Berlin, 5. Juli 2023

bdew
Energie. Wasser. Leben.

BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme zur Nationalen Sicherheitsstrategie der Bundesregierung

Transparenz-Register-ID
Registereintrag national: R000888
Registereintrag europäisch: 20457441380-38

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, und seine Landesorganisationen vertreten über 1.900 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Strom- und gut 60 Prozent des Nah- und Fernwärmeabsatzes, 90 Prozent des Erdgasabsatzes, über 90 Prozent der Energienetze sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Einleitung

Der BDEW - Bundesverband der Energie- und Wasserwirtschaft e.V. begrüßt den Leitgedanken der Nationalen Sicherheitsstrategie, innere und äußere Sicherheit im Rahmen einer Politik integrierter Sicherheit zu denken. Nur eine Politik integrierter Sicherheit ist dazu geeignet, nachhaltige Energiesicherheit zu gewähren. Dazu gehört der umfassende Schutz der Kritischen Infrastrukturen im für die Sicherheit Deutschlands und Europas besonders kritischen Sektor Energie gegenüber Cyberangriffen, Sabotage und hybriden Bedrohungen zu gewährleisten.

Gerade die Phase um den Beginn des russischen Angriffskriegs auf die Ukraine hat sich die Exponiertheit unserer Volkswirtschaft gegenüber Störungen der Energieversorgung eindrücklich offengelegt. Hier gilt es, in Zukunft einseitige Lieferbeziehungen und kritische Abhängigkeiten, v.a. bei physischen Lieferungen von Energieträgern, bei Hardware für erneuerbare Energien, bei IT-Komponenten sowie Betriebsmitteln in der Wasserwirtschaft (insbesondere Fällmitteln) abzubauen. Diese Aufgabe kann der Staat nicht allein lösen; er setzt aber entsprechende Rahmenbedingungen und bietet Schutz bei unvorhersehbaren Entwicklungen. Weiterhin wichtig ist in diesem Kontext die Verteidigung und Wiedererlangungen von technologischer Spitzenkompetenz, um auf diesem - für die Wirtschaft so essenziellen Gebiet - politisch und wirtschaftlich souverän agieren zu können.

Als vernetzter Industriestandort und klassisches Energieimportland wird Deutschland weiterhin auf internationale Kooperationen im Energiesektor angewiesen sein. Der Hauptfokus liegt dabei weiter auf einer Fortentwicklung und Stärkung des europäischen Binnenmarktes und der EU als Akteur von internationalem Gewicht und Rang in einer zunehmend multipolaren Welt. Aber auch der geplante Ausbau bilateraler Handelsabkommen mit verlässlichen Partnern bei der Rohstoffgewinnung, bei Energielieferungen oder strategischen Kooperationen können hier zusätzlich Resilienz schaffen.

Dem Schutz Kritischer Infrastrukturen im Sektor Energie gegenüber Sabotage und der Energiewirtschaft im Ganzen sowie gegenüber Cyberangriffen und Desinformationskampagnen im Besonderen kommt dabei eine Schlüsselrolle zu. Die deutsche Energiewirtschaft stand und steht aufgrund der gesellschaftspolitischen Relevanz der Energieversorgung und der Abhängigkeit beim Gas im Fokus hybrider Strategien. Es ist vor diesem Hintergrund nur folgerichtig, dass die sichere und nachhaltige Versorgung unserer Volkswirtschaft mit Energie und der Schutz entsprechender Kritischer Infrastrukturen in Zukunft als eine gesamtgesellschaftliche Anstrengung gelebt und im Rahmen einer Politik integrierter Sicherheit weiterentwickelt werden kann. Damit die Energiewirtschaft ihren Beitrag zu dieser gesamtgesellschaftlichen Anstrengung leisten kann, müssen zukünftige Anforderungen an die Sicherheit jedoch unbürokratisch und wirtschaftlich umsetzbar sein. Aus der Bedrohungsintensität ergibt sich auch eine besondere Verantwortung des Staates bei Investitionen und der Gefahrenabwehr.

Die deutsche Energiewirtschaft begrüßt ebenso das Ziel, das internationale, regelbasierte Handelssystem zu stärken, denn Deutschland wird auch in Zukunft als klassisches Energieimportland auf zuverlässige Energielieferungen aus dem Ausland angewiesen sein. Dazu gehört auch, die Resilienz in den Lieferketten zu erhöhen. Von Rohstoffen bis zu IT-Komponenten besteht gegenwärtig eine hohe Abhängigkeit von Drittländern, die Partner, Wettbewerber und systemische Rivalen gleicher-

maßen sind. Die deutsche Energiewirtschaft bemüht sich vor diesem Hintergrund, die Diversifizierung der Lieferketten voranzutreiben. Allerdings wird diese Diversifizierung Zeit in Anspruch nehmen. Bis dahin muss die Beschaffung im Sinne der Versorgungssicherheit in Märkten systemischer Rivalen möglich bleiben, sofern eine alternative Beschaffung nicht möglich ist. Zusätzlich gilt es, die Erreichung technologischer Souveränität - gerade bei den Erzeugungsarten erneuerbarer Energien sowie bei digitalen Technologien - durch konsequente Förderung von Forschung und Entwicklung sowie aktive Standortförderung, zu stärken.

Politik integrierter Sicherheit muss sich widerspiegeln im Fortschreiben der KRITIS-Regulierung

Eine Politik integrierter Sicherheit kann aber nur gelingen, wenn ihre Elemente so ineinandergreifen, dass Bestehendes beim Schutz Kritischer Infrastrukturen optimiert und neue Anforderungen auf dem Bestehenden aufgebaut werden können. Integrierte Sicherheit muss daher bedeuten, dass die neuen Sicherheitsbedarfe keinesfalls mit steigendem bürokratischem Aufwand umgesetzt werden sollen, sondern diese müssen stringent und Synergien nutzend in die bestehende Regulierungsarchitektur für den Schutz Kritischer Infrastrukturen integriert werden. Dies gilt im besonderen Maße für das KRITIS-Dachgesetz und das NIS-2-Umsetzungsgesetz: Die Harmonisierung der Regulierung zur Cybersicherheit und des physischen Schutzes sowie die Identifizierung geeigneter branchenspezifischer Anforderungen an die physische Sicherheit sind entscheidend für die effektive Umsetzbarkeit durch die KRITIS-Betreiber. Die Identifizierung geeigneter Schutzmaßnahmen kann nur in Zusammenarbeit mit den Betreibern bzw. Betreiberverbänden erfolgen.

Besondere Verantwortung des Staates bei Investitionen und der Gefahrenabwehr

Die geforderten Investitionen in den Schutz Kritischer Infrastrukturen müssen schließlich unter dem Vorbehalt der Wirtschaftlichkeit erfolgen, sofern diese durch die Wirtschaft erfolgen sollen. Sofern die Schutzbedarfe die Wirtschaftlichkeit der Bereitstellung kritischer Dienstleistungen übersteigen, muss der Staat die für die Umsetzung der Schutzbedarfe notwendigen Investitionen mittragen. Ferner kann die Abwehr staatlicher Akteure oder terroristischer Vereinigungen durch die Betreiber Kritischer Infrastrukturen nicht umgesetzt werden und stößt auch im Sinne geeigneter Abwehr- bzw. Abschreckungsmechanismen an bestehende rechtliche Grenzen. Hier hat der Staat eine besondere Verantwortung zur Unterstützung der Betreiber und für Investitionen, wie die Nationale Sicherheitsstrategie selbst feststellt. Übernimmt der Staat diese Verantwortung im gebotenen Umfang nicht, so wird dadurch die marktwirtschaftliche Ordnung, in der die Energiewirtschaft fest verwurzelt ist - und damit auch eine wesentliche Säule der integrierten Sicherheitspolitik selbst - gefährdet.

Technologische Souveränität benötigt Zeit – wirtschaftliche Partnerschaften müssen im Sinne der Versorgungssicherheit daher auch mit systemischen Rivalen möglich bleiben

Die Nationale Sicherheitsstrategie identifiziert die Resilienz in der Lieferkette als einen wesentlichen Aspekt integrierter Sicherheit. Dies gilt für Rohstoffe, wie Seltenen-Erden-Metallen und Betriebsmitteln in der Wasserwirtschaft (insbesondere Fällmittel) - gleichermaßen wie für verarbeitete Produkte. Insbesondere IT-Komponenten nehmen dabei für die Energiewirtschaft eine herausragende Bedeutung ein. Die Versorgungssicherheit hängt von der Aufrechterhaltung genau jener kritischen Funktionen ab, die den Einsatz besonders kritischer IT-Komponenten verlangen. Bei diesen IT-Komponenten besteht gegenwärtig noch eine erhebliche Abhängigkeit von der Volksrepublik China. Die Diversifizierung der Lieferbeziehungen, wie dies die Nationale Sicherheitsstrategie fordert, wird daher nur mittel- bis langfristig gelingen können.

Im Sinne der Versorgungssicherheit sollte daher bis zum Erreichen der hinreichenden Diversifizierung sichergestellt werden, dass der Betrieb von kritischen IT-Komponenten auch in Zukunft möglich bleiben kann, wenn eine anderweitige Beschaffung der benötigten IT-Komponenten aufgrund von Beschaffungsengpässen oder mangelnder Diversifizierung nicht sofort erfolgen kann.

Der BDEW knüpft diese Einschätzung an die Erwartung, dass sich die Beschaffungsbasis mittelfristig und aufgrund anstehender Regulierungsvorhaben wie der ersten EU-weiten Rechtsvorschrift zur Cyberresilienz von Produkten mit digitalen Elementen unabhängiger und diversifizierter aufstellen wird, um künstliche Marktverknappungen besser mitigieren zu können.

Ansprechpartner:

Mathias Böswetter
Fachgebietsleiter IT-Sicherheit, Kritische Infrastrukturen
+49 30 300199 1526
mathias.boeswetter@bdew.de