Umsetzung NIS2 in Deutschland

Stand: August 2025 | Positionspapier

Die Prozesse zur Untersagung des Einsatzes kritischer Komponenten dürfen keine unternehmerischen Risiken verursachen oder die Energiewende verzögern, d.h.

Das geplante bürokratische Anzeigeverfahren sollte angesichts der ohnedies jederzeit möglichen Untersagung durch eine reine Anzeigepflicht ersetzt werden. Das BMI sollte eine „Whitelist" und „Blacklist" seiner Prüfungsergebnisse transparent machen. Die Kosten einer Untersagung müssen bei den Netzbetreibern regulatorisch anerkannt werden. Neben den Betreibern kritischer Infrastrukturen sollen auch die Hersteller die Beantragung der Nutzung beim BMI einreichen dürfen.

Die Regelungen im Zusammenhang mit dem IT-Sicherheitskatalog müssen verhältnismäßig sein, d.h.

Die Vorgaben in den Sicherheitskatalogen sollten auf das Wesentliche bezüglich Systemsicherheit beschränkt werden. Regelmäßige Audits und Zertifizierungen sollten nur für kritische Anlagen selbst erfolgen und allenfalls stichprobenartige Prüfungen für Komponenten, Prozesse etc. in den Kategorien „wichtig" oder „besonders wichtig".

Eine Überregulierung durch viele Vorgaben von Behörden muss vermieden werden, d.h.

Eine Zertifizierung sollte ausschließlich Regelungen des IT-Sicherheitskataloges betreffen. Empfehlungen sollten klar als solche und damit als unverbindlich gekennzeichnet werden. Deutsche Alleingänge sollten vermieden, eine möglichst hohe Konsistenz mit den EU-Regelungen sollte erreicht werden. Eingriffe des BSI in operative Prozesse der Industrie sollten nur auf Wunsch der betroffenen Unternehmen möglich sein.

Umsetzung der EU-NIS-2 Richtlinie in Deutschland

Ende Juli hat das Kabinett den Regierungsentwurf „Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS2UmsuCG) verabschiedet und Mitte August dem Bundesrat zugestellt. Mit dem NIS2UmsuCG soll die europäische NIS-2-Richtlinie („The Network and Information Security (NIS) Directive“) umgesetzt werden. Die NIS-2-Richtlinie der EU ist am 16.01.2023 in Kraft getreten und sollte bis 17. 10.2024 in deutsches Recht überführt werden.

Vergleichbare zeitliche Vorgaben und inhaltliche Überschneidungen bestehen für den physischen Schutz kritischer Infrastrukturen über das sog. KRITIS DachG als nationale Umsetzung der Critical Entities Resilience (CER) EU-Richtlinie.

Wir begrüßen als Betreiber Kritischer Infrastrukturen die Maßnahmen zum Schutz der öffentlichen Ordnung und Sicherheit. Dennoch muss Überregulierung und unnötiger bürokratischer Aufwand vermieden werden, operative Notwendigkeiten der Industrie („Praxis-Check“) müssen berücksichtigt werden. Schließlich besteht ein erhebliches Eigeninteresse der Unternehmen an einem ausreichenden Schutz. Staatliche Vorgaben dürfen insbesondere nicht zu Verzögerungen und dadurch sogar zur Schwächung des Schutzes der Unternehmen führen.

E.ON sieht die Gesetzesinitiative als Chance, den im Koalitionsvertrag der Bundesregierung verankerten Bürokratieabbau (z.B. über den „One-Stop-Shop“) anzugehen.

Kernforderungen

In Bezug auf den Regierungsentwurf des NIS2UmsuCG vom 28.07.25 besteht folgender Verbesserungsbedarf:

Die Prozesse zur Untersagung des Einsatzes kritischer Komponenten dürfen keine unternehmerischen Risiken verursachen und die Energiewende verzögern.

In § 41 NIS2UmsuCG wird der Prozessablauf des Antragsverfahrens eines Betreibers Kritischer Infrastrukturen für den geplanten erstmaligen Einsatz einer kritischen Komponente festgelegt. Der geplante Einsatz kann innerhalb von 2 Monaten (bzw. mit einer 2-monatigen Verlängerung) vom BMI untersagt werden. Gründe für eine Untersagung können die (politische) Bewertung eines Herstellers oder der geplante Einsatz der Komponente eines bestimmten Herstellers sein. Auch der künftige Einbau kritischer Komponenten kann untersagt, bzw. sogar der Rückbau aller bereits installierten kritischen Komponenten eines bestimmten Herstellers kann angeordnet werden.

Mit dieser Regelung wird das BMI ermächtigt, den Einsatz kritischer Komponenten zu untersagen, um die voraussichtliche Beeinträchtigung der öffentlichen Ordnung oder Sicherheit abzuwenden. Die Prüfung erfolgt dabei anhand formaler und politischer Kriterien, ein wesentlicher Beitrag zum Prüfungsergebnis durch die Betreiber Kritischer Infrastruktur selbst ist nicht erkennbar. Vielmehr soll die Prüfung durch das BMI erst erfolgen, wenn der künftige Einsatz der kritischen Komponente bereits geplant ist und somit schon Teil eines bereits laufenden Beschaffungsprozesses ist. Aber auch ohne Untersagung als Ergebnis des Anzeigeverfahrens besteht weiterhin das Risiko von Fehlinvestitionen beim Betreiber Kritischer Infrastrukturen, da durch das BMI jederzeit zu einem späteren Zeitpunkt der Betrieb gemäß § 41 Absatz 4 NIS2UmsuCG untersagt werden kann.

Änderungsbedarf aus Sicht E.ON

E.ON als Betreiber Kritischer Infrastrukturen begrüßt die Maßnahmen zum Schutz der öffentlichen Ordnung und Sicherheit. Dennoch erschließt sich nicht, warum ein separater Anzeigeprozess erforderlich ist und warum nur die Betreiber Kritischer Infrastruktur Teil des Prozesses sein sollen.

Folgende fünf Änderungen sind notwendig:

(1) Das Anzeigeverfahren gemäß Absätzen (1) und (2) sollte durch eine Anzeigepflicht ohne Fristsetzung ersetzt werden.

Für den Betreiber kritischer Anlagen ist kein Mehrwert durch den Prüfungsprozess erkennbar, insbesondere da das Ergebnis nur einer Duldung gleichkommt. Da gemäß Absatz 4 ohnedies

jederzeit ein Verbot des Betriebes kritischer Komponenten ausgesprochen werden kann, hemmt die vorgesehene Prüfungsfrist die Beschaffungsprozesse und führt bei agilen Anpassungen der Produktspezifikationen zu entsprechenden Verzögerungen. Besonders im Bereich von Software-Updates zur Fehlerbehebung sind solche Fristen zu vermeiden.
(2) Die Anzeige sollte auch direkt durch den Hersteller von Komponenten für den Einsatz in Kritischer Infrastruktur beim BMI erfolgen können.
Angesichts der Bedeutung für die Beschaffungsprozesse der Unternehmen sollte das BMI über die Kommunikation mit dem jeweiligen Antragsteller hinausgehend für die erforderliche Transparenz – mindestens gegenüber den Betreibern Kritischer Infrastrukturen – sorgen:
(3) Das BMI sollte Informationen zu Hersteller und Anwendungsbereich bei bereits erfolgten Untersagungen über eine „Blacklist" zugänglich machen und regelmäßig aktualisieren.
(4) Bei bereits geprüften Anträgen (ohne Untersagung) sollte das BMI die entsprechenden Informationen über eine „Whitelist" zugänglich machen und regelmäßig aktualisieren.
E.ON als Betreiber Kritischer Infrastrukturen unterliegt dem Risiko, dass aus Gründen, die von E.ON nicht beeinflussbar und schwer bewertbar sind, enorme Kosten durch Alternativbeschaffungen bei Untersagung oder auch bei der Verpflichtung zum Rückbau entstehen. Im Ergebnis wird dies zu einer vorsorglichen Einschränkung des Anbieterkreises und Innovationshemmnissen führen.
(5) Bei einer Untersagung einer kritischen Komponente müssen die dadurch entstehenden Kosten regulatorisch anerkannt werden, da die Untersagung im Zusammenhang mit dem Schutz der öffentlichen Ordnung und Sicherheit steht.

Die Regelungen im Zusammenhang mit dem IT-Sicherheitskatalog müssen verhältnismäßig sein.

Art. 17 NIS2UmsuCG sieht Änderungen im EnWG durch Ergänzung der neuen §§ 5c bis 5e vor. Kernelement der Regelungen ist ein Katalog von Sicherheitsanforderungen, der einen angemessenen Schutz für Energieversorgungsnetze, Energieanlagen und Energiedienste sicherstellen soll.

Dieser IT-Sicherheitskatalog ist im Einvernehmen zwischen BNetzA und BSI sowie unter Beteiligung der Industrie zu erstellen. Dennoch besteht ohne einschränkende Vorgaben im Gesetz das Risiko, dass, wie schon bei der bisherigen IT-SIG-Historie, über die Vorgaben der NIS-1-Richtlinie hinausgegangen wird.

So sieht z.B. der deutsche Gesetzesentwurf eine "Dreistufigkeit" vor ("Betreiber kritischer Anlagen", "besonders wichtige Einrichtung", "wichtige Einrichtung"). Damit besteht die Gefahr, dass die besonderen Anforderungen für "kritische Anlagen" auch für Systeme, Komponenten und Prozesse greifen, die lediglich unter die Kategorie "wichtige Einrichtungen" fallen, weil diese mit dem Betrieb der kritischen Anlage unmittelbar nichts zu tun haben.

Aus Sicht von E.ON ist es wichtig, über den IT-Sicherheitskatalog einen angemessenen und überprüfbaren formalen Rahmen vorzugeben. Aber hinsichtlich der Vorgaben zur Dokumentation und behördlichen Prüfung der Einhaltung der Vorgaben des IT-Sicherheitskataloges droht auch unnötiger bürokratischer Aufwand. Dabei bleibt offenbar unberücksichtigt, dass bereits ein erhebliches, existenzielles Eigeninteresse der Unternehmen an einem ausreichenden Schutz besteht und deshalb auch unabhängig von staatlichen Vorgaben die Unternehmen erhebliche Anstrengungen unternehmen, das Schutzniveau immer weiter zu verbessern.

Änderungsbedarf aus Sicht E.ON
E.ON als Betreiber Kritischer Infrastrukturen und damit als in der Praxis unmittelbar betroffenes Unternehmen schlägt folgende Änderungen vor:
(1) Das Ziel für Betreiber Kritischer Infrastruktur muss die Gewährleistung der Systemsicherheit sein. Die Regelungen im IT-Sicherheitskatalog sollten sich daher auf Maßnahmen bezogen auf dieses Ziel beschränken.
(2) Eine regelmäßige Überprüfung der Dokumentation sollte nur für kritische Systeme, Komponenten und Prozesse erfolgen. Für Vorgaben in den Kategorien „wichtig" und „besonders wichtig" sollten weiterhin nur Prüfungen bei Verdachtsfällen bzw. Stichproben erfolgen, wie dies durch das BSI in anderen Branchen/Sektoren mit Kritischen Infrastrukturbetreibern (z.B. im Transport-, Gesundheits- oder Ernährungssektor) umgesetzt wird.
(3) Die Vorgaben zur Erstellung des IT-Sicherheitskataloges sollten auch ein Ziel für die Abstimmung mit der Industrie vorgeben: Das Kriterium „Umsetzbarkeit" in der Praxis sollte daher explizit aufgenommen werden.
(4) Die Vorgaben zur Dokumentation sollten sich auf Inhalte beschränken. In Zeiten moderner IT sind Vorgaben zu Formaten o.ä. überholt.

Eine Überregulierung durch viele Vorgaben von Behörden muss vermieden werden.

Das BSI würde nach dem Entwurf für ein NIS2UmsuCG verschiedene neue Aufgaben erhalten. Dazu zählen die Prüfung der Konformität von IT-Systemen entsprechend technischen Richtlinien (§ 3 Absatz 1 Nr. 10), das Erteilen von Sicherheitszertifikaten (§ 3 Absatz 1 Nr. 8) und entsprechende Warnungen (§ 3 Absatz 1 Nr. 20) bzw. Empfehlungen für Sicherheitsmaßnahmen (§ 13 Absatz 3 Nr. 2). Im Einvernehmen mit der BNetzA soll das BSI über den IT-Sicherheitskatalog Systeme zur Angriffserkennung vorgeben (§ 5c Absatz 4 Nr. 11). Das BSI soll Zertifizierungen u.a. für Produkte und Leistungen durchführen (§ 52 Absatz 2). Außerdem soll zu den künftigen Aufgaben des BSI gehören, u.a. auf Anforderung einer für den Betreiber zuständigen Behörde zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des IT-Systems in den operativen Betrieb vor Ort einzugreifen (§ 11 Absatz 1).

Mit den neuen Regelungen würden formale Prozesse und Mindestanforderungen zementiert. In der Folge würde das bewährte betriebliche Risikomanagement ersetzt durch formale Rahmenbedingungen. Dies würde erhebliche Verzögerungen bereits in der Produktentwicklung (s. Smart Meter Rollout) mit sich bringen, und die Innovationstätigkeit würde sinken. Bürokratische Prozesse, wie z.B. das regelmäßige Durchführen von Audits, würden zu monatelanger Beschäftigung mit (Konformitäts-) Nachweisen führen, wie das Beispiel der vermeintlich optionalen

„Orientierungshilfe“ für Systeme zur Angriffserkennung zeigt. Diese wurde als Prüfungsgrundlage im Rahmen von Audits faktisch zum Standard deklariert, obgleich zahlreiche Anforderungen nicht passten (z.B. Anforderungen für andere Sektoren, Anforderungen an ältere Komponenten, etc.).

Änderungsbedarf aus Sicht E.ON

E.ON als Betreiber Kritischer Infrastrukturen erkennt die Notwendigkeit für staatliche Vorgaben zum Schutz der öffentlichen Ordnung und Sicherheit an. Staatliche Vorgaben sollten aber nicht indirekt zu Verzögerungen und dadurch Schwächung des Schutzes der Unternehmen führen. Deshalb sollte:

(1) sich die Prüfung auf Konformität und die ggf. notwendige Zertifizierung ausschließlich auf den IT-Sicherheitskatalog beschränken, in dem die notwendigen Regelungsinhalte verbindlich und nur nach vorheriger Abstimmung mit der Industrie aufgenommen werden sollten;

(2) in Ausdifferenzierung zu den verbindlichen Regelungsinhalten der Charakter einer Empfehlung (§13 Absatz 3 Nr. 2) auch als solcher klar gekennzeichnet werden (z.B. durch den Zusatz „unverbindlich“);

(3) jeglicher Regelungsinhalt konsistent mit EU-Regelungen sein, auf deutsche Alleingänge bei den technischen Richtlinien (wie beim Smart Meter) sollte verzichtet werden;

(4) sich die Vorschrift zur Prüfung und Auditierung allein auf den IT-Sicherheitskatalog beschränken und im international üblichen 3-Jahres-Rhythmus durchgeführt werden. Darüberhinausgehende Prüfungserfordernisse könnten stichprobenartig und nur bei begründbaren Verdachtsfällen fehlender Konformität erfolgen;

(5) die Ermächtigung für das BSI zum Eingriff in operative Prozesse der Industrie im Krisenfall explizit den Wunsch der verantwortlichen Unternehmen voraussetzen. Dieser kann indirekt durch noch zu definierende Vorgaben zur schnellen Wiedererlangung der Funktionsfähigkeit erzielt werden.

Christoph Reißfelder
Vice President Political Affairs/
Head of Representative Office Berlin

Christoph.Reißfelder@eon.com

Thomas Krauhausen
E.ON Cyber Security

Thomas.Krauhausen@eon.com