Deutscher Bundestag **Drucksache 19/21674**

19. Wahlperiode 17.08.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Mario Brandenburg, Frank Sitta, Jens Beeck, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/21459 –

Zustand der IT-Sicherheit der Energieversorgung

Vorbemerkung der Fragesteller

Die Aufrechterhaltung der Versorgungssicherheit ist eine Kernaufgabe des Staates. Nicht zuletzt die COVID-19-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 Energienetze und Kommunikationsnetze. Nach Ansicht der Fragestellerinnen und 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.

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

Deutschland ist voll in den europäischen Binnenmarkt für Strom integriert und profitiert damit von länderübergreifenden Ausgleichseffekten beim Stromverbrauch, bei der Einspeisung erneuerbarer Energien und bei Verfügbarkeiten von Kraftwerken. Somit erfolgt auch die Einschätzung der Versorgungssicher-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 17. August 2020 übermittelt.

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

heit mit Strom in Deutschland immer unter Berücksichtigung des gesamten europäischen Strommarktes. Das Bundesministerium für Wirtschaft und Energie (BMWi) führt ein kontinuierliches Monitoring der Versorgungssicherheit an der Strommärkten durch. Der aktuelle Bericht „Definition und Monitoring der Versorgungssicherheit an den europäischen Strommärkten“ ist unter folgendem Link abrufbar: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/definition-und-monitoring-der-versorgungssicherheit-an-den-europaeischen-strommaerkten.pdf.

Ab dem 1. Januar 2021 wird die Bundesnetzagentur (BNetzA) für ein weiterentwickeltes und ausgeweitetes Versorgungssicherheitsmonitoring zuständig sein. Neben der Untersuchung der Strommärkte werden zukünftig auch Netzaspekte und Extremfälle in eigenen Berechnungen geprüft werden. Damit entsteht ein integriertes Monitoring der Versorgungssicherheit in allen versorgungssicherheitsrelevanten Bereichen.

Neben dem Versorgungssicherheitsmonitoring des BMWi werden jährlich auch ein Monitoring des Verbandes der europäischen Übertragungsnetzbetreiber (ENTSO-E), „Mid-term Adequacy Forecast“ (https://www.entsoe.eu/outlooks/midterm/wp-content/uploads/2019/12/entsoe_MAF_2019.pdf) sowie ein Bericht des Pentalateralen Energieforums zur Versorgungssicherheit „Pentalateral Energy Forum Support Group 2 – Generation Adequacy Assessment April 2020“ (https://www.tennet.eu/fileadmin/user_upload/Company/Investor_Relations/2020_PLEF_GAA_3.0_report_FINAL.PDF) veröffenticht. Alle aufgeführten Analysen haben auch perspektivisch keine konkreten Gefährdungen der Versorgungssicherheit festgestellt.

Im Bereich der Gasversorgung erweitert die novellierte Verordnung über Maßnahmen zur Gewährleistung der sicheren Gasversorgung (EU) 2017/1938 die Reihe der Maßnahmen zur Sicherstellung einer unterbrechungsfreien Gasversorgung in der gesamten Europäischen Union. Die Leitprinzipien der Verordnung bilden die regionale Zusammenarbeit im Rahmen der Krisenvorsorge und die gegenseitige solidarische Unterstützung der Mitgliedsstaaten untereinander bei der Bewältigung von Gasversorgungskrisen.

Die Mitgliedstaaten ergänzen ihre Risikoanalysen, Präventions- und Notfallpläne um regionale Kapitel und arbeiten an bilateralen Abkommen zu solidarischen Gaslieferungen für den Fall eines Versorgungsdefizits, das der betroffene Mitgliedstaat nicht durch marktbasierte Maßnahmen beheben kann. Die Verordnung dient der Versorgungssicherheit mit Gas, sowohl im Rahmen der europäischen Fernleitungs- als auch der Verteilnetze. Maßnahmen zur Versorgungssicherheit in Europa werden zudem im Rahmen der „Gas Coordination Group“ in Brüssel eng abgestimmt und koordiniert.

Auch die Ölversorgungssicherheit basiert wesentlich auf dem Informationsaustausch auf der Ebene der Internationalen Energieagentur (IEA) und der Europäischen Union (EU). In regelmäßig tagenden Arbeitsgruppen in beiden Organisationen tauschen sich Experten und Behördenvertreter über die Situation der weltweiten Ölversorgungssicherheit und den daraus resultierenden jeweiligen Folgen für die jeweiligen Länder aus. Darüber hinaus finden internationale Übungen statt, die weltweite Szenarien von Versorgungsengpässen mit Öl simulieren und Lösungsansätze aufzeigen.

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

   a) überregional,

   b) bundesweit,

   c) im gesamten europäischen Verbundnetz?

Die sichere Versorgung von Verbrauchern mit Strom hängt zum einen von der Versorgungssicherheit am Strommarkt, zum anderen von Stromnetzaspekten ab.

Die Versorgungssicherheit am Strommarkt wird im Monitoring desBMWi „Definition und Monitoring der Versorgungssicherheit an den europäischen Strommärkten“ (https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/definition-und-monitoring-der-versorgungssicherheit-an-den-europaeischen-strommaerkten.pdf) anhand der Größe Lastüberhangwahrscheinlichkeit („Loss of Load Probabiliy“ kurz LoLP, in Prozent) untersucht.

Sie beschreibt die Wahrscheinlichkeit für Systemzustände, in denen die Nachfrage am Strommarkt unter Berücksichtigung der preislichen Präferenzen der Verbraucher durch das verfügbare Angebot nicht vollständig gedeckt werden kann. Zur Untersuchung der Versorgungssicherheit wird zunächst ein Standardwert für LoLP definiert, welcher der volkswirtschaftlich angemessenen Versorgungssicherheit entspricht. Im Monitoring wird dann für verschiedene Szenarien untersucht, ob dieser LoLP-Standard eingehalten werden kann.

Der „Monitoringbericht des Bundesministeriums für Wirtschaft und Energie nach § 63 i. V. m. § 51 des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG) zur Versorgungssicherheit im Bereich der leitungsgebundenen Versorgung mit Elektrizität“ (https://www.bmwi.de/Redaktion/DE/Publikationen/Energie/monitoringbericht-versorgungssicherheit-2019.pdf) gibt basierend auf dem oben genannten Monitoringbericht für Deutschland für 2020 und 2025 eine Lastausgleichswahrscheinlichkeit (Reziprok zur Lastüberhangwahrscheinlichkeit) von (rechnerisch) 100 Prozent an.

Die schwerpunktmäßig gesamteuropäischen Untersuchungen der Versorgungssicherheit durch den Verband der europäischen Übertragungsnetzbetreiber (ENTSO-E), „Mid-term Adequacy Forecast“ (https://www.entsoe.eu/outlooks/midterm/wp-content/uploads/2019/12/entsoe_MAF_2019.pdf) bzw. die Untersuchungen zur Versorgungssicherheit des Pentalateralen Energieforums, „Pentalateral Energy Forum Support Group 2 – Generation Adequacy Assessment April 2020“ (https://www.tennet.eu/fileadmin/user_upload/Company/Investor_Relations/2020_PLEF_GAA_3.0_report_FINAL.PDF) weisen auf einen sehr hohen Versorgungssicherheitsstandard im gesamten europäischen Verbundnetz hin.

Langanhaltende und mindestens überregionale Stromausfälle sind extrem selten. Das gesamte kontinentaleuropäische Verbundnetz ist noch nie schwarz gefallen, einzelne Regionen sehr selten. Die Netzbetreiber sind für einen sicheren Netzbetrieb auf regionaler, nationaler und europäischer Ebene zuständig. Sie stimmen ihre Maßnahmen regional und europäisch eng ab und entwickeln sie regelmäßig weiter. Die hohe Versorgungsqualität der letzten Jahre hat gezeigt, dass sich auch in angespannten Situationen die vorgesehenen Mechanismen der Netzbetreiber bewährt haben. Durch den Umbau der Erzeugungslandschaft, des Verbrauchs und der stärkeren Digitalisierung werden diese Prozesse permanent weiterentwickelt, um das hohe Versorgungsniveau jederzeit sicherzustellen.

Die Bundesregierung geht deshalb davon aus, dass ein langanhaltender Stromausfall in den Fällen a, b und c äußerst unwahrscheinlich ist. Eine konkrete Wahrscheinlichkeit lässt sich dafür nicht angeben. Angesichts der Vorsorgemaßnahmen der Netzbetreiber würde ein solcher Fall allenfalls aufgrund unvorhergesehener Umstände eintreten, deren Wahrscheinlichkeit sich wegen der Unvorhersehbarkeit nicht bestimmen lässt. Auch für den sehr unwahrscheinlichen Fall eines mindestens überregionalen Stromausfalls sorgen die Netzbetreiber durch ihre Netzwiederaufbaukonzepte für eine schnelle Wiederkehr der Stromversorgung vor. Hierfür werden beispielsweise sogenannte schwarzstartfähige Kraftwerke vorgehalten, die auch ohne Zufuhr elektrischer Energie von außen anfahren und einen Netzabschnitt aus einem vollständig abgeschalteten Zustand wieder unter Spannung zu setzen können.

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

IT-Sicherheit ist kein statischer Zustand, sondern ein dynamischer und fortlaufender Prozess, in dem es um den Umgang mit immer neuen Bedrohungslagen geht. Dabei ermöglicht die Analyse von Auffälligkeiten und Störungen der informationstechnischen Systeme in einem Unternehmen Rückschlüsse auf dessen IT-Sicherheit.

Mit dem IT-Sicherheitsgesetz wurden im Jahr 2015 in § 8b Absatz 4 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) und in § 11 Absatz 1c EnWG eine Meldepflicht für IT-Sicherheitsvorfälle für Betreiber Kritischer Infrastrukturen und Betreiber von Energieversorgungsnetzen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingeführt. Diese Störungsmeldungen werden durch das BSI an die BNetzA weitergeleitet.

Zudem haben alle Strom- und Gasnetzbetreiber sowie Betreiber von solchen Gasförderanlagen, Gasspeichern und Energieerzeugungsanlagen, die die jeweiligen Schwellenwerte der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) erreichen oder überschreiten, gemäß § 11 Absatz 1a, 1b EnWG die IT-Sicherheitskataloge umzusetzen und deren Umsetzung gegenüber der BNetzA nachzuweisen.

Die übrigen Betreiber Kritischer Infrastrukturen im Sektor Energie haben gemäß § 8a des BSI-Gesetzes die Einhaltung des Stands der Technik im Bereich der IT-Sicherheit gegenüber dem BSI nachzuweisen. Hierzu wurden beispielsweise für Anlagen zur Steuerung/Bündelung elektrischer Leistung oder auch im Bereich Fernwärme durch die Betreiber branchenspezifische Sicherheitsstandards erarbeitet und vom BSI eignungsgeprüft. Diese branchenspezifischen Sicherheitsstandards können daher zum Nachweis der gesetzlichen Anforderungen herangezogen werden.

Kernanforderung der oben genannten Anforderungen ist die Einführung eines Informationssicherheitsmanagementsystems. In diesem Rahmen müssen Betreiber stetig IT-Sicherheitsmaßnahmen planen, umsetzen, prüfen und erneut im Zuge eines kontinuierlichen Verbesserungsprozesses auf die angepassten Rahmenbedingungen reagieren. Das IT-Sicherheitsniveau der Kritischen Infrastrukturen verbessert sich also fortlaufend.

Auswertungen der beim BSI gemeldeten Störungen zeigen, dass es in den letzten Jahren aufgrund von Cyberangriffen in keinem Fall zu Versorgungsunterbrechungen der Energieversorgung gekommen ist. Es zeigt sich, dass die bestehenden Regelungen zu einer konstanten Weiterentwicklung und Verbesserung des Schutzniveaus gegenüber Cyberangriffen geführt haben, und in den Unter-

nehmen das Bewusstsein gegenüber modernen Cyberangriffen weiter geschärft wird.

Neben dem BSI-Gesetz und dem EnWG ist für die IT-Sicherheit im Sektor Energie auch das Gesetz zur Digitalisierung der Energiewende von wesentlicher Bedeutung. Mit ihm wurde 2016 das Gesetz für den Messstellenbetrieb und die Datenkommunikation in Intelligenten Energienetzen (MsbG) eingeführt, welches die technischen und rechtlichen Grundlagen für den Aufbau eines intelligenten Energienetzes in Deutschland regelt. Durch den stufenweise zu realisierenden Einsatz der vorgegebenen Kommunikationsinfrastruktur und eines zertifizierten Smart-Meter-Gateways nach dem MsbG in allen energiewenderelevanten Anwendungsfällen können die Sicherheit und Funktion von intelligenten Energienetzen gewährleistet werden.

In diesem Zusammenhang wird auch auf die Technische Richtlinie des BSI TR-03109 und das Schutzprofil PP-0073 sowie die Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende (GDEW) von BMWi und BSI verwiesen (https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/Standardisierungsstrategie/standardisierungsstrategie_node.html).

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

Die Zuständigkeit für die Schaffung, Einhaltung und Kontrolle von Vorschriften zur IT-Sicherheit in Kritischen Infrastrukturen nach der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) liegt für alle Anhänge der BSI-KritisV gleichermaßen beim Bund, da sowohl die Bestimmung in der BSI-KritisV, welche Einrichtungen Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik gelten (§ 10 Absatz 1 BSIG), als auch die sich daraus ergebenden Rechtsfolgen in Bundesgesetzen (u. a. BSIG, EnWG, Telekommunikationsgesetz (TKG), Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (AtG)) geregelt werden, und auch der diesbezügliche Vollzug in Zuständigkeit des Bundes liegt. Die föderale Struktur der Bundesrepublik Deutschland hat bei Vorschriften zur IT-Sicherheit in Kritischen Infrastrukturen nach BSI-KritisV daher keine unmittelbaren Auswirkungen.

5. Wie viele meldepflichtige Vorfälle nach § 8b Absatz 4 des BSI-Gesetzes (BSIG) sind in den Jahren 2017, 2018 und 2019 gemeldet worden (bitte getrennt nach Jahren und nach Meldungen nach § 8b (4) 1. und § 8b (4) 2. auflisten und nach allen Anhängen der KritisV aufschlüsseln)?

Nach den Sektoren bzw. Anhängen der BSI-KritisV aufgeschlüsselte Auswertungen zu meldepflichtigen Vorfällen nach § 8b Absatz 4 BSIG können den jährlichen Lageberichten des BSIentnommen werden, die unter der folgenden Adresse öffentlich zugänglich sind: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html. Bei der statistischen Erfassung der Meldungen nach § 8b Absatz 4 BSIG erfolgt keine Unterscheidung bezüglich Meldungen nach § 8b Absatz 4 Nummer 1 und Nummer 2 BSIG.

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

Bislang war es nicht erforderlich, die Hersteller unter Berufung auf § 8b Absatz 4 BSIG zur Mithilfe bei der Abstellung der Mängel aufzufordern. Die Hersteller kamen ihrer gesetzlichen Pflicht hierzu auch ohne eine derartige offizielle Aufforderung nach.

7. In wie vielen 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, (bitte nach Jahren getrennt auflisten):
   a) auf informationstechnische Netzwerke,
   b) auf operationstechnische Netzwerke erlangen?
   c) Bei wie vielen Vorfällen kann ein unberechtigter Zugriff zwar nicht eindeutig belegt werden, aber auch nicht ausgeschlossen werden?

Die Fragen 7a, 7b und 7c werden gemeinsam beantwortet.

Für den Zeitraum 2017 liegen dem BSI keine Meldungen vor.

Für den Zeitraum 2018 liegen dem BSI folgende Meldungen vor:

a) 3 Meldungen

b) 0 Meldungen

c) 1 Meldung

Für den Zeitraum 2019 liegen dem BSI folgende Meldungen vor:

a) 2 Meldungen

b) 0 Meldungen

c) 0 Meldungen

Seitens des BKA wurden in den Jahren 2017, 2018 und 2019 keine Ermittlungsverfahren im Zusammenhang mit Hackingangriffen auf deutsche Energieversorger geführt.

8. In wie vielen 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, (bitte nach Jahren getrennt auflisten):
   a) auf informationstechnische Netzwerke,
   b) auf operationstechnische Netzwerke erlangen?
   c) Bei wie vielen Vorfällen kann ein unberechtigter Zugriff zwar nicht eindeutig belegt werden, aber auch nicht ausgeschlossen werden?

Die Fragen 8a, 8b und 8c werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Im Zeitraum 2017 bis 2019 wurden dem BSI keine Meldungen abgegeben, bei denen der meldende Betreiber eine politische Motivation des Angreifers oder einen nachrichtendienstlichen Hintergrund angegeben hat. Seitens des Bundeskriminalamtes wurden in den Jahren 2017, 2018 sowie 2019 keine Ermittlungsverfahren gegen Unbekannt beziehungsweise Personen oder Personengruppen

mit Bezug zu oder im Auftrag von fremden Staaten aufgrund eines grundsätzlichen Zugriffs auf die Netzwerke der deutschen Energieversorger geführt. Das Bundesamt für Verfassungsschutz führt keine Statistik zur Anzahl von Vorfällen auf Netzwerke deutscher Energieversorger, da diese die tatsächliche Bedrohungslage durch Cyberangriffe mit nachrichtendienstlichem Hintergrund nicht belastbar abbilden können.

9. Welche Bemühungen hat die Bundesregierung unternommen, um die Empfehlungen der Enquete Kommission für Internet und digitale Gesellschaft (EIDG) auf Bundestagsdrucksache 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?

Die Fragen 9 bis 9b werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Bezüglich der Empfehlungen der Enquete Kommission in Abschnitt 4a zu Standards in Kritischen Infrastrukturen zur Gewährleistung eines hohen IT-Sicherheitsniveaus wird auf die Antwort zu Frage 3 verwiesen. Die von der Enquete-Kommission vorgeschlagene Verpflichtung von Betreibern Kritischer Infrastrukturen zur Erfüllung von Mindestanforderungen an die IT-Sicherheit (Stand der Technik) durch eine gesetzliche Regelung wurde im ersten IT-Sicherheitsgesetz von 2015 eingeführt.

Bezüglich der Empfehlungen zur Verbesserung der IT-Sicherheit in SCADA- und PLC-Systemen in Abschnitt 4 b) hat das BSI hat eine Reihe von Publikationen zum Schutz industrieller Automatisierungs- und Kontrollsysteme veröffentlicht, zu denen die SCADA- und PLC-Systeme gehören. Diese sollen Hersteller unter anderem bei der Entwicklung sicherer Komponenten und bei der Reaktion auf Schwachstellen unterstützen. Zudem wurden Empfehlungen für Betreiber dieser Systeme veröffentlicht, die technische und organisatorische Maßnahmen für einen sicheren Betrieb beschreiben. Diese Dokumente sind öffentlich einsehbar unter den folgenden Adressen:

https://www.bsi.bund.de/DE/Themen/ICS/Empfehlungen/ICS-Hersteller/empfehlungen_hersteller_node.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html#download=1.

Zudem ist das BSI bei der Deutschen Kommission für Elektrotechnik (DKE) und der Plattform Industrie 4.0 an der Erarbeitung von sicheren Konzepten und internationalen Standards für Industrielle Automatisierungs- und Kontrollsysteme beteiligt.

Darüberhinausgehende Maßnahmen, um Hersteller von SCADA- und PLC-Systemen zur Veröffentlichung ihres Quellcodes zu bringen, sind der Bundesregierung nicht bekannt. Diesbezüglich verpflichtende Maßnahmen könnten zudem aufgrund des europäischen Binnenmarkts sinnvoll nur auf europäischer Ebene eingeführt werden. Die Bundesregierung weist zudem darauf hin, dass das Offenlegen von Quellcode allein noch nicht zwangsläufig die Sicherheit erhöht, da der Quellcode potentiellen Evaluatoren und potentiellen Angreifern gleichermaßen offengelegt wird. Das Auffinden etwaig vorhandener Schwachstellen erfordert dennoch oft erhebliche Aufwände.

Bei der Behebung von Schwachstellen kann Open-Source-Software Vorteile bieten, wenn z. B. entsprechende Updates/Patches notfalls auch durch andere fachkundige Mitglieder der Community herausgegeben werden.

Dieser Vorteil von Open-Source-Software gilt nicht zwangsläufig auch für proprietäre Software, deren Quellcode lediglich zur Einsichtnahme offengelegt wird (sogenannte Shared-Source-Software).

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 auflisten)?

Die Cyber-Sicherheitsstrategie für Deutschland 2016 formuliert Leitlinien der Cyber-Sicherheitsstrategie und beschreibt vier Handlungsfelder mit Maßnahmen, um eine zukunftsgerichtete Cyber-Sicherheitspolitik zu gestalten. Die beschriebenen Maßnahmen sind nicht verbindlich. Eine Zuordnung der Empfehlungen zu Maßnahmen ist nicht gegeben.

a) Welche Empfehlungen wurden wann erfolgreich umgesetzt?

b) Welche Empfehlungen sind aktuell in der Umsetzung?

Bis wann wird die Umsetzung vorrausichtlich abgeschlossen sein?

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

Derzeit wird eine Evaluierung der Cyber-Sicherheitsstrategie 2016 durchgeführt und erfasst, welche Maßnahmen erfolgreich umgesetzt wurden bzw. noch umgesetzt werden.

c) Welche Empfehlungen sind geplant umzusetzen?

Wann wird die Umsetzung beginnen?

Im Anschluss an die Evaluierung ist eine Fortschreibung der Cyber-Sicherheitsstrategie geplant. Im Rahmen des Fortschreibungsprozesses wird festgelegt, welche Empfehlungen oder Maßnahmen zukünftig Berücksichtigung finden.

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?

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

Vorgaben des Energiewirtschaftsgesetzes fördern sichere digitale Informations- und Kommunikationsprozesse für Strom- und Gasnetze sowie Energieanlagen (§ 11 Absatz 1a und b EnWG). § 11 EnWG formuliert in diesem Zusammenhang bestimmte Schutzziele, nämlich den Schutz der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systemen.

Basierend auf § 11 Absatz 1a und 1b EnWG sind von der BNetzA im Benehmen mit dem BSI Sicherheitskataloge erstellt worden. Die Regelungen aus den Sicherheitskatalogen gelten für alle Strom- und Gasnetzbetreiber sowie für Betreiber von Energieanlagen, die als Kritische Infrastruktur nach der BSI-KritisV bestimmt wurden.

Die Sicherheitskataloge etablieren einen angemessenen Schutz gegen Bedrohungen für IKT-Systeme, die für einen sicheren Netz- bzw. Anlagenbetrieb notwendig sind. Soweit nötig umfassen die Sicherheitskataloge auch die Verwendung von Verschlüsselung, Authentifizierung und digitalen Signaturen im Bereich der drahtgebundenen operations- und informationstechnischen Netzwerke, sowie der drahtlosen operationstechnischen Netzwerke.

Die Kernanforderung der Sicherheitskataloge ist die Einführung, Umsetzung und Betrieb eines Informationssicherheits-Managementsystems (ISMS), das den Anforderungen der DIN ISO/IEC 27001 in der jeweils geltenden Fassung genügt. Das ISMS muss kontinuierlich auf seine Wirksamkeit überprüft und im Bedarfsfall angepasst werden. Damit ist sichergestellt, dass jedes Unternehmen in Abhängigkeit der für dieses Unternehmen maßgeblichen Rahmenbedingungen die im Einzelfall angemessenen Schutzmaßnahmen ergreift. Dabei können

die Unternehmen auf verschiedene technische Vorschriften, Standards, Normen, Leitlinien und Empfehlungen zurückgreifen.

Weitere Normen formulieren Umsetzungsempfehlungen für die verbindlichen Maßnahmen des Anhangs A der DIN EN ISO/IEC 27001. Die DIN EN ISO/IEC 27002 gibt u. a. konkrete Richtlinien zur Verschlüsselung von Informationen vor, die von jedem Unternehmen bei der Einführung eines ISMS beachtet und je nach Notwendigkeit individuell umgesetzt werden müssen (Punkt 10. „Cryptography"). Hierdurch wird die Vertraulichkeit, die Authentizität und die Integrität von Informationen geschützt. Die DIN EN ISO/IEC 27019 erweitert die DIN EN ISO/IEC 27002 in verschiedenen Punkten um Besonderheiten im Bereich der Prozesssteuerung der Energieversorgung. Unter Verweis auf weitere Spezialnormen beinhaltet dies z. B. auch die Nutzung (Erzeugung, Verteilung und Aufhebung) von digitalen Zertifikaten und kryptographischen Schlüsseln in der Kommunikation von elektrischen Energieversorgungssystemen: Unter dem Kapitel 10.1.2 „Key management" wird beispielsweise auf die IEC 62351-9 zum Umgang mit kryptographischen Schlüsseln, Zertifikaten etc. in „Power systems communications" verwiesen.

Die Normenreihe IEC 62351 – „Power systems management and associated information exchange – Data and communications security" beschreibt Anforderungen und Maßnahmen zur Absicherung der Kommunikationsprotokolle in der Energieversorgung. Fokus ist u. a. eine Ende-zu-Ende-Absicherung, Zertifikats- und Schlüsselmanagement sowie Authentisierung und Autorisierung.

Die IEC 62351-9 „Cyber security key management for power system equipment" beschreibt detailliert den Aufbau sowie den Betrieb einer Public-Key-Infrastruktur (PKI) im Einsatz bei Energieversorgern.

Netzbetreiber und Energieanlagenbetreiber sind verpflichtet, die Konformität ihres ISMS mit den Anforderungen des jeweiligen IT-Sicherheitskatalogs durch ein Zertifikat zu belegen. Der Zertifizierungsprozess erfordert ein jährliches Überwachungsaudit und eine Rezertifizierung alle drei Jahre.

Nur so kann die Gültigkeit des Zertifikats aufrechterhalten werden. Für Energieanlagenbetreiber besteht diese Verpflichtung erstmalig zum 31. März 2021.

Die Zertifizierung muss durch eine unabhängige und für die Zertifizierung akkreditierte Stelle durchgeführt werden. Der Abschluss des Zertifizierungsverfahrens ist der Bundesnetzagentur durch Vorlage einer Kopie des Zertifikats mitzuteilen. Die Akkreditierung der zertifizierten Stelle erfolgt im Auftrag der Bundesnetzagentur durch die Deutsche Akkreditierungsstelle (DAkkS) und wird auf Grundlage der ISO 27006 durchgeführt. Werden während der Audits Mängel aufgedeckt, die einer erfolgreichen Zertifizierung entgegenstehen, sind diese in Abstimmung mit den jeweiligen Auditoren innerhalb einer durch die einschlägigen Normen vorgegebenen Frist abzustellen. Der Bundesregierung liegen keine Informationen darüber vor, wie oft hierbei Mängel festgestellt wurden.

Das von der Bundesnetzagentur veröffentlichte Konformitätsbewertungsprogramm gibt die Standards für die Akkreditierung vor, u. a. Anforderungen an die Expertise von Auditoren und den Umfang von Audits.

Für alle übrigen Betreiber Kritischer Infrastrukturen im Energiesektor gelten die diesbezüglichen Anforderungen nach § 8a Absatz 1 des BSI-Gesetzes, welcher Betreiber zur Umsetzung von angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse verpflichtet, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Es wird in diesem Zusammenhang auf die Antwort zu Frage 3 verwiesen. Auch die dort

erwähnten branchenspezifischen Sicherheitsstandards sehen in der Regel verschiedene Anforderungen zur Verschlüsselung z. B. nach Anhang A der DIN EN ISO/IEC 27001 vor. Die Erfüllung dieser Anforderungen ist gemäß § 8a Absatz 3 BSIG alle zwei Jahre gegenüber dem BSI nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Soweit während den Audits, Prüfungen oder Zertifizierungen hier Nachbesserungsbedarf oder relevante Mängel ersichtlich werden, sind diese abzustellen. Das BSI kann gemäß § 8a Absatz 3 Satz 5 BSIG auch die Beseitigung von Sicherheitsmängeln verlangen.

Um möglichen Angriffen auf das Energienetz zu begegnen, sind nachweislich sichere und standardisierte Produktkomponenten und Systeme sowie eine sichere Kommunikationsinfrastruktur entscheidend.

Das zertifizierte Smart-Meter-Gateway nach Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (MsbG) stellt insofern ein wichtiges Element zur Absicherung von Kritischen Infrastrukturen dar und wird stufenweise nach und nach in allen energiewenderelevanten Anwendungsfällen zum Einsatz kommen. Verwiesen wird in diesem Zusammenhang auch auf die Technische Richtlinie des BSI TR-03109 das Schutzprofil PP-0073 sowie die Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende (GDEW) von BMWi und BSI (https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/Standardisierungsstrategie/standardisierungsstrategie_node.html).

Für diesbezügliche Datenkommunikation in informationstechnischen Netzwerken wird in § 52 Absatz 1 bis 4 MsbG eine verschlüsselte elektronische Kommunikation unter Nutzung der Smart-Metering-Public-Key-Infrastruktur des BSI vorgeschrieben. Gemäß der Festlegungen BK6-18-032, BK6-16-200 und BK7-16-142 der BNetzA-Beschlusskammern 6 und 7 werden für die elektronische Marktkommunikation zwischen den Teilnehmern des deutschen Energiemarkts hier die Anforderungen der Technischen Richtlinie des BSI TR-3109 für die Verschlüsselung und Signierung verpflichtend vorgeschrieben. Sofern der für die Vollzugsüberwachung zuständigen BNetzA Anhaltspunkte für eine unvollständige oder fehlerhafte Umsetzung dieser Vorgaben bekannt werden, hat diese die Möglichkeit, formelle Maßnahmen, etwa solche der Zwangsvollstreckung zu ergreifen. Aufgrund nicht termingerechter Umsetzung der Vorgaben zur Verschlüsselung ist die BNetzA im Jahr 2017 vereinzelt außerhalb formloser Aufsichtsverfahren auf Marktakteure zugegangen, was zur Abhilfe führte.

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 Liefermengen 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?

Die Fragen 14a bis 14c sowie 14d und 14e werden aufgrund ihres inhaltlichen Zusammenhangs zusammen beantwortet.

Die EPEX als Stromspotmarktbetreiberin hat ihren Sitz in Paris und befindet sich hinsichtlich der Absicherung ihrer digitalen Kommunikation mit Marktteilnehmern und Netzbetreibern unter regulatorischer Aufsicht der französischen Agentur für Sicherheit der Informationssysteme (Agence nationale de la sécurité des systèmes d'information – ANSSI). Für andere in Deutschland aktive Stromspotmarktbetreiber gelten, sofern die diesbezüglichen Schwellenwerte der BSI-KritisV erreicht oder überschritten werden, analog die Regelungen des § 8a Absatz 1 BSI-Gesetz, diesbezüglich wird auf die Antwort zu den Fragen 11 bis 11e, 12 bis 12e, 13 bis 13e verwiesen.

Daneben gibt es auch für die Verwendung von Verschlüsselung, Authentifizierung und digitalen Signaturen technische Vorschriften, die von den Börsenunternehmen bei der digitalen Kommunikation berücksichtigt werden. Von Bedeutung ist hier insbesondere die ISO/IEC 27000-Reihe. Soweit personenbezogene Daten übertragen werden, sind diese zudem auch aufgrund von Artikel 32 der EU-Datenschutzgrundverordnung zu verschlüsseln. Für die Kontrolle der diesbezüglichen Vorschriften sind die jeweiligen Datenschutzbeauftragten der Länder zuständig. Für die elektronische Marktkommunikation der deutschen Energiewirtschaft sind zudem auch der § 52 MsbG sowie die Festlegungen BK6-18-032, BK6-16-200 und BK7-16-142 der BNetzA-Beschlusskammern 6 und 7 relevant, welche die Verschlüsselung und Signierung in der elektronischen Marktkommunikation gemäß der Anforderungen der BSI-TR 3109 vorschreibt. Sofern der für die Vollzugsüberwachung zuständigen BNetzA Anhaltspunkte für eine unvollständige oder fehlerhafte Umsetzung dieser Vorgaben bekannt werden, hat diese die Möglichkeit, formelle Maßnahmen, etwa solche der Zwangsvollstreckung zu ergreifen. Aufgrund nicht termingerechter Umsetzung der Vorgaben zur Verschlüsselung ist die BNetzA im Jahr 2017 vereinzelt außerhalb formloser Aufsichtsverfahren auf Marktakteure zugegangen, was zur Abhilfe führte.

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

Der Bevölkerung stehen grundsätzlich Festnetztelefonie, Mobilfunk, Internet, Rundfunk, Presse und verschiedene funkbasierte Lösungen (in Not- und Katastrophenfällen auch Amateurfunk) als Kommunikationsmittel zur Verfügung. Das Mindestangebot an Telekommunikationsdiensten, das bei einer Krise oder Katastrophe zu gewährleisten ist, ist im Gesetz zur Sicherstellung von Postdienstleistungen und Telekommunikationsdiensten in besonderen Fällen (Post- und Telekommunikationssicherstellungsgesetz (PTSG)) festgelegt.

Allgemein sind zudem solche Kommunikationsmittel für die Alltagskommunikation verfügbar, die stromlos funktionieren. Behördliche Informationen werden beispielsweise über Flugblätter, Anschläge oder mobile Lautsprecherdurchsagen an die Bevölkerung weitergegeben. In der Vergangenheit wurden auch lokale Rundfunksender für die Weitergabe von Informationen genutzt, da z. B. über das Autoradio oft über einen längeren Zeitraum Radioempfang möglich ist.

Daneben liegt die Planung von Vorsorgemaßnahmen, z. B. im Bereich des Katastrophenschutzes gegen langanhaltende und überregionale Stromausfälle in der Zuständigkeit der Länder. Zu diesen Vorsorgemaßnahmen gehören auch Planungen zur Aufrechterhaltung von Kommunikationsmöglichkeiten. Zur konkreten Ausgestaltung der Vorsorgemaßnahmen in den Ländern kann die Bundesregierung keine Aussage treffen.

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

Die Zeitspanne, die Mobilfunknetze ohne Versorgungseinschränkung der Mobilfunkversorgung der Bevölkerung einen Stromausfall tolerieren können, kann einige Minuten betragen.

In § 109 Absatz 2 TKG wird geregelt, dass Betreiber von öffentlichen Telekommunikationsnetzen angemessene technischen Vorkehrungen und Maßnahmen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch soweit sie durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, zu treffen haben. Konkrete zeitliche Vorgaben zur Aufrechterhaltung der Verfügbarkeit bei einem Stromausfall werden jedoch nicht vorgegeben.

In den Mobilfunknetzen gibt es sowohl Basisstationen, die nicht gegen Versorgungsunterbrechungen gesichert sind, als auch einige Stationen, die über eine unterbrechungsfreie Stromversorgung (USV) verfügen, und solche, die über stationäre Netzersatzanlagen (NEA) (je nach Risikoabschätzung des Betreibers) mehrere Stunden mit Notstrom versorgt werden können.

Die zentralen Einrichtungen der Mobilfunk-Netzinfrastruktur sind i. d. R. für mehrere Stunden bis einzelne Tage notstromversorgt. Auch wenn konkrete Daten über die Verfügbarkeit der Basisstationen bei einem Stromausfall nicht vorliegen, muss davon ausgegangen werden, dass sie ohne entsprechende Ersatzstromversorgung ca. 0 bis 3 Stunden nach Eintritt eines Stromausfalls nicht mehr zur Verfügung stehen würden.

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

Hinsichtlich der rechtlichen Vorgaben nach § 109 Absatz 2 TKG wird auf die Antwort zu Frage 15a hingewiesen.

Im festen Telefonnetz kann die Zeitspanne, in der ein Stromausfall ohne Versorgungseinschränkung der Bevölkerung überbrückt werden kann, ebenfalls einige Minuten bis wenige Stunden betragen. Im Bereich der Festnetztelefonie sind zentrale Knoten zur Steuerung und Vermittlung mit Notstromkapazitäten bis zu einigen Tagen ausgestattet. Die Verfügbarkeit der zentralen Knoten kann bei Einsatz von Dieselgeneratoren grundsätzlich solange sichergestellt werden, wie die Zulieferung von Diesel gewährleistet ist.

Da jedoch das Zugangsnetz (auch DSLAM = Digital Subscriber Line Access Multiplexer) und Endeinrichtungen der Netzteilnehmer auf die öffentliche Stromversorgung angewiesen sind, versprechen zentrale Maßnahmen zur Aufrechterhaltung der Stromversorgung für den Teilnehmer wenig erfolgreich zu sein.

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

Die Planung von Vorsorgemaßnahmen z. B. im Bereich des Katastrophenschutzes gegen Stromausfälle – zu denen auch Planungen zur Aufrechterhaltung der Notrufmöglichkeiten gehören – liegt in der Zuständigkeit der Länder. Zur konkreten Ausgestaltung der Vorsorgemaßnahmen in den Ländern kann die Bundesregierung keine Aussage treffen.

Für langanhaltende, großflächige Stromausfälle halten die jeweils örtlichen Katastrophenschutzbehörden Notfallpläne vor, die auch das Ermöglichen von

Notrufen für die Bevölkerung vorsehen. Oft werden hierfür beispielsweise Anlaufstellen an Polizeistationen oder Feuer- und Rettungswachen etabliert, von denen der Notruf über den BOS-Funk (BOS: Behörden und Organisationen mit Sicherheitsaufgaben) weitergeleitet werden kann. Zudem können Einsatzkräfte vor Ort, die über eigene Kommunikationsmittel verfügen, direkt angesprochen werden.

Der Bevölkerung stehen zudem verschiedene funkbasierte Lösungen (unter Anderem Satellitentelefone, CB- und Jedermannfunk) zur Verfügung. Bei Ausfall der öffentlichen Telekommunikationsnetze können Notrufe gegebenenfalls über Betriebs- und Bündelfunknetze (zum Beispiel von Unternehmen des öffentlichen Personennahverkehrs einschließlich Taxen) oder mit Hilfe von Funkamateuren abgesetzt werden.

d) Welche Veränderung der Angaben auf die Antworten zu den Fragen 15a bis15c beobachtet die Bundesregierung im Vergleich zur Versorgungssicherheit vor der Umstellung auf NGN (New Generation Network) oder VoIP (Voice over IP)?

Die nach § 109 TKG für Betreiber erforderlichen Schutzmaßnahmen gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, unterscheiden nicht nach den verschiedenen technischen Systemen. Die Anforderungen gelten systemunabhängig. Dennoch hat der Umbau der Telekommunikationsnetze auf Next Generation Network (NGN) (IP-basierte Netzarchitektur) Veränderungen in der Versorgungssicherheit zur Folge. Durch die Umstellung auf Next Generation Access Network (NGA-Netze) sind die daran angeschlossenen Modems, Router oder/und Endgeräte von einer externen Stromversorgung abhängig. Endnutzer können in begrenztem Umfang durch Bereithaltung eines externen Netzersatzes für die Stromversorgung (z. B. durch Batteriepufferung) für eine höhere Verfügbarkeit der TK-Dienste sorgen.

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