06.01.2022

Stellungnahme zu BNetzA-Ankündigung zur Zertifizierung unter Betriebsführung durch Dritte

1. Einleitung

Die Bundesnetzagentur (BNetzA) hat mit Stand 13.12.2021 eine „Ankündigung zur Zertifizierung unter Betriebsführung durch Dritte“ veröffentlicht und um Stellungnahme bis zum 14.01.2022 gebeten.

Die datenschutz cert GmbH ist bei der DAkkS akkreditierte Zertifizierungsstelle für das Regelwerk „IT-Sicherheitskatalog gem. §11 Abs. 1a EnWG“ für Netzbetreiber und befindet sich im Prozess der Erweiterung der Akkreditierung auf den „IT-Sicherheitskatalog gem. §11 Abs. 1b EnWG“ für Energieanlagenbetreiber (Kraftwerksbetreiber).

Zur BNetzA-Ankündigung nimmt die datenschutz cert GmbH wie folgt Stellung:

2. Eigenständige Zertifizierung von Betreibern

Alle Netzbetreiber sind gem. IT-Sicherheitskatalog gem. §11 Abs. 1a EnWG verpflichtet, ein Informationssicherheits-Managementsystem (ISMS) zu etablieren und zertifizieren zu lassen.

In der Praxis hat sich jedoch herausgestellt, dass es Szenarien gibt, wonach ein Netzbetreiber seinen Netzbetrieb an einen sogenannten Betriebsführer ausgelagert hat. Die Auswirkungen auf die Zertifizierung wurde u.a. in der BNetzA-Mitteilung „Mitteilung bezüglich der Zertifizierung nach dem IT-Sicherheitskatalog § 11 Abs. 1a EnWG im Falle der Betriebsführung durch Dritte“ vom 19.01.2021 konkretisiert.

In der BNetzA-Ankündigung „Ankündigung zur Zertifizierung unter Betriebsführung durch Dritte“ vom 13.12.2021 wird darauf verwiesen, dass „die Bundesnetzagentur bis heute nicht den erwarteten Rücklauf an gültigen Zertifikaten“ verzeichnet hat. Als Grund wird angegeben, „dass laut der Deutschen Akkreditierungsstelle GmbH ein betriebsgeführter Betreiber, welcher sich eines Betriebsführers auf vertraglicher Grundlage bedient, außer in bestimmten Ausnahmefällen nicht über seinen Betriebsführer mitzertifiziert werden kann.“

Aus diesem Grund wird in der BNetzA-Ankündigung ausgeführt, dass sich

- Netzbetreiber und
- Energieanlagenbetreiber

„eigenständig zertifizieren lassen“ müssen. Es werden also keine Ausnahmen mehr zugelassen. Gleichwohl kann der „Umfang der Zertifizierung [...] voraussichtlich reduziert werden [...]“, wenn

- der Betreiber den „operativen Betrieb an einen Betriebsführer auslagert“ hat und
- ein „Zertifikat gemäß IT- Sicherheitskatalog des Betriebsführers vorgewiesen werden“ kann.

3. Klare Begrifflichkeiten

Die datenschutz cert GmbH begrüßt die Klarstellung. Gerade im Hinblick auf die Sicherheit Kritischer Infrastrukturen ist es wichtig, dass sowohl Netz- als auch Energieanlagenbetreiber ein Informationssicherheits-Managementsystem (ISMS) einführen und zertifizieren lassen.

Aus Sicht der datenschutz cert GmbH ist es aber erforderlich, dass die verwendeten **Begriffe eindeutig definiert** werden müssen, insb. betrifft dies

- „betriebsgeführte Netzbetreiber“,
- „betriebsgeführte Betreiber“ und
- Betriebsführer – gerade in Abgrenzung zu anderen Dienstleistern.

Es muss eindeutig sein, **wann ein Dienstleister als Betriebsführer** gilt.

Zudem sollten die Adressaten – Netz- und Energieanlagenbetreiber – klarer genannt werden. In der BNetzA-Ankündigung werden als Adressaten genannt: „Betreiber von Energieversorgungsnetzen, die vom Geltungsbereich des IT-Sicherheitskatalogs gemäß § 11 Abs. 1a EnWG“ sowie „Betreiber von Energieanlagen, die nach der BSI-Kritisverordnung als kritische Infrastrukturen klassifiziert sind“.

Aus Sicht der datenschutz cert GmbH sollte deutlicher dargestellt werden, dass

- Netzbetreiber und
- Energieanlagenbetreiber

von den Regelungen adressiert werden. **Damit sind einschlägig**:

- IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG (Netzbetreiber);
- IT-Sicherheitskatalog gemäß § 11 Abs. 1b EnWG (Energieanlagenbetreiber).

4. Klare Problemexposition

Als Grund, weshalb die bisherige BNetzA-Regelung zur Betriebsführung durch Dritte nicht hinreichend umgesetzt wurde, wird genannt, dass sich ein „betriebsgeführter Betreiber“, welcher sich eines Betriebsführers auf vertraglicher Grundlage bedient, außer in bestimmten Ausnahmefällen nicht über seinen Betriebsführer mitzertifiziert werden kann.“

Es sollte klarer präzisiert werden, worin das Problem besteht. Auch sollte dargestellt werden, ob hier ein **grundsätzliches Problem** vorliegt oder von **Einzelfällen** die Rede ist.

5. Zertifizierungspflicht Betreiber

Die BNetzA-Ankündigung sieht nunmehr eine **Zertifizierungspflicht für alle Betreiber** vor – auch wenn der operative Betrieb an einen Betriebsführer ausgelagert wurde.

In diesem Zusammenhang sei darauf hingewiesen, dass ein Zertifikat gem. IT-Sicherheitskatalog ein Informationssicherheits-Managementsystem (ISMS) auszeichnet; ISO/IEC 27001 und ISO/IEC 27019 sind die Basis.

(Hinweis: Aus diesem Grund ist die Erläuterung „Die Bundesnetzagentur weist darauf hin, dass im Fall 1 Betreiber auch organisatorische Anforderungen unter anderem aus der Norm DIN EN ISO/IEC 27001 erfüllen müssten." eigentlich unnötig.)

Bei einem ISO/IEC 27001-konformen ISMS müssen aber gewisse **Assets zur Informationssicherheit** vorhanden sein. Wenn im Extremfall tatsächlich der komplette operative Betrieb ausgelagert ist und der Betreiber lediglich einen Vertrag mit seinem Betriebsführer hält, erscheint ein ISMS wenig zielführend. Denn hier wäre als Asset nur „ein Kraftwerk" und „ein Dienstleister" aufzunehmen; zudem hätte der Betreiber nur wenig Einfluss auf die Stabilität der Kritischen Infrastruktur. Auch wenn man an die anwendbaren Controls der Norm denkt, würden wahrscheinlich sehr viele ausgeschlossen werden, weil – wie ausgeführt – der komplette operative Betrieb dem Dienstleister obliegt. Es besteht die Gefahr, dass hier ein ISMS zu einer **leeren Hülle** verkommt.

Da in der Praxis sehr unterschiedliche Szenarien vorkommen können – der Arbeitsauftrag an den Dienstleister (Betriebsführer) also sehr stark variieren kann –, sind aus Sicht der datenschutz cert sehr **individuelle Bewertungen** erforderlich.

Dass es im Hinblick auf die generelle Zertifizierungspflicht von Betreibern auch Ausnahmen geben könnte, sieht auch die BNetzA-Ankündigung: „Die betroffenen Betreiber sollten prüfen, ob die eigene Unternehmensstruktur sowie personelle/sachliche Ausstattung die Anforderungen zur Implementierung eines Informationssicherheits-Managementsystems erfüllen können." Ein weiterer Hinweis: „Die Bundesnetzagentur ist bereit, weitere Möglichkeiten zur Nachweiserbringung im Zertifizierungsprozess in Betracht zu ziehen, sofern diese in Einklang mit den Zertifizierungsregelungen gebracht werden können."

Hierzu sind also weitere **Vorgaben erforderlich**.

6. Zertifizierungspflicht Betriebsführer

Mit der BNetzA-Ankündigung kommt zudem eine Art **Zertifizierungspflicht durch die Hintertür**, wenn ein Betreiber auf ein „Zertifikat gemäß IT- Sicherheitskatalog des Betriebsführers" verweisen kann.

Dies ist in zweierlei Hinsicht interessant:

1. Bislang gibt es überhaupt keine gesetzlichen Vorgaben an Betriebsführer – weder in den IT-Sicherheitskatalogen gem. §11 Abs. 1a oder 1b EnWG noch den zugehörigen Konformitätsbewertungsprogrammen.
2. Mehr noch schließen die gegenwärtig gültigen Konformitätsbewertungsprogramme die Zertifizierung von Betriebsführern – die kein Betreiber sind und keine BNetzA-Zulassungsnummer haben – explizit aus.

Nach den gegenwärtigen Vorgaben ist also ein „Zertifikat gemäß IT- Sicherheitskatalog des Betriebsführers" nicht möglich.

7. Verantwortung von Zertifizierungsstellen

Zu guter Letzt wird in der BNetzA-Ankündigung den akkreditieren Zertifizierungsstellen auferlegt, Einzelfragen mit Betreibern und Betriebsführern zu klären: „Detailfragen zum Zertifizierungsumfang sind mit den von der Deutschen Akkreditierungsstelle GmbH akkreditierten Zertifizierungsstellen individuell zu klären."

Aus Sicht der datenschutz cert – als bei der DAkkS akkreditierte Zertifizierungsstelle – sind dazu von den Behörden weitergehende Vorgaben erforderlich, insbesondere sind dies – wie oben ausgeführt – folgende Punkte:

- **Vorgaben, wann ein Dienstleister ein Betriebsführer ist;**
- **Erläuterung der bisherigen Probleme;**
- **Vorgaben zu möglichen Ausnahmen von der Zertifizierungspflicht für Betreiber;**
- **Vorgaben zur Zertifizierung von Betriebsführern.**

Zudem sollten die akkreditierten Zertifizierungsstellen in den Informationsfluss eingebunden werden.