20. Wahlperiode

Drucksache **20/3360**

HESSISCHER LANDTAG

08. 10. 2020

Kleine Anfrage

Stefan Müller (Freie Demokraten) und Oliver Stirböck (Freie Demokraten)
vom 10.08.2020

Cybersicherheit im Bereich der Wasserversorgung

und

Antwort

Ministerin für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz

Vorbemerkung Fragesteller:

Die Digitalisierung soll eine „smarte“ und ressourceneffiziente Wasserversorgung und Abwasserbeseitigung ermöglichen. Mit der zunehmenden Digitalisierung der Wasserversorgung steigt jedoch auch die Anfälligkeit für Cyberangriffe. Das Gesetz zur IT-Sicherheit (IT-SiG) regelt die Sicherheit informationstechnischer Systeme sowie den Schutz Kritischer Infrastrukturen (KRITIS) und verpflichtet ihre Betreiber zur Einhaltung eines Mindestmaßes an IT-Sicherheit. Im Bereich der Wasserversorgung werden Anlagen als KRITIS eingestuft, die einen Schwellenwert von 500.000 Personen erreichen oder überschreiten (Anhang 2, Teil 5 der BSI-KRITIS-Verordnung). Viele kommunale sowie kleine und mittlere Unternehmen der Wasserversorgung sind demnach nicht als KRITIS eingestuft, obwohl sie eine wichtige Rolle für die Wasserversorgung der Bevölkerung spielen. Zudem verfügen nicht alle kommunalen und kleineren Versorger über die Ressourcen und Mittel, um ein hohes Schutzniveau gegen Cyberangriffe zu garantieren.

Diese Vorbemerkung der Fragesteller vorangestellt beantworte ich die Kleine Anfrage mit dem Hessischen Minister des Innern und für Sport wie folgt:

Frage 1. Wie schätzt die Landesregierung das Risiko von Cyberangriffen auf kritische Infrastrukturen und insbesondere Wasserversorger aktuell ein?

Die Hessische Landesregierung sieht ein insgesamt hohes Risiko für Cyberangriffe. Dies betrifft sowohl die Landesverwaltung, Kommunen als auch Bürgerinnen und Bürger sowie Unternehmen. Hiervon umfasst sind auch die Betreiber von Anlagen der Kritischen Infrastruktur (KRITIS).

Bei den dem Hessen CyberCompetenceCenter (Hessen3C) des Hessischen Ministeriums des Innern und für Sport gemeldeten Cyber-Angriffen handelt es sich nahezu ausnahmslos um breit gestreute Angriffe, bei denen die Opfer der initialen Angriffe nicht gezielt ausgewählt wurden. Häufungen ergeben sich aus einzelnen Schritten der vorherrschenden Angriffsmethoden. Hierzu zählt insbesondere das sog. „outlook-harvesting“. Beim „outlook-harvesting“ werden Inhalte der E-Mail-Postfächer eines Opfers verwendet, um gezielt dessen Kommunikationspartner anzugreifen und diesen Angriff zu tarnen. Unabhängig von den sich ergebenden Häufungen geht es den Angreifern nicht um die Störung einer Versorgungsleistung, sondern um die Erpressung der Opfer durch Verschlüsselung von Daten oder die Drohung mit der Veröffentlichung von Kundendaten und Geschäftsgeheimnissen.

Frage 2. Wie viele Wasserversorger gibt es in Hessen?

Im Fachinformationssystem sind in Hessen 365 öffentliche Wasserversorger aufgeführt.

Frage 3. Wie viele davon sind nicht als KRITIS nach der BSI-KRITIS-Verordnung eingestuft?

Mit Stand Februar 2020 waren dies 362 öffentliche Wasserversorger.

Frage 4. Welche Cybersicherheitsstandards gelten für Wasserversorger, die als KRITIS eingestuft sind?

Eingegangen am 8. Oktober 2020 · Bearbeitet am 8. Oktober 2020 · Ausgegeben am 13. Oktober 2020
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Frage 5. Welche Cybersicherheitsstandards gelten für Wasserversorger, die nicht als KRITIS eingestuft sind?

Die Fragen 4 und 5 werden aufgrund des Sachzusammenhangs zusammen beantwortet.

Betreiber von KRITIS-Anlagen haben – in Bezug auf den Betrieb der Anlagen – folgende Pflichten zu erfüllen:

a) Umsetzung von IT-Sicherheitsmaßnahmen nach dem Stand der Technik,

b) Pflicht zur Überprüfung und dem Nachweis der Einhaltung des Standes der Technik (alle zwei Jahre, z.B.: durch Audits),

c) Meldepflicht für IT-Sicherheitsvorfälle beim Betrieb der Anlagen der kritischen Infrastruktur.

Der Stand der Technik wird dabei durch den BSI-Grundschutz in der jeweils geltenden Fassung in Verbindung mit branchenspezifischen Sicherheitsstandards („B3S“) bestimmt.

Für die Wasserwirtschaft gilt der B3S „WA“ (Wasser/Abwasser). Die Eignung des B3S „WA“ gem. § 8a Absatz 2 BSIG wurde durch das BSI festgestellt und veröffentlicht. Damit ist der B3S „WA“ eine verbindliche Vorgabe für die Betreiber von Anlagen der Kritischen Infrastruktur im Bereich Wasser und Abwasser; allen anderen Unternehmen der Wasserwirtschaft wird die Umsetzung empfohlen.

Kommunen sind von einem möglichen Ausfall von Kritischen Infrastrukturen unmittelbar betroffen. Sie sind für den sicheren Betrieb sowie die Erbringung der Infrastrukturleistungen zuständig und verantwortlich im Normalbetrieb wie auch im Krisenfall. Darum müssen auch nicht KRITIS-Betreiber nach der BSI-KRITIS V ein Mindestschutzniveau der IT-Sicherheit erreichen, um auf Cyber-Angriffe vorbereitet zu sein. Im IT-Sicherheitsleitfaden des Deutschen Vereins des Gas- und Wasserfaches e. V. (DVGW) „Branchenspezifischer Sicherheitsstandard Wasser/Abwasser“ sind für die Betreiber von Wasserversorgungsanlagen Hinweise aufgeführt, wie ein Mindestschutzniveau der IT-Sicherheit erreicht werden kann. Der DVGW hat den B3S „WA“ zusätzlich im technischen Hinweis „Merkblatt DVGW W1060 M“ umgesetzt. Ergänzt wird das Merkblatt W1060 M durch einen IT-gestützten Sicherheitsleitfaden, der die korrekte Umsetzung des B3S „WA“ unterstützt.

Frage 6. Sind die Cybersicherheitsstandards, insbesondere für Wasserversorger, die nicht als KRITIS eingestuft sind, aus Sicht der Landesregierung ausreichend?

Die Sicherstellung der Öffentlichen Wasserversorgung ist gemäß § 36 HWG Aufgabe der Kommunen im Rahmen der Kommunalen Daseinsvorsorge. Die eigenverantwortlich wahrzunehmenden Aufgaben ergeben sich aus den Vorgaben des BSI sowie den fachlichen Leitlinien der Verbände. Die Regelwerke des DVGW sind als anerkannte Regeln der Technik von den Wasserversorgern zu beachten. Gemäß § 31 Hessisches Wassergesetz (HWG) sind Anlagen zum Verteilen, Behandeln und Speichern von Wasser nach den allgemein anerkannten Regeln der Technik und der Wasserwirtschaft herzustellen, zu betreiben und zu unterhalten.

Der Bundesgesetzgeber hat mit §10 Abs. 1 BSI-G das Bundesministerium des Innern zum Erlass der BSI-KRITIS-Verordnung ermächtigt. Das Bundesministerium des Innern hat mit der BIS-KRITIS-Verordnung eine grundsätzliche Risikobewertung vorgenommen. Gemäß Anhang 2, Teil 5 der BSI-KRITIS-VO ist der Schwellenwert für Anlagen der Trinkwasser-Gewinnung, -Aufbereitung, - Verteilung und Leitzentralen auf 22 Mio. m³/Jahr festgelegt. Damit sind solche Anlagen, die weniger als 22 Mio. m³/Jahr verarbeiten, nicht als KRITIS im Sinne der Verordnung einzustufen. Ergänzend wird darauf hingewiesen, dass ein Wasseraufkommen von 22 Mio. m³ pro Jahr im bundesweiten Durchschnitt der Versorgung von ca. 500.000 Personen im Regelbetrieb entspricht. Grundlage der Schwellenwerte sind Erfahrungen des Krisenmanagements des Bundes (BBK) nach denen Störungen einzelner Versorgungsleistungen, unabhängig von ihrer Ursache, weder die Handlungsfähigkeit des Staates noch die Versorgung der Bevölkerung gefährden, wenn nicht mehr als eine halbe Million Einwohner betroffen sind. Bis zu diesem Schwellenwert können Ersatzleistungen im Rahmen der bestehenden Strukturen Störungen auffangen.

Auch für Anlagen der Wasserwirtschaft, die diesen Schwellenwert nicht erreichen, ergreifen die Betreiber umfangreiche Maßnahmen im Kontext des Risiko-Managements und des Business-Continuity-Managements. Dabei werden auch Maßnahmen der Cybersicherheit berücksichtigt. Auf die Antwort zu den Fragen 4 und 5 wird verwiesen. Aus dem Bereich der hessischen Wasserwirtschaft wurden dem Hessen3C in den letzten drei Jahren keine IT-Sicherheitsvorfälle, bei denen die Versorgungsleistung bedroht war oder beeinträchtigt wurde, bekannt.

Frage 7. Inwieweit evaluiert die Landesregierung die Cybersicherheit der hessischen Wasserversorger und erstellt Risikoanalysen?

Im Rahmen des Runden Tisches KRITIS Hessen, an dem neben dem Hessischen Ministerium des Innern und für Sport, dem Hessischen Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz auch der Verband kommunaler Unternehmen (VKU) – Landesgruppe Hessen sowie im Verband vertretene Mitgliedsunternehmen teilnehmen, wird die Sensibilisierung für neue Herausforderungen und Risiken der IT-Sicherheit und Vernetzung gemeinsam behandelt.

Frage 8. Inwieweit unterstützt die Landesregierung Wasserversorger und insbesondere Kommunen sowie kleine und mittlere Unternehmen der Wasserversorgung bei der Abwehr von Cybersicherheitsrisiken?

Hessen3C bietet den hessischen Kommunen und allen hessischen Unternehmen unter der 24/7 erreichbaren Hotline (0611) 353-9900 Unterstützung bei der Behandlung von IT-Sicherheitsvorfällen durch das Computer Emergency Response Team (CERT) an. Bei schweren Vorfällen erfolgt durch das Mobile Incident Response Team (MIRT) des Hessen3C auch eine Beratung vor Ort. Darüber hinaus bietet Hessen3C eine produkt-neutrale Beratung zu Fragen der technischen IT-Sicherheitsarchitektur und zu IT-Sicherheitsprozessen an. Diese Leistungen sind für die Unternehmen kostenfrei und stehen auch Wasserversorgern zur Verfügung.

Das Hessische Ministerium des Innern und für Sport unterstützte Veranstaltungen des DVGW bzw. des Landesverbandes Hessen-Rheinland-Pfalz der Energie und Wasserwirtschaft (LDEW) durch Referenten zu Cybersicherheitsthemen. Zudem wurde gemeinsam mit der Landesgruppe Hessen des Verbands kommunaler Unternehmen (VKU) und dem LDEW am 25. November 2019 die Fachtagung „Der große Black-Out“ durchgeführt, bei der rd. 170 Teilnehmerinnen und Teilnehmer aus allen KRITIS-Branchen sowie aus den Gefahrenabwehrbehörden von Bund und Ländern u.a. zur Cybersicherheit im KRITIS einen intensiven Erfahrungsaustausch gepflegt haben.

Unter Wahrung der Selbstverwaltung können hessische Kommunen – auf freiwilliger Basis und ohne Kostenbeteiligung – CERT-Dienstleistungen des Hessen3C nutzen. Dies schließt sowohl die Kommunalverwaltungen von hessischen Gebietskörperschaften als auch deren Eigenbetriebe (z.B. Energie- und Wasserversorgung sowie ÖPNV) mit ein.

Im Weiteren erfolgen anlassbezogene Unterstützungsmaßnahmen zum Beispiel durch Fachbeiträge im Rahmen der Pandemie-Maßnahmen des VKU oder für den „Runden Tisch KRITIS-Betreiber“.

Wiesbaden, 1. Oktober 2020

Priska Hinz