Bundesnetzagentur

Mitteilung

zur Zertifizierung nach IT-Sicherheitskatalog § 11 Abs. 1a und 1b EnWG im Fall einer Betriebsführung durch Dritte

Mitteilung zur Zertifizierung nach IT-Sicherheitskatalog § 11 Abs. 1a und 1b EnWG im Fall einer Betriebsführung durch Dritte

Stand: 29. März 2022

**Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen**

Referat 627

Tulpenfeld 4

53113 Bonn

Tel.: +49 228 14-0

Fax: +49 228 14-8872

E-Mail: IT-Sicherheitskatalog@BNetzA.de

Inhaltsverzeichnis

Kurzfassung

Die vorliegende Mitteilung passt die am 19. Januar 2021 im Rahmen der „Mitteilung bezüglich der Zertifizierung nach dem IT-Sicherheitskatalog § 11 Abs. 1a EnWG im Falle der Betriebsführung durch Dritte“ aufgezeigten Lösungsoptionen an. Die Mitteilung vom 19. Januar 2021 ist damit obsolet. Mit der aktuellen Mitteilung werden bestehende Widersprüche im Zertifizierungsverfahren aufgelöst. Das wesentliche Resultat der Anpassung ist, dass sich die Netzbetreiber und die Betreiber von als Kritische Infrastruktur klassifizierten Energieanlagen in der Konstellation „Betriebsführung durch Dritte“ selbst zu zertifizieren haben. Hierüber ist ein Nachweis zu erbringen. Für die Nachweiserbringung wird eine angemessene Frist bis zum 31.03.2024 gewährt.

1 Hintergrund der Mitteilung

Die Regelung des § 11 Abs. 1a und b EnWG verpflichtet Betreiber von Energieversorgungsnetzen und Betreiber von als Kritische Infrastruktur klassifizierten Energieanlagen zur Umsetzung der IT-Sicherheitskataloge. Damit einher geht auch die Vorlage einer Kopie des Zertifikats gegenüber der Bundesnetzagentur als Nachweis darüber, dass die Anforderungen der IT-Sicherheitskataloge umgesetzt worden sind.

Bisher war in zwei Konstellationen die Zertifizierung eines Netzbetreibers nach IT-Sicherheitskatalog gegenüber der Bundesnetzagentur nicht nachzuweisen. Dies galt für

1) Betreiber von Energieversorgungsnetzen, in deren Netz keine Systeme, Anwendungen und Komponenten zum Einsatz kommen, die für einen sicheren Netzbetrieb notwendig sind, sodass die Voraussetzungen des § 11 Abs. 1a EnWG nicht vorliegen („Nicht-Anwendbarkeit“) und
2) Betreiber von Energieversorgungsnetzen, deren Systeme, Anwendungen und Komponenten im Geltungsbereich des IT-Sicherheitskatalogs liegen, welche aber vollständig von einem oder mehreren Dritten betrieben werden („Betriebsführung durch Dritte“).

Während die Konstellation der „Nicht-Anwendbarkeit“ von den folgenden Neuregelungen dieser Mitteilung unberührt bleibt, werden in der Konstellation der „Betriebsführung durch Dritte“ die bestehenden Regelungen angepasst. Wesentliches Resultat der Neuregelung ist, dass der Netzbetreiber in dieser Konstellation ein eigenes Zertifikat vorzuweisen hat. Auch für Betreiber von als Kritische Infrastruktur klassifizierten Energieanlagen gilt diese Vorgabe. Für die Umsetzung der Selbst-Zertifizierung wird eine Frist bis zum 31.03.2024 gewährt.

2 Begründung der Neuregelung

In Fällen der Betriebsführung durch Dritte hielt die Bundesnetzagentur in der Vergangenheit zum Nachweis des angemessenen Schutzes von Systemen, Anwendungen und Komponenten des betriebsgeführten Netzbetreibers im Rahmen des § 11 Abs. 1a EnWG eine Kopie des Zertifikats der oder des Dritten für ausreichend. Zudem war eine Erklärung der oder des Dritten notwendig, als Nachweis darüber, dass im Zertifizierungsprozess auch alle im Geltungsbereich des IT-Sicherheitskatalogs befindlichen Systeme, Anwendungen und Komponenten des betriebsgeführten Netzbetreibers berücksichtigt worden sind. Die Kopie des Zertifikats und die Erklärung der oder des Dritten wurden vom betriebsgeführten Netzbetreiber der Bundesnetzagentur vorgelegt. Darüber hinaus war der Bundesnetzagentur durch den betriebsgeführten Netzbetreiber eine „Verbindliche Erklärung des Netzbetreibers zur Betriebsführung durch Dritte“ vorzulegen. Diese Erklärung diente der Bestätigung durch den betriebsgeführten Netzbetreiber, dass keine vom Geltungsbereich des IT-Sicherheitskatalogs erfassten Systeme, Anwendungen und Komponenten eigenständig betrieben werden.

Im Rahmen von Akkreditierungsverfahren der Deutschen Akkreditierungsstelle wurde nunmehr offenkundig, dass das bisher angewandte Verfahren im Falle der Betriebsführung durch Dritte teilweise im Widerspruch zu geltenden Zertifizierungsnormen steht. Insbesondere ist der Verweis auf die Zertifizierungsurkunden eines Dritten anstelle einer eigenen Zertifizierung gemäß Tz. 8.3.5 der ISO/IEC 17021-1:2015 ausgeschlossen. Auch das Abgeben einer Erklärung über die Einbeziehung von Systemen, Anwendungen und Komponenten eines betriebsgeführten Netzbetreibers in den Geltungsbereich der Zertifizierung eines Dritten ist unzureichend. Dem betriebsgeführten Netzbetreiber, auf dessen Systeme, Anwendungen und Komponenten sich die Zertifizierung eines Betriebsführers bezieht, mangelt es an einer wirksamen Zertifizierungsvereinbarung mit der Zertifizierungsstelle gemäß Tz. 5.1.2 ISO/IEC 17021-1:2015. Damit fehlt der Zertifizierungsstelle die Möglichkeit, ihr Zertifizierungsprogramm rechtlich wirksam gegenüber dem betriebsgeführten Netzbetreiber durchzusetzen. Die Zertifizierungsstelle kann in der beschriebenen Konstellation unter anderem keine Regelungen zur Einführung der geforderten Maßnahmen gegenüber dem betriebsgeführten Netzbetreiber durchsetzen. Dies bedeutet, dass im Falle der Betriebsführung durch Dritte trotz der Zertifizierungspflicht des betriebsgeführten Netzbetreibers gemäß § 11 Abs. 1a EnWG rechtlich nur der Dritte oder die Dritten ein gültiges Zertifikat besitzt. Dieses Zertifikat gilt ausschließlich für den Dritten und kann daher nicht seitens des betriebsgeführten Netzbetreibers der Bundesnetzagentur als Nachweis zur Umsetzung des IT-Sicherheitskatalogs vorgelegt werden.

Die im Rahmen der „Mitteilung bezüglich der Zertifizierung nach dem IT-Sicherheitskatalog § 11 Abs. 1a EnWG im Falle der Betriebsführung durch Dritte“ vom 19. Januar 2021 aufgezeigten Lösungsoptionen in der Konstellation der Betriebsführung durch Dritte werden deshalb durch die folgenden Ausführungen angepasst. Auf diese Weise sollen die bestehenden Widersprüche aufgelöst werden. Zusätzlich soll das unter Punkt 3 aufgezeigte Vorgehen analog für die Umsetzung von Betriebsführungen durch Dritte im Rahmen des § 11 Abs. 1b EnWG gelten. Die Frist bis zum 31.03.2024 ermöglicht eine Umsetzung der geänderten Anforderungen.

3 Beispiele für Zertifizierungsverfahren anhand möglicher Betriebsführungsstrukturen

Voraussetzung ist stets, dass die beteiligten Akteure auch tatsächlich eine zertifizierungsfähige Unternehmensstruktur vorweisen können. Grundsätzlich muss jeder Betreiber von Energieversorgungsnetzen beziehungsweise jeder Betreiber von als Kritische Infrastruktur klassifizierten Energieanlagen der Bundesnetzagentur ein eigenes Zertifikat beziehungsweise dessen Kopie als Nachweis zur Umsetzung des jeweiligen IT-Sicherheitskatalogs vorlegen. Dieser Nachweis bescheinigt, dass in der auditierten Organisation unter anderem ein funktionsfähiges Informationssicherheits-Managementsystem (ISMS) etabliert ist. Die Funktionsfähigkeit eines ISMS setzt voraus, dass der Betreiber dieses Managementsystems die oberste Leitung über alle von dem ISMS berührten Bereiche innehat. In Abhängigkeit der Unternehmensstruktur besteht eine Vielzahl an Möglichkeiten, ein funktionsfähiges ISMS zu etablieren. Die folgenden Ausführungen sollen beispielhaft mögliche Zertifizierungskonstellationen skizzieren. Die Auflistung der Fälle ist dabei ausdrücklich nicht abschließend. Aufgrund der Vielfalt möglicher Strukturen gilt es die genaue Umsetzung der Anforderungen des jeweiligen IT-Sicherheitskatalogs mit einer Zertifizierungsstelle zu planen.

1) Betreiber von Energieversorgungsnetzen oder als Kritische Infrastruktur klassifizierten Energieanlagen, die sich für den Betrieb von Systemen, Anwendungen oder Komponenten im Geltungsbereich des IT-Sicherheitskatalogs eines konzernfremden Betriebsführers auf vertraglicher Grundlage bedienen, müssen die Anforderungen des jeweiligen IT-Sicherheitskatalogs erfüllen. Dies ist der Bundesnetzagentur in Form eines Zertifikats nachzuweisen.

   Unabhängig davon muss der Betriebsführer bestimmte Sicherheitskriterien erfüllen, um als Dienstleister geeignet zu sein. Der Erfüllungsnachweis dieser Sicherheitskriterien erfolgt durch ein eigenständiges Zertifizierungsverfahren gemäß des jeweiligen IT-Sicherheitskatalogs. Ein solches, gültiges Zertifikat – gegebenenfalls mit weiteren erforderlichen Nachweisen – muss der Betriebsführer dem betriebsgeführten Betreiber vorlegen. Nur so kann im Rahmen der Zertifizierung des betriebsgeführten Betreibers die Erfüllung der Sicherheitskriterien seitens des Betriebsführers sichergestellt werden. In der Konsequenz müssen sich sowohl der betriebsgeführte Betreiber als auch der Betriebsführer gemäß des jeweiligen IT-Sicherheitskatalog zertifizieren lassen.[1]

   Für den Fall, dass ein Betreiber von Energieversorgungsnetzen oder als Kritische Infrastruktur klassifizierten Energieanlagen zusätzlich die Aufgabe als Betriebsführer für einen anderen Betreiber von Energieversorgungsnetzen oder eine als Kritische Infrastruktur klassifizierte Energieanlage wahrnimmt, kann dieser Betreiber ein ISMS etablieren, welches unter anderem auch Systeme, Anwendungen oder Komponenten, die notwendig für die Betriebsführung sind, umfasst. Die Zertifizierung eines solchen

[1] Es gilt zu beachten, dass die Anforderungen im Rahmen eines Informationssicherheits-Managementsystems davon abhängig sind, welche Aufgaben und Organisationsstrukturen vorliegen. So kann beispielsweise der Betriebsführer im Rahmen seines Informationssicherheits-Managementsystems Risiken adressieren, die im Zusammenhang mit dem operativen Betrieb stehen. Der betriebsgeführte Betreiber selber, der den operativen Betrieb an den Betriebsführer ausgelagert hat, überprüft im Rahmen seiner Zertifizierung, ob der Betriebsführer in der Rolle eines Dienstleisters als Qualitätsmerkmal über ein Informationssicherheits-Managementsystem nach IT-SiKat § 11 Abs. 1 a oder 1b EnWG verfügt. Jedoch muss der betriebsgeführte Betreiber im Rahmen seines eigenen Informationssicherheits-Managementsystems organisatorische und weitere Risiken adressieren, die beispielsweise im Zusammenhang mit der Abhängigkeit vom Betriebsführer stehen. So ergibt sich pro Organisation ein Zertifizierungsverfahren.

ISMS kann dann als Nachweis zur Erfüllung von Sicherheitskriterien dem betriebsgeführten Betreiber – gegeben einer Betriebsführung auf *vertraglicher Grundlage* – vorgelegt werden.

2) Falls ein Betreiber von Energieversorgungsnetzen oder als Kritische Infrastruktur klassifizierten Energieanlagen sich für den Betrieb von Systemen, Anwendungen oder Komponenten, die im Geltungsbereich der IT-Sicherheitskataloge liegen, eines konzerneigenen Betriebsführers bedient, muss sichergestellt sein, dass der Betreiber des ISMS die notwendige oberste Leitung über vom ISMS berührte Bereiche innehat. Dies kann beispielsweise durch Beherrschungsrechte im Sinne des §§ 15, 18 AktG erfolgen. In dieser Konstellation bedarf es keiner gesonderten Zertifizierung

   (i) des konzerneigenen Betriebsführers, sofern der betriebsgeführte Betreiber das ISMS betreibt und die notwendige oberste Leitung über die vom ISMS berührten Bereiche innehat. Der Betriebsführer stellt sich als Standort – das heißt Teil der einheitlichen Konzernorganisation – des betriebsgeführten Betreibers dar.

   (ii) des konzerneigenen Betreibers, sofern der Betriebsführer das ISMS betreibt und die notwendige oberste Leitung über die vom ISMS berührten Bereiche innehat. Der Betreiber stellt sich als Standort – das heißt Teil der einheitlichen Konzernorganisation – des Betriebsführers dar.

   (iii) des konzerneigenen Betreibers sowie konzerneigenen Betriebsführers, sofern eine Konzernmutter das ISMS betreibt und die notwendige oberste Leitung über die vom ISMS berührten Bereiche innehat. Der Betreiber sowie Betriebsführer stellen sich als Standorte – das heißt Teil der einheitlichen Konzernorganisation – der Konzernmutter dar.

   In den Fällen (ii) und (iii) kann der Betreiber das Zertifikat des / der konzerneigenen Dritten, in welchem der Betreiber selbst wiederum als Standort gelistet ist, der Bundesnetzagentur vorlegen.

4 Umsetzungs- und Nachweisfrist zur Erfüllung der IT-Sicherheitskataloge

Aufgrund dieser Mitteilung und der damit verbundenen Neuregelung kann es Netzbetreiber und Betreiber von als Kritische Infrastruktur klassifizierten Energieanlagen geben, die bisher nicht zur Zertifizierung Ihres Unternehmens in dieser Form verpflichtet waren. Der Bundesnetzagentur ist bewusst, dass die Einführung eines ISMS nach den IT-Sicherheitskatalogen und deren Zertifizierung für diese Betreiber einen neuen Aufwand verursachen könnte. Die Neuregelung ist allerdings notwendig, um die Zertifizierungsanforderungen vollumfänglich zu erfüllen. Diese Zertifizierungsanforderungen bestehen auch in anderen Sektoren.

Um eine Umsetzbarkeit der Anpassungen sicherzustellen, wird ein hinreichend langer Umsetzungszeitraum gewährt. Zum Nachweis darüber, dass die Anforderungen der IT-Sicherheitskataloge erfüllt worden sind, haben die betroffenen Netzbetreiber und die Betreiber von als Kritische Infrastruktur klassifizierten Energieanlagen der Bundesnetzagentur bis zum 31.03.2024 den Abschluss des Zertifizierungsverfahrens durch Vorlage einer Kopie des Zertifikats nachzuweisen.

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen
Tulpenfeld 4
53113 Bonn
Telefon: +49 228 14-0
Telefax: +49 228 14-8872
E-Mail: info@bnetza.de
www.bundesnetzagentur.de