VERBAND KOMMUNALER UNTERNEHMEN e.V.

bdew
Energie. Wasser. Leben.

Berlin, 10. September 2025

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

# Positionspapier

## Positionen des BDEW Bundesverband der Energie- und Wasserwirtschaft und VKU Verband kommunaler Unternehmen zum § 41 BSIG:

## Die Untersagung des Einsatzes kritischer Komponenten in der Energiebranche und die Risiken der aktuellen Ausgestaltung für Versorgungssicherheit, Energiewende, Digitalisierung und Wirtschaftlichkeit

Versionsnummer: 1.0

## Inhalt

**1 Die Sicherheit der kritischen Energieinfrastruktur praxiswirksam gestalten ..... 4**

1.1 Geopolitischer Kontext ..... 4

1.2 Schaffung von Prüfverfahren und Anzeigepflicht gemäß § 9b BSIG mit Fokus auf 5G-Technologie ..... 5

1.3 Duldungswirkung der BSIG-Regelung erzeugt Rechtsunsicherheit, steigende Energiekosten drohen ..... 6

1.4 § 11 Abs. 1g S. 1 Nr. 2 EnWG: Massive Ausweitung des Geltungsbereiches gegenüber TK-Sektor ..... 6

**2 Hauptbedenken der Energiebranche bzgl. §41 BSIG ..... 6**

**3 Zusammenfassung möglicher Auswirkungen auf die deutsche Energiewirtschaft ..... 7**

3.1 Rückwirkendes Verbot bereits eingesetzter Komponenten (§ 41 Abs. 4 BSIG) ..... 7

3.2 Anzeigeverfahren (§ 41 Abs. 1–3 BSIG) ..... 8

3.3 Hemmnis für Netzausbau und Digitalisierung ..... 8

3.4 Systemische Risiken durch Oligopole und Ersatzbeschaffung ..... 8

3.5 Praktische Umsetzbarkeit ..... 8

3.6 Weiter steigende Energiepreise ..... 8

**4 Handlungsempfehlungen an die Politik ..... 9**

4.1 Verfahren abschaffen oder mindestens vereinfachen ..... 9

4.2 Bestandsschutz sicherstellen ..... 9

4.3 Übergangs- und Klarstellungsregelungen schaffen ..... 9

**5 Fazit ..... 9**

## Management Summary: Abhängigkeiten verringern & Energiesicherheit wirksam stärken, Gesetzesanpassung im §41 BSIG mit praktikablen Lösungen gestalten

**Unser Ziel:** Abhängigkeiten bei kritischen IT-Komponenten verringern und dabei die Versorgungssicherheit nicht gefährden.

Anzeigepflicht und Prüfverfahren gem. § 9b BSIG bzw. § 41 BSIG (NIS2UmsuCG) schaffen jedoch Rechts- und Planungsunsicherheiten und beeinflussen Netzausbau und Versorgungssicherheit. Für die Bereitstellung kritischer Funktionen muss die Verfügbarkeit kritischer IT-Komponenten gewährleistet werden können.

### Das Kernproblem…

…liegt in einem für den Sektor Energie ungeeigneten Verfahren: Übernahme eines Verfahrens aus der Telekommunikationsbranche (5G), das nicht auf die Energiebranche übertragbar ist:

- Wenige Lieferanten mit Bezug auf eine spezifische Technologie (TK) gegenüber unterschiedlichsten technischen Komponenten mit tausenden Lieferanten (Energie)
- Vier Netzbetreiber betroffen (TK), aber Hunderte KRITIS-Betreiber (Energie)
- Komponenten bei einer Technologie (5G-Netzwerktechnik) zu ersetzen (TK) --> viele tausende Komponenten in sehr unterschiedlichen, technischen Zusammenhängen (Energie)

### Dies führt zu…

…einem **hohen Bürokratieaufwand**: Mehrere Prüfverfahren pro Projekt → Verzögerungen.

… **Kostensteigerung:** Anpassung von Beschaffungsprozessen, Rückstellungen, Rückbau von Komponenten → höhere Energiekosten für Bürger, Industrie und Gewerbe sowie Gefährdung der Wettbewerbsfähigkeit des Energie-Standortes Deutschland.

… **Gefahr für Versorgungssicherheit**: Hemmnisse für Netzausbau und Digitalisierung durch Verknappung und Verteuerung wesentlicher Komponenten.

### Daher ist jetzt notwendig…

… die Anzeigepflicht und das Prüfverfahren gem. **§9b BSIG / §41 BSIG zu streichen.**

… oder mindestens **auf die spezifischen Voraussetzungen der Energiewirtschaft anzupassen**: schnelle und klare Prüfprozesse mit der Branche entwickeln, Rechtssicherheit für Vergabe- und Wettbewerbsverfahren schaffen und Ausbau von Komponenten durch risikobasierten Einsatz von Mitigationsmaßnahmen ersetzen.

# 1 Die Sicherheit der kritischen Energieinfrastruktur praxiswirksam gestalten

Mit dem § 41 BSIG im Rahmen des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) soll der Einsatz kritischer IT-Komponenten insbesondere von nicht-vertrauenswürdigen Herstellern aus Drittstaaten untersagt werden können.

**Die Energiebranche erkennt die sicherheitspolitische Zielsetzung ausdrücklich an. Jedoch ist klarzustellen, dass erhebliche negative Auswirkungen der aktuellen Ausgestaltung auf Versorgungssicherheit, Innovationskraft und Wirtschaftlichkeit zu erwarten sind, die in Verbindung mit der aktuellen Festlegung der Liste kritischer Funktionen gemäß § 11 Abs. 1g S. 1 Nr. 2 EnWG und dem darin dargelegten Zeitplan entstehen. Zudem sollte sich die Maßnahmen zur Bewältigung aktueller Herausforderungen unbedingt am gesamteuropäischen Kontext und an den europäischen Regulierungen orientieren.**

Diese Position wird im weiteren Text hergeleitet und ausgeführt.

## 1.1 Geopolitischer Kontext

Die Versorgungssicherheit der Zukunft geht schon heute mit hohen Bedarfen bei Digitalisierung und IT einher: Energiewende und der dafür notwendige Netzausbau helfen so dabei, die Energieversorgung klimafreundlich und ohne geopolitische Abhängigkeiten von fossilen Energieträgern zu sichern. Wie in allen anderen Sektoren auch, die über hohe Digitalisierungsbedarfe verfügen, bestehen gleichwohl hohe Abhängigkeiten bei IT-Komponenten von Herstellern aus Drittstaaten. Dafür entscheidende Drittstaaten wie die Volksrepublik China sind dabei für Deutschland und die EU zugleich wichtiger Partner, Wettbewerber und zunehmend auch systemische Rivalen. Insbesondere die Volksrepublik China ist zu einem wichtigen Handelspartner für kostengünstige Energiewende- und IT-Komponenten geworden, ohne den der wirtschaftliche Hochlauf der Erneuerbaren kaum möglich gewesen wäre. Die geopolitische Zeitenwende führt nun aber auch zu einer Neubewertung der Abhängigkeiten bei kritischen Komponenten für IT und Energiewende insbesondere von der Volksrepublik China.

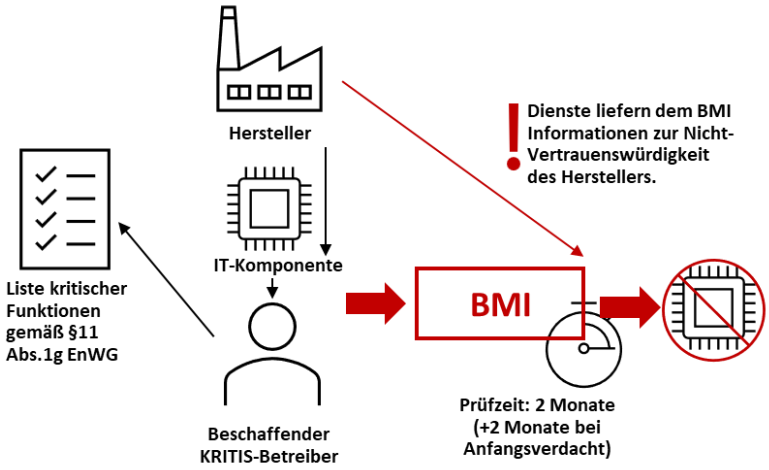
Der russische Angriffskrieg gegen die Ukraine hat deutlich gemacht, welche Folgen eine Abhängigkeit haben kann, wenn Partnerschaften einer Rivalität weichen. Um einer potenziellen Erpressbarkeit Deutschlands im Kontext seiner Versorgungssicherheit aufgrund der Abhängigkeit bei IT-Komponenten begegnen zu können, sollten die politischen und rechtlichen Rahmenbedingungen für eine Diversifizierung und Stärkung der industriellen Basis in Europa geschaffen werden.

Die Abhängigkeiten bei IT- und Energiewende-Komponenten sowie Rohstoffen sind mittelfristig aber aus Sicht des BDEW und des VKU durch Diversifizierung und dem Aufbau heimischer Industriekapazitäten nicht hinreichend zu verringern. Hier ist eine besonnene und ausgewogene Wahl geeigneter rechtlicher sowie politischer Instrumente zur Verringerung der Abhängigkeiten unter Berücksichtigung der handelspolitischen Realitäten zwingend erforderlich.

### 1.2 Schaffung von Prüfverfahren und Anzeigepflicht gemäß § 9b BSIG mit Fokus auf 5G-Technologie

Die Einführung des § 9b BSIG erfolgte ursprünglich vor dem Hintergrund der Diskussion um die technologische Souveränität und der befürchteten technologischen Abhängigkeit von wenigen Herstellern bei der Spitzentechnologie 5G.

Mit dem § 9b BSIG wurde deshalb die gesetzliche Grundlage dafür geschaffen, dass der Betrieb von 5G-Komponenten bestimmter Hersteller durch das Bundesministerium des Inneren (BMI) immer dann untersagt werden kann, wenn Erkenntnisse zu den betroffenen Herstellern vorliegen, die den sicheren Betrieb der 5G-Komponenten infrage stellen lassen könnten.




**1. Schritt:** KRITIS-Betreiber prüfen, ob die eingesetzten IT-Komponenten als „kritische Komponenten" im Sinne des BSIG (§ 2 Abs. 13 S. 1 Nr. 3 lit. b BSIG) gelten. Hierzu prüfen die KRITIS-Betreiber, ob die einzusetzende IT-Komponente in einer der durch die Bundesnetzagentur festgelegten kritischen Funktionen gemäß §11 Abs.1g EnWG zum Einsatz kommen soll. In diesem Fall kommt es zu einer Meldung der Komponente inkl. Herstellerangabe an das Bundesministerium des Innern (BMI).

**2. Schritt:** Prüfung der gemeldeten Komponente (Prüfzeit von 2 Monaten). Bei Vorliegen eines Anfangsverdachts kann die Prüfzeit noch einmal um zwei Monate verlängert werden. Bei Vorliegen von Informationen über die Nicht-Vertrauenswürdigkeit des Herstellers wird der Einsatz untersagt. Da jede Komponente komplexer Projekte einzeln geprüft werden muss, verzögern Projekte entsprechend

Im Rahmen des konkreten Prüfverfahrens übermitteln die betroffenen Betreiber Kritischer Infrastrukturen dem BMI Listen kritischer IT-Komponenten, die im Rahmen des Netz- oder Anlagenbetriebs zum Einsatz kommen sollen. Nach Einreichung hat das BMI zwei Monate Zeit, den Einsatz dieser IT-Komponenten zu prüfen. Sofern IT-Komponenten im Rahmen der Prüfung beanstandet werden und ein abschließendes Ergebnis über die Untersagung noch nicht vorliegt, wird der betroffene Betreiber darüber informiert und das Verfahren jeweils um zwei Monate bis zur abschließenden Klärung verlängert.

Wenn ein abschließendes Ergebnis über die Untersagung innerhalb von zwei Monaten vorliegt, wird der betroffene Betreiber über die Untersagung des Einsatzes der kritischen IT-Komponenten informiert. Wenn innerhalb von zwei Monaten aber keine Informationen über einen bestimmten Hersteller vorliegen, die eine Untersagung des Einsatzes der kritischen IT-Komponenten rechtfertigen würden, erfolgt keine Meldung an den betroffenen Betreiber.

### 1.3 Duldungswirkung der BSIG-Regelung erzeugt Rechtsunsicherheit, steigende Energiekosten drohen

Der § 9b BSIG bzw. der neue § 41 BSIG entfaltet lediglich Duldungswirkung. 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 Energiewirtschaft. Das Fehlen eines Bestandsschutzes bei kritischen IT-Komponenten könnte im schlimmsten Fall dazu führen, dass die Unternehmen der Energiewirtschaft erhebliche finanzielle Rückstellungen bilden müssen.

### 1.4 § 11 Abs. 1g S. 1 Nr. 2 EnWG: Massive Ausweitung des Geltungsbereiches gegenüber TK-Sektor

Im Gegensatz zur Bestimmung im Sektor Telekommunikation nach § 109 Abs. 6 Satz 1 Nr. 2 TKG, dessen Geltungsbereich bisher auf die 5G-Netze von vier Telekommunikationsnetzbetreibern beschränkt blieb, weitet der § 11 Abs. 1g EnWG diesen Geltungsbereich für den Sektor Energie erheblich aus. Nun sind anstatt vier Telekommunikationsnetzbetreiber alle Betreiber von Netzen nach IT-Sicherheitskatalogs gemäß § 11 Abs. 1a EnWG, die zugleich unter die Versorgungsgrade der BSI-KritisV fallen, sowie alle Betreiber von kritischen Erzeugungsanlagen gemäß § 11 Abs. 1b EnWG verpflichtet, dem BMI den Einsatz kritischer IT-Komponenten zu melden.

Vor diesem Hintergrund konfrontiert der § 11 Abs.1g EnWG das bestehende Prüfverfahren somit mit einer Aufgabe, für die es nicht konzipiert wurde, weil das BMI in Zukunft die Meldungen zu kritischen IT-Komponenten hunderter KRITIS-Betreiber des Sektors Energie bearbeiten müsste. Gerade aber die Bewertung der Vertrauenswürdigkeit eines Herstellers wird sich als eine ressourcenintensive Herausforderung darstellen, weil der großen und heterogenen Akteurslandschaft der KRITIS-Betreiber im Sektor Energie und insbesondere im Bereich der Erzeugung eine ebenso heterogene wie kleinteilige Lieferantenlandschaft gegenübersteht.

Durch die umfängliche, pauschale Betrachtung über alle Spannungsebenen bei allen Netzbetreibern oder auch über alle Erzeugungsanlagen, ohne differenzierende Kritikalitätsbetrachtung für Energieversorgung/Systemrelevanz in Summe, fehlt hier eine Fokussierung auf die relevanten Risiken und/oder auch auf die gegebenenfalls zentral kritischen Komponenten.

## 2 Hauptbedenken der Energiebranche bzgl. §41 BSIG

BDEW und VKU weisen mit Nachdruck darauf hin, dass ein rückwirkendes Verbot bereits eingesetzter kritischer Komponenten die nachfolgenden aufgeführten, erheblichen Risiken und wirtschaftliche Belastungen für Betreiber kritischer Infrastrukturen mit sich bringt. Die beabsichtigten Sicherheitsgewinne im

Umgang mit kritischen Komponenten müssen daher sorgfältig gegen die potenziell entstehenden Folgekosten und systemischen Auswirkungen, insbesondere auch auf die Versorgungssicherheit, abgewogen und ins Verhältnis gesetzt werden.

- *Marktabhängigkeiten und Wettbewerbsverzerrungen:*

Im Bereich besonders spezialisierter kritischer Komponenten besteht in vielen Fällen ein faktisches Oligopol mit sehr begrenzter Anbieteranzahl. Ein pauschales oder rückwirkendes Verbot kann zu massiven Beschaffungsengpässen, Lieferverzögerungen und erheblichen Preissteigerungen führen – mit unmittelbaren Auswirkungen auf Versorgungssicherheit, Ausbauprojekte und letztlich die Strom- und Energiepreise für Endkunden. Oligopole weniger Anbieter sind zudem aus einer systemischen Sicherheitsperspektive selbst als Klumpenrisiko für die Verfügbarkeit von kritischen Komponenten zu bewerten.

- *Finanzielle und betriebswirtschaftliche Risiken:*

Ein rückwirkendes Verbot von Komponenten, die zum Zeitpunkt der Beschaffung rechtskonform eingesetzt wurden, führt zu einer erheblichen Rechts- und Investitionsunsicherheit. Betreiber müssten gegebenenfalls Rückstellungen für mögliche Untersagungen bilden, mit der Folge erheblicher bilanzieller Belastungen und Projektverzögerungen. Zusätzlich entstehen hohe Folgekosten für Ausbau, Ersatz und Neuplanung bestehender Anlagen.

- *IT-/OT-Sicherheitsarchitektur und Integrationsaufwand:*

Die betroffenen Komponenten sind regelmäßig tief in bestehende IT- und OT-Strukturen integriert. Ein Austausch erfordert nicht nur den physischen Ersatz der Hardware, sondern auch die vollständige sicherheitstechnische Neuintegration in bestehende Sicherheitsverfahren, einschließlich Systemintegration und Anlernverfahren (SzA), Risikoanalysen, Anomalieerkennungsverfahren und laufende Betriebsprozesse. Dies bindet personelle und finanzielle Ressourcen, die an anderer Stelle für operative Sicherheitsmaßnahmen fehlen würden und somit der Intention der Regelung entgegenstehen.

# 3 Zusammenfassung möglicher Auswirkungen auf die deutsche Energiewirtschaft

## 3.1 Rückwirkendes Verbot bereits eingesetzter Komponenten (§ 41 Abs. 4 BSIG)

Ein rückwirkender Rückbau von Komponenten birgt gravierende Risiken:

- Versorgungssicherheit: Physisch und organisatorisch tief integrierte Komponenten lassen sich nicht kurzfristig ersetzen.
- Marktabhängigkeit: In vielen Segmenten bestehen faktisch Oligopole. Alternativen sind zeitlich, technisch oder wirtschaftlich nicht verfügbar.
- Kostenrisiken: Enorme Investitionsunsicherheit und drohende Projektverzögerungen gefährden Netz- und Anlagenprojekte, insbesondere im Kontext der Energiewende.

### 3.2 Anzeigeverfahren (§ 41 Abs. 1–3 BSIG)

Das vorgesehene Anzeigeverfahren erzeugt einen unverhältnismäßigen Verwaltungsaufwand:

- Hoher Aufwand: Jährlich hunderttausende Verwaltungsakte allein im Energiesektor.
- Unklare Entscheidungsgrundlage: Entscheidungen des BMI erfolgen auf Basis politischer und formaler Kriterien, nicht auf Basis der sicherheitstechnischen Prüfung durch Betreiber.
- Geringer Sicherheitsgewinn: Kein erkennbarer Mehrwert gegenüber alternativen Instrumenten wie Ausschluss- oder Positivlisten.

### 3.3 Hemmnis für Netzausbau und Digitalisierung

- Verzögerung von Projekten zur Digitalisierung und zum Netzausbau um Monate.
- Beschaffungsprozesse müssen aufwendig angepasst werden.
- Erhöhung von Netzentgelten und Energiepreisen infolge ineffizienter Verfahren.

### 3.4 Systemische Risiken durch Oligopole und Ersatzbeschaffung

- Einseitige Marktverengung durch vorsorglichen Ausschluss potenziell „unsicherer“ Anbieter, was wiederum ein Sicherheitsrisiko in der Lieferkette darstellt.
- Innovationshemmnis durch Einschränkungen im Technologiewettbewerb.
- Rechtliche Unsicherheiten und Klagemöglichkeiten ausgeschlossener Hersteller bei unklaren Abgrenzungen zu weiteren Regulierungen wie z.B. der Sektorenverordnung oder europäischen Regulierungen

### 3.5 Praktische Umsetzbarkeit

- Das BMI wird Schwierigkeiten bekommen, realistisch tausende Komponentenmeldungen pro Jahr zeitnah zu prüfen was zu Verzögerungen führt.
- In Turnkey-Projekten ist eine Bewertung von Teilkomponenten oft gar nicht möglich.

### 3.6 Weiter steigende Energiepreise

- sofern Funktionen und Komponenten nicht einheitlich im europäischen Energieverbundsystem untersagt werden und Verbote nur in Deutschland gelten, werden die jeweiligen dadurch ausgelösten Transformationskosten dazu führen, dass die Netzbetreiberentgelte weiter stark steigen und sich vor allem die Energiepreise für Endkunden im europäischen Wettbewerb nicht mehr wettbewerbsfähig sein können.

# 4 Handlungsempfehlungen an die Politik

## 4.1 Verfahren abschaffen oder mindestens vereinfachen

- **Petitum:** Prüfung unter Einbeziehung der Branche vor Einführung, ob Verfahren den angestrebten Zielen dienlich ist.
- Ansonsten:
    - Ersetzen des Anzeigeverfahrens durch eine Blacklist nicht vertrauenswürdiger Hersteller.
    - Alternativ: Aufbau einer Whitelist vertrauenswürdiger Hersteller (mit freiwilliger Prüfung).
    - Verzicht auf Anzeige bei Upgrades/Updates bereits eingesetzter Komponenten.
    - Keine Anzeige für Hersteller aus Deutschland, EU und NATO.

## 4.2 Bestandsschutz sicherstellen

- Keine rückwirkende Anwendung ohne zwingende Sicherheitsbegründung.
- Risikobasierte Einzel-Prüfung statt pauschaler Rückbaupflicht.
- Mitigationsmaßnahmen vorrangig prüfen. Sind alternative Hersteller verfügbar?
- Entschädigungs- und Finanzierungsregelungen für Rückbauanordnungen schaffen.

## 4.3 Übergangs- und Klarstellungsregelungen schaffen

- Einführung praktikabler Übergangsfristen.
- Klare Definition, was als „kritische Komponente“ gilt, idealerweise durch Branchenverbände.
- Harmonisierung mit europäischen Standards: In der EU zugelassene Komponenten sollen grundsätzlich auch in Deutschland einsetzbar sein.

# 5 Fazit

Die Energiewirtschaft unterstützt die Zielrichtung des Gesetzes zur Stärkung der Cybersicherheit. Die aktuelle Ausgestaltung des § 41 BSIG konterkariert jedoch dieses Ziel durch übermäßige Bürokratie, Unsicherheiten und Risiken für Versorgung und Innovation. Es braucht pragmatische, rechtssichere und wirtschaftlich tragfähige Lösungen etwa durch Blacklists, Bestandsschutz und risikobasierte Prüfverfahren.

Damit die deutsche Energiewirtschaft, auch im Kontext des europäischen Wettbewerbes, hier keine behördliche Einzelentscheidung für den deutschen Markt festlegt, mit der Wirkung von weiter steigenden Strompreisen, muss hier ein einheitlich europäisches Verfahren umgesetzt werden. Insbesondere unter der Betrachtung der Abhängigkeiten im europäischen Verbundnetz.

- **BDEW und VKU fordern daher den Paragrafen in der aktuellen Ausgestaltung zu streichen oder die ausgewiesenen Anpassungen unter Einbeziehung der Branche zu überarbeiten.**

Nur so kann Cybersicherheit gestärkt werden, ohne die Energieversorgung und die Wettbewerbsfähigkeit der Energiewirtschaft in Europa zu gefährden. BDEW und VKU stehen als Spitzenverbände der deutschen Versorgerlandschaft sehr gerne für weitere inhaltliche Ausführungen und Austausche zur Thematik Schutz kritischer Infrastrukturen zur Verfügung.