Deutscher Bundestag **Drucksache 19/20965**

19. Wahlperiode 10.07.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Lukas Köhler, Frank Sitta, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/ 19967 –

Sicherheit der Wasserversorgung in Deutschland

Vorbemerkung der Fragesteller

Eine funktionierende und sichere Wasserversorgung, die Versorgung der Allgemeinheit mit Trinkwasser (Trinkwasserversorgung) sowie die Beseitigung von Abwasser der Allgemeinheit (Abwasserbeseitigung) leisten nicht nur einen wichtigen Beitrag zur gesicherten Lebensgrundlage in Deutschland, sondern sind auch Grundvoraussetzung für die Wirtschaft und Hygiene der Bevölkerung. Betreiber solcher Kritischen Infrastrukturen (sog. KRITIS-Betreiber) unterliegen als Dienstleister der Wasserver- und Wasserentsorgung daher strikten Auflagen und Regelungen.

Laut EU-Richtlinie 2008/114/EG über die Ermittlung und Ausweisung europäischer Kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32008L0114 ist eine Kritische Infrastruktur definiert als: „eine Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung ist und deren Störung oder Zerstörung erhebliche Auswirkungen hätte, da ihre Funktionen nicht aufrechterhalten werden könnten."

In Deutschland regelt seit 2009 das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (§ 2 Absatz 10 BSIG und § 10 Absatz 1 BSIG) sowie die zugehörige BSI-Kritisverordnung (BSI-KritisV) näher die betroffenen Branchen und Anlagen in den Sektoren Wasser, Energie, Ernährung, Informationstechnik und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr: „Die Betreiber dieser Kritischen Infrastrukturen, unabhängig davon, ob privatwirtschaftlich oder öffentlich-rechtlich organisiert, erbringen die kritischen, für die Versorgung der Bevölkerung zwingend notwendigen Dienstleistungen in hoher Qualität und Stabilität. Die ausgeprägte Widerstandsfähigkeit dieser kritischen Dienstleistungen gegen vielfältige Bedrohungen ist der Beweis für das Verantwortungsbewusstsein der KRITIS-Betreiber und bildet eine wesentliche Grundlage für das Funktionieren der Gesellschaft." (https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html#:~:text=Die%20Betreiber%20dieser%20Kritischen%20Infrastrukturen,in%20hoher%20Qualit%C3%A4t%20und%20Stabilit%C3%A4t). Darüber hinaus existieren in Deutschland noch die Sektoren Staat

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 10. Juli 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

und Verwaltung sowie Medien und Kultur. Die Wassersicherstellungsgesetz (1965) über die Sicherstellung von Leistungen auf dem Gebiet der Wasserwirtschaft für Zwecke der Verteidigung regelt die Versorgung der Zivilbevölkerung und der Streitkräfte mit Trinkwasser im Verteidigungsfall.

Seit 2015 regelt das Gesetz zur IT-Sicherheit (IT-SiG) die Sicherheit informationstechnischer Systeme sowie den Schutz Kritischer Infrastrukturen (KRITIS) und verpflichtet ihre Betreiber zur Einhaltung eines definierten Mindestmaßes an IT-Sicherheit, angemessene technische und organisatorische Maßnahmen zu treffen und diese nachzuweisen. Einer Meldepflicht gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und gegenüber Kunden muss nachgekommen werden.

Rechtsverordnungen aus den Jahren 2016 und 2017 geben die Einstufung von Anlagen als Kritische Infrastruktur vor und grenzen durch Regelschwellenwerte genauer ab, welche Betreiber unter die KRITIS-Regelungen fallen, um die Instandsetzung und den Schutz Kritischer Infrastrukturen und deren Dienstleister zu gewährleisten. Einen branchenspezifischen IT-Sicherheitsstandard Wasser/Abwasser (B3S) haben die beiden Verbände DVGW (Deutscher Verein des Gas- und Wasserfaches) und DWA (Deutsche Vereinigung für Wasserwirtschaft, Abwasser Abfall) gemeinsam entwickelt, „der sowohl den von der BSI-KritisV betroffenen Unternehmen wie auch kleinen und mittleren Wasserver- und Abwasserentsorgungsunternehmen ein Instrument an die Hand gibt, um ein Schutzniveau zu implementieren, dass dem Stand der Technik entspricht.“ (http://www.protekt.de/de/Aktuelles/itsicherheit-nachweispflicht-fuer-vier-kritissektoren-tritt-heute-in-kraft/794277). Das BSI hat die Eignung des IT-Sicherheitsstandards für den Sektor Wasser gemäß § 8a Absatz 2 des BSI-Gesetzes festgestellt. Nach zwei Jahren Gültigkeit ist der Standard 2019 abgelaufen. Ein neuer Standard wurde am 27. März 2020 auf dem Webportal der Lizenzträger der Verbände veröffentlicht (https://b3s-wa.de/). Die Eignungsfeststellung des BSI wurde laut Aussagen der Verbände im Januar 2020 festgestellt.

Die in Anhang 2, Teil 3 der BSI-KritisV aufgeführten Regelschwellenwerte geben an, dass die Verordnung für Kritische Infrastrukturen nur für Anlagen verpflichtend gilt, die den Schwellenwert von 500 000 Personen erreichen oder überschreiten (bzw. Millionen m³, als Summe des Durchschnittswerts pro Einwohner). Laut Zahlen des Statistischen Bundesamtes zur öffentlichen Wasserversorgung und öffentlichen Abwasserentsorgung 2016, https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Umwelt/Wasserwirtschaft/Publikationen/Downloads-Wasserwirtschaft/wasser-oeffentlich-2190211169004.pdf?__blob=publicationFile, ist zu entnehmen, dass weniger als 1 Prozent (17 von 5 845) der Wasserversorgungsunternehmen in Deutschland aus dieser Ableitung verpflichtend unter Auflagen der Verordnung fallen (https://de.statista.com/statistik/daten/studie/289703/umfrage/anzahl-der-wasserversorgungsunternehmen-in-deutschland-nach-anzahl-der-versorgten-einwohner/). Die Regelschwellenwerte wurden zuletzt Juni 2016 und Juni 2017 überprüft und angepasst. § 9 der BSI-Kritisverordnung sieht eine Anpassung der Regelschwellenwerte mindestens alle zwei Jahre vor.

Der Referentenentwurf des seit 2018 angekündigten „Kritische Infrastrukturen im IT-Sicherheitsgesetz 2.0“ (IT-SiG 2.0) sah zudem eine Anzahl an Neuerungen vor. Beispielsweise wurde die Aufnahme des Bereichs „Entsorgung“ in die Liste der Betreiber vorgesehen. Für die Kategorien „Infrastrukturen von besonderem öffentlichem Interesse“, wie Rüstung, Kultur und Medien, sowie Infrastrukturen mit kritischer Bedeutung für die Geschäftstätigkeit von Unternehmen des Prime Standard an der Frankfurter Wertpapierbörse sollten ebenfalls besondere Auflagen gelten. Die Rechtsverordnung dazu als auch das IT-SiG 2.0 stehen jedoch immer noch aus.

Im Zuge der Corona-Pandemie hat das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe in seinen Handlungsempfehlungen für Unternehmen, insbesondere für Betreiber Kritischer Infrastrukturen, Folgendes bestätigt: „Cyberkriminelle machen sich oft das erhöhte Informationsbedürfnis in aktuellen Lagen zunutze, schädliche Links und manipulierte Anhänge mit Schad-

software zu verbreiten. Dies wird bezogen auf COVID-19 bereits weltweit beobachtet, auch Deutschland-spezifische Mails sind bereits im Umlauf.“ Über die Anlagen der Betreiber werden keine speziellen Aussagen getroffen.

Laut Wassersicherstellungsgesetz besteht eine Notversicherung von Trinkwasser durch ein Netzwerk an verstreuten Trinkwassernotbrunnen. In Deutschland gibt es laut Aussage des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) rund 5 000 solcher Anlagen. Das Gesetz bezieht sich dabei auf Verteidigungsfälle und in geringem Maße auf Naturkatastrophen.

1. Wie definiert die Bundesregierung einen Cyberangriff auf Kritische Infrastrukturen?

Gemäß der Cyber-Sicherheitsstrategie der Bundesregierung 2016 ist ein Cyberangriff definiert als eine Einwirkung auf ein oder mehrere andere informationstechnische Systeme im oder durch den Cyber-Raum, die zum Ziel hat, deren IT-Sicherheit durch informationstechnische Mittel ganz oder teilweise zu beeinträchtigen. Kritische Infrastrukturen (KRITIS) im Sinne des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-G) sind gemäß § 2 Absatz 10 BSI-Gesetz definiert als Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die Kritischen Infrastrukturen im Sinne des BSI-Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 BSI-Gesetz näher bestimmt.

2. Welche Informationen liegen der Bundesregierung zu den jeweiligen Branchen der KRITIS-Betreiber vor, die laut BSI-Lagebericht 2019 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7) Angriffe auf ihre Anlagen vermeldeten?

Gemäß § 8b Absatz 4 BSI-Gesetz haben die Meldungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung zu enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

Gemäß § 8d Absatz 3 BSI-Gesetz gelten für folgende Betreiber nicht die vorgenannten Regelungen des § 8b Absatz 4 BSI-G, sondern entsprechende spezialgesetzliche Regelungen u. a. im Telekommunikationsgesetz (§ 109 TKG), im Energiewirtschaftsgesetz (§ 11 EnWG), im Atomgesetz (§ 44b AtG), sowie im Fünften Buch des Sozialgesetzbuches (§ 291b SGB 5):

- Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,
- Betreiber von Energieversorgungsnetzen oder Energieanlagen, soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen,

- die Gesellschaft für Telematik nach § 291a Absatz 7 Satz 2 des Fünften Buches Sozialgesetzbuch und § 291b des Fünften Buches Sozialgesetzbuch,
- Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 291b Absatz 1a und 1e des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 291b Absatz 1b des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzen,
- Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie
- sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 4 vergleichbar oder weitergehend sind.

3. Wie schätzt die Bundesregierung das Risiko von Cyberangriffen auf Kritische Infrastrukturen, insbesondere Wasserversorger, in der aktuellen Notlage durch COVID-19 ein, und inwiefern sieht sie diese durch die aktuell geltenden Regelungen gewappnet?

Der Bundesregierung ist keine substanzielle Zunahme von schwerwiegenden Angriffen auf Kritische Infrastrukturen in der aktuellen COVID-19 Lage bekannt. Das COVID-19 Thema wird jedoch allgemein bei der Durchführung von Phishing-Kampagnen als thematischer Aufhänger genutzt.

Die aktuell mit dem BSI-Gesetz und der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) bestehenden Regelungen haben in den vergangenen Jahren aus Sicht der Bundesregierung zu einer signifikanten Verbesserung der Cybersicherheit in Kritischen Infrastrukturen in Deutschland geführt, wodurch Betreiber Kritischer Infrastrukturen in diesem Bereich deutlich besser aufgestellt sind.

4. Welche Herausforderungen sieht die Bundesregierung aktuell für die Sicherheit der einen flächendeckenden großen Anteil der Wasserversorgung stellenden kommunalen kleinen und mittleren Unternehmen?

Die Fragestellung wird in Bezug auf Herausforderungen im Bereich der IT-Sicherheit beantwortet. Auch kommunale kleine und mittlere Unternehmen der Wasserversorgung sind grundsätzlich vergleichbaren Risiken im Bereich der Cybersicherheit ausgesetzt, haben jedoch nicht immer auch vergleichbare Ressourcen und Mittel wie größere Unternehmen zur Verfügung. Es ist daher wichtig, dass z. B. branchenspezifische Sicherheitsstandards nach § 8a Absatz 2 BSI-Gesetz so ausgestaltet werden, dass sie auch ganz oder in Teilen von Betreibern eingesetzt werden können, welche die Schwellenwerte der BSI-KritisV nicht erreichen.

5. Welcher Anteil der Bevölkerung ist nach Einschätzungen der Bundesregierung von den Auflagen der KRITIS-Verordnung abgedeckt?

Diese Frage kann aufgrund von Überschneidungen zwischen den und innerhalb der einzelnen Sektoren, z. B. durch Mehrfachversorgung von Bürgern durch mehrere KRITIS-Betreiber aus einem oder mehreren Sektoren nicht genauer beantwortet werden.

Gemäß § 2 Absatz 10 BSI-G i.v.m. der Rechtsverordnung nach § 10 Absatz 1 BSI-G gelten diejenigen Einrichtungen, Anlagen oder Teile davon der Sektoren

Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit,

Wasser, Ernährung sowie Finanz- und Versicherungswesen als Kritische Infrastrukturen und fallen somit unter die entsprechenden Auflagen des BSI-Gesetzes, die einen Versorgungsgrad erreichen oder überschreiten, gemäß § 1 Satz 1 BSI-KritisV als bedeutend anzusehen ist.

6. Wie systemrelevant schätzt die Bundesregierung die Anzahl der KRITIS-Betreiber und deren Anlagen in Bezug auf die Gesamtbevölkerung ein?

Die durch das das BSI-Gesetz und die BSI-KritisV bestimmten KRITIS-Betreiber sind von hoher Bedeutung für das Funktionieren des Gemeinwesens in Deutschland, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Aus der unmittelbaren tatbestandlichen Anknüpfung in § 10 Absatz 1 BSI-Gesetz an den als bedeutend anzusehenden Versorgungsgrad lässt sich ableiten, dass KRITIS-Betreiber versorgungsrelevant sind. Dies ist jedoch nicht immer zwangsläufig gleichbedeutend mit einer Systemrelevanz im Kontext der Bekämpfung einer akuten Notlage, wie der derzeitigen Corona-Pandemie.

7. Welche Risiken sieht sie hier durch mögliche Cyberangriffe auf die Wasserversorgung in Deutschland?

Erfolgreiche Cyberangriffe können grundsätzlich zu Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse der Wasserversorgung in Deutschland führen. Hierdurch sind prinzipiell auch Auswirkungen auf die Versorgungssicherheit möglich.

8. Welchen Zeitplan verfolgt die Bundesregierung für das bereits angekündigte IT-Sicherheitsgesetz 2.0?

Welche konkreten Änderungen sind betreffend Kritische Infrastrukturen vorgesehen?

Der Entwurf des IT-Sicherheitsgesetzes 2.0 befindet sich in der Ressortabstimmung. Zu Zeitplan und konkret geplanten Änderungen kann daher derzeit keine Aussage getroffen werden.

9. Welche Akteure aus dem Bereich der Kritischen Infrastrukturen plant die Bundesregierung, in die Verbändebeteiligung zu dem Gesetz mit einzubeziehen?

In die Verbändebeteiligung gemäß § 47 der Gemeinsamen Geschäftsordnung (GGO) werden die einschlägigen Industrie- und Branchenverbände sowie die öffentlich-private Zusammenarbeit UP KRITIS einbezogen.

10. Werden Anstrengungen unternommen, um einen ausreichenden Einbezug von sowohl unabhängigen Experten und Wissenschaftlern als auch den betroffenen Wirtschaftsverbänden zu gewährleisten?

Erkenntnisse und Empfehlungen von unabhängigen Experten, Wissenschaftlern, Wirtschaftsverbänden und der öffentlich-privaten Zusammenarbeit UP KRITIS fließen in den Gesetzentwurf ein.

11. Sieht die Bundesregierung dahin gehend Nachbesserungsbedarf für Betriebe, die aufgrund der Regelschwellenwerte nicht unter die IT-Sicherheitsauflagen der BSI-KritisV fallen?

12. Wenn ja, welche Evaluationsbegründung legt die Bundesregierung der Entscheidung zugrunde, diese nicht anzupassen?

13. Wenn nein, wie erklärt die Bundesregierung, dass die Verordnung nicht gemäß § 9 BSI-KritisV evaluiert und ggf. angepasst wurde?

Die Fragen 11, 12 und 13 werden aufgrund ihres inhaltlichen Zusammenhangs zusammen beantwortet.

Eine 2019 durchgeführte Evaluierung der BSI-KritisV hat Anpassungsbedarf an einigen Stellen der Verordnung ergeben. Ein Entwurf einer Änderungsverordnung wird derzeit erstellt.

14. Sieht die Bundesregierung Bedarf, die Regelschwellenwerte abzusenken?

    a) Wenn nein, warum nicht?

    b) Wenn ja, nach welchem Zeitplan sollte dies geschehen?

Die Fragen 14, 14 a) und 14 b) werden aufgrund ihres inhaltlichen Zusammenhangs zusammen beantwortet.

Es wird auf die Antwort zu den Fragen 11, 12 und 13 verwiesen. Die diesbezügliche Änderungsverordnung wird aktuell noch erstellt. Aufgrund der noch nicht abgeschlossenen Ressortabstimmungen können zum aktuellen Zeitpunkt keine Aussagen zum Inhalt und Zeitplan getroffen werden.

15. Welche Maßnahmen sieht die Bundesregierung für Betreiber, die aufgrund der Schwellenwerte nicht unter die BSI-KritisV fallen, vor?

Bei Erreichen oder Überschreiten der Schwellenwerte der BSI-KritisV liegt gemäß § 1 Satz 1 Nummer 5 BSI-KritisV ein Versorgungsgrad vor, der aus Bundessicht als bedeutend im Sinne von § 10 Absatz 1 Satz 1 des BSI-Gesetzes anzusehen ist.Gegebenenfalls notwendige weitergehende verpflichtende Maßnahmen für Betreiber, welche die aus Bundessicht festgelegten Schwellenwerte nicht erreichen, liegen im Übrigen im Zuständigkeitsbereich der Länder.

Jedoch können auch Betreiber, welche die Schwellenwerte der BSI-KritisV nicht erreichen, vom Bundesamt für Sicherheit in der Informationstechnik eignungsgeprüfte branchenspezifische Sicherheitsstandards gemäß § 8a Absatz 2 BSI-Gesetz sowie weitergehende Empfehlungen des BSI vollständig oder in Teilen freiwillig umsetzen. Auch freiwillige Meldungen zu IT-Sicherheitsvorfällen oder der Austausch mit anderen Betreibern und Behörden in der öffentlich-privaten Partnerschaft UP KRITIS sowie in der Allianz für Cybersicherheit sind grundsätzlich unabhängig vom Erreichen der Schwellenwerte der BSI-KritisV möglich.

16. Teilt die Bundesregierung die Ansicht der Fragesteller, dass auch kleine und mittlere Wasserversorger ein Mindestmaß an Schutz vor digitalen Angriffen gewährleisten sollten?

Ja.

17. Wenn ja, welche Schritte hält die Bundesregierung für notwendig, um diesen Mindestmaßstab festzulegen und zu überprüfen?

Es wird auf die Antwort zu Frage 15 verwiesen.

18. Welche Möglichkeiten stehen Bund und Ländern in der aktuellen Notlage der COVID-19-Pandemie zur Verfügung, um Sicherheitsstandards zu überprüfen und gewährleisten zu können?

Die Fragestellung wird in Bezug auf die Überprüfung und Gewährleistung von Sicherheitsstandards im Bereich der IT-Sicherheit beantwortet.

Gemäß § 8a Absatz 3 Satz 4 BSI-Gesetz kann das BSI die Vorlage der Dokumentation, die der Überprüfung der nach § 8a Absatz 1 BSI-Gesetz umzusetzenden Maßnahmen zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen. Weiterhin kann das BSI gemäß § 8a Absatz 4 BSI-G die Einhaltung der vorgenannten Anforderungen überprüfen; es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Der Betreiber Kritischer Infrastrukturen hat dem BSI und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Gemäß § 8a Absatz 5 BSI-Gesetz kann das BSI zur Ausgestaltung des Verfahrens von Sicherheitsaudits, Prüfungen und Zertifizierungen auch Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen. Von dieser Regelung hat das BSI beispielsweise in der diesbezüglichen Veröffentlichung für Rechenzentren gemäß der Anlagenkategorie 2.1.1 nach Anhang 4, Teil 3 BSI-KritisV am 22. April 2020 gebraucht gemacht (vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Anforderungen_Anlage_RZ.pdf?__blob=publicationFile&v=3).

Gemäß § 8d Absatz 3 BSI-Gesetz gelten für folgende Betreiber nicht die vorgenannten Regelungen des § 8a BSI-G, sondern entsprechende spezialgesetzliche Regelungen u. a. im Telekommunikationsgesetz (TKG), im Energiewirtschaftsgesetz (EnWG), im Atomgesetz (AtG) sowie im Fünften Buch des Sozialgesetzbuches (SGB 5):

- Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,
- Betreiber von Energieversorgungsnetzen oder Energieanlagen, soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen,
- die Gesellschaft für Telematik nach § 291a Absatz 7 Satz 2 des Fünften Buches Sozialgesetzbuch und § 291b des Fünften Buches Sozialgesetzbuch,

- Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 291b Absatz 1a und 1e des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 291b Absatz 1b des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzen,
- Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie
- sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 4 vergleichbar oder weitergehend sind.

Gesonderte Befugnisse oder Möglichkeiten des Bundes aufgrund der aktuellen Notlage der COVID-19-Pandemie bestehen nicht. Möglichkeiten und Befugnisse der Länder liegen im Zuständigkeitsbereich der Länder.

19. Sieht die Bundesregierung Bedarf, die Gesetzesregelung zur Notversicherung verstärkt an zivile Katastrophen, Extremwetterereignisse und Cybersecurity-Angriffe anzupassen?

Der Katastrophenschutz als Teil der allgemeinen Gefahrenabwehr, die polizeiliche Gefahrenabwehr, sowie diesbezügliche Vorsorgemaßnahmen liegen in der Zuständigkeit der Länder, die entsprechend auch etwaige Anpassungsbedarfe bei bestehenden Landesgesetzen identifizieren.

20. Welche Informationen liegen der Bundesregierung zum aktuellen Zustand aller Trinkwassernotbrunnen in Deutschland vor?

Die Trinkwassernotbrunnen werden nach § 9 des Wassersicherstellungsgesetzes (WasSG) von den leistungspflichtigen Betreibern in den Ländern, dort in den Kreisen und kreisfreien Städten jährlich gewartet und instandgehalten.

Die nach § 26 WasSG zuständige Behörde koordiniert die Umsetzung des WasSG zwischen Bund und Leistungspflichtigen im Rahmen der Bundesauftragsverwaltung. Der Bund erhält Informationen über die Funktionsfähigkeit der Brunnen durch die Haushaltsmittelanforderungen für Erhaltungsmaßnahmen.

21. Wie viele der Trinkwassernotbrunnen sind aktuell in Funktion, und wo befinden sich diese?

Notbrunnen und Quellen nach WasSG sind in der Regel nicht im genutzten Betrieb, sondern werden für den Verteidigungsfall bzw. zur Minderung einer schweren Wasserkrise in Siedlungsgebieten vorgehalten und erst bei Bedarf in Betrieb gesetzt. Nach Einweisung durch die zuständigen Behörden holt sich die Bevölkerung das Wasser von den dann bekannt gegebenen Brunnen (Holwasser).

Notbrunnen sind ein wesentlicher Bestandteil der zivilen Verteidigung. Eine Preisgabe einzelner Standorte, Anlagenkonzeptionen, verwendeter Technik und Zugänglichkeit würde die Notbrunnen angreifbarer machen und damit die zivile Verteidigungsfähigkeit unterminieren.

22. Sind die Informationen zu Trinkwassernotbrunnen öffentlich zugänglich?

    Wenn ja, wo sind diese hinterlegt?

Nein, zur Absicherung der zivilen Verteidigungsfähigkeit sind nur den zuständigen Stellen in Bund, Ländern und Kommunen Informationen zu Trinkwassernotbrunnen bekannt.

23. Mit welchen Mitteln unterstützt die Bundesregierung Kommunen, um die Instandsetzung der Brunnen zu gewährleisten?

Nach § 9 Absatz 1 WasSG hat der Leistungspflichtige die Anlagen auf eigene Kosten ordnungsgemäß zu warten und betriebsfähig zu halten.

Aufwendungsersatz für die Kosten der Instandhaltung erfolgt nur, soweit dies zum Ausgleich oder zur Abwendung unbilliger Härten geboten erscheint (§ 10 Absatz 2 WasSG). Im Jahr 2019 hat der Bund den Bundesländern für die Wassersicherstellung (Trinkwassernotversorgung) verfügbare Haushaltsmittel in Höhe von rd. 1.800.000 Euro zur Verfügung gestellt. Für das Jahr 2020 steht der gleiche Betrag zur Verfügung.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333