ISO/IEC 27001 Zertifizierung für kleine und mittlere Energieversorger

Energieversorger müssen unabhängig von Ihrer Größe eine Zertifizierung ihres Informationssicherheit-Managements nach ISO/IEC 27001 durchführen. Dazu sind sie nach dem IT-Sicherheitskatalog der Bundesnetzagentur (BNetzA) verpflichtet. Für kleinere Unternehmen bedeutet dies eine erhebliche Belastung. Wie können kleine Energieversorger die Zertifizierung vermeiden oder wie lassen sich die Kosten dafür senken?

Gemäß dem IT-Sicherheitskatalog der BNetzA müssen alle Energieversorger grundsätzlich bis Januar 2018 eine Zertifizierung nach ISO/IEC 27001 abgeschlossen haben. Für die größeren Stadtwerke und Energieversorger mit eigener Leitwarte ist das Thema klar und viele haben bereits begonnen sich auf eine Zertifizierung vorzubereiten. Für die ca. 1000 kleinen und mittelgroßen Energieversorger, mit zum Teil nur Tausend oder wenigen Hundert Kunden, stellt sich die Frage: „Muss ich Wirklich? Und wenn ja, wie kann ich die Kosten in einem vertretbaren Rahmen halten?

Wer muss Zertifizieren

Im Abschnitt D des IT-Sicherheitskataloges ist dessen Geltungsbereich beschrieben. Schon im ersten Satz ist klagestellt dass der Zweck des Kataloges die „Sicherstellung eines angemessenen Schutzes gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind“ ist. Im Umkehrschluss kann gefolgert werden, dass ein Energieversorger, der keine solchen Systeme betreibt, auch keine Zertifizierung durchführen muss. Im Wesentlichen lässt sich die Frage ob eine Zertifizierung erforderlich ist auf drei Kontrollfragen zurückführen:

1. Werden Schalthandlungen am Netz unter Verwendung von ITK-Systemen durchgeführt?
2. Würde der Ausfall von ITK Systemen die Sicherheit des Netzbetriebes gefährden?
3. Sind für die Wiederherstellung der Energieversorgung nach einem Schwarzfall ITK Systeme erforderlich?

Wenn zumindest eine dieser Fragen mit „Ja“ beantwortet wird, ist eine Zertifizierung erforderlich.

Kleine und kleinste Energieversorger

Wie z.B. auf der letzten Mitgliederversammlung der Einkaufsgemeinschaft Energieversorgungsunternehmen (EGEVU eG) ausführlich diskutiert, beantworten viele der kleinen und kleinsten Energieversorger alle Kontrollfragen mit Nein. Ob dies im Einzelfall jedoch tatsächlich zu einem Wegfall der Zertifizierungspflicht führt ist jedoch unklar, weil es noch keine Praxis hinsichtlich der Interpretation von verschiedenen Sachverhalten gibt. So

haben die meisten Energieversorger, aufgrund von Vorschriften des Erneuerbaren-Energien-Gesetzes (EEG), technische Vorrichtungen um die Leistung von z.B. Photovoltaikanlagen (PV) aus der Ferne zu drosseln. Die bedeutet eigentlich ein klares „Ja“ zu Kontrollfrage 2. Jedoch erfolgt die Leistungsregelung in der Regel über externe Dienstleister. Auch lässt sich nicht von der Hand weisen, dass, aufgrund der zumeist geringen Leistungen dieser PV Anlagen, diese für einen sicheren Netzbetrieb bedeutungslos sind. Selbst ein gleichzeitiges Versagen der Vorrichtungen zur Leistungsdrosselung bei allen ca. 500 klein- und kleinst-Betreibern ist für die Stabilität des Stromnetzes vermutlich ohne Bedeutung. Wie diese Umstände zu werten sind und ob sie tatsächlich zu einem Wegfall der Zertifizierungspflicht führen, sollten jetzt die entsprechenden Verbände der Energieversorger zusammen mit der BNetzA klären.

Kleine bis mittelgroße Energieversorger.

Ab einer gewissen Größe können und wollen die meisten Energieversorger nicht auf Fernwirktechnik zur Steuerung ihres Netzes verzichten. Damit ist eine Zertifizierung wohl zwingend erforderlich. Für Versorger mit vielleicht einigen wenigen Tausend angeschlossenen Verbrauchern bedeutet eine Zertifizierung jedoch einer erheblichen finanziellen Belastung. Selbst wenn die Aufwände im „Fotojahr“ 2016 getätigt werden und damit zu höheren Erlösen bei den Netzentgelten in der folgenden Regulierungsperiode führen.

Um die Aufwände so gering wie möglich zu halten, bietet sich ein Zusammenschluss von 2 bis maximal 5 Energieversorgern bei der Vorbereitung und Durchführung der Zertifizierung an. Wenn die Unternehmen ähnlich strukturiert und räumlich nicht zu weit getrennt sind, kann jedes einzelne Unternehmen bis zu 50 Prozent der externen Kosten einsparen. So können Vorbereitungs-Workshops gemeinsam abgehalten werden sowie gemeinsame Dokumente erarbeitet werden und damit auch interne Aufwände reduziert werden. Die größtmögliche Einsparung ergibt sich, wenn weitgehend identisch Managementsysteme aufgebaut werden. Nach einer Entscheidung der Deutschen Akkreditierungsstelle (DAKKS) vom Januar dieses Jahres eine gemeinsame Zertifizierung aber nicht mehr möglich.

Fazit

Kleine Energieversorger, die eine Chance sehen keine Zertifizierung machen zu müssen, sollten auf Ihre Verbände zugehen, damit diese mit der Bundesnetzagentur klären unter welchen Umständen auf eine Zertifizierung bei ihnen verzichtet werden kann. Sofern eine Zertifizierung unumgänglich ist, besteht die Möglichkeit durch einen Zusammenschluss mit anderen ähnlichen Energieversorgern Kosten zu sparen. Damit sollten sie aber nicht zu lange warten, damit die Kosten auch in 2016 wirksam werden und in den kommenden Jahren zu erhöhten Erlösen führen können.“

ISO/IEC 27001 Zertifizierung für kleine und mittlere Energieversorger

Über Süd-IT AG

Die Münchner Süd-IT AG unterstützt vor allem mittelständische Unternehmen im Bereich Zertifizierung, Compliance und Informations-Sicherheitsmanagement. Die Kernleistungen rund um Auditing, Beratung und Vorbereitung von ISO/IEC 27001-Zertifizierungen können von Anwendern jederzeit erweitert werden. Für Aufbau sowie Optimierung von ISMS, IT-Sicherheitssystemen und IT-Infrastrukturen stehen gegenwärtig über 250 hochkarätige Spezialisten bereit. Sie liefern Unternehmen u.a. aus den Marktsegmenten Automotive, Medizin, Energie und Dienstleistungen komplette Lösungen aus einer Hand. Dabei verfolgt die Süd-IT das Konzept „Ihre Experten vor Ort“ und ist daher mit mehreren Standorten im süddeutschen Raum sowie in Berlin und Rom kundennah aufgestellt.

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 27001 Auditor, Datenschutzbeauftragter