FAQ zum IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz

Verantwortlichkeit für die Umsetzung des IT-Sicherheitskataloges

Wer ist für die Umsetzung des IT-Sicherheitskatalogs verantwortlich?

Die Verantwortung für die Umsetzung der Vorgaben des IT-Sicherheitskatalogs obliegt ausschließlich den (bei der Bundesnetzagentur unter einer entsprechenden Betriebsnummer gelisteten) Betreibern eines Strom- oder Gasnetzes. Dies gilt unabhängig davon, ob ein Netzbetreiber ein Strom- oder Gasnetz als Eigentümer oder im Rahmen eines Pachtmodells betreibt. Ausnahmen von der Umsetzungspflicht, etwa in Abhängigkeit von der Größe eines Netzbetreibers, bestehen nicht.

Was ist, wenn ich die vom IT-Sicherheitskatalog betroffenen Systeme nicht selbst betreibe, sondern durch Dritte betreiben lasse (Outsourcing, Betriebsführung durch Dienstleister)?

Betreibt ein Netzbetreiber die Anwendungen, Systeme und Komponenten, auf die sich die Sicherheitsanforderungen des IT-Sicherheitskatalogs beziehen, nicht selbst, sondern durch einen externen Dienstleister, entbindet ihn das nicht von seiner eigenen Verantwortung zur Umsetzung des IT-Sicherheitskatalogs. Er muss in diesem Falle durch entsprechende vertragliche Vereinbarungen sicherstellen, dass der beauftragte Dienstleister die Sicherheitsanforderungen einhält (zur Frage, welche Auswirkungen dies auf die erforderliche Zertifizierung hat, s. u.).

Ansprechpartner IT-Sicherheit

Was bedeutet die Aussage „Bei der Bestimmung des Ansprechpartners sind – soweit einschlägig – die Vorschriften des Sicherheitsüberprüfungsgesetzes (SÜG) und der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) zu beachten“?

Das SÜG sieht im Bereich des vorbeugenden personellen Sabotageschutzes für Personen, die an einer sicherheitsempfindlichen Stelle innerhalb einer lebenswichtigen Einrichtung beschäftigt sind, nach § 1 Absätze 1 und 4 eine Sicherheitsüberprüfung vor. Zu den lebenswichtigen Einrichtungen gehören im Zuständigkeitsbereich des BMWi u.a. „die Teile von Unternehmen, die Leitstellen für das Elektrizitätsübertragungsnetz betreiben, deren Ausfall die überregionale Elektrizitätsversorgung erheblich beeinträchtigen kann“, § 10 Absatz 1 Nr. 4 SÜFV. Einer Sicherheitsüberprüfung müssen sich daher nur die an einer sicherheitsempfindlichen Stelle der Elektrizitätsübertragungsnetzbetreiber tätigen Personen unterziehen. Zuständig für die Durchführung der Sicherheitsüberprüfung ist nach § 12 SÜFV das BMWi.

Zertifizierung

Ist für die Sparten Strom und Gas eine gesonderte Zertifizierung durchzuführen?

Soweit die Tätigkeiten der Elektrizitätsübertragung, Elektrizitätsverteilung, Gasfernleitung oder Gasverteilung durch ein Mehrspartenunternehmen wahrgenommen werden, ist keine gesonderte Zertifizierung für die Sparten Strom und Gas erforderlich. Es ist jedoch in jedem Fall sicherzustellen, dass alle Telekommunikations- und elektronischen Datenverarbeitungssysteme, die für einen sicheren Strom- und Gasnetzbetrieb notwendig sind, vom Anwendungsbereich (Scope) des Zertifikats erfasst sind. Systeme, die ausschließlich für den Betrieb sonstiger Sparten eines EVU (z. B. Fernwärme) benötigt werden und keine Relevanz für den sicheren Betrieb des Strom- oder Gasnetzes entfalten, sind nicht vom Anwendungsbereich des IT-Sicherheitskataloges erfasst.

Ich bin bereits zertifiziert nach DIN ISO 27001, BSI Grundschutz oder TSM. Wird dieses Zertifikat anerkannt?

Zum Nachweis, dass die Anforderungen des IT-Sicherheitskataloges erfüllt werden, erarbeitet die Bundesnetzagentur gemeinsam mit der Deutschen Akkreditierungsstelle (DAkkS) ein eigenes Zertifikat. Das Zertifikat wird dabei im Wesentlichen auf dem bereits existierenden Zertifikat bzw. Zertifizierungsschema zur ISO/IEC 27001 basieren und dieses um die zusätzlichen Anforderungen des IT-Sicherheitskataloges ergänzen. Des Weiteren soll der Anwendungsbereich (Scope) spezifiziert werden, um sicherzustellen, dass zumindest die für einen sicheren Netzbetrieb notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme von der Zertifizierung erfasst sind. Bereits bestehende Zertifizierungen nach ISO/IEC 27001, BSI Grundschutz usw. sind daher nicht ausreichend, um die Erfüllung der Anforderungen des IT-Sicherheitskatalogs nachzuweisen.

Ich betreibe nur Anlagen ohne Gefährdungspotential, ohne Anschluss an das Internet oder habe kein Leitsystem. Benötige ich dennoch eine Zertifizierung?

Betreibt ein Strom- oder Gasnetzbetreiber keine vom IT-Sicherheitskatalog erfassten Systeme in seinem Netz und lässt diese auch nicht von einem externen Dienstleister betreiben bzw. handelt es sich nur um Systeme ohne Gefährdungspotential, besteht auch keine Umsetzungspflicht für die diesbezüglichen Sicherheitsanforderungen des IT-Sicherheitskatalogs. Es bedarf dann auch keiner Zertifizierung. Dies ist jedoch zu begründen und durch geeignete Nachweise zu belegen. Die Telekommunikations- und elektronischen Datenverarbeitungssysteme eines Netzbetreibers, die für einen sicheren Netzbetrieb notwendig sind, sind im Rahmen der geforderten Risikoeinschätzung zu ermitteln. Insofern kann ein geeigneter Nachweis durch Vorlage der Dokumentation zur dieser Risikoanalyse oder durch sonstige Pläne zur Struktur des Netzes erfolgen.

Die vom IT-Sicherheitskatalog erfassten TK- und EDV-Systeme, die für einen sicheren Netzbetrieb notwendig sind, lasse ich über einen Betriebsführungsvertrag von einem Dritten betreiben. Muss sich der Netzbetreiber trotzdem selbst zertifizieren lassen?

Bei dieser Frage sind zwei Konstellationen zu unterscheiden:

1. Ein Teil der vom IT-Sicherheitskatalog erfassten Systeme wird von einem Dienstleister betrieben, ein Teil vom Netzbetreiber selbst

   Da der Netzbetreiber selbst auch Systeme betreibt, die vom Anwendungsbereich des IT-Sicherheitskatalogs erfasst sind, muss er zum Nachweis der Umsetzung des IT-Sicherheitskatalogs eine Zertifizierung vornehmen lassen. Im Rahmen der Zertifizierung sind sowohl die selbst betriebenen Systeme als auch die vom Dienstleister betreuten Systeme mit zu berücksichtigen.

2. Alle vom IT-Sicherheitskatalog erfassten Systeme werden vollständig von einem Dienstleister betrieben

   In diesem Fall muss der Netzbetreiber Umsetzung und Einhaltung des IT-Sicherheitskataloges durch den Dienstleister sicherstellen. Zum Nachweis darüber reicht es im Rahmen der Zertifizierung aus, dass ein Duplikat des Zertifikates, das auf den mit der Betriebsführung beauftragten Dienstleister ausgestellt ist, vorgelegt wird. Eine darüber hinausgehende Zertifizierung des Netzbetreibers ist in diesem Fall nicht erforderlich. Im Regelfall wird die Betriebsführung nämlich durch einen Dienstleister erfolgen, der selbst Netzbetreiber und somit zur Einhaltung des IT-Sicherheitskataloges und zur Zertifizierung verpflichtet ist. Darüber hinaus ist ein Nachweis darüber zu erbringen, dass der Netzbetreiber selbst keine weiteren Systeme betreibt, die vom IT-Sicherheitskatalog erfasst sind.