BREKO
Bundesverband
Breitbandkommunikation e.V.

17.11.2026

BREKO-Stellungnahme zum Entwurf eines Gesetzes zur Anpassung von Transparenz-, Veröffentlichungs- und Informationspflichten zum angemessenen Schutz kritischer Infrastrukturen

Einleitung

Mit dem vorgelegten Gesetzesentwurf zielt das Bundesministerium des Innern (BMI) darauf ab, bestehende Information-, Transparenz- und Veröffentlichungspflichten für Betreiber kritischer Infrastrukturen (KRITIS-Betreiber) zu überprüfen und soweit erforderlich zum Schutz von KRITIS anzupassen.

Der BREKO und seine über 550 Mitgliedsunternehmen setzen sich für einen zukunftssicheren Ausbau digitaler Infrastruktur ein. Die über 260 im Verband organisierten Telekommunikations-Netzbetreiber versorgen sowohl Ballungsräume als auch ländliche Gebiete mit zukunftssicheren Glasfaseranschlüssen, die nicht nur Endkundinnen und Endkunden im Privatkunden- und Geschäftskundenbereich versorgen, sondern auch Datenübertragungswege für kritische Infrastrukturen wie Energieanlagen, Rechenzentren oder auch sichere Behördenkommunikation bereitstellen.

Der BREKO stimmt der Annahme des BMI zu, dass Informationen zu kritischen Infrastrukturen Ausspähversuche, Sabotageakte oder Anschläge erleichtern oder ermöglichen. Die Absicht des Gesetzentwurfs, der veränderten geopolitischen Bedrohungslage Rechnung zu tragen und potenziellen Angreifern durch eine Zusammenschau zahlreicher Infrastrukturdaten eine Angriffsvorbereitung zu erleichtern, ist richtig und wichtig.

Der Anschlag auf die Berliner Strom- und Kommunikationsversorgung hat erst kürzlich erneut verdeutlicht, welchen Stellenwert der Schutz von Informationen über kritische Infrastruktur einnehmen muss.

Nicht zuzustimmen ist dem BMI allerdings darin, dass nur *veröffentlichte* Informationen dem Risiko von Ausspähversuchen und Angriffen unterliegen. Damit übersieht es die Gefahren, die sich bereits aus der bloßen *Speicherung* von Informationen zu kritischen Infrastrukturen ergeben, besonders wenn es sich um einen zentralen Speicherort für eine Vielzahl von Infrastrukturen handelt. In der Informationssicherheit ist anerkannt, dass der Schutz von Daten bereits bei der Speicherung ansetzen muss (Datenvermeidung), weil alle gespeicherten Daten dem Risiko einer Überwindung der Sicherungsmaßnahmen unterliegen. Besonders sichtbar wird das Risiko, wenn die detaillierten Geodaten aller deutschen Versorgungsnetze mit Ausnahme des Frischwassers an zentral gespeichert sind, wie es beim Infrastrukturatlas der Bundesnetzagentur der Fall ist.

Der vorgelegte Entwurf ist ein wichtiger erster Schritt, greift mit punktuellen Änderungen einzelner Vorschriften jedoch zu kurz. Erforderlich ist ein umfassender, sektorübergreifender Ansatz zum Schutz kritischer Infrastrukturen. Transparenz muss dort begrenzt werden, wo sie Sicherheitsrisiken schafft. Dafür ist ein einheitlicher Schutzvorbehalt für sämtliche gesetzlichen Informations-, Transparenz-, Datenbereitstellungs- und Veröffentlichungspflichten in Bezug auf kritische Infrastrukturen zu verankern. Dieser muss gewährleisten, dass sicherheitsrelevante Informationen nicht offengelegt oder bereitgestellt werden müssen, soweit sie allein oder in Verbindung mit anderen zugänglichen Informationen die Sicherheit kritischer Infrastrukturen gefährden können. Dabei sind insbesondere

sektorübergreifende Abhängigkeiten und die Risiken der Verknüpfung unterschiedlicher Datenbestände zu berücksichtigen.

Sicherheitsrisiken des Gigabit-Grundbuchs und notwendiger Änderungsbedarf im Telekommunikations-Änderungsgesetz

Ein solcher sektorübergreifender Schutzansatz muss auch die Telekommunikationsinfrastruktur erfassen. Der vorgelegte Gesetzentwurf sieht jedoch keine zum Energiewirtschaftsgesetz analoge Anpassung des Telekommunikationsgesetzes vor. Ganz im Gegensatz zum Ansatz des Transparenz-Änderungsgesetzes wird mit dem aktuell in der Diskussion befindlichen Entwurf des Telekommunikations-Änderungsgesetzes (TKG-ÄG) sogar eine gegenläufige Richtung eingeschlagen. Trotz wiederholt eingebrachter Bedenken soll mit dem TKG-ÄG das Gigabit-Grundbuch als zentralisierte Datenbank weiter institutionalisiert werden, ohne ein entsprechendes Sicherheitskonzept zu verankern. Auch der jüngste Cyberangriff auf die zentral geführte Grundbuchdatenbank der rumänischen Katasterbehörde hat gezeigt, welche erheblichen Risiken mit der Zentralisierung sensibler Infrastrukturdaten verbunden sind. Der Angriff führte zeitweise zum Ausfall zentraler Register und legte wesentliche Teile des Immobilienverkehrs lahm. Damit wird erneut deutlich, dass die Konzentration besonders schützenswerter Datenbestände zusätzliche Angriffsflächen schafft und hohe Anforderungen an deren Schutz stellt.

Vor diesem Hintergrund hält der BREKO unverändert an seiner Position fest, dass die Ziele des Gigabit-Grundbuchs auch **ohne eine zentrale Speicherung von Infrastrukturdaten** erreicht werden können. Statt einer zentralen Datenvorhaltung bei der Bundesnetzagentur sollte der mehrfach vorgeschlagene Ansatz eines **dezentralen Infrastrukturatlas (dISA)** verfolgt werden, bei dem die Daten bei den jeweiligen Infrastrukturinhabern verbleiben und lediglich über geeignete **Schnittstellen** für berechtigte Zwecke zugänglich gemacht werden. Ein solcher Ansatz würde den Transparenzinteressen Rechnung tragen, ohne die Risiken einer Kompromittierung zentral gehaltener Daten unnötig zu erhöhen. Das auch hier nicht auszuschließende Risiko einer Überwindung der Datensicherheitsmaßnahmen wird wirksam dadurch begrenzt, dass bei einem Vorfall nur ein Versorgungsnetz betroffen ist. Die Ausweitung des Schadensszenarios durch eine Zentralisierung, der kein nennenswerter Vorteil gegenübersteht, entfällt.

Da weder dieser Ansatz noch der Vorschlag der Verankerung eines verbindlichen Bezugs zu einem nach § 86 TKG-ÄG festzulegenden und mit dem BSI abgestimmten **Sicherheitskonzepts** bislang aufgegriffen worden sind, halten wir eine **entsprechende Änderung jener Aspekte im Zuge des Transparenz-Änderungsgesetzes für sinnvoll und erforderlich**. Dies wäre insbesondere mit Blick auf § 85 TKG-ÄG sinnvoll, welcher nicht nur öffentlichen Stellen einen umfassenden Zugang zu Infrastrukturinformationen ermöglicht, sondern auch deren **Auftragnehmern**. Insbesondere die Ermöglichung einer **Datenweitergabe an Dritte** ist kritisch zu bewerten, da unklar bleibt, ob jene Dritte einer Sicherheitsüberprüfung unterliegen würden. Öffentliche Stellen und Auftragnehmer sollten entsprechend nur dann Zugang zu Infrastrukturdaten erhalten, wenn sie deren Schutz durch ein geeignetes und mit dem BSI abgestimmtes Sicherheitskonzept nachweisen.

Auch die Informationspflichten zu Infrastruktur und Baustellen (§§ 79, 82) berücksichtigen die Belange Kritischer Infrastrukturen weiterhin nicht ausreichend. Insbesondere bleiben Infrastrukturen unberücksichtigt, deren Ausfall die Funktionsfähigkeit anderer Kritischer Infrastrukturen gefährden würde. Zudem halten wir die zentrale Vorhaltung detaillierter Infrastrukturdaten insbesondere in einer umfangreichen Attributierung weiterhin für sicherheitspolitisch problematisch. Der übermäßig geforderte Detailgrad ist zumeist für konkrete Ausbau- und Mitnutzungszwecke nicht erforderlich – es genügt regelmäßig die Bereitstellung von **Ansprechpartnern**. Außerdem ist darauf hinzuweisen, dass auch durch die Kombination detaillierter Lage-, Trassen- und Sachdaten Rückschlüsse auf Kreuzungs-,

Bündelungs- und Engstellen sowie benachbarte kritische Infrastruktur möglich sind. Solche Rückschlussmöglichkeiten auf konkrete und granulare Lagen kritischer Infrastruktur sollten unbedingt vermieden werden. Stattdessen sollte nach dem **Need-to-Know-Prinzip** gehandelt werden.

Weiterhin bleiben die definierten **Ausnahmetatbestände in § 79 insgesamt zu eng gefasst** und orientieren sich nicht an dem tatsächlichen Schutzbedürfnis der Kritischen Infrastruktur. Die gesetzliche Einstufung als Kritische Infrastruktur sollte für eine Ausnahme von Datenlieferungspflichten ausreichen. Zusätzliche Nachweise einer besonderen Schutzbedürftigkeit sind nicht sachgerecht.

Fazit

Insgesamt vermittelt sowohl der Entwurf des TKG-ÄG den Eindruck, dass die **sicherheitspolitischen Risiken einer zentralen Sammlung und Verarbeitung sensibler Infrastrukturdaten weiterhin unterschätzt** werden und zentrale Fragen wie auch der künftige Umgang mit der derzeit erforderlichen Lieferung der Daten für die Breitbandmessung ungeklärt bleiben. Die aus Sicht des BREKO erforderliche sicherheitspolitische Neubewertung des Gigabit-Grundbuchs ist ausgeblieben. Angesichts der aktuellen Bedrohungslage und konkreter Beispiele erfolgreicher Angriffe auf zentralisierte Register erscheint dies weder technisch noch sicherheitspolitisch überzeugend. **Der BREKO bekräftigt daher seine Forderung nach einem dezentralen Infrastrukturatlas sowie nach deutlich strengeren und verbindlichen Sicherheitsanforderungen für den Umgang mit kritischen Infrastrukturdaten und regt zu einer Aufnahme jener Aspekte im Transparenz-Anpassungsgesetz an.**

Die notwendigen Anpassungen im Telekommunikationsrecht müssen dabei Teil eines umfassenden, sektorübergreifenden Schutzansatzes sein, der sämtliche gesetzlichen Informations-, Transparenz-, Datenbereitstellungs- und Veröffentlichungspflichten einem einheitlichen KRITIS-Schutzvorbehalt unterstellt.

BREKO ist im Lobbyregister (R002215) für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung sowie im Europäischen Transparenzregister (028570718529-43) für die Interessenvertretung gegenüber den EU-Institutionen eingetragen.