Berlin, 23. Oktober 2024

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme zum § 41 BSIG (kritische IT-Komponenten) gemäß Regierungsentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz vom 22. Juli 2024

Transparenz-Register-ID des BDEW: 20457441380-38

Der Regierungsentwurf des NIS2UmsuCG vom 22. Juli 2024 weist im Vergleich zum Referentenentwurf vom 24. Juni 2024 wesentliche Verbesserungen mit Blick auf die Energiewirtschaft auf.

Allerdings muss aus Sicht des BDEW das **unverhältnismäßig bürokratische Prüfverfahren gemäß § 41 BSIG zwingend gestrichen** und durch eine **Ausschlussliste generell nicht-vertrauenswürdiger Hersteller** ersetzt werden. **Das Prüfverfahren bietet gegenüber einer Ausschlussliste keinen ersichtlichen Sicherheitsgewinn,** hat aber Auswirkungen auf die **Versorgungssicherheit,** die **Energiewende** und vor allem den **Netzausbau**. Diese benötigen wir aber nicht zuletzt vor dem **Hintergrund des russischen Angriffskriegs** unbedingt, um die **Resilienz im Energiesystem** sowie die **Energiesicherheit in Deutschland und Europa nachhaltig zu stärken**.

1. Auswirkungen der Regelung auf die Versorgungssicherheit, Energiewende und Netzausbau

Die **Untersagung des Einsatzes kritischer IT-Komponenten** hängt im vorgeschlagenen Prüfverfahren nicht maßgeblich von der Prüfung der Komponenten-Meldungen ab, die durch die KRITIS-Betreiber an das Bundesministerium des Innern und für Heimat (BMI) übermittelt werden, **sondern von Informationen über Hersteller, die den Diensten schon vorher vorliegen und im BMI die eigentliche Entscheidungsgrundlage für die Untersagung bilden**. Deswegen bietet es keinen Sicherheitsgewinn, sondern nur ein Mehr an Bürokratie.

Das Prüfverfahren gemäß § 41 BSIG wird für die KRITIS-Betreiber dagegen **erhebliche bürokratische Mehraufwände sowie zusätzliche Kosten** mit sich bringen aufgrund von:

- Einplanung des Prüfverfahrens in Energiewende- und Netzausbauprojekte (Verlängerung um mindestens zwei Monate)
- Umfassende Anpassung der Beschaffungs- und Einsatzprozesse
- Bildung von Rückstellungen aufgrund der bloßen Duldungswirkung des § 41 BSIG
- Langfristige Ausrichtung von Beschaffungs- und Einsatzprozessen

Folgen dieser Mehraufwände und Mehrkosten für Betreiber, Verwaltung und Bevölkerung sind dabei:

- **Auswirkungen auf die Versorgungsicherheit**, weil **kritische Komponenten für den sicheren Netz- und Anlagenbetrieb nicht rechtzeitig beschafft und ersetzt** werden können.
- Aus der Einplanung des Prüfverfahrens in **Energiewende- und Netzausbauprojekten** ergibt sich eine **Projektverlängerung um mindestens zwei Monate pro gemeldeter kritischer IT-Komponente**. Da in komplexen energiewirtschaftlichen IT-Projekten in der Regel nicht alle zu meldenden kritischen IT-Komponenten vom selben Hersteller stammen, ergeben sich ggf. unterschiedliche Prüfungslängen, die wiederum auf das Gesamtprojektlänge negativ zurückwirken können.
- Eine **Erhöhung von Netzentgelten** und **Energiekosten für die Verbraucherinnen und Verbraucher**.
- **Schwächung des energiewirtschaftlichen Standorts Deutschland**, da indirekt Marktkapazitäten an das europäische Ausland verloren gehen können.

- Gegenwärtig ist aus Sicht des BDEW völlig unklar, wie das **BMI zukünftig viele tausende Meldungen kritischen Komponenten im Jahr in gebotener Qualität und Zeit prüfen möchte.**

2. Bürokratiearme Lösungen: Abhängigkeiten bei IT verringern und Resilienz stärken

Um **Abhängigkeiten zu Drittländern bei kritischen IT-Komponenten** – insbesondere in **Zeiten geopolitischer Spannungen** mit großem Einfluss auf die Energie- und Digitalpolitik – **zu verringern** und die **Resilienz der Lieferketten sowie unserer kritischen Infrastrukturen zu stärken**, müssen **gesetzliche Grundlagen** geschaffen werden, **damit KRITIS-Betreiber im Sektor Energie rechts- und planungssicher Hersteller aus Drittländern bei der Beschaffung ausschließen können**. Dies muss auch konform sein zu gesetzlichen Regelungen zu Wettbewerb und Ausschreibungen in Deutschland und Europa.

Aufgrund der **gebotenen Eile und des hohen Digitalisierungsdrucks bei Energiewende sowie dem dafür notwendigen Netzausbaus** braucht es dafür **verlässliche, transparente und bürokratiearme Lösungen**, damit eine schnelle und rechtsichere Untersagung des Einsatzes von kritischen IT-Komponenten bestimmter Hersteller aus Drittländern durch das BMI erfolgen kann.

Die Vereinigten Staaten von Amerika oder das Vereinigte Königreich folgen deshalb auch dem Ansatz der Erstellung von Ausschlusslisten von Herstellern aus Drittstaaten (sogenanntes Blacklisting), deren IT-Komponenten nicht mehr zum Einsatz kommen dürfen. Alternativ könnte ein **Whitelisting, also einer Liste von geeigneten Herstellern, in Verbindung mit geeigneten Bestandsschutzregelungen** eine geeignete Lösung sein.

3. Geopolitisches Risiko darf nicht mit Produktsicherheit von IT-Komponenten verwechselt werden

Die Unterbrechung von globalen Lieferketten während der Pandemie hat auch die Abhängigkeit bei der Beschaffung von IT-Komponenten aus bestimmten Drittländern gezeigt. Alternativbeschaffungen waren damals schwer oder gar nicht möglich. Diese Abhängigkeit kann in Zukunft im Rahmen geopolitischer Spannungen ausgenutzt und die **Lieferketten selbst zum Druckmittel gegen die Versorgungssicherheit in Deutschland gewendet werden**: **Die Verfügbarkeit einer IT-Komponente** ist dabei ein **viel mächtigeres** und zugleich **niederschwelliges Druckmittel als eine Manipulation von IT-Komponenten ab Werk.** Eine **künstliche Marktverknappung als Supply-Chain-Angriff** lässt sich dagegen nur schwer attribuieren und rechtlich überhaupt nicht verfolgen. Die Entdeckung einer Manipulation von IT-Komponenten ab Werk hätte dagegen schon heute erhebliche wirtschaftliche Schäden und nachhaltige Reputationsschäden für einen Hersteller zur Folge. Wie das **Beispiel Kaspersky** zu Beginn des Ukraine-Krieges zeigt, kann die Sorge vor Manipulation von IT-Komponenten ab Werk ohnehin schon **heute im**

Rahmen der Produktsicherheit durch das Bundesamt für Sicherheit in der Informationssicherheit (BSI) adressiert und der **Einsatz von IT-Komponenten effektiv unterbunden werden**.

Die Verringerung des oben beschriebenen Risikos verlangt deshalb auch primär die **Betrachtung der Vertrauenswürdigkeit eines Herstellers** (d.h. insbesondere dessen Unabhängigkeit vom politischen, militärischen oder geheimdienstlichen Apparat eines Drittstaats) **und erst sekundär die Betrachtung der Produktsicherheit der Komponenten.**

4. Prüfverfahren gemäß § 41 BSIG i.V.m. der Liste kritischer Funktionen gemäß § 11 Abs. 1g S. 1 Nr. 2 EnWG ohne klaren Sicherheitsgewinn und mit methodischen Schwächen

Der ursprüngliche § 9b BSIG, der unverändert als § 41 BSIG im Rahmen der NIS-2-Umsetzung in den Regierungsentwurf des NIS2UmsuCG übernommen wurde, wird den Anforderungen eines bürokratiearmen und zügigen Verfahrens nicht gerecht**.** Zudem ist aus Sicht der Energiewirtschaft gegenwärtig nicht ersichtlich, wie das BMI in Zukunft **hunderte bis tausende Meldungen von kritischen IT-Komponenten pro KRITIS-Betreiber (> 1.000 KRITIS-Betreiber in Deutschland) im Jahr** im Rahmen des Prüfverfahrens gemäß § 41 BSIG bewältigen möchte.

Statt eines bürokratiearmen und zügigen Verfahrens folgt das Prüfverfahren gemäß § 41 BSIG einem **mehrstufigen und langwierigen Prozess (siehe Abbildung 1), der aus Sicht der Energiewirtschaft zur Bewältigung des oben beschrieben geopolitischen Risikos selbst nicht beitragen kann, sondern dem eigentlichen Ziel sogar entgegenwirkt.**

Dazu tragen insbesondere die bloße **Duldungswirkung des Prüfverfahrens gemäß § 41 BSIG** und die durch die Bundesnetzagentur (BNetzA) noch festzulegende **Liste kritischer Funktionen gemäß § 11 Abs. 1g S. 1 Nr. 2 EnWG** bei. Eine Festlegung dieser Liste kritischer Funktionen erfolgt trotz einer gesetzlichen Umsetzungsfrist bis zum 22. Mai 2023 bisher nicht, weil zwischen der BNetzA und dem BSI das notwendige Einvernehmen bisher nicht hergestellt werden konnte.

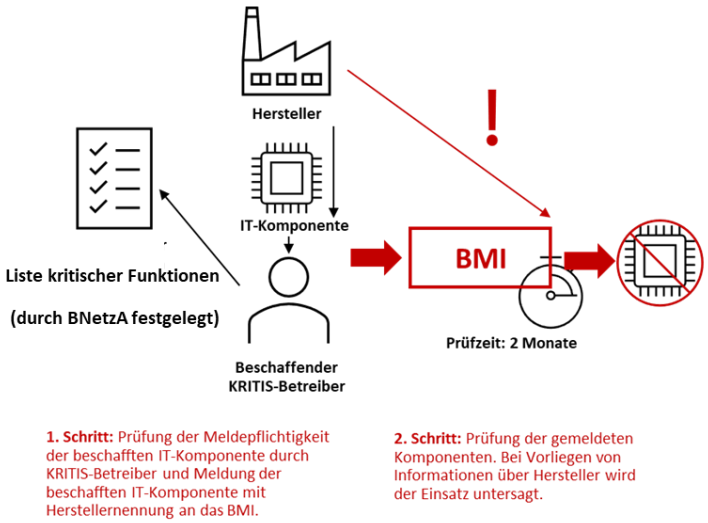

Abbildung 1 Das Prüfverfahren gemäß § 41 BSIG im Überblick

Die Duldungswirkung des Prüfverfahrens gemäß § 41 BSIG steht einem rechts- und planungssicheren Einsatz von kritischen IT-Komponenten durch die KRITIS-Betreiber auch nach dem zweimonatigen (bzw. viermonatigen nach Erstverdacht) Prüfintervalls entgegen. Ohne geeignete Übergangs- und Bestandsschutzregungen kann die Regelung des § 41 BSIG schließlich auch Auswirkungen auf die Versorgungssicherheit selbst haben, da für die Bereitstellung kritischer Funktionen im Anlagen- und Netzbetrieb notwendige IT-Komponenten im schlimmsten Fall ausgebaut werden müssten, ohne dass dafür aufgrund der Weltmarktlage zeitnah kein adäquater Ersatz beschafft werden und zum Einsatz kommen kann.

Darüber hinaus erfolgt durch die KRITIS-Betreiber die Bestimmung, was meldepflichtige IT-Komponenten sind, über die noch festzulegende Liste kritischer Funktionen gemäß § 11 Abs. 1g S. 1 Nr. 2 EnWG. **Die Ableitung durch die KRITIS-Betreiber, was kritische und damit meldepflichtige IT-Komponenten sind, birgt das Risiko abweichender Meldungen sowie Falschmeldungen durch die KRITIS-Betreiber.** Grund hierfür ist insbesondere, dass unter die kritischen Funktionen gemäß der Festlegung auch solche IT-Komponenten fallen, die als Standard-IT grundsätzlich als unkritisch zu betrachten sind und jederzeit anderweitig beschafft werden können. Schließlich ist gerade bei Turn-Key-Projekten eine Beurteilung der Kritikalität von Teilkomponenten durch die KRITIS-Betreiber schlechthin nicht möglich.