Pressemitteilung

SÜD-IT AG
Dr. Stefan Krempl
ISO 27001 Auditor, Datenschutzbeauftragter
Stahlgruberring 11
81829 München
Tel.: 089 461 3505 12
E-Mail: krempl@sued-it.de

INTERFACE FACTORS GmbH
Dr. Ralph Klöwer
Grünwalder Str. 1
81547 München
Tel.: 089-552688-66
E-Mail: SuedIT@interface-factors.de

Dr. Stefan Krempl, Süd-IT AG

IT-Sicherheitskatalog verabschiedet: Energieversorger sind ab sofort gefordert und müssen ihre IT-Sicherheit nach ISO/IEC 27001 zertifizieren

Die Deadline steht: Energieversorger sind verpflichtet, den effektiven Schutz ihrer IT-Infrastrukturen bis zum 31.1.2018 gemäß ISO/IEC 27001 nachzuweisen. Die betroffenen Unternehmen sollten ihre Planungen zeitnah starten, um Fristen problemlos einzuhalten und ein effektives Sicherheitsmanagement einzuführen, das für sie auch betriebswirtschaftlich adäquat ist.

München, 24.08.2015 – Nach mehrjähriger Beratung hat die Bundesnetzagentur (BNetzA) den IT-Sicherheitskatalog für Energieversorger gemäß §11 Abs. 1a des Energiewirtschaftsgesetzes (EnWG) veröffentlicht. Damit steht jetzt der 31.1.2018 als Termin fest, bis zu dem die Urkunde der ISO/IEC 27001 Zertifizierung bei der BNetzA eingegangen sein muss. Diese Anforderung präzisiert das im Juni verabschiedete IT-Sicherheitsgesetz, das bereits auf den Katalog verwiesen hatte. Energieversorger haben damit Klarheit über ihre Aufgaben und sind gleichzeitig in der Pflicht. Hier gilt: Wer unverzüglich mit den Planungen für das Zertifizierungsprojekt beginnt, hat einen deutlichen Vorsprung beim Aufbau des geforderten Informationssicherheits-Managementsystems (ISMS). Bei frühzeitiger Projektplanung bleibt Energieversorgern – über die Normerfüllung hinaus – genug Spielraum, ihr ISMS nach betriebswirtschaftlichen, organisatorischen und individuellen Leistungskriterien einzurichten. Damit lässt sich die ISO/IEC 27001 Zertifizierung auch als Chance nutzen, um Prozesse kontrollierter und produktiver zu gestalten. Im Ergebnis können Energieversorger von einem starken Schutz ihrer Geschäftsmodelle und einem kostengünstig handhabbaren Sicherheitsmanagement dauerhaft profitieren.

IT-Sicherheitskatalog schafft Klarheit

Die Veröffentlichung des IT-Sicherheitskatalogs hat insgesamt mehr Klarheit gebracht: Eindeutiger geregelt sind neben der Fristsetzung nun auch wichtige Details, wie der Geltungsbereich des IT-Sicherheitsgesetzes.

Wer muss die Zertifizierung durchführen?

Energieversorger sind in aller Regel zur ISO/IEC 27001 Zertifizierung verpflichtet. Das geht aus dem IT-Sicherheitskatalog[1] hervor, der in Abschnitt D definiert, welche Einrichtungen in den Geltungsbereich fallen. Dieser umfasst insbesondere „alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind". Darin enthalten sind alle TK- und EDV-Systeme (ITK), die als integraler Teil der Netzsteuerung Einfluss auf die Netzfahrweise nehmen. Ebenso gilt das für alle ITK-Systeme, die zwar nicht direkt zur Netzsteuerung gehören, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte.

Besonders kleinere Energieversorger fragen sich, ob Sie damit unter die Regelung fallen und zertifizierungspflichtig sind. Dies lässt sich anhand von drei Kontrollfragen beantworten:

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

Wenn eine dieser Fragen mit „Ja" beantwortet wird, ist eine Zertifizierung erforderlich. Energieversorger, die weiterhin unsicher sind, sollten ihre Verpflichtung – z.B. mit Zertifizierungs- und Sicherheitsspezialisten – möglichst zeitnah klären.

Was muss zertifiziert werden?

Gegenstand der Zertifizierung ist vorrangig der Bereich der Netzsteuerung, also typischer Weise die Netzleitwarte sowie angeschlossene Mess- und Steuereinrichtungen. Im Fokus stehen ebenso die wichtigsten unterstützenden Prozesse, darunter IT-Administration und Personalwesen. Entferntere Bereiche wie Abrechnung oder Kundenpflege müssen dagegen nicht zwingend mitbetrachtet werden. Für den Bereich der Smart-Meter stellt der IT-Sicherheitskatalog keine neuen Anforderungen an eine Zertifizierung – hier gelten weiterhin die Verpflichtungen aus dem EnWG (§21) sowie den Schutzprofilen des BSI.

Empfehlungen der Süd-IT für die Zeit- und Projektplanung

Aus der Frist zur Abgabe der Zertifizierungsbestätigung (31.01.2018) lässt sich rückwärts berechnen, wann das Projekt zur Vorbereitung der ISO/IEC 27001 Zertifizierung spätestens starten muss. Da die Ausfertigung der Bestätigung durch den akkreditierten Zertifizierer in aller Regel mehrere Wochen dauert, sollte die Zertifizierung in jedem Fall vor Weihnachten 2017 erfolgen. Um Probleme im „Finalen Run" auf den Endtermin zu vermeiden, wäre der Zertifizierungsaudit daher spätestens bis Ende September 2017 durchzuführen. Da nach den Vorgaben der ISO/IEC 27001:2013 das ISMS vor der Zertifizierung „gelebt werden" sollte, ist ein ISMS-Aufbau zumindest 9 Monate vor der Zertifizierung anzuraten. Damit das gelingt, ist die Projektplanung dafür idealerweise bis Mitte/Ende 2016 abgeschlossen.

Daraus resultieren folgende Handlungsempfehlungen an die betroffenen Energieversorger:

1. Am praktikabelsten ist es, die Planungen des Zertifizierungsprojekts mit einer Ist-Aufnahme und Abschätzung des Gesamtaufwandes zu starten.

[1] http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html

2. Die Ist-Aufnahme und Aufwandschätzung wird am besten noch in diesem Jahr durchgeführt, um die erforderlichen Mittel in den Wirtschaftsplan 2016/17 einstellen zu können.
3. Energieversorger sollten zügig einen Ansprechpartner für die Koordination und Kommunikation der IT-Sicherheit benennen. Hier gilt eine Frist bis zum 30.11.2015 für die Meldung der Kontaktdaten an die BNetzA. Energieversorger, die nach IT-Sicherheitsgesetz zu den kritischen Infrastrukturen und damit zu den 2000 wichtigsten Infrastrukturprovidern der Republik zählen, müssen vorher noch eine Sicherheitsüberprüfung des Ansprechpartners nach dem Sicherheitsüberprüfungsgesetz (SÜG) einplanen.

Fazit von Dr. Stefan Krempl, ISO 27001 Auditor bei der Süd-IT AG:
„Der IT-Sicherheitskatalog setzt Energieversorgern eine anspruchsvolle, aber faire Frist. Jetzt kommt es darauf an, das Zertifizierungsprojekt zügig einzuleiten: Denn je großzügiger die Zeitplanung, desto mehr Optionen haben Energieversorger, ihre Verpflichtungen zu erfüllen und gleichzeitig betriebswirtschaftlichen Gesichtspunkten Rechnung zu tragen. Denn letztlich sollten Unternehmen über die reine Zertifizierung hinaus von einem praktikablen Sicherheitsmanagement profitieren, das den Kapital- und Personaleinsatz so gering wie möglich hält."

***

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.