Deutscher Verein des
Gas- und Wasserfaches e.V.

www.dvgw.de

STELLUNGNAHME

vom 21. Dezember 2016 zu

Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL-Umsetzungsgesetz)

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

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 Verein initiiert und fördert Forschungsvorhaben und schult zum gesamten Themenspektrum des Gas- und Wasserfaches. Ferner unterhält er ein Prüf- und Zertifizierungswesen für Produkte, Personen sowie Unternehmen. Die technischen Regeln des DVGW bilden das Fundament für die technische Selbstverwaltung und Eigenverantwortung der Gas- und Wasserwirtschaft in Deutschland. Sie sind der Garant für eine sichere Gas- und Wasserversorgung auf international höchstem Standard. Der gemeinnützige Verein wurde 1859 in Frankfurt am Main gegründet. Der DVGW ist wirtschaftlich unabhängig und politisch neutral.

Ansprechpartner

Für den Bereich Wasser:
Dipl.-Ing. Kirsten Wagner
Josef-Wirmer-Straße 1-3
D-53123 Bonn
Tel.: +49 228 9188-868
E-Mail: wagner@dvgw.de

Für den Bereich Gas:
Verm.-Ass. Dipl.-Ing. Frank Dietzsch
Josef-Wirmer-Straße 1-3
D-53123 Bonn
Tel.: +49 228 9188-914
E-Mail: dietzsch@dvgw.de

1 Einleitung

Das Bundesministerium des Innern (BMI) hat dem DVGW Deutscher Verein des Gas- und Wasserfaches am 9. Dezember 2016 den Referentenentwurf des Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL-Umsetzungsgesetz; Bearbeitungsstand: 07.12.2016) zur Eingabe einer Stellungnahme zugesandt.

Der DVGW begrüßt die Vorlage des Referentenentwurfes und dankt für die Möglichkeit zur Stellungnahme. Aufgrund des bereits im Juli 2015 in Kraft getretenen IT-Sicherheitsgesetzes wurden die wesentlichen Maßnahmen umgesetzt, somit ist aus Sicht des DVGW nur bei wenigen Punkten ein Änderungsbedarf notwendig.

Aus Sicht der Gas- und Wasserversorgung sind lediglich die Änderungen des BSI-Gesetzes (BSIG) für eine fachliche Kommentierung relevant. Hervorzuheben sind die erweiterten Regelungen zum Nachweis des Branchenstandards nach § 8a Abs. 4 BSIG sowie die Meldeschwelle nach § 8b Abs. 4 BSIG.

2 Zu den Regelungen des Gesetzesentwurfes im Einzelnen

- **Zum Artikel § 5a BSIG „Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen“**

§ 5a Abs. 1 BSIG versetzt das BSI in der Lage, im Falle einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems […] eines Betreibers einer Kritischen Infrastruktur, auf deren Ersuchen die informationstechnischen Maßnahmen zu treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind, wenn es sich um einen herausgehobenen Fall, d.h. wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems im besonderen öffentlichen Interesse ist (vgl. § 5a Abs. 2 BSIG).

Sofern dem Betreiber Kritischer Infrastrukturen keine obligatorische Beratung durch das BSI abverlangt wird, sondern stattdessen eine explizite Einwilligung eingehalten wird, ist das Angebot zur Unterstützung durch Fachleute aus dem BSI begrüßenswert.

In Absatz 5 wird festgelegt, dass das BSI mit der Einwilligung des Ersuchenden die Hilfe qualifizierter Dritter in Anspruch nehmen kann, wenn dies erforderlich ist. In Satz 3 ist jedoch angegeben, dass das BSI den Ersuchenden jederzeit ohne Einschränkung auch auf qualifizierte Dritte verweisen kann, ohne selbst tätig zu werden. Dies sollte nur im Ausnahmefall möglich sein, da der Vertrauensschutz in erster Linie zwischen dem Betreiber Kritischer Infrastruktur und dem BSI besteht. Es sollte darüber hinaus sichergestellt werden, dass die Dritten neben einer Qualifizierung auch über entsprechende Branchenkenntnisse verfügen.

Der DVGW schlägt folgende Textänderung für den 5. Absatz vor:
„Das Bundesamt kann sich bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden der Hilfe qualifizierter Dritter bedienen, […] Statt selbst tätig zu werden, kann das Bundesamt in **begründeten Fällen** die ersuchende Stelle auch auf qualifizierte Dritte **mit entsprechender Branchenkenntnis** verweisen. […]“

- **Zum Artikel § 8a Abs. 4 BSIG „Sicherheit in der Informationstechnik Kritischer Infrastrukturen“**

Der eingefügte neue § 8a Abs. 4 BSIG gibt dem BSI die Befugnis, die Einhaltung der Branchenstandards beim Betreiber selbst zu überprüfen. Dabei erhält das BSI die Möglichkeit sich einer qualifizierten Stelle zu bedienen. Erfolgt die Überprüfung aufgrund von Anhaltspunkten, die einen berechtigten Zweifel an der ordnungsgemäßen Einhaltung der Anforderungen gemäß § 8a Abs. 1 BSIG bieten, trägt der Betreiber Kritischer Infrastruktur die Kosten.

Grundsätzlich ist es nachvollziehbar, dass das BSI eine Handhabung benötigt, um in Fällen, in denen berechtigte Zweifel an der Einhaltung der Sicherheitsmaßnahmen zum Schutz der IT-Infrastruktur vorliegen, eine Überprüfung vornehmen zu können. Allerdings spezifiziert der Artikel nicht abschließend, in welchen Fällen diese Überprüfung erfolgen kann. In der Begründung ist nur angegeben, dass von der Möglichkeit zur Einsichtnahme beim Betreiber unter anderem dann Gebrauch gemacht werden soll, wenn die Prüfung der vom Betreiber nach § 8a Abs. 3, Satz 1 vorgelegten Nachweisen in begründeten Einzelfällen nicht ausreichend ist. Diese Formulierung lässt die Frage offen, in welchen anderen Fällen eine Überprüfung vorgenommen werden darf.

Des Weiteren legt § 8a Abs. 4 fest, dass der Betreiber Kritischer Infrastruktur die Kosten für die Überprüfung übernehmen muss, wenn die Überprüfung aufgrund von berechtigten Zweifeln an der Umsetzung der Sicherheitsmaßnahmen erfolgt, d.h. auch wenn die Überprüfung als Ergebnis ergibt, dass diese Zweifel nicht berechtigt waren. Eine Kostenübernahme durch den Betreiber Kritischer Infrastruktur ist nur zu rechtfertigen, wenn durch die Überprüfung festgestellt wird, dass tatsächlich eine fehlerhafte Umsetzung der Sicherheitsmaßnahmen vorgenommen wurde. In allen anderen Fällen ist eine Kostenübernahme durch den Betreiber nicht vertretbar.

Für die Überprüfung des Betreibers kann das BSI sich einer qualifizierten Stelle bedienen, z.B. einem vom BSI zertifizierten IT-Sicherheitsdienstleister wie Penetrationstestern oder Grundschutz-Auditoren. Durch diese Konstruktion entsteht eine nicht wünschenswerte Konkurrenzsituation zwischen der Person / Institution, welche die Einhaltung des Branchenstandards ursprünglich als akkreditierter (anerkannter) Auditor beim Betreiber Kritischer Infrastruktur durchgeführt hat und der Person / Institution des Unternehmens das vom BSI für die erneute Überprüfung beauftragt wird.

Der DVGW schlägt folgende Textänderung vor:
„Das Bundesamt kann **bei vorliegender schriftlicher Begründung, in der der Anlass der Überprüfung explizit aufgeführt ist,** beim Betreiber die Einhaltung der Anforderungen nach Absatz 1 überprüfen; es kann sich **im Ausnahmefall** bei der Durchführung der Aufsicht einer qualifizierten Stelle **mit entsprechender Branchenkenntnis** bedienen. Der Betreiber hat dem Bundesamt und den in seinem Auftrag handelnden Personen zu diesem Zweck das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstige Unterlagen in geeigneter Weise

vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Er trägt die Kosten dieser Überprüfung, sofern **die Überprüfung die berechtigten Zweifel an der ordnungsgemäßen Einhaltung der Anforderungen nach Absatz 1 bestätigt und beim Betreiber eine fehlerhafte Umsetzung der Sicherheitsmaßnahmen festgestellt wurde.** ~~das aufsichtsrechtliche Tätigwerden des Bundesamts aufgrund von Anhaltspunkten erfolgte, die berechtigte Zweifel an der ordnungsgemäßen Einhaltung der Anforderungen nach Absatz 1 begründen~~."

- **Zum Artikel § 8b Abs. 2 Nr. 4d und 4 BSIG „Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen"**

Nach § 8b Abs. 2 Nr. 4d muss das BSI unverzüglich Vorfälle an die zuständigen Behörden in einem anderen Mitgliedstaat der EU melden, wenn Auswirkungen auf Kritische Infrastrukturen von EU-Mitgliedsstaaten zu erwarten sind.

Diese Herangehensweise ist aus gasfachlicher Sicht sehr zu begrüßen, da Deutschlands Gasinfrastruktur innerhalb des europäischen Gasinfrastrukturverbundes hochgradig vernetzt ist.

Der DVGW begrüßt auch, dass die Nomenklatur zur Meldepflicht nach § 8b Abs. 4 inhaltlich im Vergleich zum bisherigen Gesetzestext angepasst wurde, so dass:

- nach Absatz 4 Nr. 1 „einfache" *Störungen* an informationstechnischen Systemen, Komponenten oder Prozessen, die zu einem Ausfall oder einer erheblichen Beeinträchtigung *geführt haben*, zu melden.
- sowie nach § 8b Absatz 4 Nr. 2 Vorfälle zu melden, sofern *erhebliche Störungen* der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse vorliegen, die zu einem Ausfall oder einer erheblichen Beeinträchtigung *führen können*.

- **Zum Artikel § 8d Abs. 4 BSIG „Anwendungsbereich"**

Der § 8d Abs. 4 BSIG legt fest, das auf Kleinstunternehmen und kleine Unternehmen die Anforderungen des § 8a und § 8b nicht anzuwenden sind. Diese Ausnahmeregelung für Kleinstunternehmen und kleine Unternehmen begrüßt der DVGW, allerdings ist die Einstufung gekoppelt an die europäische Richtlinie 2003/362/EG der Kommission vom 6. Mai 2003. Auf Kleinstunternehmen und kleine Unternehmen, deren Anteile zu mindestens 25 Prozent von einer staatlichen Stelle oder Körperschaft des öffentlichen Rechts kontrolliert werden, ist diese Ausnahmeregelung somit nicht anwendbar, so dass die jetzige Formulierung vor allem zu einer Ungleichbehandlung führt.

Da es nicht zielführend ist, diese Unternehmen (trifft in unserem Fall insbesondere auf kommunale Wasserversorgungsunternehmen zu) von der Kleinstregelung auszunehmen, schlägt der DVGW vor, beim Verweis der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 auf die Teilregelung für die kommunalen Anteilseigner zu verzichten und den § 8d Abs. 4 BSIG in folgender Weise anzupassen:

„§ 8c Absatz 1 und 2 gilt nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission. Artikel 3 Absatz 4 des Anhangs der Empfehlung ist nicht anzuwenden. […].“