§ 5c EnWG 2005 — IT-Sicherheit im Anlagen- und im Netzbetrieb, Festlegungskompetenz

Energiewirtschaftsgesetz
Stand: 07.12.2025 (konsolidierte Textfassung, kein amtliches Inkrafttretensdatum)

(1) Die folgenden Betreiber haben für die genannten Systeme einen angemessenen Schutz gegen Bedrohungen zu gewährleisten:

1. der Betreiber eines Energieversorgungsnetzes für Telekommunikationssysteme und für elektronische Datenverarbeitungssysteme, die für den sicheren Betrieb des Energieversorgungsnetzes notwendig sind,
2. der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, für Telekommunikationssysteme sowie für elektronische Datenverarbeitungssysteme, die für einen sicheren Betrieb der Energieanlage notwendig sind,
3. der Betreiber eines digitalen Energiedienstes, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 des BSI-Gesetzes ist und der den digitalen Energiedienst an einer Energieanlage ausübt, die an ein Energieversorgungsnetz angeschlossen ist, für Telekommunikationssysteme sowie für elektronische Datenverarbeitungssysteme, die für einen sicheren Betrieb der Anlage notwendig sind.

Der angemessene Schutz nach Satz 1 ist bereits bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen.

(2) Die Anforderungen an den angemessenen Schutz werden von der Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik in einem Katalog von Sicherheitsanforderungen (IT-Sicherheitskatalog) durch Festlegung nach § 29 Absatz 1 bestimmt. Die Bundesnetzagentur kann die Anforderungen an einen angemessenen Schutz eines Energieversorgungsnetzes, einer Energieanlage oder eines Energiedienstes auch jeweils in einem gesonderten IT-Sicherheitskatalog durch Festlegung nach § 29 Absatz 1 bestimmen. Die Bundesnetzagentur beteiligt jeweils die Betreiber nach Absatz 1 Satz 1 Nummer 1 bis 3 und deren Branchenverbände entsprechend ihrer Betroffenheit. Für Telekommunikationssysteme sowie für elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes sind ergänzend für die Erarbeitung des IT-Sicherheitskatalogs die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder zu beteiligen. Vorgaben auf Grund des Atomgesetzes haben Vorrang vor den Anforderungen des IT-Sicherheitskatalogs. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Mit der Einhaltung des IT-Sicherheitskatalogs durch den Betreiber nach Absatz 1 Satz 1 Nummer 1 bis 3 gilt der angemessene Schutz als eingehalten.

(3) Der IT-Sicherheitskatalog soll ein Sicherheitsniveau der informationstechnischen Systeme, Komponenten und Prozesse gewährleisten, das dem bestehenden Risiko angemessen ist. Der IT-Sicherheitskatalog soll unter Berücksichtigung der einschlägigen europäischen Normen oder internationalen Normen, der Einhaltung des Standes der Technik sowie der Umsetzungskosten erstellt werden. Zur Wahrung der Angemessenheit der Anforderungen des jeweiligen IT-Sicherheitskatalogs sind bei der Erstellung folgende Faktoren zu berücksichtigen:

1. das Ausmaß der Risikoexposition,
2. die Größe des Betreibers,
3. die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie
4. die gesellschaftlichen und wirtschaftlichen Auswirkungen.

(4) Der IT-Sicherheitskatalog hat mindestens Vorgaben zu enthalten für:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationstechnik,
2. die Bewältigung von Sicherheitsvorfällen,
3. die Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und das Krisenmanagement,
4. die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit der Informationstechnik,
7. grundlegende Verfahren im Bereich der Cyberhygiene und für Schulungen im Bereich der Sicherheit der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. die Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen,
10. die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung,
11. den Einsatz von Systemen zur Angriffserkennung nach § 2 Nummer 41 des BSI-Gesetzes,
12. den Einsatz eines Elements oder einer Gruppe von Elementen eines Netz- oder Informationssystems (IKT-Produkt), eines Dienstes, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht (IKT-Dienst), und jeglicher Tätigkeiten, mit denen ein IKT-Produkt oder ein IKT-Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll (IKT-Prozess), mit Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881.

(5) Die Bundesnetzagentur kann in dem IT-Sicherheitskatalog

1. nähere Bestimmungen treffen zu Format, Inhalt und Gestaltung der nach § 5d Absatz 1 Satz 1 erforderlichen Dokumentation über die Einhaltung der Anforderungen des IT-Sicherheitskatalogs,
2. nähere Bestimmungen zur Behebung von Sicherheitsmängeln sowie
3. Regelungen festlegen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen.

(6) Die Bundesnetzagentur legt bis zum Ablauf des 6. Januar 2026 im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem Katalog für den Betrieb von Energieversorgungsnetzen und Energieanlagen fest,

1. welche Komponenten kritische Komponenten nach § 2 Nummer 23 Buchstabe c Doppelbuchstabe aa des BSI-Gesetzes sind oder
2. welche Funktionen kritisch bestimmte Funktionen nach § 2 Nummer 23 Buchstabe c Doppelbuchstabe bb des BSI-Gesetzes sind.

Der Betreiber nach Absatz 1 Satz 1 Nummer 1 und 2, der zugleich eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes betreibt, hat die Vorgaben des Katalogs spätestens sechs Monate nach dessen in der Festlegung nach § 29 Absatz 1 bestimmten Inkrafttretens zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden. Die Befugnis der Bundesnetzagentur nach Satz 1 besteht bis zum Erlass einer Rechtsverordnung nach § 56 Absatz 7 des BSI-Gesetzes für den Sektor Energie fort. Eine von der Bundesnetzagentur auf der Grundlage von Satz 1 oder auf der Grundlage von § 11 Absatz 1a Satz 2 des Energiewirtschaftsgesetzes in der am 5. Dezember 2025 geltenden Fassung erlassene Allgemeinverfügung ist mit dem Inkrafttreten einer

Rechtsverordnung nach § 56 Absatz 7 des BSI-Gesetzes für Energieversorgungsnetze und Energieanlagen aufzuheben.