TÜV SÜD Management Service

Mehr Wert.
Mehr Vertrauen.

Zertifizierung gemäß IT-Sicherheitskatalog

ISMS für Energienetzbetreiber

Eine dezentrale Stromerzeugung benötigt eine zuverlässige – und vor allem sichere – Netzsteuerung. Diese wiederum ist in hohem Maße von einer intakten Informations- und Kommunikationstechnologie (IKT) des Netzbetreibers abhängig. Deshalb hat die Bundesnetzagentur (BNetzA) im August 2015 den IT-Sicherheitskatalog für Energienetzbetreiber verabschiedet.

IT-Sicherheitskatalog für Energienetzbetreiber

Für Energienetzbetreiber hat die BNetzA gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz (EnWG) erarbeitet. Demnach müssen alle Strom- und Gasnetzbetreiber bis zum 31. Januar 2018 ein Informationssicherheits-Managementsystem (ISMS) auf Basis der um spezifische Aspekte aus der Netzsteuerung erweiterten ISO/IEC 27001 einführen und zertifizieren lassen. Mit der Konkretisierung der BNetzA werden die Anforderungen zunehmend klarer.

Konformitätsbewertungsprogramm der BNetzA bringt weitere Klarheit

Im April 2016 veröffentlichte die Bundesnetzagentur das Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen. Damit wurden die Anforderungen beschrieben, deren Erfüllung eine Zertifizierungsstelle für eine Akkreditierung nachweisen muss. Allerdings finden auch Energieversorger wichtige Hinweise darin. Jetzt ist sicher: Das Zertifizierungsschema nach dem IT-Sicherheitskatalog folgt wie erwartet den Normen ISO/IEC 27001 und ISO/IEC 27019. In der Veröffentlichung werden für die Zertifizierung folgende bedeutende Konkretisierungen festgelegt:
Das Risikomanagement der Organisation gemäß Abschnitt 6.1.3 und 8 der DIN ISO/IEC 27001 muss auch sämtliche Maßnahmen der DIN ISO/IEC TR 27019:2015-03; DIN SPEC 27019:2015-03 berücksichtigen. Das heißt, der Begriff „Anhang A“ in Abschnitt 6.1.3 ist als „Anhang A sowie sämtliche Maßnahmen der DIN ISO/IEC TR 27019:2015-03; DIN SPEC 27019:2015-03“ zu verstehen.

Die in den Normen genannten Maßnahmen sind also nicht zwingend vollständig umzusetzen, aber im Rahmen des Risikomanagements vollständig auf ihre Relevanz zu prüfen.

Der Auditumfang

Die Anforderungen der ISO/IEC 27006 sowie der ISO/IEC 17021-1 bezüglich der Auditdauer und der Wahl von Stichproben sowie der entsprechenden DAkkS-Regeln gelten, ergänzt um die folgenden Anforderungen.

1. Nicht dauerhaft besetzte Betriebsstätten werden zu geeigneten Gruppen zusammengefasst. Dabei ist die Relevanz der Standorte für das Gesamtnetz sowie die Möglichkeit der Ferneinwirkung über IKT auf diesen Standort zu berücksichtigen.

2. Eine Betriebsstätte, die Teil des Scopes ist, gilt als Standort, wenn sie zumindest an regulären Arbeitstagen mit Personal besetzt ist.

3. Es ist zulässig, bei der Auditierung eine Stichprobe der Standorte zu wählen. Hierbei sind die Vorgaben der ISO/IEC 27006:2015 zu beachten. Zusätzlich sind im Rahmen der Audits von jeder Gruppe der nicht dauerhaft besetzten Betriebsstätten, die Teil des Scopes sind, je Zertifizierungszyklus mindestens zwei Betriebsstätten zu auditieren.

4. Ergänzend zu den Vorgaben der ISO/IEC 27006:2015 ist bei der Wahl der Stichproben darauf zu achten, dass in der Gesamtheit der Stichproben eine gute netztopologische Abdeckung erzielt wird, also auch geographisch möglichst viele Teile des Scopes berücksichtigt werden.

5. Die Gesamtheit der Stichproben richtet sich nach folgenden Formeln:

- beim Erstzertifizierungsaudit:
  Stichprobe = √Standorte
- Beim Rezertifizierungsaudit:
  Stichprobe = 0,8 * √Standorte
- Beim Überwachungsaudit:
  Stichprobe = 0,6 * √Standorte

6. Für die Auditdauer gelten die Vorgaben von Anhang B der ISO/IEC 27006:2015. Die Formel zur Ermittlung der Auditdauer gemäß ISO/IEC 27006:2015 Anhang B.3.4 ist auf die besondere Situation der Netzbetreiber hin anzupassen, wobei neben den Standorten auch die Anzahl der nicht dauerhaftbesetzten Betriebsstätten zu berücksichtigen ist. In Abweichung zu ISO/IEC 27006:2015 Anhang B.3.5 ist eine Reduzierung der Auditdauer um höchstens zehn Prozent zulässig.

Ausblick und Empfehlung

Energienetzbetreiber können – so nicht bereits geschehen – jetzt mit der Einführung des ISMS auf der Basis der DIN ISO/IEC 27001 und gemäß des IT-Sicherheitskatalogs loslegen. Das ist eine ressourcenintensive Aufgabe. Als Projektdauer vom Planungsstart bis zur Zertifizierung lassen sich– je nach Ausgangslage – durchschnittlich 6 bis 24 Monate veranschlagen. Wichtig: Strom- und Gasnetzbetreiber müssen das ISMS nicht nur einführen, sondern auch die Wirksamkeit der Maßnahmen bestätigen, um sie im Audit nachweisen zu können. Darüber hinaus kommt es zum Ende der Deadline bei den Zertifizierern erfahrungsgemäß zu einem Terminstau. Eine freie Terminwahl ist zu früheren Zeitpunkten besser gewährleitet. Ein frühzeitiger Projektstart ist deshalb empfehlenswert.

TÜV SÜD Management Service GmbH Ridlerstrasse 57, 80339 München, Deutschland
Tel.: 0800 5791-5000 ms-anfragen@tuev-sued.de
www.tuev-sued.de/management-systeme/it-dienstleistungen/it-sicherheitskatalog