xmera

November 2017

BSI-Kriterium hebelt Meldepflicht für Energieversorger wieder aus

Darstellung und kritische Betrachtung der BSI-Stellungnahme zur Meldepflicht für Nicht-KRITIS-Energieversorgungsnetzbetreiber.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung

Nicht-KRITIS-Energieversorgungsnetzbetreiber nehmen im Rahmen der neuen IT-Sicherheitsregelungen für KRITIS-Unternehmen eine Sonderrolle ein. Problematisch sind dabei die bisherigen Kriterien für die Meldung von IT-Sicherheitsvorfällen, da sie ausschließlich auf KRITIS-Unternehmen ausgelegt sind.

xmera hat ausführlich im Beitrag „Meldepflicht doch nicht für alle Energieversorger relevant?“ über dieses Thema berichtet und das Bundesamt für Sicherheit in der Informationstechnik (BSI) um eine Stellungnahme gebeten.

Erfahren Sie in diesem Beitrag welche Kriterien das BSI für Nicht-KRITIS-Energieversorger bezüglich der Meldepflicht von IT-Sicherheitsvorfällen vorsieht und warum dadurch die Meldepflicht für Nicht-KRITIS-Energieversorgungsnetzbetreiber wieder nahezu vollständig ausgehebelt wird.

Gesetzliche Meldepflicht für Energieversorger

Mit dem IT-Sicherheitsgesetz (IT-SiG) wurden in 2015 zahlreiche Gesetze geändert, um Unternehmen Kritischer Infrastrukturen zur Einführung informationssicherheitsrelevanter Maßnahmen zu verpflichten. Die Pflicht zur Meldung von IT-Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik ist eine dieser Maßnahmen.

Lesen Sie hierzu unseren Beitrag „IT-Sicherheitsgesetz Energieversorger & Neuregelung“.

Seit dem Jahre 2016 regelt das EnWG in § 11 Absatz 1c die Meldepflicht für KRITIS-Energieversorgungsnetzbetreiber und KRITIS-Energieanlagenbetreiber. Erst seit diesem Sommer gilt die Meldepflicht für alle Energieversorgungsnetzbetreiber unabhängig davon, ob sie zu den Kritischen Infrastrukturen in Deutschland gehören oder nicht.

Den Energieversorgungsnetzbetreiber des KRITIS-Sektors Energie wird hier eine Sonderrolle innerhalb der übrigen KRITIS-Unternehmen zugesprochen. Diese Sonderrolle betont die herausragende Bedeutung der Strom- und Gasversorgung für unsere Gesellschaft. Der Schutz vor Cyber-Angriffen und anderen Bedrohungen hat somit eine besonders hohe Priorität in Deutschland.

Die vom Gesetzgeber eingeführte Meldepflicht für IT-Sicherheitsvorfälle, die die Strom- oder Gasversorgung beeinträchtigen (könnten), soll das BSI dabei unterstützen schnellst möglichst Warnmeldungen an alle Versorgungsunternehmen herauszugeben.

Der Schwarzfall darf nicht Realität werden.

KRITIS-Energieversorgungsnetzbetreiber und Nicht-KRITIS-Energieversorgungsnetzbetreiber

Zu den KRITIS-Energieversorgungsnetzbetreibern gehören gemäß Anhang 1 BSI-KritisV Strom- und Gasversorger, dessen Versorgungsgrad den Schwellenwert für das entsprechende Netz erreicht oder überschreitet.

Schwellenwerte Energieversorgungsnetz	Transportnetz	Verteilernetz
Strom	3.700 GWh/Jahr	3.700 GWh/Jahr
Gas	5.190 GWh/Jahr	5.190 GWh/Jahr

TABELLE 1: SCHWELLENWERTE FÜR ENERGIEVERSORGUNGSNETZE[1]

Für das Stromtransport- und –verteilernetz ist die durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit ausschlaggebend. Für das Gastransportnetz gilt dasselbe. Basis des Gasverteilernetzes ist lediglich die entnommene Arbeit.

Die Berechnung der Schwellenwerte basiert auf der Versorgung von 500.000 Personen im Jahr. Dabei werden Durchschnittsverbräuche mit dem Regelschwellenwert von 500.000 Personen multipliziert, um den für das entsprechende Netz relevanten Schwellenwert zu ermitteln.

Alle Energieversorgungsnetzbetreiber, die den für sie relevanten Schwellenwert nicht erreichen sind Nicht-KRITIS-Energieversorgungsnetzbetreiber.

Die folgende Strukturanalyse der Energieversorgungsnetzbetreiber auf Basis von versorgten Personen soll einen Eindruck darüber vermitteln wie viele Nicht-KRITIS-Energieversorgungsnetzbetreiber es schätzungsweise in Deutschland gibt.

Struktur der Energieversorgungsnetzbetreiber in Deutschland

Strom- und Gasnetzbetreiber sind gesetzlich verpflichtet Netzstrukturdaten zu veröffentlichen. Auf Basis dessen erhebt die Bundesnetzagentur regelmäßig Daten und fasst sie zu einem Monitoringbericht zusammen.

Der Monitoringbericht 2016 enthält Strukturdaten über Energieversorgungsnetzbetreiber nach Zählpunkten. Nachfolgend werden Faktoren hergeleitet, die eine Schätzung für versorgte Personen pro Zählpunkt erlauben.

[1] Entnommen aus dem Anhang1 der BSI-KritisV.

Personenfaktor pro Stromzählpunkt

In 2015 gab es deutschlandweit rund 47,3 Millionen Stromzählpunkte von Haushaltskunden, die allesamt von Verteilnetzbetreibern versorgt wurden. Bei ca. 82,18 Millionen Einwohnern im selben Jahr in Deutschland[2], steht ein Stromzählpunkt für durchschnittlich ca. 1,7 Personen.

Personenfaktor pro Gaszählpunkt

Deutschlands Gasversorgungsnetzbetreiber versorgten in 2015 rund 12,39 Millionen Haushalte. In 2015 gab es deutschlandweit 40,78 Millionen Haushalte.[3] Bei rund 82,18 Millionen Einwohnern im selben Jahr sind das ca. 2,02 Personen pro Haushalt. Für Gasnetzbetreiber ergibt sich ein Durchschnittsfaktor von ca. 2,02 Personen pro Zählpunkt.

Strukturdaten Stromnetzbetreiber

Aus dem Monitoringbericht 2016 der Bundesnetzagentur geht hervor, dass die Struktur der Verteilnetzbetreiber sehr regional geprägt ist. Es gibt daher sehr viele kleine Netzbetreiber. Rund 48 % aller Netzbetreiber versorgten 2015 zwischen 1.001 und 15.000 Zählpunkte. Höchstens 100.000 Zählpunkte pro Versorgungsnetzbetreiber wurden von 90% der Unternehmen versorgt.

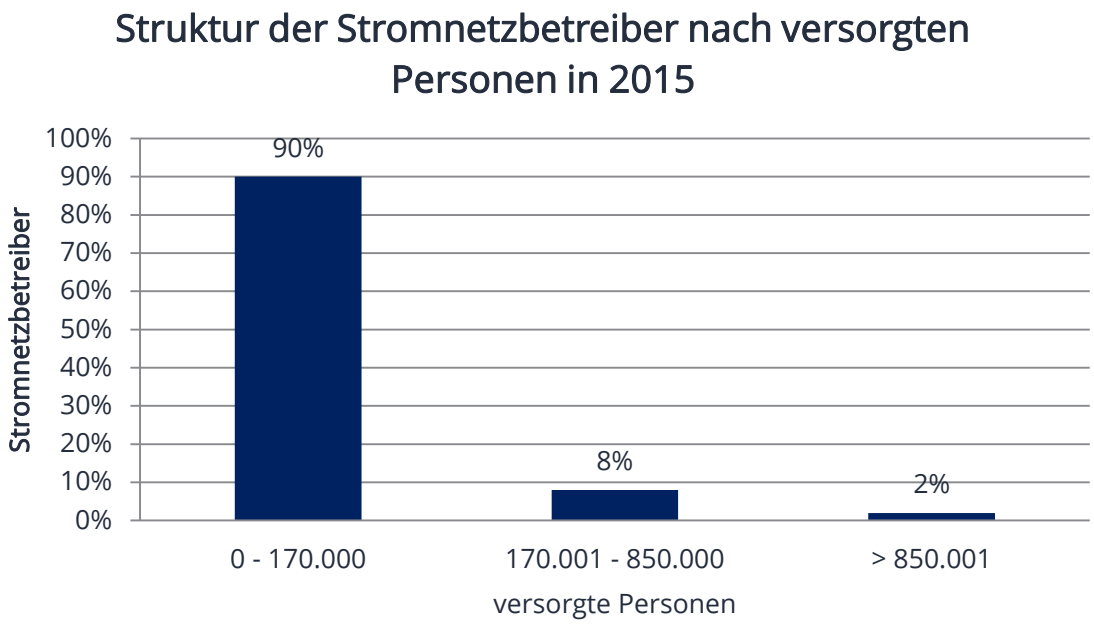

ABBILDUNG 1: STRUKTUR DER STROMNETZBETREIBER NACH VERSORGTEN PERSONEN[4]

[2] Vgl. Statista (2016).
[3] Vgl. Statista (2017).
[4] Eigene Darstellung nach Daten der Bundesnetzagentur aus dem Monitoringbericht 2016.

Unter Einbeziehung des Personenfaktors ergibt sich, dass 90% aller Stromnetzbetreiber nicht mehr als 170.000 Personen in ihrem jeweiligen Versorgungsgebiet versorgten.

Von allen 884 Stromnetzbetreibern in 2015 sind das 803 Verteilnetzbetreiber[5], die vermutlich zu den Nicht-KRITIS-Energieversorgungsnetzbetreibern gehören. Selbst von den verbleibenden 81 Stromnetzbetreibern werden nicht alle KRITIS-Energieversorgungsnetzbetreiber sein.

Strukturdaten Gasnetzbetreiber

Die Struktur der Gasversorgungsnetzbetreiber ist vergleichbar mit der Struktur der Stromversorgungsnetzbetreiber. Sie ist ebenfalls sehr regional geprägt. Im Jahre 2015 gab es 731 Gasversorgungsnetzbetreiber. Davon waren 17 Transportnetzbetreiber. Die übrigen 714 waren Verteilnetzbetreiber.

Rund 58 % aller Gasnetzbetreiber versorgten in ihrem Gebiet nicht mehr als 10.000 Haushalte. Gute 96 % belieferten weniger als 100.000 Haushalte in ihrem jeweiligen Versorgungsgebiet.

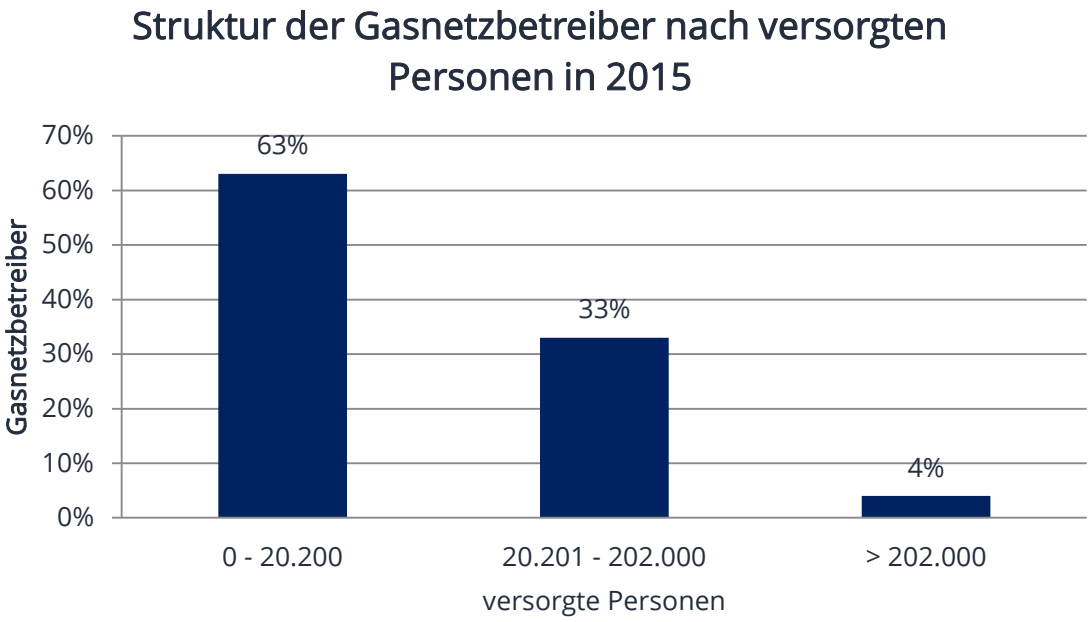

ABBILDUNG 2: STRUKTUR DER GASNETZBETREIBER NACH VERSORGTEN PERSONEN[6]

[5] Vgl. Bundesnetzagentur, Bundeskartellamt (2016).
[6] Eigene Darstellung nach Daten der Bundesnetzagentur aus dem Monitoringbericht 2016.

Wird der Personenfaktor pro Zählpunkt berücksichtigt, versorgten rund 96 % der Gasnetzbetreiber schätzungsweise weniger als 202.000 Personen in ihrem jeweiligen Versorgungsgebiet.

Gut 90 % aller Energieversorgungsnetzbetreiber sind vermutlich Nicht-KRITIS-Unternehmen.

BSI-Kriterien zur Meldepflicht für Nicht-KRITIS-Energieversorgungsnetzbetreiber

Für KRITIS-Energieversorgungsnetzbetreiber gilt die Meldepflicht bereits seit 2016. In diesem Kontext hat das BSI den Gesetzestext, verankert in § 8b Absatz 4 BSIG, ausgelegt und Kriterien für KRITIS-Unternehmen formuliert. Der Absatz zur Meldepflicht im Energiewirtschaftsgesetz stimmte damals wie heute fast wortgleich überein.

Da die Meldepflicht in 2016 ausschließlich für KRITIS-Energieversorgungsnetzbetreiber und KRITIS-Energieanlagenbetreiber und andere KRITIS-Unternehmen der entsprechenden Sektoren galt, waren auch die BSI-Kriterien zur Meldepflicht ausschließlich auf KRITIS-Unternehmen abgestimmt.

Dies zeigt sich insbesondere in den quantitativen Kriterien zur Bestimmung einer erheblichen Beeinträchtigung der Versorgungssicherheit. Sie basieren auf den in der BSI-KritisV definierten Schwellenwerten.

Mit der Neuregelung durch die NIS-Richtlinie wurde die Meldepflicht auf alle Energieversorgungsnetzbetreiber ausgeweitet. Somit müssen seit dem 30. Juni 2017 auch Nicht-KRITIS-Energieversorgungsnetzbetreiber unter bestimmten Umständen IT-Sicherheitsvorfälle an das BSI melden.

Problematisch daran ist, dass von Seiten des BSI keine Kriterien für diese Sondergruppe von Nicht-KRITIS-Unternehmen zur Bestimmung der bestimmten Umstände formuliert wurden. Nicht-KRITIS-Energieversorgungsnetzbetreiber hängen diesbezüglich in der Luft.

xmera berichtete über diese Situation bereits im vergangenen Monat und bat das Bundesamt für Sicherheit in der Informationstechnik um Stellungnahme.

Lesen Sie hierzu unseren Beitrag „Meldepflicht doch nicht für alle Energieversorger relevant?“.

Wir fragten: “

1. Ist es von Seiten des BSI geplant Schwellenwerte für Nicht-KRITIS-Energieversorgungsnetzbetreiber auszuarbeiten?
2. Wie sollen Nicht-KRITIS-Energieversorgungsnetzbetreiber mit dem Thema Beeinträchtigung als Kriterium für eine Meldepflicht umgehen?“

Das BSI antwortete: “

1. Nein, es ist nicht geplant, Schwellenwerte speziell für Nicht-KRITIS-Energieversorgungsnetzbetreiber festzulegen.

2. Mit Wirkung vom 23.Juni 2017 heißt es in § 11 1c wie folgt:
   Betreiber von Energieversorgungsnetzen [...] haben

   1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben,

   2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können über die Kontaktstelle unverzüglich an das BSI zu melden:

   Eine "erhebliche" Beeinträchtigung ist in diesem Zusammenhang definiert als eine Beeinträchtigung, die mehr als 250.000 Personen betrifft. Dies bedeutet somit für kleine Stadtwerke (< 250.000 Personen), dass i. d. R. nur Störungen die zu Ausfällen geführt haben oder hätten führen können meldepflichtig sind, da "erhebliche" Beeinträchtigungen i. d. R. nicht auftreten können. Sollte die Beeinträchtigung allerdings über das eigene Versorgungsgebiet hinaus bestehen, so wäre sie ggf. auch wieder meldepflichtig.“

! Eine "erhebliche" Beeinträchtigung ist i.V.m § 11 Absatz 1c EnWG definiert als eine Beeinträchtigung, die mehr als 250.000 Personen betrifft.

Auf Basis der obigen Strukturanalyse und des vom BSI genannten Kriteriums von 250.000 versorgten Personen sind vermutlich über 90% der Energieversorgungsnetzbetreiber von der Meldepflicht nur im Falle eines tatsächlichen oder drohenden Totalausfalls betroffen. Das Kriterium der erheblichen Beeinträchtigung ist für sie nicht anwendbar.

Was bedeutet das BSI-Kriterium für Deutschlands Energieversorgungssicherheit?

BSI-Kriterium ohne Berücksichtigung der regionalen Struktur

Deutschlands Strom- und Gasnetze werden von sehr vielen kleinen Netzgesellschaften betrieben. Die jeweiligen Versorgungsgebiete der Netzgesellschaften versorgen überwiegend weniger als 250.000 Personen, dem Grenzwert des BSI für eine erhebliche Beeinträchtigung.

Aufgrund der herausragenden Bedeutung der Strom- und Gasversorgung für unsere Gesellschaft hat der Gesetzgeber für Energieversorgungsnetzbetreiber eine Sonderregelung eingeführt und alle Betreiber von Strom- und Gasnetzen dazu verpflichtet Störungen der Informationssicherheitsschutzziele, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Versorgungssicherheit führen (könnten), zu melden.

Im BSI-Kriterium von 250.000 versorgten Personen spiegelt sich die sehr regional geprägte Struktur unserer Energieversorgungsnetze nicht wieder. Rund 90 % der Strom- und Gasnetzbetreiber müssen einen IT-Sicherheitsvorfall lediglich dann melden, wenn es deswegen zu einem Totalausfall in ihrem Versorgungsgebiet kommt oder kommen könnte.

Totalausfall eines kleinen Netzbetreibers

Der Totalausfall eines der kleinen Versorgungsgebiete stellt sicher keine große Herausforderung für unsere Versorgungssicherheit dar. Problematisch wird es erst, wenn mehrere kleine Versorger keine Energie mehr liefern können. Je nach Größe können zwei Netzbetreiber zusammen durchaus die kritische Grenze von 250.000 versorgten Personen erreichen.

Totalausfall mehrerer kleiner Netzbetreiber

Unwahrscheinlich, dass gleich mehrere Netzbetreiber gleichzeitig wegen eines Cyber-Angriffs ausfallen? Nicht unbedingt!

Genauso überschaubar wie die Zahl der Netzbetreiber ist das Angebot an Software für Leitsysteme. Insbesondere die kleinen Netzbetreiber verwenden für ihre Leitsysteme Software von maximal einer Handvoll Anbietern. Gäbe es bei einem der Softwarepakete eine Sicherheitslücke, wäre es ein leichtes für Cyberkriminelle mit einer Lücke halb Deutschland den Strom abzudrehen.

Das BSI würde von den betroffenen Netzbetreibern jedoch nur dann eine Meldung erhalten, wenn ein Totalausfall vorliegt oder droht. Ist die Versorgungssicherheit jedes einzelnen Betreibers lediglich beeinträchtigt, muss keine Meldung erstattet werden. Eine Frühwarnung an alle Versorger, die dieselbe Software verwenden, wäre dann nicht möglich.

Deutschlands Energieversorgungssicherheit

Das BSI-Kriterium basiert auf KRITIS-Grenzwerten und berücksichtigt damit nicht die regionale Struktur der Energieversorger. Kommt es zu Strom- oder Gasausfällen aufgrund von IT-Sicherheitsvorfällen, erhalten das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur daher nur von rund 10 % der Energieversorgungsnetzbetreiber Meldung darüber.

Ob die Ausweitung der Meldepflicht unter diesen Umständen überhaupt wirkungsvoll ist, darf an dieser Stelle durchaus in Frage gestellt werden.

Allerdings hängt Deutschlands Energieversorgungssicherheit sicherlich nicht allein von einer wirkungsvollen Meldepflicht ab. Nur mit zusätzlichen präventiven IT-Sicherheitsmaßnahmen kann der wachsenden Cyberbedrohung entgegengetreten werden. Das Management der Informationssicherheit (ISMS), wie es im IT-Sicherheitskatalog gefordert wird, nimmt hierbei eine tragende Rolle ein.

Wird in dieser Gesetzesvorgabe nicht nur eine lästige Pflicht sondern eine Chance zur proaktiven Stabilisierung unserer Energieversorgungssicherheit gesehen, sind wir auf einem guten Weg.

Zudem spricht nichts dagegen trotz der gesetzesaushebelnden Wirkung des BSI-Kriteriums freiwillig Meldungen abzusetzen.

Einbeziehung der Hersteller von Leitsystemsoftware oder Einführung eines speziellen Grenzwertes?

Die Leitsystemhersteller haben eine verantwortungsvolle Rolle im Rahmen der Informationssicherheit von Netzleitsystemen. Ein Schadprogramm in einem der Systeme wäre in jedem Fall kritisch für die Energieversorgungssysteme. Ein Lösungsansatz könnte sein, die Leitsystemhersteller in die Meldeprozesse mit einzubeziehen.

Ein weiterer Ansatz könnte die Einführung eines verpflichtenden technischen Sicherheitsstandards für Leitsysteme sein. Das bdew Whitepaper wäre dafür eine mögliche Vorlage. Dabei darf es jedoch nicht zu einer Vereinheitlichung der Systemstrukturen kommen, denn heterogene Strukturen bieten einen zusätzlichen Sicherheitsvorteil.

Oder sollte es einen speziellen Grenzwert für die erhebliche Beeinträchtigung der Strom- und Gasversorgungssicherheit geben, der die regionale Struktur unserer Energieversorgungsnetze wiederspiegelt?

Diese Lösung hätte zur Folge, dass wesentlich mehr Meldungen eingehen würden als bisher zu erwarten sind. Der Verarbeitungsaufwand würde steigen, der Anteil der relevanten Meldungen wiederum würde abnehmen. Dafür bestünde jedoch die Möglichkeit größere Zusammenhänge aus mehreren kleineren IT-Sicherheitsvorfällen aufzudecken.

Zusammenfassung

Im Sommer dieses Jahres hat die Bundesregierung im Zusammenhang mit der NIS-Richtlinie die Meldepflicht für IT-Sicherheitsvorfälle im KRITIS-Sektor Energie auf alle Energieversorgungsnetzbetreiber ausgeweitet.

Die Meldepflicht wird in § 11 Absatz 1c EnWG geregelt. Sie betrifft deutschlandweit in etwa 880 Stromnetzbetreiber und 730 Gasnetzbetreiber. Die Meldungen müssen an das BSI gesendet werden. Dabei sind nur solche IT-Sicherheitsvorfälle meldepflichtig, die die Kriterien des BSI erfüllen.

Die BSI-Kriterien zur Meldepflicht basieren auf den Schwellenwerten der KritisV. KRITIS-Energieversorgungsnetzbetreiber sind bereits seit einem Jahr dazu verpflichtet entsprechende Vorfälle nach den Kriterien zu melden.

Für Nicht-KRITIS-Energieversorgungsnetzbetreiber wird es keine Spezialkriterien von Seiten des BSI geben. Das BSI nennt nach Rückfrage von xmera den Grenzwert von 250.000 versorgten Personen als Kriterium für eine erhebliche Beeinträchtigung der Versorgungssicherheit.

Aufgrund der regional geprägten Struktur der Strom- und Gasnetzbetreiber werden schätzungsweise 90 % der Netzbetreiber durch das BSI-Kriterium Meldungen über IT-Sicherheitsvorfälle nur dann absetzen müssen, wenn die Versorgung in ihrem Gebiet dadurch vollständig ausfällt oder ausfallen könnte. IT-Sicherheitsvorfälle, die zu Beeinträchtigungen führen, werden wegen des Kriteriums nicht meldepflichtig.

War die Ausweitung der Meldepflicht überhaupt wirkungsvoll, wenn vermutlich weniger als 10 % der Energieversorgungsnetzbetreiber IT-Sicherheitsvorfälle vollumfänglich melden müssen?

Gibt es vielleicht eine bessere Lösung? xmera schlägt drei Lösungsansätze vor und lädt zur offenen Diskussion ein:

1. Leitsystemhersteller in den Meldeprozess einbeziehen.
2. Einführung eines verpflichtenden technischen Sicherheitsstandards für Leitsysteme.
3. Erarbeitung eines eigenen Grenzwertes für Nicht-KRITIS-Energieversorgungsnetzbetreiber.

Abschließend bleiben die Fragen:

Wieviel Aufwand ist für die Sicherheit der Energieversorgung notwendig?

Wie geht jeder einzelne Energieversorger unabhängig von gesetzlichen Verpflichtungen mit dem Thema Informationssicherheit um?

Literatur

Bundesnetzagentur, Bundeskartellamt (2016): Monitoringbericht 2016, Bonn.

Statista (2016): Bevölkerung - Zahl der Einwohner in Deutschland von 2002 bis 2015 (in 1.000), Hamburg.

Statista (2017): Anzahl der Privathaushalte in Deutschland von 1991 bis 2016 (in 1.000), Hamburg.

Impressum

Herausgeber
xmera e.K.

Hainbuchenstr. 13
45881 Gelsenkirchen

Autorin
Liane Hampe

T 0209 590 888 63
F 0209 947 085 07
E liane.hampe@xmera.de
W https://xmera.de

Stand
November 2017

Bildnachweis
Abbildungen: Eigene Darstellungen der xmera.

Titelbild: https://stockata.de

x m e r a : werte schützen