Oktober 2025

Hinweise zum Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (Kritis-DachG) sowie eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG)

Die Bundesregierung hat am 30. Juli den Gesetzesentwurf für das NIS2UmsuCG und am 10. September den Gesetzesentwurf für das Kritis-DachG verabschiedet. Mit beiden Gesetzesentwürfen bringt die Bundesregierung wichtige Gesetze im Bereich der Resilienz und Cybersicherheit auf den Weg. Die Beratungen zum Entwurf des NIS2UmsuCG im Deutschen Bundestag haben bereits begonnen, für das Kritis-DachG beginnen sie im Laufe des Novembers. In den Gesetzesentwürfen geht es u. a. um neue Vorkehrungen für Betreiber kritischer Infrastrukturen, welche die veränderte Sicherheitslage besser abbilden sollen.

Wir unterstützen ausdrücklich die entsprechenden Anpassungen in den Novellen. Aufgrund der langjährigen Erfahrungen der Fernleitungsnetzbetreiber (FNB) im Betrieb kritischer Anlagen möchten wir für die anstehenden Beratungen im Deutschen Bundestag noch auf zusätzliche Aspekte hinweisen, um die Sicherheit der Gastransportnetze und die Versorgungssicherheit nicht zu gefährden:

1. Anpassung von Transparenz- und Veröffentlichungspflichten in Zeiten veränderter Sicherheitslagen

Die Sicherheitslage in Deutschland und der Welt hat sich in den vergangenen Jahren grundlegend verändert. Netzbetreiber sehen sich einer Vielzahl von Bedrohungen gegenüber, die massive Auswirkungen auf die Systemstabilität des Gasnetzes und zukünftig des Wasserstoffnetzes haben können. Dazu zählen Cyberangriffe genauso wie die Gefahren durch physische Angriffe und Sabotageakte auf die kritische Infrastruktur. Gleichzeitig wurden die Transparenz- und Veröffentlichungspflichten der FNB durch europäische und nationale Regelungen immer weiter erhöht.

Zwei aktuelle Beispiele erfüllen die Netzbetreiber mit besonderer Sorge:

Gemäß den Vorgaben von § 78 Abs. 1 Nr. 1 iVm. § 79 Abs. 1 Nr. 1 Telekommunikationsgesetzes (TKG) sind die FNB dazu verpflichtet, Daten zu der von ihnen betriebenen Telekommunikationsstruktur der zentralen Informationsstelle des Bundes (ZIS) der Bundesnetzagentur (BNetzA) zu übermitteln. Diese Daten werden sodann im Infrastrukturatlas (ISA) veröffentlicht.

Da die über den ISA veröffentlichte Telekommunikationsinfrastruktur parallel zu den von den FNB betriebenen Gasversorgungsleitungen verläuft, ermöglicht diese Veröffentlichung ein genaues Lagebild des deutschen Erdgasversorgungssystems. Zwar hat der Gesetzgeber die Möglichkeit für die Netzbetreiber geschaffen, Ausnahmen bei der BNetzA zu beantragen. Diese wurden bis zuletzt, anders als bei den Übertragungsnetzbetreibern Strom, immer wieder verweigert und die Netzbetreiber damit gezwungen, ihre Leitungsverläufe im ISA zu veröffentlichen.

Die FNB schlagen daher vor, im Rahmen des Kritis-DachG eine Ausnahme von den Veröffentlichungspflichten der FNB mit Blick auf ihre Telekommunikationsinfrastruktur zu verankern.

Ein weiteres Beispiel betrifft die Schaffung einer neuen Transparenzplattform durch die BNetzA (vgl. § 111g EnWG) zum 26.12.2026. In der Folge können aufgrund der geplanten Schnittstellen zwischen Transparenzplattform und Marktstammdatenregister Bewegungsdaten aus der neuen Transparenzplattform problemlos mit Stammdaten aus dem Marktstammdatenregister kombiniert werden. Auf künstlicher Intelligenz basierende Algorithmen können im Internet verfügbare Informationen, d. h. sowohl in öffentlich zugänglichen Datenbanken und Plattformen als auch auf sonstigen Internetseiten verfügbare Informationen, problemlos erfassen, auswerten und zusammenführen und für die Planung und Durchführung von gezielten Sabotageakten auf kritische Anlagen genutzt werden. Die FNB empfehlen daher, auf die Veröffentlichung von Stammdaten und Geodaten zu kritischen Anlagen gänzlich zu verzichten.

Hinweisen möchten die FNB an dieser Stelle darauf, dass in einer Vielzahl von Gesetzen eine umfassende Beteiligung der Öffentlichkeit im Rahmen der Planungs- und Genehmigungsprozesse durch die Veröffentlichung von Dokumenten, Karten und Informationen vorgesehen ist: z. B. im Rahmen der Netzentwicklungsplanung (§§ 15a ff. EnWG), im Rahmen der Planfeststellungsverfahren (§§ 72 ff. VwVfG) oder im Rahmen des Incremental-Verfahrens (Art. 22 ff. VO (EU) 2017/459). Transparenz ist zweifelsohne ein wichtiges Element, um Akzeptanz für die Realisierung von Infrastrukturprojekten zu schaffen oder marktliche Entwicklungen zu fördern. Dennoch sollten alle Veröffentlichungs- und Transparenzpflichten im Sinne des Kritis-DachG vor dem Hintergrund der aktuellen Bedrohungslage neu bewertet und die betreffenden gesetzlichen Grundlagen ggf. entsprechend angepasst werden. Sofern Daten in öffentlich zugänglichen Portalen und Datenbanken abgerufen werden, sollte für den Betreiber des jeweiligen Portals bzw. der jeweiligen Datenbank vor dem jeweiligen Datenabruf ersichtlich sein, wer Daten zu kritischen Anlagen abrufen möchte. Dabei besteht zudem die Möglichkeit, den Zugang zu behördlich notwendigen Datenbanken auf Personen mit berechtigtem Interesse zu begrenzen und somit den Schutz von sensiblen Daten zu erhöhen.

2. Nachweise für betriebsgeführte Netzbetreiber

Bei einigen Netzbetreibern ist es geübte Praxis, dass dritte Netzbetreiber mit der technischen Betriebsführung beauftragt werden, die selbst Betreiber kritischer Anlagen sind und den entsprechenden Nachweispflichten unterliegen. Zur Reduzierung des Verwaltungsaufwandes sollten betriebsgeführte Netzbetreiber, die Maßnahmen nach § 13 Abs. 1 Kritis-DachG-E durch einen beauftragten technischen Betriebsführer erbringen lassen, der selbst Betreiber kritischer Anlagen ist, den Nachweis durch Vorlage des entsprechenden Nachweises des technischen Betriebsführers erbringen können.

3. Praxistaugliche Ausgestaltung von Anzeige- und Prüfverfahren für „Kritische Komponenten“ im NIS2-Entwurf

Im aktuellen Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) soll nach § 41 BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) der Einsatz kritischer IT-Komponenten insbesondere von nicht-vertrauenswürdigen Herstellern aus Drittstaaten untersagt werden können. FNB Gas erkennt die sicherheitspolitische Zielsetzung dieser Regelung ausdrücklich an. Allerdings sind in Verbindung mit der Liste kritischer Funktionen gemäß § 11 Abs. 1g S. 1 Nr. 2 EnWG und dem darin dargelegten Zeitplan Rechts- und Planungsunsicherheiten zu erwarten, mit Auswirkungen auf den Netzausbau und die Versorgungssicherheit. Vor diesem Hintergrund empfiehlt FNB Gas die folgenden Aspekte in den Beratungen zu berücksichtigen und Anpassungen vorzunehmen, die den sektorspezifischen Herausforderungen der Netzwirtschaft gerecht werden.

So sollen gem. § 9b BSIG bzw. § 41 BSIG (NIS2UmsuCG) Anzeigepflichten und Prüfverfahren lediglich Duldungswirkung für den Einsatz kritischer Komponenten entfalten. Sofern also neue Erkenntnisse über einen Hersteller vorliegen, kann auch nachträglich der Weiterbetrieb jederzeit durch das BMI untersagt werden. Insbesondere vor dem Hintergrund der für Netzausbau und Energiewende entscheidenden Planungs- und Investitionssicherheit ist die Duldungswirkung eine große Herausforderung für die FNB. Das Fehlen eines Bestandsschutzes bei kritischen IT-Komponenten könnte im schlimmsten Fall dazu führen, dass die FNB erhebliche finanzielle Rückstellungen bilden müssen. Um den Bestandsschutz zu sichern, braucht es eine Regelung, die rückwirkende Verbote nur bei zwingender Sicherheitsbegründung zulässt und Maßnahmen zur Risikominderung priorisiert.

Zudem erzeugt das in § 41 Abs. 1–3 BSIG vorgesehene Anzeigeverfahren einen unverhältnismäßigen Verwaltungsaufwand. Der Aufwand zeigt sich daran, dass kritische Komponenten jede einzelne informations- oder kommunikationstechnische Funktion umfassen, die unsere Mitgliedsunternehmen beim Netzbetrieb bzw. bei der Netzsteuerung einsetzen (d.h. jegliche Hardware, Server, Software, Clients, Übertragungstechnik, programmierte Steuerungen für Armaturen etc.). Bei mehreren hunderten Funktionen bzw. Komponenten bedeutet dies bei Meldungs- und Prüffrist von mehreren Wochen einen besonders großen Aufwand für die Betreiber von Gasnetzen. Daher sollte das Anzeigeverfahren vereinfacht werden. Anstelle von Einzelmeldungen schlagen wir die Einführung von Ausschlusslisten für nicht vertrauenswürdiger oder Positivlisten für vertrauenswürdiger Hersteller vor.

Grundsätzlich sollte es für die Anwendung der neuen Regelungen praktikable Übergangsfristen und eine klare Definition von „kritischen Komponenten“ (idealerweise durch Branchenverbände) geben. Zudem sollten sich die Maßnahmen zur Bewältigung aktueller Herausforderungen unbedingt am gesamteuropäischen Kontext und an den europäischen Regulierungen orientieren und harmonisiert werden. In der EU zugelassene Komponenten sollen auch in Deutschland einsetzbar sein.

4. Einbeziehung von Dienstleistern in den Adressatenkreis des Gesetzes (§ 28 Abs. 1 Nr. 4 BSIG)

In § 28 Abs. 1 Nr. 4 BSIG sind Dienstleister adressiert, die Dienstleistungen erbringen, die einer Einrichtungsart nach Anlage 1 zugeordnet sind. FNB Gas geht davon aus, dass dies auch Dienstleister erfasst, die ihre Leistungen den in Anlage 1 genannten Marktteilnehmern und nicht den Endkunden selbst gegenüber erbringen.

Dies ist begrüßenswert. Allerdings bestehen weiterhin Unklarheiten hinsichtlich des genauen Anwendungsbereichs und der konkreten Adressaten der Regelung. Insbesondere sollte die Formulierung in § 28 Abs. 5 präzisiert werden. Sie bezieht sich auf Energieversorgungsnetze, Energieanlagen sowie digitale Energiedienste im Sinne des Energiewirtschaftsgesetzes. Das Energiewirtschaftsgesetz definiert den Begriff „digitale Energiedienstleister“ allerdings nicht. Eine Definition findet sich dagegen in Anlage 1 der BSI-Verordnung-E. Danach ist ein digitaler Energiedienst „eine Anlage oder ein System, das den zentralen, standortübergreifenden Zugriff auf die Steuerung oder die unmittelbare Beeinflussung von Energieanlagen oder zentralen, standortübergreifenden Zugriff auf die Steuerung oder die unmittelbare Beeinflussung dezentralen Anlagen zum Verbrauch elektrischer Energie oder Gas ermöglicht“.

Durch die Verwendung der unterschiedlichen Begriffe und unklaren Verweise bleibt offen, welche Unternehmen oder Dienstleister durch die § 28 Abs. 1 Nr. 4 einerseits und § 28 Abs. 5 andererseits genau angesprochen werden sollen. Die Klarstellung ist essenziell, um für die betroffenen Unternehmen Klarheit über Handlungspflichten und -verantwortungen zu schaffen. Darüber hinaus müssen Rechts- und Planungssicherheit bzgl. zu erwartender Belastungen gewährleistet sein.

FNB Gas schlägt vor, den Gesetzestext in § 28 Abs. 1 Nr. 4 BSIG wie folgt zu ergänzen oder die Anwendung auf die Dienstleistungen, digitale Dienstleistungen und Funktionen zumindest in der Gesetzesbegründung klarzustellen:

„4. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen oder digitalen Dienstleistung anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind und die a) mindestens 250 Mitarbeiter beschäftigen oder b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen. Dies gilt insbesondere, wenn es sich bei der Dienstleistung um eine kritische Dienstleistung oder digitale Dienstleistung handelt.“