Bundesnetzagentur

Mitteilung

bezüglich der Zertifizierung nach dem IT-Sicherheitskatalog § 11 Abs. 1a EnWG im Falle der Betriebsführung durch Dritte

Mitteilung bezüglich der Zertifizierung nach dem IT-Sicherheitskatalog § 11 Abs. 1a EnWG im Falle der Betriebsführung durch Dritte

Stand: 19.01.2021

**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: info@bnetza.de

Inhaltsverzeichnis

1 Zusammenfassung

Im Rahmen der Akkreditierungsverfahren der Deutschen Akkreditierungsstelle GmbH (DAkkS) sind zuletzt Widersprüche zwischen geltenden Zertifizierungsnormen und dem von der Bundesnetzagentur bislang angewendeten Verfahren für die Nachweispflicht der Zertifizierung bei einer Betriebsführung durch einen Dritten offenkundig geworden. Betriebsführung durch Dritte meint in diesem Kontext, dass alle Systeme, Anwendungen und Komponenten im Geltungsbereich des IT-Sicherheitskatalogs von einem oder mehreren Dritten betrieben werden. Diese Widersprüche beziehen sich insbesondere auf den Umgang mit und die Weitergabe von Zertifikaten sowie die Integration der Systeme, Anwendungen und Komponenten eines betriebsgeführten Unternehmens in den Geltungsbereich der eigenen Zertifizierung. Dies hat zur Folge, dass für die Systeme, Anwendungen und Komponenten von Netzbetreibern[1], die die Umsetzung des IT-Sicherheitskatalogs bisher durch Vorlage eines Zertifikats eines oder gegebenenfalls von mehreren Dritten nachgewiesen haben, aktuell kein gültiger Nachweis zur Umsetzung des IT-Sicherheitskatalogs vorliegt. Um Ihrer Pflicht zur Umsetzung des IT-Sicherheitskatalogs nachzukommen, muss sich künftig jeder nach dem IT-Sicherheitskatalog verpflichtete Netzbetreiber mit Systemen, Anwendungen oder Komponenten im Geltungsbereich grundsätzlich selbst zertifizieren lassen, sofern die beauftragte akkreditierte Zertifizierungsstelle nicht festgestellt hat, dass ein Betreiber nicht zertifizierbar ist. Für Netzbetreiber, in deren Netz keine IKT-Systeme im Geltungsbereich des IT-Sicherheitskatalogs zum Einsatz kommen und die aus diesem Grund nicht zur Vorlage eines Zertifikats gegenüber der Bundesnetzagentur verpflichtet sind (sog. Nicht-Anwendbarkeit), ändert sich durch die vorliegende Regelung nichts.

2 Kontext

Die Regelung des § 11 Abs. 1a EnWG verpflichtet explizit "Betreiber von Energieversorgungsnetzen“ zur Umsetzung des IT-Sicherheitskatalogs und damit auch zur Vorlage einer Kopie des Zertifikats als Nachweis darüber, dass die Anforderungen des IT-Sicherheitskatalogs umgesetzt wurden.

Bislang bestehen zwei Konstellationen, in denen die eigene Zertifizierung nach IT-Sicherheitskatalog für Netzbetreiber nicht erforderlich ist. Dies betrifft zum einen Netzbetreiber, in deren Netz keine Systeme, Anwendungen und Komponenten zum Einsatz kommen, die für einen sicheren Netzbetrieb notwendig sind, sodass die Voraussetzungen des § 11 Absatz 1a EnWG nicht vorliegen (Nicht-Anwendbarkeit). Diese Konstellation ist von den hier getroffenen Regelungen unberührt.

Zum anderen gibt es Netzbetreiber, deren Systeme, Anwendungen und Komponenten im Geltungsbereich des IT-Sicherheitskatalogs vollständig von einem oder mehreren Dritten betrieben werden. In dem bislang angewendeten Verfahren für die Nachweispflicht der Zertifizierung im Falle einer Betriebsführung durch

[1] Netzbetreiber ist grundsätzlich, wer bei der Bundesnetzagentur als solcher mit Netzbetreibernummer registriert ist und die Konzession für ein bestimmtes Netzgebiet hält. In der Regel verfügt der Netzbetreiber über die tatsächliche und rechtliche Verfügungsgewalt in Bezug auf den Netzbetrieb.

einen Dritten, hat die Bundesnetzagentur bisher als Nachweis für einen angemessenen Schutz von IKT-Systemen des betriebsgeführten Unternehmens im Geltungsbereich des IT-Sicherheitskatalogs, ein Duplikat des Zertifikats eines Dritten akzeptiert. Dabei gibt es auch Konstellationen, in denen die Systeme im Geltungsbereich von verschiedenen Dritten betrieben werden. Hierbei war von jedem Dritten ein Duplikat des Zertifikats vorzulegen. Zudem war eine Erklärung der Dritten notwendig, dass im Zertifizierungsprozess all diese Systeme, Anwendungen und Komponenten des betriebsgeführten Unternehmens berücksichtigt wurden. Des Weiteren war durch den betriebsgeführten Netzbetreiber eine „Verbindliche Erklärung des Netzbetreibers zur Betriebsführung durch Dritte“ der Bundesnetzagentur vorzulegen, in welcher der Netzbetreiber bestätigte, dass darüber hinaus keine vom Geltungsbereich des IT-Sicherheitskatalogs erfasste Netzinfrastruktur vom Netzbetreiber selbst betrieben wird.

Im Rahmen von Akkreditierungsverfahren der DAkkS wurde zuletzt offenkundig, dass das bisher angewandte Verfahren im Falle der Betriebsführung durch Dritte jedoch teilweise im Widerspruch zu geltenden Zertifizierungsnormen steht. Insbesondere ist die Weitergabe von Zertifizierungsurkunden nach Tz. 8.3.5 der ISO/IEC 17021-1:2015 ausgeschlossen und auch das Abgeben einer Erklärung über das Miteinbeziehen von Assets betriebsgeführter Unternehmen in den Geltungsbereich der eigenen Zertifizierung ist unzulässig. Dem Netzbetreiber, auf dessen Systeme sich die Zertifizierung des Betriebsführers bezogen hat, mangelt es hierbei an einer wirksamen Zertifizierungsvereinbarung gemäß Tz. 5.1.2 ISO/IEC 17021-1:2015 mit der Zertifizierungsstelle. Damit fehlt der Zertifizierungsstelle die Möglichkeit, ihr Zertifizierungsprogramm rechtlich wirksam gegenüber dem verpflichteten Netzbetreiber durchzusetzen. Sie kann insbesondere keine Regelungen zur Überwachung der geforderten Maßnahmen gegenüber dem betriebsgeführten Unternehmen selbst durchsetzen. Dies bedeutet, dass im Falle der Betriebsführung durch Dritte trotz der Zertifizierungspflicht des Netzbetreibers nach § 11 Abs. 1a EnWG nur der Dritte ein gültiges Zertifikat ausschließlich für sein Unternehmen besitzt. Das betriebsgeführte Unternehmen hingegen besitzt somit kein gültiges Zertifikat.

Dies hat zur Folge, dass sich grundsätzlich jeder Netzbetreiber, in dessen Netz Systeme, Anwendungen oder Komponenten, die für den sicheren Netzbetrieb notwendig sind, eingesetzt werden, ab sofort selbst zertifizieren lassen muss.

3 Lösungsmöglichkeiten

Folgende Lösungsmöglichkeiten liegen vor und sind vom Netzbetreiber zu bestimmen:

1. Falls der Netzbetreiber sich für den Betrieb dieser Systeme eines Betriebsführers bemüht, muss sichergestellt sein, dass er sein für die Zertifizierung notwendiges „Durchgriffsrecht“ in Bezug auf Maßnahmen und Anforderungen seines ISMS und alle Akkreditierungs- und Zertifizierungsregeln gegenüber Dritten vertraglich absichern kann.
2. Sollte die vertragliche Absicherung des Durchgriffsrechts nur für einen Teil und für nicht alle zum Einsatz kommenden Systeme im Geltungsbereich möglich sein, dann ist der Netzbetreiber verpflichtet sicherzustellen, dass sein Betriebsführer ebenfalls nach dem IT-Sicherheitskatalog zertifiziert ist, und der

Geltungsbereich der Zertifzierung und die Erklärung Dritter zur Anwendbarkeit mit der Zertifizierung des Netzbetreibers übereinstimmen.

In beiden Fällen muss auch der Netzbetreiber ein eigenes Zertifikat vorweisen, solange der Netzbetreiber zertifizierungsfähig ist.

3. Ist ein Netzbetreiber nicht zertifizierungsfähig, muss der Betriebsführer zertifiziert werden. In diesem Fall muss sich der Betriebsführer vom Netzbetreiber das vollumfängliche und organisatorische Durchgriffsrecht auf die sich im Geltungsbereich der Zertifizierung befindlichen Assets des Netzbetreibers vertraglich zusichern lassen. Diese Konstellation setzt einerseits voraus, dass alle Zertifizierungs- und Akkreditierungsregeln eingehalten werden und bedingt andererseits, dass in der Vereinbarung zwischen Netzbetreiber und Betriebsführer eine Nachweispflicht für den Betriebsführer für die nach IT-Sicherheitskatalog abgeschlossene Zertifizierung gegenüber der Bundesnetzagentur festgehalten wird. Gegen eine Zertifizierfähigkeit spricht, wenn die im Geltungsbereich der Zertifizierung befindlichen Assets vollständig von Dritten betrieben werden, der Netzbetreiber keine Durchgriffsrechte auf Assets sowie keine Weisungsrechte gegenüber Mitarbeitern des Dritten besitzt. Hierbei ist auch die „Amtliche Mittteilung zur Unzulässigkeit von Matrixzertifizierungen“ der DAkkS vom 10.05.2019 zu beachten.

4 Umsetzungsfristen

Aufgrund dieser Mitteilung und der Anpassung bei der Nachweispflicht der Zertifizierung im Falle der Betriebsführung durch einen Dritten kann es Netzbetreiber geben, welche bisher nicht zur Zertifizierung Ihres Unternehmens verpflichtet waren, die fortan die Umsetzung des IT-Sicherheitskatalogs durch Vorlage eines eigenen Zertifikats nachweisen müssen. Der Bundesnetzagentur ist bewusst, dass die Einführung eines Informationssicherheits-Managementsystems (ISMS) nach IT-Sicherheitskatalog und dessen Zertifizierung einen hohen zeitlichen und personellen Aufwand verursacht. Zum Nachweis darüber, dass die Anforderungen des IT-Sicherheitskatalogs umgesetzt wurden, haben die neu zu zertifizierenden Netzbetreiber der Bundesnetzagentur bis zum 30.11.2022 den Abschluss des Zertifizierungsverfahrens durch Vorlage einer Kopie des Zertifikats mitzuteilen.

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