Ständerat

Conseil des Etats

Consiglio degli Stati

Cussegl dals stadis

17.3496 n Mo. Nationalrat (Graf-Litscher). Verpflichtender Grundschutz für kritische Strominfrastrukturen

Bericht der Kommission für Umwelt, Raumplanung und Energie vom 10. Oktober 2019

Die Kommission hat an ihrer Sitzung vom 10. Oktober 2019 die Motion Graf-Litscher 17.3496 beraten. Die Motion wurde am 15. Juni 2017 eingereicht und vom Nationalrat am 4. Juni 2019 angenommen.

Die Motion verlangt vom Bundesrat, die gesetzlichen Grundlagen zu schaffen, damit die Betreiber kritischer Strominfrastrukturen zu einem risikobasierten Grundschutz gegenüber Cyberangriffen und anderen relevanten Risiken verpflichtet werden können.

Antrag der Kommission

Die Kommission beantragt einstimmig, die Motion abzulehnen.

Berichterstattung: Schmid Martin

Im Namen der Kommission
Der Präsident:

Roland Eberle

Inhalt des Berichtes

1 Text und Begründung

1.1 Text

Der Bundesrat wird eingeladen, die gesetzlichen Grundlagen dergestalt zu präzisieren, dass für die Betreiber kritischer Strominfrastrukturen ein verpflichtender, branchenspezifischer Grundschutz gegenüber Cyberangriffen und anderen relevanten Risiken wie Naturgefahren besteht. Dieser Grundschutz soll risikobasiert ausgestaltet sein und die Bedeutung der jeweiligen Betreiber für eine sichere Stromversorgung berücksichtigen.

1.2 Begründung

Eine funktionierende Stromversorgung ist für das Wohlergehen der Bevölkerung und die Volkswirtschaft in der Schweiz von essenzieller Bedeutung. Ein schwerwiegender Stromausfall, beispielsweise verursacht durch einen Cyberangriff oder eine Naturkatastrophe, würde die Bevölkerung massiv beeinträchtigen und zu milliardenschweren Schäden in der Wirtschaft führen. Unter anderem würde die Wasserversorgung ausfallen, der öffentliche Verkehr zusammenbrechen, oder die Grossverteiler in der Lebensmittelversorgung würden lahmgelegt.
Die aktuellen Rechtsgrundlagen sowie die nationale Strategie zum Schutz kritischer Infrastrukturen und die nationale Cyberstrategie (NCS) enthalten keine sektorübergreifenden Vorgaben zum Sicherheitsniveau, welches die Betreiber kritischer Infrastrukturen erreichen sollen. Für die Betreiber massgebend sind die sektoriellen Fachgesetze (z. B. Energiegesetz und Stromversorgungsgesetz für die Betreiber der Stromnetze). Im Bereich der Stromversorgung ist allerdings nicht ausreichend präzisiert, welchen branchenspezifischen Grundschutz die Betreiber aufweisen müssen. Dieser Grundschutz soll risikobasiert ausgestaltet sein und die Bedeutung der jeweiligen Betreiber für eine sichere Stromversorgung in der Schweiz berücksichtigen. Zentrale Betreiber sollen einen höheren Grundschutz aufweisen, weil ein Ausfall gravierendere Konsequenzen hätte. Für kleinere Netzbetreiber kann dagegen ein tieferes Schutzniveau angemessen sein.

2 Stellungnahme des Bundesrates vom 30. August 2017

Der Bundesrat hat bereits 2012 nationale Strategien zum Schutz kritischer Infrastrukturen (SKI) und zum Schutz der Schweiz vor Cyberrisiken (NCS) verabschiedet. Als Grundsatz ist dabei zu beachten, dass die Umsetzung der Strategien massgeblich im Rahmen der etablierten Prozesse und innerhalb der bestehenden Strukturen und Zuständigkeiten erfolgt. Im Rahmen der nationalen SKI-Strategie wurde der Leitfaden SKI (2015) erarbeitet, der die Betreiber kritischer Infrastrukturen unterstützen soll, die Resilienz zu steigern und ein angemessenes Schutzniveau zu gewährleisten. Die Zweckmässigkeit dieses Leitfadens wurde in einem Pilotprojekt mit der nationalen Netzgesellschaft Swissgrid aufgezeigt. Als Massnahme aus der NCS wurde beim Verband Schweizerischer Elektrizitätsunternehmen (VSE) eine Arbeitsgruppe gebildet, die aktuell Minimalstandards für die Sicherheit der Informations- und Kommunikationstechnologien für die Schweizer Strombranche erarbeitet. Diese Arbeiten ergänzen eine Branchenempfehlung "ICT Continuity" (2011) des VSE und orientieren sich an international etablierten Standards für die Sicherheit von Informations- und Kommunikationstechnik (IKT).
Im revidierten Energiegesetz, das voraussichtlich Anfang 2018 in Kraft treten wird (BBl 2016 7683), wird in den Leitlinien für die

sichere Energieversorgung neu der Schutz kritischer Infrastrukturen einschliesslich der zugehörigen IKT explizit erwähnt (Art. 7 Abs. 1).
Im Zusammenhang mit dem revidierten Energiegesetz werden zudem Bereiche der Datensicherheit erstmalig geregelt. Von den Betreibern der Elektrizitätsnetze wird die Erfüllung von Sicherheitsanforderungen für die Datenübermittlung und -bearbeitung gefordert. Diese zielen auf einen gewissen Grundschutz der Netzbetreiber gegenüber Cyberrisiken wie auch auf den sicheren Betrieb von intelligenten Mess-, Steuer- und Regelsystemen ab.
Der Bund erlässt weiter explizite Sicherheits- und Schutzvorgaben primär in Bezug auf Strominfrastrukturen, die direkt seiner Aufsicht unterstehen, beispielsweise für Talsperren und Kernanlagen. In Bezug auf die Netzinfrastruktur sind hingegen vor allem die Netzbetreiber in der Pflicht, welche nach Artikel 8 Absatz 1 des Stromversorgungsgesetzes vom 23. März 2007 (StromVG; SR 734.7) nicht nur für ein effizientes und leistungsfähiges, sondern insbesondere auch für ein in jeder Hinsicht sicheres Netz zu sorgen haben. Es ist denn nach dem StromVG auch an ihnen, die entsprechenden technischen und betrieblichen Mindestanforderungen für den Netzbetrieb zu erarbeiten. Die Aufwände für ein angemessen hohes Sicherheitsniveau zählen somit zu den anrechenbaren Netzkosten gemäss Artikel 15 Absatz 1 StromVG.
Der Bundesrat unterstützt grundsätzlich die Stossrichtung der Motion, dass kritische Strominfrastrukturen ein geeignetes Schutzniveau aufweisen sollen. Er will vorerst jedoch die weitere Entwicklung der laufenden Arbeiten (insbesondere in Zusammenhang mit den nationalen Strategien SKI und NCS) abwarten.

Der Bundesrat beantragt die Ablehnung der Motion.

3 Verhandlungen und Beschluss des Erstrates

Der Nationalrat hat die Motion am 4. Juni 2019 mit 114 zu 77 Stimmen angenommen.

4 Erwägungen der Kommission

In der Begründung zur Motion weist die Motionärin auf die essenzielle Bedeutung einer sicheren Stromversorgung hin. Konkret fehlten der nationalen Cyberstrategie NCS sektorübergreifende Vorgaben zum Sicherheitsniveau, und die sektoriellen Fachgesetze, das heisst das Energiegesetz und das Stromversorgungsgesetz, seien nicht ausreichend präzisiert. Die Kommission ist jedoch der Auffassung, dass das Anliegen der Motionärin mittlerweile bereits umgesetzt werde. Seit Einreichung der Motion habe im Bereich der kritischen Strominfrastrukturen und deren Schutz eine grosse Entwicklung stattgefunden. Die Kommission hält fest, dass der Bundesrat die Signale aus dem Parlament ernst genommen und eigenverantwortlich gehandelt hätte. So habe er konkret die "Nationale Strategie zum Schutz kritischer Infrastrukturen 2018-2022" herausgegeben und einen Umsetzungsplan vorgelegt. Gerade im Strombereich sei damit anerkannt worden, dass der Grundschutz einer sehr kritischen Infrastruktur von grosser Bedeutung sei. Die laufende Umsetzung der Strategie Schutz kritischer Infrastrukturen (SKI) und der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) beinhalte eine Vielzahl von Massnahmen, welche dem Anliegen der vorliegenden Motion Rechnung tragen würden. Im Bereich des Schutzes kritischer Infrastrukturen sei eine der Massnahmen die Durchführung bzw. Aktualisierung von Risiko- und Verwundbarkeitsanalysen, welche sodann neu durch die Nicht-IKT-Risiken ergänzt würden. Auch Naturgefahren, gesellschaftliche Gefahren – Sabotage, Terror, Pandemie – und sonstige technische Risiken würden beurteilt. Die Kommission sieht es im Weiteren als sinnvoll an, dass der Teilsektor Stromversorgung 2020 in Angriff genommen werde, da aktuell zuerst der Teilsektor Erdgas im

Vordergrund stehe. Damit -werde das Vorgehen im Sinne einer Pilotanwendung beim Erdgas getestet und zusammen mit der Branche werden Erfahrungen gesammelt, womit das Verfahren beim Strom letztlich bereits eine gewisse Reife aufweise. Sodann hält die Kommission fest, dass ein neues Kompetenzzentrum für Cybersicherheit gegründet worden sei und der Bundesrat hierbei auch auf die Motion Bezug genommen habe. Weitere Massnahmen in der NCS, welche ebenfalls dem Anliegen der Motionärin Rechnung tragen, seien die Prüfung der Meldepflicht für Cybervorfälle, der Aufbau der Expertise bei den Fachämtern und Regulatoren und gemeinsame Übungen zum Krisenmanagement.

Die Kommission ist zusammengefasst überzeugt, dass die laufenden, in Angriff genommenen Massnahmen im Bereich der kritischen Strominfrastrukturen auf dem richtigen Weg seien, die Thematik aber begleitet und beobachtet werden müsse und die getroffenen Massnahmen nötigenfalls anzupassen seien. Ohnehin solle weniger ein spezialgesetzlicher Rahmen angestrebt werden, der die Problematik vermeintlich löse, sondern vielmehr sei das Thema des Schutzes der kritischen Strominfrastrukturen übergeordnet in Kooperation von Bund, Branchen und allen beteiligten Stellen anzugehen.