Energie. Wasser. Leben.

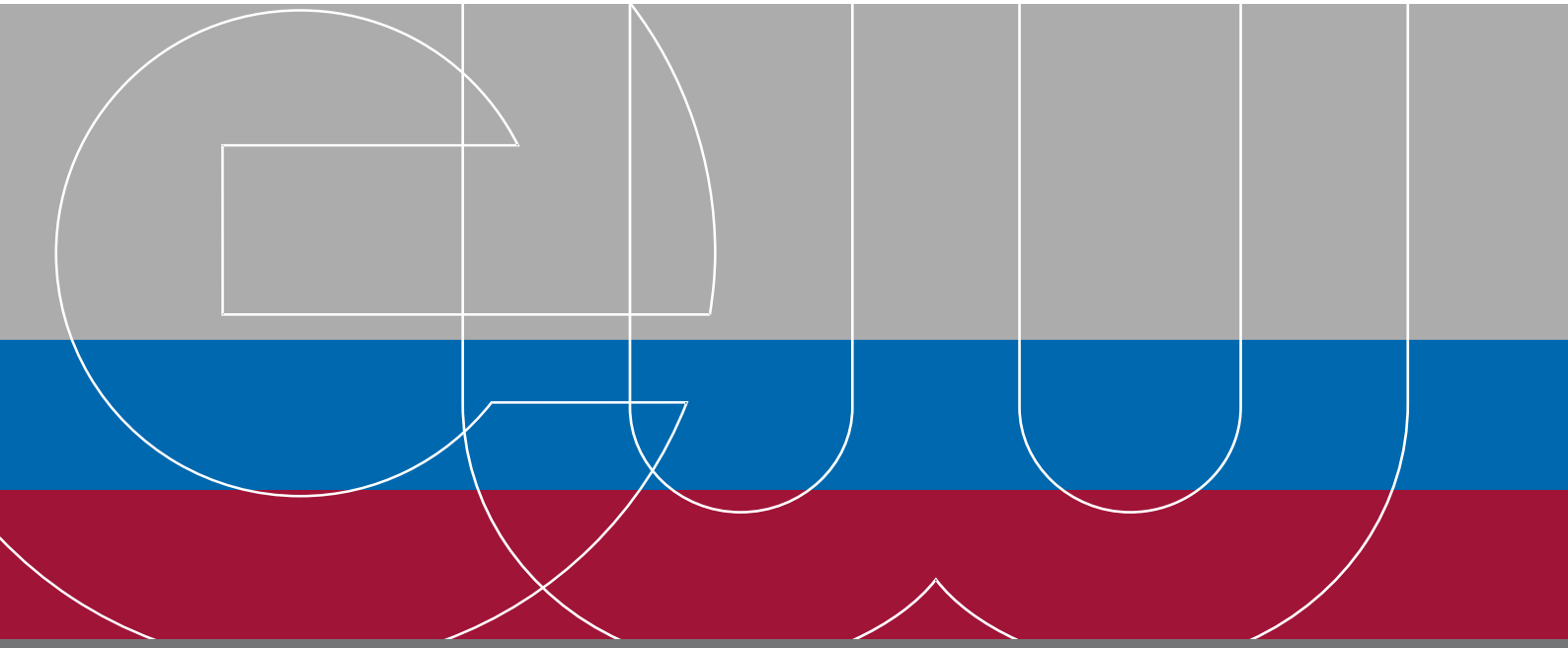
BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin
Telefon +49 30 300 199-0
Telefax +49 30 300 199-3900
E-Mail info@bdew.de
www.bdew.de

Stellungnahme

Referentenentwurf des Bundesministeriums des Innern

Entwurf eines 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

Berlin, 16. Dezember 2016



bdew
Energie. Wasser. Leben.

1 Einleitung

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) vertritt Betreiber Kritischer Infrastrukturen in den Sektoren Energie und Wasser / Abwasser.

Das Bundesministerium des Innern (BMI) hat dem BDEW 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) zugesandt. Der BDEW begrüßt die Vorlage des Referentenentwurfes und dankt für die Möglichkeit zur Stellungnahme.

Die Kernforderungen des BDEW zum Gesetzentwurf sind:

- Klarstellung an geeigneter Stelle, dass Web-Dienste zum Vertragsabschluss sowie Online-Shops für Waren und Dienstleistungen von Unternehmen der Energie- und Wasserwirtschaft auf deren eigenen Webseiten keine „Online-Marktplätze“ im Sinne des § 2 Abs. 9 BSI-G darstellen
- Konkretisierung der in § 5a BSI-G genannten Maßnahmen zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen sowie Einbeziehung des UP KRITIS beim Treffen dieser Maßnahmen
- Ergänzung des § 8a Abs. 3 BSI-G, um Unternehmen zur Entbürokratisierung die Vorlage der Dokumente, die den Überprüfungen nach § 8a Abs. 1 BSI-G zugrunde gelegt wurden, wahlweise in deutscher oder englischer Sprache zu ermöglichen
- Verpflichtung des BSI, die Auswahl qualifizierter Stellen bei der Durchführung der Aufsicht nach § 8a Abs. 4 BSI-G im Benehmen mit dem Betreiber zu treffen, um eine Wahrung der Vertraulichkeit der informationstechnischen Systeme des Betreibers zu ermöglichen
- Eine unverschuldet anfänglich nicht-richtig vorgenommene Bewertung „möglicher grenzüberschreitender Auswirkungen“ bei Meldungen nach § 8b Abs. 4 BSI-G und § 11 Abs. 1c EnWG sollte keine Ordnungswidrigkeit darstellen
- Anpassung der Ausnahmeregelung für Kleinstunternehmen und kleine Unternehmen für Anbieter digitaler Dienste in § 8d Abs. 4 BSI-G analog zur bereits bestehenden Ausnahmeregelung für Kleinstunternehmen im derzeitigen § 8c Abs. 1 BSI-G. Es muss sichergestellt werden, dass Unternehmen mit einem überwiegenden Teil kommunaler Anteilseigner von der Ausnahmeregelung erfasst werden.
- Genaue Erläuterung und Konkretisierung, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Wahrung der Vertraulichkeit bei Übermittlung von Informationen nach § 13 Abs. 5 BSI-G an die Kooperationsgruppe der EU nach Artikel 11 der Richtlinie (EU) 2016/1148 sicherstellt

- Darüber hinaus wird das BMI gebeten, darauf hinzuwirken, dass die Mitgliedsstaaten der EU bei Umsetzung des Artikels 19 der NIS-Richtlinie auch weiterhin die Möglichkeit haben, branchenspezifische Mindeststandards festzulegen, die nationale, europäische sowie internationale Normen und Standards (siehe dazu auch Hinweise des BSI) berücksichtigen. Dabei sollte auch sichergestellt werden, dass die von der Bundesnetzagentur erstellten IT-Sicherheitskataloge nach § 11 Abs. 1a und 1b EnWG anerkannt werden können. Weiterhin wird angeregt, zu prüfen, ob die ISO/IEC 27000-Reihe als europäische Norm festgelegt werden kann.

2 Artikel 1 – Änderungen des BSI-Gesetzes

2.1 Vorschriften für Anbieter digitaler Dienste, Änderung des § 2 Abs. 9 BSI-G

Gemäß den Anforderungen der NIS-Richtlinie werden im vorliegenden Gesetzesentwurf zahlreiche neue Pflichten für Anbieter digitaler Dienste wie Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste eingeführt. Nach der Gesetzesbegründung fallen hierunter ausdrücklich keine Unternehmen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienstleistungen erbringen.

Der BDEW bittet darüber hinaus um eine Klarstellung an geeigneter Stelle, dass mit „Online-Marktplätzen“ Plattformen zum Abschließen von Kauf- oder Dienstleistungsverträgen mit anderen juristischen oder natürlichen Personen als dem Eigentümer oder Betreiber der Webseite oder des Dienstes selbst gemeint sind, und somit beispielsweise Web-Dienste zum Vertragsabschluss sowie Online-Shops für Waren und Dienstleistungen von Unternehmen der Energie- und Wasserwirtschaft auf deren eigenen Webseiten ausgeschlossen sind.

2.2 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen, Neueinfügung des § 5a BSI-G

Der BDEW begrüßt ausdrücklich, dass Betreiber Kritischer Infrastrukturen durch die hier beschriebenen Maßnahmen bei herausgehobenen Fällen Unterstützung des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Anspruch nehmen können. Hier ist es besonders wichtig, dass diese Unterstützung auf das Ersuchen des Betreibers hin erfolgt und eine Weitergabe von im Rahmen dieser Vorschrift anfallenden Informationen nur nach ausdrücklicher Einwilligung des betroffenen Betreibers einer Kritischen Infrastruktur möglich ist. Im Sektor Wasser/Abwasser ist darüber hinaus sicherzustellen, dass ein Eingriff in die kommunale Entscheidungshoheit der Wasserwirtschaft und insbesondere im hoheitlichen Sektor Abwasser ausgeschlossen wird.

In § 5a Abs. 2 BSI-G werden herausgehobene Fälle, bei denen das BSI Unterstützung leisten kann, näher eingegrenzt. Da die hier getroffene Eingrenzung auf herausgehobene Fälle bereits hinreichend spezifisch ist und somit alltägliche Beeinträchtigungen oder Beeinträchtigungen, bei denen die zügige Wiederherstellung der Systeme nicht in besonderem öffentlichen Interesse stehen, ausgeschlossen sind, ist es für Betreiber Kritischer Infrastrukturen der

Energie- und Wasserwirtschaft jedoch wichtig, dass sie sich im Zweifelsfall in diesen Situationen auch auf eine Unterstützung des BSI verlassen können. Daher plädiert der BDEW dafür, die „kann“-Formulierung in Absatz 1 zu ändern:

§ 5a Abs. 1 BSI-G

Im Falle einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur ~~kann~~ **trifft** das Bundesamt auf deren Ersuchen die Maßnahmen ~~treffen~~, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind, wenn es sich um einen herausgehobenen Fall handelt.

Die Wasserwirtschaft bittet darüber hinaus darum, den UP KRITIS sowie die entsprechenden Sektorreferate des BSI beim Treffen der Maßnahmen einzubinden.

In Absatz 5 ist geregelt, dass das BSI mit der Einwilligung des Ersuchenden auch die Hilfe qualifizierter Dritter in Anspruch nehmen kann, wenn dies erforderlich ist. Dies ist im Grunde nachvollziehbar und kann auch hilfreich sein, wenn es der frühzeitigen Beseitigung einer Störung dient. In Satz 3 ist jedoch geregelt, dass das BSI den Ersuchenden jederzeit ohne Einschränkung auch auf qualifizierte Dritte verweisen kann, ohne selbst tätig zu werden. Vor dem Hintergrund der vorgenannten Argumente, dass sich Betreiber im Zweifelsfall auf die Unterstützung des BSI verlassen können, sollte dies jedoch nur für begründete Fälle möglich sein. Darüber hinaus sollte sichergestellt sein, dass die vorgeschlagenen Dritten über Branchenkenntnis verfügen. Der BDEW schlägt daher folgende Änderung des Absatz 5 vor:

§ 5a Abs. 5 BSI-G

Das Bundesamt kann sich bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden der Hilfe qualifizierter Dritter bedienen, wenn dies zur rechtzeitigen oder umfänglichen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat der Ersuchende zu tragen. Statt selbst tätig zu werden, kann das Bundesamt **in begründeten Fällen** die ersuchende Stelle auch auf qualifizierte Dritte **mit Branchenkenntnis** verweisen.

2.3 Überprüfung der Dokumentationen, die der Überprüfung zugrunde gelegt wurden, Änderung des § 8a Abs. 3

Durch die Änderung in Absatz 3 wird es dem BSI zukünftig ermöglicht, die Dokumentationen, die der Überprüfung zugrunde gelegt wurden, zu verlangen, auch wenn vorher keine Mängel angezeigt wurden. Diese Änderung ist erforderlich, um Artikel 15 der NIS-Richtlinie umzusetzen. Vor allem bei internationalen Unternehmen wird ein Großteil der erforderlichen Dokumentation in der Regel in englischer Sprache geführt. Zur Vermeidung zusätzlicher Übersetzungskosten und zur Entbürokratisierung plädiert der BDEW mit Nachdruck dafür, dass im Gesetz klargestellt wird, dass diese Dokumentationen neben Deutsch auch in englischer Sprache vorgelegt werden dürfen:

§ 8a Abs. 3 BSI-G

Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. **Die Dokumentation kann wahlweise in deutscher oder englischer Sprache vorgelegt werden.**

2.4 Überprüfung der Einhaltung der Anforderungen durch das BSI unter Einbeziehung qualifizierter Stellen, Neueinfügung des § 8a Abs. 4 BSI-G

Zur Wahrung der Vertraulichkeit der informationstechnischen Systeme ist es für Betreiber Kritischer Infrastrukturen wichtig, dass bei der Überprüfung der Anforderungen nach § 8a Abs. 1 BSI-G nicht beliebige Dritte hinzugezogen werden können. Nachvollziehbar ist jedoch auch, dass das BSI zur Wahrung seiner Aufgaben eine gewisse Entscheidungskompetenz bei der Auswahl einer qualifizierten Stelle benötigt. Daher sollte das BSI verpflichtet werden, die Auswahl der qualifizierten Stelle im Benehmen mit dem betroffenen Betreiber zu treffen. Konkret schlägt der BDEW folgende Formulierung vor:

§ 8a Abs. 4 BSI-G

Das Bundesamt kann beim Betreiber die Einhaltung der Anforderungen nach Absatz 1 überprüfen; es kann sich bei der Durchführung der Aufsicht einer qualifizierten Stelle bedienen. **Die Auswahl der qualifizierten Stelle durch das BSI erfolgt im Benehmen mit dem Betreiber.**

2.5 Meldepflichten für Betreiber Kritischer Infrastrukturen, Änderung des § 8b BSI-G

Nach der Neufassung müssen Meldungen an das BSI zusätzlich zu den Angaben zur Störung auch Angaben zu „möglichen grenzübergreifenden Auswirkungen“ enthalten. Diese Ausweitung ist durch Anforderungen aus Artikel 14 Abs. 3 der NIS-Richtlinie erforderlich. Der Aspekt der grenzübergreifenden Auswirkungen ist u. a. für Betreiber von Energieversorgungsnetzen zwar bereits Bestandteil der durchzuführenden Risikoanalyse nach dem IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG, aber bisher bewusst kein Bestandteil der Meldeprozesse. Vor dem Hintergrund, dass nach der Änderung des § 95 Abs. 1 EnWG künftig auch „nicht richtige“ Meldungen eine Ordnungswidrigkeit darstellen und somit direkte finanzielle Folgen für Betreiber haben können, weist der BDEW darauf hin, dass die Bewertung „möglicher grenzübergreifender Auswirkungen“ im Einzelfall schwierig ist und sich diese Bewertung auch im Laufe der Beseitigung einer Störung ändern kann. Der BDEW plädiert daher dafür, an geeigneter Stelle klarzustellen, dass eine anfänglich unverschuldete nicht-richtig vorgenommene Bewertung „möglicher grenzübergreifender Auswirkungen“ keine Ordnungswidrigkeit darstellt.

2.6 Änderung des Anwendungsbereichs des BSI-Gesetzes für Betreiber von Energieanlagen und Energieversorgungsnetzen, Änderung des § 8d Abs. 3 BSI-G (ehemals § 8c)

Durch die Änderung des neuen § 8d Abs. 3 BSI-G werden Betreiber von Energieanlagen und Energieversorgungsnetzen, die auch Betreiber Kritischer Infrastrukturen sind, fortan verpflichtet, beim BSI eine Kontaktstelle nach § 8a Abs. 3 BSI-G zu benennen. Dies führt bei Betreibern von Energieanlagen und Energieversorgungsnetzen zu Erfüllungsaufwand, ist jedoch konsequent, da das BSI nur so seinem Informationsauftrag für Betreiber Kritischer Infrastrukturen nach § 8b Abs. 2 Nr. 4a BSI-G nachkommen kann. Der BDEW hatte seinen Mitgliedsunternehmen daher bereits seit Inkrafttreten der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) eine freiwillige Benennung einer Kontaktstelle beim BSI empfohlen.

2.7 Ausnahme für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission, Einfügung des § 8d Abs. 4 (ehemals § 8c)

Der BDEW begrüßt die hier vorgeschlagene Ausnahme für Kleinstunternehmen und kleine Unternehmen. Mit diesem Regelungsvorschlag trägt der Entwurf dem Grundsatz der Verhältnismäßigkeit Rechnung. Der Verweis auf die Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 führt jedoch dazu, dass diese Ausnahme für zahlreiche Kleinstunternehmen und kleine Unternehmen nicht anwendbar ist und daher der Zweck der Ausnahme für Kleinstunternehmen und kleine Unternehmen verfehlt wird.

Die Definition der Kommission zählt Unternehmen, deren Anteile zu mindestens 25 % von einer staatlichen Stelle oder Körperschaft des öffentlichen Rechts kontrolliert werden, grundsätzlich nicht zu den KMU. Damit sind beispielsweise Kleinstunternehmen und kleine Unternehmen, die zu einem überwiegenden Teil kommunale Anteilseigner haben, automatisch ausgeschlossen.

Für Regelungen mit Bezug zur Finanzierung von KMU ist diese Einschränkung anwendbar. Im Kontext IT-Sicherheit ist sie dagegen kein tragfähiges Differenzierungsmerkmal und führt zu einer systematischen Ungleichbehandlung im Vergleich zu Unternehmen anderer Branchen.

Der BDEW schlägt daher vor, wie bereits im derzeit gültigen § 8c Abs. 1 Satz 2 BSI-G im Verweis auf die Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003, auf die Teilregelung für die kommunalen Anteilseigner zu verzichten. Die Kriterien Mitarbeiteranzahl und Gesamtumsatz sind aus Sicht des BDEW eine geeignetere Grundlage. Zusätzlich wird hierdurch sichergestellt, dass die Ausnahmeregelungen für Kleinstunternehmen und kleine Unternehmen innerhalb des BSI-Gesetzes einheitlich sind. Der BDEW schlägt folgenden Regelungsansatz vor:

§ 8d Abs. 4 BSI-G

§ 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.**

2.8 Übermittlung eines zusammenfassenden Berichts nach § 13 Abs. 5 BSI-G an die Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 unter Wahrung der Vertraulichkeit

In Absatz 4 wird das BSI verpflichtet, unter Wahrung der Vertraulichkeit bis zum 9. August 2018 und danach jährlich einen zusammenfassenden Bericht zu den eingegangenen Meldungen nach § 8b und 8c BSI-G an die Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 zu übermitteln. Da die darin enthaltenen Informationen zur Art der gemeldeten Sicherheitsvorfälle sowie die ergriffenen Maßnahmen sensible Inhalte darstellen, fordert der BDEW eine genaue Erläuterung und Konkretisierung, wie das Bundesamt die Wahrung der Vertraulichkeit gewährleistet.

Ansprechpartner:

Für den Sektor Energie
Kay Tidten
Telefon: +49 30 300 199-1526
kay.tidten@bdew.de

Für den Sektor Wasser/Abwasser
Dr. Michaela Schmitz
Telefon: +49 30 300 199-1200
michaela.schmitz@bdew.de