Deutscher Bundestag **Drucksache 19/28113**

19. Wahlperiode 30.03.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Stephan Thomae, Grigorios Aggelidis, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/27641 –

Sicherheit von Stromnetzen und anderer kritischer Infrastrukturen gegenüber Cyberangriffen

Vorbemerkung der Fragesteller

Cyberangriffe auf Stromnetze und andere kritische Infrastrukturen können erheblichen Schaden anrichten. Darauf hatte bereits in den vergangenen Jahren auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hingewiesen.

1. Welche Erkenntnisse besitzt die Bundesregierung über bereits abgewehrte Cyberangriffe auf Stromnetze in Deutschland und im europäischen Verbund (bitte ggf. mit Anzahl, Zeitpunkte sowie Ursprung und Herkunft der Angriffe angeben)?

Netzbetreiber sind nach § 11 Absatz 1c des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG) verpflichtet, Störfälle im Zusammenhang mit der Informations- und Kommunikationstechnik an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Die Bundesnetzagentur erhält diese Meldungen unverzüglich vom BSI. So verzeichnete die Bundesnetzagentur im Jahr 2020 in Summe zwölf Störmeldungen von Stromnetzbetreibern. Diese Störmeldungen können auch Störfälle auf Grund von schadhafter Software enthalten.

Explizite Meldungen der Netzbetreiber über abgewehrte Cyber-Angriffe erfolgen nicht, und somit auch keine Erfassung der allgemeinen Angriffslage.

Als Angriffsmethoden beobachteten die Betreiber gemäß ihren Meldungen an das BSI verstärkt aktives Scanning, um vorhandene Schwachstellen in den direkt mit dem Internet verbundenen Systemen zu finden und diese gegebenenfalls auszunutzen. Auch das Abgreifen von Zugangs- und Kontaktdaten über das Ausspähen von mit der Elektrizitätsbranche verbundenen Dritten wurde beobachtet.

Hinsichtlich des europäischen Verbundsystems liegen der Bundesnetzagentur keine Informationen vor; es bestehen keine Berichtspflichten. Die Herkunft der

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 29. März 2021 übermittelt.

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

Angriffe ist kein Bestandteil der Meldungen an die Bundesnetzagentur und dürfte den meldenden Unternehmen in der Regel unbekannt sein.

2. Welche Erkenntnisse besitzt die Bundesregierung über bereits abgewehrte Cyberangriffe auf andere Kritische Infrastrukturen in Deutschland und im europäischen Verbund (bitte ggf. Anzahl, Zeitpunkte sowie Ursprung und Herkunft der Angriffe angeben)?

Explizite Meldungen der Netzbetreiber über abgewehrte Cyber-Angriffe erfolgen nicht, und somit auch keine Erfassung der allgemeinen Angriffslage.

Für die Betreiber Kritischer Infrastrukturen (KRITIS) besteht nur bei festgestellten Störungen gem. § 8b des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) eine Verpflichtung zur Meldung an das BSI.

Die Meldezahlen werden im regelmäßigen Lagebericht des BSI veröffentlicht. Die für das Jahr 2020 noch nicht veröffentlichten Zahlen können der Tabelle in der Anlage entnommen werden.

Angaben zu genauen Zeitpunkten liegen dem BSI mit den Meldungen nicht vor und sind teilweise den Betroffenen selbst nicht bekannt, da der Angriff u. U. Monate vorher passieren kann, bevor dieser entdeckt und gemeldet wird.

Verschiedenste Studien und Unternehmensbefragungen unterstreichen die wiederholt im Bundeslagebild Cybercrime des Bundeskriminalamtes getroffene Einschätzung, wonach im Bereich des Cybercrime allgemein, aber auch im Bereich der Angriffe auf Kritische Infrastrukturen im Speziellen, von einem hohen Dunkelfeld ausgegangen werden muss.

Zur Verdeutlichung der diesbezüglichen Dunkelziffer kann der 2020 publizierte Forschungsbericht Nr. 152 „Cyberangriffe gegen Unternehmen in Deutschland – Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019“ des Kriminologischen Forschungsinstituts (KFN) Niedersachsen e. V. angeführt werden. Demzufolge werden nur 11,9 Prozent der schwerwiegenden Cyberangriffe angezeigt.

Auch diese Studie hebt nicht explizit auf KRITIS-Unternehmen ab – dezidiertere Erkenntnisse hierzu liegen der Bundesregierung nicht vor.

3. Welche Erkenntnisse besitzt die Bundesregierung über mögliche und drohende Aktivitäten in Form von Cyberangriffen auf Stromnetze auf andere Kritische Infrastrukturen in Deutschland und im europäischen Verbund (bitte ggf. mögliche Auswirkungen sowie Ursprung und Herkunft der Bedrohung angeben)?

Die Anzahl und Vielfalt möglicher Bedrohungen in Form von Cyber-Angriffen für den Bereich KRITIS Energie sind kontinuierlich hoch und können sich im Rahmen der Digitalisierung stetig weiterentwickeln. Die meistgenutzten Methoden, um ein Unternehmen zu kompromittieren, sind dem aktuellen BSI Lagebericht (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2) zu entnehmen.

Generell waren und bleiben Unternehmen auch aus dem KRITIS-Bereich aufgrund ihrer Bedeutung für die Gesellschaft und die Wirtschaft ein relevantes Angriffsziel für Cyberkriminelle, wobei die Angriffe finanziell oder staatlich motiviert sein können. Eine akteurs- oder länderspezifische Eingrenzung solcher Angriffe kann dabei im Voraus nicht ausreichend verifizierbar getroffen werden.

In diesem Zusammenhang wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 8 der Abgeordneten Sandra Bubendorfer-Licht auf Bundestagsdrucksache 19/21248 verwiesen.

4. Was unternimmt die Bundesregierung, um die Sicherheit unserer Stromnetze und anderer Kritischer Infrastrukturen zu gewährleisten und die Abwehr von Cyberangriffen zu verbessern?

Die Stromversorgung zählt zu den Kritischen Infrastrukturen in Deutschland. Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Betreiber Kritischer Einrichtungen – und damit auch Betreiber von Energieversorgungsnetzen – müssen sich wegen ihrer besonderen Bedeutung für die Versorgung der Bevölkerung besonders gegen etwaige Bedrohungen schützen.

Die Bundesregierung hat vor diesem Hintergrund einen Rechtsrahmen geschaffen, der Betreiber Kritischer Infrastrukturen zur Einhaltung von bestimmten Mindestanforderungen im Bereich Cybersicherheit und zur Meldung von erheblichen IT-Sicherheitsvorfällen verpflichtet. Die entsprechenden Vorgaben finden sich im BSIG und – soweit es um Betreiber von Energieversorgungsnetzen geht – im EnWG. Dieser Rechtsrahmen wird fortlaufend weiterentwickelt.

Für Betreiber von Energieversorgungsnetzen gelten sektorspezifische Regelungen im EnWG, die mit dem BSIG vergleichbare Anforderungen an sie stellen.

§ 11 Absatz 1a EnWG stellt zunächst klar, dass der Betrieb eines sicheren Energieversorgungsnetzes insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind, umfasst. Betreiber von Energieversorgungsnetzen müssen überdies einen Katalog von Sicherheitsanforderungen erfüllen, der von der Bundesnetzagentur als Regulierungsbehörde im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik erstellt wurde.

Dieser Katalog von Sicherheitsanforderungen für Betreiber von Energieversorgungsnetzen wurde im August 2015 von der Bundesnetzagentur veröffentlicht. Die Ziele des IT-Sicherheitskatalogs sind dabei die Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten, die Sicherstellung der Integrität der verarbeiteten Informationen und Systeme und die Gewährleistung der Vertraulichkeit der verarbeiteten Informationen. Zentrale Anforderung des IT-Sicherheitskatalogs für Netzbetreiber ist die Einrichtung eines so genannten Informationssicherheits-Managementsystems (ISMS) auf der Grundlage der international anerkannten und verbreiteten DIN ISO/IEC 27001 unter zusätzlicher Berücksichtigung der DIN ISO/IEC 27002 sowie der speziell für Prozessleitsysteme und Automatisierungstechnik im Energiesektor einschlägigen DIN ISO/IEC 27019. Ein solches ISMS ermöglicht ein den individuell vorhandenen Risiken eines Betreibers entsprechendes IT-Sicherheitsniveau und muss vom Betreiber dauerhaft überwacht und angepasst werden, so dass auch künftige sicherheitsrelevante Herausforderungen der zunehmenden Digitalisierung jederzeit berücksichtigt werden müssen.

Die Betreiber haben die erfolgreiche Umsetzung des IT-Sicherheitskatalogs durch ein unabhängiges Zertifizierungsverfahren gegenüber der Bundesnetzagentur nachzuweisen. Diese Zertifizierung muss regelmäßig wiederholt werden.

§ 11 Absatz 1c EnWG verpflichtet die Betreiber von Energieversorgungsnetzen überdies dazu, Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben, oder erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können, über die Kontaktstelle unverzüglich an das BSI zu melden. Das BSI wertet die Meldungen aus und berät und unterstützt auch Betreiber Kritischer Infrastrukturen bei Fragen der Sicherheit in der Informationstechnik (§ 3 BSIG).

Der Bund bereitet sich im Rahmen seiner Zuständigkeiten ebenfalls auf Ereignisse wie einen großflächigen Stromausfall vor. Hier ist beispielsweise die ressort- und länderübergreifende Krisenmanagementübung „LÜKEX 2004“ zu nennen, in der die Übungsteilnehmenden das Szenario einer winterlichen Extremwetterlage mit großflächigem Stromausfall geübt haben. Darüber hinaus bietet das Bundesamt für Bevölkerungs- und Katastrophenschutz (BBK) Betreibern Kritischer Infrastrukturen und Akteuren des Bevölkerungsschutzes Empfehlungen zur Vorsorge und Bewältigung eines großflächigen Stromausfalls an, hier besonders die Empfehlung zur Treibstoffversorgung bei Stromausfall (BBK, 2017) und Notstromversorgung für Unternehmen und Behörden (BBK, 2015). Die Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ) bietet zudem im Rahmen der Ausbildung im Bevölkerungsschutz Führungs- und Stabslehre sowie Krisenmanagement-Lehrgänge an.

Aufgrund der hohen Abhängigkeit der öffentlichen Wasserversorgung (und damit mittelbar auch der Abwasserentsorgung) von der Stromversorgung hat der Bund den Ländern auf Grundlage des Wassersicherstellungsgesetzes mit Hilfe von Konjunkturfördermitteln bislang in den Jahren 2020/2021 knapp 60 Mio. Euro zusätzlich für Härtungsmaßnahmen der öffentlichen Wasserversorgung zur Verfügung gestellt. Die Mittel wurden überwiegend für die Beschaffung von Notstromaggregaten zur Aufrechterhaltung der öffentlichen Wasserversorgung verwendet. Daneben wurden auch andere Maßnahmen finanziert, die zusätzliche Redundanzen der Wasserversorgung erzielen, wie z. B. die Errichtung von Verbundleitungen, zusätzlichen Wasser(speicher-)behältern, die Beschaffung von mobilen Aufbereitungsanlagen und Redundanzpumpen.

Zum schnellen Informationsaustausch und zur besseren Koordinierung von Schutz- und Abwehrmaßnahmen gegen Cybervorfälle allgemein kommen die relevanten (Sicherheits-)Behörden des Bundes im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) zusammen. Neben der akuten Vorfallkoordinierung werden im Cyber-AZ unter Federführung des BBK Erkenntnisse und Risikobewertungen der beteiligten Einrichtungen zu einer gemeinsamen Bewertung der Gefährdungslage Kritischer Infrastrukturen zusammengeführt und Handlungsempfehlungen abgeleitet.

Über den UP KRITIS stehen die zuständigen Behörden, darunter das BBK, in ständigem Austausch mit den Betreibern Kritischer Infrastrukturen und deren Verbänden. Ziel dieser Kooperation ist es, die Versorgung mit kritischen Infrastrukturdienstleistungen in Deutschland aufrechtzuerhalten. Neben einem regelmäßigen Informationsaustausch werden auch hier gemeinsam Standards und Handlungsempfehlungen erarbeitet.

Anlage zu Frage 2

Statistische Auswertung der eingegangenen Störungsmeldungen

Zeitraum:	**01.01.2020 bis 31.12.2020**

Sektor	**Anzahl gemeldeter Störungen**
Energie	**55**
Ernährung	**6**
Finanz- und Versicherungswesen	**62**
Wasser	**10**
Informationstechnik und Telekommunikation	**66**
Gesundheit	**148**
Transport und Verkehr	**25**
Meldungen ingesamt[1]	**337**

[1] Die Gesamtanzahl der Meldungen entspricht nicht der Summe der Meldungen der einzelnen Sektoren, da eine gemeldete Störung mehrere Sektoren betreffen kann

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