Deutscher Bundestag **Drucksache 19/21459**

19. Wahlperiode 04.08.2020

Kleine Anfrage

der Abgeordneten Mario Brandenburg, Frank Sitta, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Britta Katharina Dassler, Dr. Marcus Faber, Otto Fricke, Markus Herbrand, Torsten Herbst, Manuel Höferlin, Reinhard Houben, Ulla Ihnen, Dr. Christian Jung, Pascal Kober, Alexander Müller, Frank Müller-Rosentritt, Dr. h. c. Thomas Sattelberger, Dr. Marie-Agnes Strack-Zimmermann, Linda Teuteberg, Michael Theurer, Gerald Ullrich und der Fraktion der FDP

Zustand der IT-Sicherheit der Energieversorgung

Die Aufrechterhaltung der Versorgungssicherheit ist eine Kernaufgabe des Staates. Nicht zuletzt die COVID19-Krise hat den Fokus verstärkt auf das Funktionieren der wichtigsten und kritischen Infrastrukturen auch in Krisensituationen gelenkt. Entscheidend für die Aufrechterhaltung der öffentlichen Ordnung ist unter anderem die Resilienz der Energie- und Kommunikationsnetze. Nach Ansicht der Fragesteller kann die fortschreitende Digitalisierung zu einer erhöhten Eintrittswahrscheinlichkeit von Ausfällen der Energieversorgung führen, da die fortschreitende Digitalisierung und Automatisierung die Angriffsoberfläche der Energieversorger und Energieversorgungsnetzbetreiber vergrößert. Komponenten die früher noch rein analog waren, sind an vielen Stellen inzwischen nicht nur digitalisiert worden, sondern auch mit Datennetzen verbunden.

Die fortschreitende Digitalisierung und Automatisierung in der Energieversorgung gewährleistet deren effiziente Bereitstellung und stetige Verfügbarkeit, bringt aber auch größere Herausforderungen bezüglich der IT-Sicherheit bei Energieversorgern und Energieversorgungsnetzbetreibern mit sich. Dabei sind die Aufrechterhaltung der Informations- und Kommunikationsinfrastruktur und der Energiesicherheit wechselseitig voneinander abhängig.

Diese kritischen Komponenten gelten daher als Ziele von Cyberkriminellen, möglicherweise aber auch von fremden Staaten. Vor diesem Hintergrund interessiert eine aktuelle Bestandsaufnahme der IT-Sicherheit in der Energieversorgung sowie der damit zusammenhängenden Resilienz der Informations- und Kommunikationsinfrastruktur.

Wir fragen die Bundesregierung:

1. Wie schätzt die Bundesregierung die Versorgungssicherheit der Energieversorgung im europäischen Verbundnetz ein?

2. Wie groß schätzt die Bundesregierung die Gefahr eines teilweisen oder vollständigen Blackouts (langanhaltenden und mindestens überregionalen Stromausfall) in den nächsten fünf Jahren? (bitte getrennt nach den untenstehenden Buchstaben a-c beantworten)

   a) überregional

   b) bundesweit

   c) im gesamten europäischen Verbundnetz

3. Wie schätzt die Bundesregierung die tatsächliche IT-Sicherheit der deutschen Energieversorger und Energieversorgungsnetze ein?

4. Wie bewertet die Bundesregierung die föderale Struktur der Bundesrepublik im Hinblick auf die Schaffung, Einhaltung und Kontrolle von Vorschriften zur IT-Sicherheit in kritischen Infrastrukturen nach KritisV (bitte getrennt beantworten, aufgeschlüsselt nach allen Anhängen der KritisV)

5. Wieviele meldepflichtige Vorfälle nach § 8b Absatz 4 BSIG sind im Jahr 2017, 2018 und 2019 gemeldet worden? (Bitte getrennt auflisten nach Jahren und nach Meldungen nach § 8b (4) 1. und § 8b (4) 2. und aufgeschlüsselt nach allen Anhängen der KritisV)

6. Wie oft wurden Hersteller im Jahr 2017, 2018 und 2019 nach § 8b Absatz 6 BSIG zur Mitwirkung bei der Beseitigung oder Vermeidung einer Störung aufgefordert? (Bitte getrennt auflisten nach Jahren)

7. In wievielen Vorfällen in den Jahren 2017, 2018 und 2019 konnten Cyberkriminelle teilweisen, vollständigen, oder auch rein lesenden Zugriff auf die Netzwerke der deutschen Energieversorger, die unter Anhang 1 Teil 3 KritisV fallen, erlangen? (Bitte getrennt auflisten nach Jahren)

   a) auf informationstechnische Netzwerke

   b) auf operationstechnische Netzwerke

   c) bei wievielen Vorfällen kann ein unberechtigter Zugriff zwar nicht eindeutig belegt werden, aber auch nicht ausgeschlossen werden?

8. In wievielen Vorfällen in den Jahren 2017, 2018 und 2019 konnten Personen oder Personengruppen mit Bezug zu oder im Auftrag von fremden Staaten teilweisen, vollständigen, oder auch rein lesenden Zugriff auf die Netzwerke der deutschen Energieversorger, die unter Anhang 1 Teil 3 KritisV fallen, erlangen? (Bitte getrennt auflisten nach Jahren)

   a) auf informationstechnische Netzwerke

   b) auf operationstechnische Netzwerke

   c) bei wievielen Vorfällen kann ein unberechtigter Zugriff zwar nicht eindeutig belegt werden, aber auch nicht ausgeschlossen werden?

9. Welche Bemühungen hat die Bundesregierung unternommen, um die Empfehlungen der Enquete Komission für Internet und digitale Gesellschaft (EIDG) auf Drucksache 17/12541, insbesondere die Empfehlungen auf Seite 97 Abschnitt 4. „Sicherstellung des technischen Schutzes“ Unterabschnitt b) „SCADA- und PLC-Systeme“ umzusetzen?

   a) Welche Maßnahmen hat die Bundesregierung durchgeführt um Hersteller von SCADA und PLC-Systeme dazu zu bringen, den Quellcode in kritischen Infrastrukturen zugänglich zu machen?

   b) Wie erfolgreich waren diese Maßnahmen?

10. Welche Empfehlungen der EIDG hat die Bundesregierung in die Cybersicherheitsstrategie verbindlich aufgenommen, umgesetzt oder plant die Umsetzung der Empfehlungen? (Bitte auflisten nach Drucksache der EIDG, Kapitel und Abschnitt)

    a) welche Empfehlungen wurden wann erfolgreich umgesetzt?

    b) welche Empfehlungen sind aktuell in der Umsetzung?

    Bis wann wird die Umsetzung vorrausichtlich abgeschlossen sein?

    c) welche Empfehlungen sind geplant umzusetzen?

    Wann wird die Umsetzung beginnen?

    d) welche Empfehlungen wurden bisher nur in die Cybersicherheitsstrategie aufgenommen?

11. Welche Vorschriften existieren nach Kenntnis der Bundesregierung zur Verwendung von Verschlüsselung, Authentifizierung und digitalen Signaturen im Bereich der fernwirkenden drahtgebundenen operationstechnischen Netzwerke von Energieversorgern, die unter Anhang 1 Teil 3 KritisV fallen?

    a) Ist ein unverschlüsselter Betrieb von operationstechnischen Netzwerken zulässig?

    b) Ist es rechtlich zulässig, Steuerbefehle in operationstechnischen Netzwerken ohne Authentifizierung zu verwenden?

    c) Ist es rechtlich zulässig, Steuerbefehle in operationstechnischen Netzwerken ohne digitale Signatur zu verwenden?

    d) Wie oft wird die Einhaltung dieser Vorschriften durch wen geprüft?

    e) Wie oft wurden Mängel festgestellt?

12. Welche Vorschriften existieren nach Kenntnis der Bundesregierung zur Verwendung von Verschlüsselung, Authentifizierung und digitalen Signaturen im Bereich der drahtgebundenen informationstechnischen Netzwerke von Energieversorger die unter Anhang 1 Teil 3 KritisV fallen?

    a) Ist ein unverschlüsselter Betrieb von informationstechnischen Netzwerken zulässig?

    b) Ist es rechtlich zulässig, Betriebsdaten in informationstechnischen Netzwerken ohne Authentifizierung zu versenden?

    c) Ist es rechtlich zulässig, Betriebsdaten in informationstechnischen Netzwerken ohne digitale Signatur zu versenden?

    d) Wie oft wird die Einhaltung dieser Vorschriften durch wen geprüft?

    e) Wie oft wurden Mängel festgestellt?

13. Welche Vorschriften existieren nach Kenntnis der Bundesregierung zur Verwendung von Verschlüsselung, Authentifizierung und digitalen Signaturen im Bereich der drahtlosen operationstechnischen Netzwerke, beispielsweise auf Basis von TETRA, von Energieversorgern die unter Anhang 1 Teil 3 KritisV fallen? (vgl. auch https://fragdenstaat.de/a/170138 und https://fragdenstaat.de/a/171389)

    a) Ist ein unverschlüsselter Datenfunk in operationstechnischen Netzwerken zulässig?

    b) Ist es rechtlich zulässig, Steuerbefehle in drahtlosen operationstechnischen Netzwerken ohne Authentifizierung zu verwenden?

    c) Ist es rechtlich zulässig, Steuerbefehle in drahtlosen operationstechnischen Netzwerken ohne digitale Signatur zu verwenden?

    d) Wie oft wird die Einhaltung dieser Vorschriften durch wen geprüft?

    e) Wie oft wurden Mängel festgestellt?

14. Welche Vorschriften existieren nach Kenntnis der Bundesregierung zur Verwendung von Verschlüsselung, Authentifizierung und digitalen Signaturen beim Handel von Energieprodukten an Strombörsen, die unter KritisV Anhang 1 Teil 1 Absatz 2. Buchstabe g fallen

    a) für die digitale Kommunikation zwischen den Marktteilnehmern an der Börse

    b) für die digitale Kommunikation der Liefer- und Abnahmemengen an die Leitstände der Energieversorger

    c) für die digitale Kommunikation der Handelsergebnisse an die Übertragungsnetzbetreiber

    d) Wie oft wird die Einhaltung dieser Vorschriften durch wen geprüft?

    e) Wie oft wurden Mängel festgestellt?

15. Welche Kommunikationsmittel stehen der Bevölkerung während einem langanhaltenden und überregionalen Stromausfall zur Verfügung?

    a) Wieviele Stunden Stromausfall können die Mobilfunknetze ohne Versorgungseinschränkung der Mobilfunkversorgung der Bevölkerung (nicht nur Notrufe) tolerieren?

    b) Wieviele Stunden Stromausfall kann das Festnetztelefonnetz ohne Versorgungseinschränkung der Bevölkerung überbrücken?

    c) Welche Möglichkeiten für Notrufe stehen der Bevölkerung zur Verfügung nach Ablauf der Zeit in Unterfrage a und b zur Verfügung?

    d) Welche Veränderung der Angaben auf die Antworten 15a – 15c beobachtet die Bundesregierung im Vergleich zur Versorgungssicherheit vor der Umstellung auf NGN (New Generation Network) oder VoIP (Voice over IP)?

Berlin, den 29. Juli 2020

Christian Lindner und Fraktion

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