Zertifizierungspflicht von Energienetzbetreibern bei Betriebsführung durch Dritte

In einigen Fällen haben Energienetzbetreiber die Betriebsführung ihres Energieversorgungsnetzes an Dritte, den Betriebsführer, ausgelagert. Damit erlosch bisher in der Regel auch die Pflicht des Netzbetreibers eine eigene Zertifizierung nach dem IT-Sicherheitskatalog durchzuführen. Mit einem Schreiben hat die Bundesnetzagentur diese Netzbetreiber adressiert. In Zukunft müssen diese in der Regel selbst eine Zertifizierung nachweisen. Ausnahmen davon sind jedoch in einem begrenztem Umfang möglich.

Situation

Netzbetreiber müssen gemäß §11 Abs. 1a EnWG den Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sicherstellen. Der Nachweis erfolgt durch eine Zertifizierung gemäß den Vorgaben des „IT-Sicherheitskatalog gemäß § 11 Abs. 1a Energiewirtschaftsgesetz“ der Bundesnetzagentur.

Netzbetreiber, die den Betrieb Ihres Netzes ausgelagert haben, konnten bisher relativ einfach dieser oft lästige und immer kostenträchtige Pflicht entkommen. Zukünftig ist dies schwieriger geworden. Mit Recht weist die BNetzA darauf hin, dass Netzbetreiber in Zukunft grundsätzlich selbst zertifizieren müssen. Zum Teil folgt dies aus den allgemeingültigen Zertifizierungsvorgaben der ISO/IEC 17021. Dazu macht es durchaus Sinn, dass Netzbetreiber eine eigene Zertifizierung anstreben müssen, wenn zumindest Teilprozesse im Unternehmen angesiedelt sind, die in den Geltungsbereich der IT-Sicherheitskatalogs fallen. Ebenso wenn Netzbetreiber sich Durchgriffsrechte auf die Systeme oder Weisungsbefugnisse vorbehalten.

Konsequenz

Zukünftig müssen nicht nur die Betriebsführer, sondern auch Netzbetreiber, die den Netzbetrieb nicht so weit ausgelagert haben, dass sie nicht mehr zertifizierfähig sind, eine eigene Zertifizierung nach IT-Sicherheitskatalog nachweisen. Dabei ist zu beachten, dass die Verantwortlichkeiten und Weisungsbefugnisse des Netzbetreibers und des Betriebsführers genau zu den Geltungsbereichen der jeweiligen Geltungsbereiche der Zertifizierungen passen müssen.

In Zukunft müssen daher nicht nur der Betriebsführer sondern auch der Netzbetreiber eine eigene Zertifizierung nach IT-Sicherheitskatalog nachweisen, wenn Sie den Netzbetrieb nicht so weit ausgelagert haben, dass sie nicht mehr zertifizierfähig sind. Dabei ist zu beachten, dass die Verantwortlichkeiten und Weisungsbefugnisse des Netzbetreibers und des Betriebsführers genau zu den Geltungsbereichen der jeweiligen Geltungsbereiche der Zertifizierungen passen müssen.

In solchen und ähnlichen Fällen müssen die im Schreiben der BNetzA aufgeführten Kriterien geprüft und bewertet werden. Letztlich stellt sich die Frage, ob bei dem Netzbetreiber noch

etwas vorhanden ist, was in den Geltungsbereich der IT-Sicherheitskatalog Zertifizierung fällt. Diese Prüfung kann im Einzelfall durchaus komplex sein. Nach den Vorstellungen der BNetzA soll die Prüfung durch die Zertifizierungsstellen erfolgen. Diese sind derzeit dafür jedoch nicht vorbereitet. Aufgabe einer Zertifizierungsstelle ist es eine Firma danach zu beurteilen, ob sie die Anforderungen einer Norm erfüllt, und nicht, ob eine Norm unter gewissen Randbedingungen sinnvoll anwendbar ist.

Die Süd IT bietet daher Netzbetreibern an in Workshops die Situation zu analysieren und danach Lösungen zu suchen weiter der Zertifizierungspflicht zu entgehen oder, wenn gewünscht, auch eine Zertifizierung anzustreben.

Kontakt

Falls Sie noch Fragen zu dem Thema haben freue ich mich auf Ihre Kontaktaufnahme

Dr. Stefan Krempl
089 461 3505 12
krempl@sued-it.de

ISO/IEC 27001 Lead-Auditor im Auftrag des TÜV Rheinland, Lead-Auditor & Fachexperte IT-Sicherheitskatalog nach §11 Abs. 1a / 1b EnWG, Lead Auditor ISO 22301 Business Continuity Management, Auditor für kritische Infrastrukturen gemäß §8a BSIG, Datenschutzbeauftragter IHK, Datenschutzauditor ISO/IEC 27701