer-Straße 1-3
D-53123 Bonn
Tel.: +49 152 08512647
E-Mail: kirsten.wagner@dvgw.de

Verm.-Ass. Dipl.-Ing. Frank Dietzsch
Josef-Wirmer-Straße 1-3
D-53123 Bonn
Tel.: +49 160 5379931
E-Mail: frank.dietzsch@dvgw.de

Vorbemerkung

Der **DVGW Deutscher Verein des Gas- und Wasserfaches e. V.** – Technisch-wissenschaftlicher Verein – fördert das Gas- und Wasserfach mit den Schwerpunkten Sicherheit, Hygiene und Umweltschutz. Mit seinen rund 13.000 Mitgliedern erarbeitet der DVGW die allgemein anerkannten Regeln der Technik für Gas und Wasser. Der DVGW ist wirtschaftlich unabhängig und politisch neutral.

Der DVGW bedankt sich für die Möglichkeit, zum Entwurf eines „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“ (IT-Sicherheitsgesetz 2.0, IT-SiG 2.0) vom 9. Dezember 2020 Stellung nehmen zu können. Wir begrüßen die Weiterentwicklung des IT-SiG 2.0 mit dem Ziel, die Informationssicherheit der Kritischen Infrastrukturen weiter zu stärken, ausdrücklich. Vor dem Hintergrund der zunehmend komplexeren Cyberangriffe wird die ständige Verbesserung der IT-Sicherheit der Kritischen Infrastrukturen vom DVGW für eine wichtige gesellschaftliche Aufgabe angesehen.

Zu diesem Zweck befürworten wir ausdrücklich, dass Hersteller von IT-Produkten und Anbieter digitaler Dienste zukünftig verbindlich verpflichtet werden, einen Beitrag zu den Schutzzielen der Informationssicherheit von Kritischen Infrastrukturen zu leisten. Bei einer Reihe der neuen Regelungsvorschlägen bedarf es aus Sicht des DVGW einer Anpassung oder Konkretisierung, auch sind längere Umsetzungsfristen notwendig.

Anzumerken bleibt, dass die gesetzlich festgelegte Evaluierung des IT-SIG 1.0 gemäß Artikel 10 „unter Einbezug eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird" bisher noch nicht durch das Bundesinnenministerium erfolgt ist. Aus Sicht des DVGW wäre es sinnvoll und zielführend, die Erweiterung der Anforderungen an die IT-Sicherheit der Betreiber Kritischer Infrastrukturen auf Basis der gewonnenen Erkenntnisse (Lessons Learned) im Rahmen der Implementierung des IT-SiG 1.0 vorzunehmen.

Im Sinne eines kontinuierlichen Verbesserungsprozesses sind die Betreiber von Gas- und Wasserversorgungsinfrastrukturen grundsätzlich angehalten, ihre systemkritischen Prozesse und Systeme einem ganzheitlichen Sicherheitskonzeptes auf Grundlage von gesetzlichen und untergesetzlichen Vorgaben und an die aktuelle Bedrohungslage anzupassen.

Im Kontext des BMI-Basisschutzkonzeptes zum Schutz kritischer Infrastrukturen kann der DVGW auf sein Technisches Regelwerk zur Gewährleistung der Aufbau- und Ablauforganisation von Gas- und Wasserversorgungsunternehmen verweisen.

Für die Gasversorgung gelten:

- DVGW G 1000 Anforderungen an die Qualifikation und die Organisation von Unternehmen für den Betrieb von Anlagen zur leitungsgebundenen Versorgung der Allgemeinheit mit Gas (Gasversorgungsanlagen)
- DVGW G 1001 Sicherheit in der Gasversorgung - Risikomanagement im Normalbetrieb

- DVGW G 1002 Sicherheit in der Gasversorgung/Trinkwasserversorgung - Organisation und Management im Krisenfall

Für die Wasserversorgung gelten:

- DVGW W 1000 Anforderungen an die Qualifikation und die Organisation von Trinkwasserversorgern
- DVGW W 1001 Anforderungen an die Qualifikation und die Organisation von Trinkwasserversorgern
- DIN EN 15975-1 Sicherheit der Trinkwasserversorgung – Leitlinien für das Risiko- und Krisenmanagement – Teil 1: Krisenmanagement
- DIN EN 15975-2 Sicherheit der Trinkwasserversorgung – Leitlinien für das Risiko- und Krisenmanagement – Teil 2: Risikomanagement
- DVGW W 1020 Empfehlungen und Hinweise für den Fall von Abweichungen von Anforderungen der Trinkwasserverordnung; Maßnahmenplan und Handlungsplan
- DVGW W 1050 Objektschutz von Wasserversorgungsanlagen
- DVGW W 1060 IT-Sicherheit – Branchenstandard Wasser/Abwasser

Die Umsetzung in den Mitgliedsunternehmen des DVGW wird durch das Technische Sicherheitsmanagement (TSM) gemäß DVGW G 1001 und DVGW W 1000 gewährleistet.

Der DVGW betreut das Thema IT-Sicherheit seit 2015 technisch-wissenschaftlich in einem spartenübergreifendes Technisches Komitee „IT-Sicherheit“. In einer gemeinsamen Arbeitsgruppe mit der Deutschen Vereinigung Wasserwirtschaft, Abwasser und Abfall e.V. (DWA) wurde im Benehmen mit dem Branchenarbeitskreis Wasser/Abwasser des UP KRITIS für die Wasserversorgungs- und Abwasserentsorgungsunternehmen der branchenspezifische IT-Sicherheitsstandard Wasser/Abwasser erarbeitet, für den das BSI im Januar 2020 erneut die Eignungsfeststellung gemäß § 8a Abs. 2 BSI-Gesetz (BSIG) erteilt hat.

Die Betreiber von Energieinfrastrukturen haben ihre IT-sicherheitstechnische Eignung im Sinne eines Informationssicherheitsmanagementsystems (ISMS) nach den Grundsätzen des IT-Sicherheitskataloges nach § 11 Abs. 1a und Abs. 1b Energiewirtschaftsgesetz (EnWG) nachgewiesen. Auch hier ist ein kontinuierliches Verbesserungswesen angelegt.

Zu den Regelungen des Gesetzesentwurfes im Einzelnen

Zu Artikel 1 des BSIG und Artikel 3 des EnWG

§ 3 BSIG „Aufgaben des Bundesamtes“

Die Formulierung des § 3 Abs. 1, Nr. 20 BSIG sollte dahingehend ergänzt werden, dass die Festlegung des Standes der Technik von IT-Produkten immer unter Berücksichtigung von bestehenden, anerkannten Normen und Standards unter Beteiligung der betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschaftsverbände zu erfolgen hat.

Die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen an IT-Produkte nach § 3 Abs. 1 Satz 2, Nummer 20 BSIG durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) darf nicht in einen nationalen Alleingang münden. Der Stand der Technik sollte, wie bisher, auf Basis anerkannter Normen und Standards ausgelegt werden, an deren Erarbeitung die betroffenen Sektoren der Kritischen Infrastrukturen und deren Wirtschafsverbände beteiligt sind.

Betreiber Kritischer Infrastrukturen sind gemäß § 8a Abs. 1 BSIG zur Umsetzung von technischen und organisatorischen Maßnahmen nach dem Stand der Technik verpflichtet. Diese Betreiber sind daher als unmittelbar Betroffene bei der Entwicklung eines Standes der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte einzubeziehen, analog zu Beteiligungsmöglichkeiten in der nationalen, europäischen und internationalen Normung (WTO-Richtlinien). Bei einer Festlegung des Standes der Technik durch das BSI ohne Beteilung der betroffenen Betreiber Kritischer Infrastrukturen und deren Wirtschaftsverbände steht zu erwarten, dass die umfangreiche praktische Expertise aus den Unternehmen in nicht ausreichendem Maße bei der Festlegung des Standes der Technik berücksichtigt wird.

Zusätzlich muss berücksichtigt werden, dass sich der Stand der Technik bei IT-Produkte sehr dynamisch weiterentwickelt. Auch hier haben sich die etablierten Strukturen der nationalen, europäischen und internationalen Normung bewährt. Zertifizierungen, die nach dem Stand der Technik anderer Organisationen bzw. Branchenverbänden für Informationssicherheit erfolgen, sind ebenfalls anzuerkennen.

Vor diesem Hintergrund schlägt der DVGW vor, den § 3 Abs. 1, Nr. 20 BSIG dahingehend zu ergänzen, dass ein Stand der Technik unter Berücksichtigung von bestehenden, anerkannten Normen und Standards und unter Beteiligung der betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschaftsverbände erfolgen muss.

§ 8a BSIG „Sicherheit in der Informationstechnik Kritischer Infrastrukturen“ und § 11 EnWG „Betrieb von Energieversorgungsnetzen“

Die Übergangsfrist für die Einführung von Systemen zur Angriffserkennung (§ 8a Abs. 1a BSIG und § 11 Abs. 1d EnWG) sollte mindestens zwei Jahren betragen. Es dürfen keine steuernden Eingriffe der Systeme zur Angriffserkennung in die Prozessführung vorgeschrieben werden.

Für die Auswahl und Installierung geeigneter Systeme zur Angriffserkennung und für eine vorher durchgeführte Identifikation der notwendigen Monitoring-, Detektions-, Analyse-, Alarmierungs- und Reaktionsprozesse im Unternehmen greift der im Gesetz vorgegebene Zeitraum von einem Jahr zu kurz. Der finanzielle und personelle Aufwand, der damit einhergeht, ist beträchtlich und für einen Großteil der vom Gesetzgeber als Betreiber Kritischer Infrastrukturen eingestuften Gas- und Wasserversorgungsunternehmen kurzfristig nicht leistbar.

Systeme zur Angriffserkennung können ganz unterschiedliche Ausprägungen haben. Daher sollten für den verpflichtenden Einsatz von Systemen zur Angriffserkennung nach § 8a Abs. 1a BSIG und § 11 Abs. 1d EnWG die Rahmenbedingungen dargelegt und die Anforderungen an den Einsatz solcher Systeme im Sinne von IT-technischen Eigenschaften auf Mindestanforderungen begrenzt werden.

Die Versorgung der Bevölkerung mit Gas und Trinkwasser ist ein wesentlicher Bestandteil der gesellschaftlichen Daseinsvorsorge und des Wirtschaftsstandortes Deutschland. Die Wahrnehmung dieser Aufgabe muss bei allen Handlungen und auch bei den vom Gesetzgeber auferlegten Verpflichtungen stets im Vordergrund stehen. Daher ist es nicht zielführend, zur Aufrechterhaltung der Versorgungssicherheit eine nachgelagerte Abschaltmatrix allein aufgrund eines IT-Angriffes in die Netzsteuerungssysteme zu implementieren. Dadurch besteht die Gefahr, dass es zur Abschaltung einer oder mehrerer für die Gas- und Wasserversorgung wesentlichen Anlagen kommt und vermeidbare Versorgungsunterbrechungen entstehen. Der Eintritt eines solchen Betriebszustandes wird üblicherweise durch das verantwortliche Personal verhindert.

Die zeitlichen Vorgaben für eine Speicherung von für die Angriffserkennungs- und -nachverfolgung relevanten Protokollierungs- und Log-Daten (§ 8a Abs. 1b BSIG und § 11 Abs. 1e EnWG) sollten auf drei Monate im Normalfall und bei Verdacht auf einen Angriff auf bis zu 12 Monate herabgesetzt werden.

Im Entwurf des IT-SiG 2.0 wurde für die Speicherung der für die Angriffserkennungs- und -nachverfolgung relevanten nicht personenbezogenen Daten ein Zeitraum von 4 Jahren festgelegt. Das erscheint nicht zielführend und ist angesichts des erforderlichen Archivierungsaufwands unverhältnismäßig. Darüber hinaus wird nicht dargelegt, warum der Gesetzgeber einen Zeitraum von 4 Jahren für die Speicherung gewählt hat.

Die vom Gesetzgeber vorgegebene Trennung von personen- und nichtpersonenbezogenen Daten ist in der Praxis bei großen Datenmengen technisch nicht zu realisieren. Um im Ernstfall aufgrund dieser Daten den Hergang

eines Angriffs (ggf. den Angreifer) nachzuvollziehen, ist eine Analyse und Auswertung von nicht personenbezogenen Daten nicht ausreichend. Da z.B. IP-Adressen als personenbezogene Daten gelten, entfällt ansonsten die Aussagekraft der gespeicherten Protokollierungs- und Log-Daten.

Der DVGW empfiehlt daher dringend § 8a Abs. 1a und Abs. 1b BSIG sowie § 11 Abs. 1d und Abs. 1e EnWG entsprechend anzupassen.

§ 9b „Untersagung des Einsatzes kritischer Komponenten“

Der Gesetzgeber muss bei der Untersagung des Einsatzes kritischer Komponenten eine realistische Übergangsfrist für deren Austausch festlegen und verfügbare Austauschprodukte nennen. Eine Verknappung von kritischen Komponenten durch Monopolbildung ist zu verhindern.

Von der Einholung der Garantieerklärung für kritische Komponenten, über deren Administration bis zu den potenziellen betrieblichen und wirtschaftlichen Folgeschäden durch die Untersagung eines Komponenteneinsatzes, müssten Betreiber die Auswirkungen tragen. Das Vorgehen greift durch die Zwangsvorgaben auch in das EU-Ausschreibungsrecht zu Lasten der betroffenen Unternehmen ein und kann zu Marktverzerrungen wegen Ungleichbehandlung führen. Die Kriterien zur Auswahl von einsetzbaren „kritischen Komponenten“ müssen zwingend festgelegt werden, um auf Betreiberseite Beschaffungsprozesse und die notwendige kurzfristige Reaktionsfähigkeit zur Aufrechterhaltung der Informationssicherheit auch im Gefahrenfall zu ermöglichen. Die angedachte Neuregelung birgt ansonsten die Gefahr die Informationssicherheit in Kritischen Infrastrukturen zu schwächen.

Bei der Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller sind gesetzlich weitere Maßnahmen vorzusehen, die für die Aufrechterhaltung der kritischen Geschäftsprozesse (trotz Untersagung) sorgen. Es sind realistische Übergangsfristen anzugeben, verfügbaren Austauschprodukte zu nennen und eine langfristige Verhinderung der Monopolbildung für Produkte zu verhindern. Der DVGW empfiehlt, diese Punkte bei der Gesetzgebung zu beachten.

Betreiber werden an Stelle des Gesetzgebers in die Pflicht genommen, beim Hersteller eine Garantieerklärung einzuholen, welche an das BMI gesendet werden soll. Die Verwaltung und Übermittlung von Garantieerklärungen stellen einen zusätzlichen Aufwand dar, aus dem kein Mehrwert für den effektiven Schutz Kritischer Infrastrukturen generiert wird.

§ 14 „Bußgeldvorschriften“

Der Verweis auf das Ordnungswidrigkeitsgesetz sollte gestrichen werden.

Das sich der Ansatz beim Strafmaß im Falle von ordnungswidrigen Handlungen am europäischen Bußgeldrahmen orientiert, begrüßt der DVGW. Die vorgesehene abgestufte Höhe der Bußgelder ist aus unserer Sicht angemessen und sachgemäß. Allerdings hält der DVGW den eingeführten Verweis auf das Ordnungswidrigkeitsgesetz für nicht zielführend, da der Gesetzgeber sich hierdurch die Möglichkeit verschafft, den Bußgeldrahmen für juristische Personen und Personenvereinigungen unverhältnismäßig, um den Faktor 10, gegenüber dem Sanktionsmaß im vorliegenden Entwurf des IT-SiG 2.0, zu erhöhen.

Wir bitten daher um eine ersatzlose Streichung des Verweises auf das Ordnungswidrigkeitsgesetz im § 14 Abs. 2 BSIG. Es ist ferner sicher zu stellen, dass es nicht zu einer Doppelregulierung /-santionierung durch DSGVO und IT-SIG 2.0 kommen kann (sobald personenbezogene Daten betroffen sind).