Zum Geltungsbereich einer ISO/IEC ISO 27001 Zertifizierung für Energieversorger unter Berücksichtigung der ISO/IEC TR 27019, den Vorgaben der IT-Sicherheitsgesetzes und des IT-Sicherheitskataloges der BNetzA

Code	-
Version	0.7
Datum	22.06.2015
Ersteller	Dr. Stefan Krempl
Freigegeben durch	Dr. Stefan Krempl
Vertraulichkeitsstufe	Intern + Vertrieb

Inhaltsverzeichnis

Über dieses Dokument

Historie

Datum	Bearbeiter	Beschreibung	Seiten
19.06.2015	Dr. Krempl	Ersterstellung	Alle
22.06.2015	Dr. Krempl	Überarbeitung	Alle

Referenzdokumente

Dokument
ISO 27001:2013
ISO/IEC TR 27019:2013 (Din Spek 27009)
IT-Sicherheitsgesetz
Entwurfsfassung des IT-Sicherheitskatalogs nach §11 1a des EnWG

Zweck

Der Zweck dieses Dokuments ist eine Orientierungshilfe zur Notwendigkeit und zum Geltungsbereich einer Zertifizierung nach ISO/IEC 27001 unter Berücksichtigung der ISO/IEC 27019 für Energieversorger zu geben. Dazu werden verschiedenen Informationsquellen analysiert und die wesentlichen Textstellen wiedergegeben.

Änderungen durch das IT-Sicherheitsgesetz sind in den Zitaten gelb hervorgehoben, wichtige Stellen durch Unterstreichen.

Zusammenfassung

Geltungsbereich

Für die Definition des Geltungsbereichs (Scope) könnten nach den vorliegenden Informationen etwa folgende Formulierungen geeignet sein

1. Planung, Aufbau, Betrieb und Wartung von Telekommunikations- und elektronischen Datenverarbeitungssysteme für einen sicheren Netzbetrieb der Elektrizitäts-/Gasversorgung...

2. Der sichere und zuverlässige Betrieb der Leitstelle und der angeschlossenen Infrastruktur der Stadtwerke XY

3. Sicherer Betrieb einschließlich Planung, Aufbau, und Wartung der Systeme der Prozesssteuerung der Energieversorgung die zur Steuerung und Überwachung von Erzeugung, Übertragung, Speicherung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen dienen.

Letztlich ist davon auszugehen, dass zumindest alle in dem unter Anwendungsbereich in der ISO/IEC TR 27009 genannten Einrichtungen (siehe 1 Anwendungsbereich) im Anwendungsbereich bzw. Scope der Zertifizierung einzuschließen sind. Eine Ausnahme bilden dabei laut Entwurfsfassung des IT-Sicherheitskataloges die Messsysteme der Letztverbraucher für die auch bereits die Schutzprofile BSI-CC-PP-0073/BSI-CC-PP-0077 vorliegen.

Notwendigkeit einer Zertifizierung

Nach Verabschiedung des IT-Sicherheitsgesetzes ist damit zu rechnen, dass auch kurzfristig der IT-Sicherheitskatalog nach §11 Absatz 1a der BNetzA in Kraft tritt, das dieser im Gesetz explizit erwähnt wird. Die Kernforderung des IT-Sicherheitskataloges ist eine Zertifizierung der Unternehmen nach ISO/IEC 27001.

Es ist somit davon auszugehen, dass Energieversorger, die

- unter das EnWG fallen und
- DV- oder Telekommunikationsanlagen betreiben, die der Steuerung oder Überwachung der Netze dienen

mittelfristig eine ISO 27001 Zertifizierung durchführen müssen.

Unter die oben erwähnten DV- und Telko-Anlagen fallen auch Zitat[1]:„Messeinrichtungen an Trafo- oder Netzkoppelstationen, welche durch die Bereitstellung von (Mess-)Daten einen direkten Einfluss auf die Netzsteuerung nehmen. Und Zitat:“Der Anwendungsbereich des IT-Sicherheitskatalogs erstreckt sich demnach auf Netzkomponenten oder Teilsysteme, die steuerbar sind und somit die Fahrweise des Netzes unmittelbar beeinflussen, oder aber Netzkomponenten, die selbst zwar nicht steuerbar sind, aber beispielsweise durch Bereitstellung von Daten mittelbar die Netzfahrweise beeinflussen und auf diese Weise auch der Netzsteuerung dienlich sind“.

[1] IT-Sicherheitskatalog BNetzA Entwurfsfassung S.8

Zitate

Aus EnWG

§ 11 Betrieb von Energieversorgungsnetzen

(1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, ~~die der Netzsteuerung dienen~~ die für einen sicheren Netzbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes ~~wird vermutet~~ liegt vor, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Regulierungsbehörde überprüft werden. ~~Die Regulierungsbehörde kann durch Festlegung im Verfahren nach § 29 Absatz 1 nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 3 treffen~~ Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 4 treffen.

Aus IT-Sicherheitskatalog der BNetzA

D.TK- und EDV-Systeme zur Netzsteuerung

Der sachliche Rahmen des IT-Sicherheitskataloges umfasst gemäß § 11 Abs. 1a Satz 1 EnWG einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, ~~die der Netzsteuerung dienen~~ die für einen sicheren Netzbetrieb notwendig sind. Um die sich daraus ableitenden Sicherheitsanforderungen für die verschiedenen Betreiber von Energieversorgungsnetzen im Einzelnen zu ermitteln, bedarf es einer an den Schutzzielen ausgerichteten Vorgehensweise zur Identifizierung der betroffenen TK- und EDV-Systeme, die der Netzsteuerung dienlich sind, in Abgrenzung zum übrigen Netzbetrieb.

Die Netzsteuerungsdienlichkeit ist somit von besonderer Bedeutung. Netzsteuerung im Sinne dieses IT-Sicherheitskataloges bedeutet unter Zugrundelegung der oben benannten Schutzziele die unmittelbare Einflussnahme auf die Fahrweise von Transport- und Verteil- netzen im Strom- und Gasbereich. Dieser IT-Sicherheitskatalog umfasst demnach zum einen alle TK- und EDV-Systeme des Netzbetreibers, welche direkt Teil der Netzsteuerung sind, d.h. unmittelbar Einfluss nehmen auf die Netzfahrweise. Darunter fallen zum Beispiel zentrale Netzleit- und Netzführungssysteme. Im Hinblick auf die weitergehende Eigenschaft der Netzsteuerungsdienlichkeit können aber auch TK- und EDV-Systeme im Netz betroffen sein, die selbst zwar nicht direkt Teil der Netzsteuerung sind, dieser aber unmittelbar dienen. Dar- unter fallen z.B. Messeinrichtungen an Trafo- oder Netzkoppelstationen, welche durch die Bereitstellung von (Mess-)Daten einen direkten Einfluss auf die Netzsteuerung nehmen. Da- von abzugrenzen sind TK- und EDV-Systeme, die nur mittelbaren oder gar keinen Einfluss auf die Netzsteuerung ausüben oder Systeme, die nicht Teil des Energieversorgungsnetzes nach § 3 Nr. 16 EnWG sind. Zu diesen nicht vom IT-Sicherheitskatalog umfassten Systemen gehören zum Beispiel kundenseitige Messsysteme gemäß § 21d EnWG (Smart Meter).

Zwar können Messsysteme der Letztverbraucher mittelbar Einfluss auf die Netzsteuerung ausüben, indem sie Netzzustandsinformationen (z.B. Spannung, Frequenz und Phasenwinkel) bereitstellen sowie netzindizierte Schalthandlungen ermöglichen. Allerdings sind diese nicht Teil des Energieversorgungsnetzes nach § 3 Nr. 16 EnWG. Die Kommunikationseinheit des Messsystems

(Smart Meter Gateway) ist zudem durch die Vorgaben der BSI-Schutzprofile (BSI-CC-PP-0073/BSI-CC-PP-0077) und die zugehörige Technische Richtlinie (BSI TR-03109) bereits hinreichend geschützt.

Der Anwendungsbereich des IT-Sicherheitskatalogs erstreckt sich demnach auf Netzkomponenten oder Teilsysteme, die steuerbar sind und somit die Fahrweise des Netzes unmittelbar beeinflussen, oder aber Netzkomponenten, die selbst zwar nicht steuerbar sind, aber beispielsweise durch Bereitstellung von Daten mittelbar die Netzfahrweise beeinflussen und auf diese Weise auch der Netzsteuerung dienlich sind.

Die Ermittlung der im Einzelfall betroffenen (Teil-)Systeme eines Netzes erfolgt durch den jeweiligen Netzbetreiber selbst unter Beachtung der in diesem IT-Sicherheitskatalog vorgegebenen Kriterien. Werden (Teil-)Systeme, die der Anwendung des Katalogs unterliegen, nicht vom Netzbetreiber selbst betrieben, sondern von Dritten, beispielsweise im Rahmen von Outsourcing, so ist die Anwendung und Umsetzung des Katalogs vertraglich sicherzustellen. Die volle Verantwortung in Bezug auf die Einhaltung des Katalogs bleibt dabei beim Betreiber des Energieversorgungsnetzes.

Aus Erfahrungsaustausch TÜV-Auditoren

Definition des Anwendungsbereichs

- Der Scope braucht „Fleisch und Blut“, also auch Mitarbeiter und Leben drumherum Da die ISMS ein Managementprozess ist, muss der Scope bestenfalls ein Prozess und kein „Ding“ sein.
- „Leitstelle“ als Scope wäre nicht optimal, besser wäre „Der sichere und zuverlässige Betrieb der Leitstelle und der angeschlossenen Infrastruktur der Stadtwerke XY“
- Formulierung unter Berücksichtigung des Geschäfts, der Organisation, des Standortes, der Assets, der Technologie ▪

Grenzen des ISMS

- Räumliche, logische, technische, organisatorische Trennung –
- z.B. nur Leitstelle (Technik, Orga, Prozesse, Personal)

Rechtfertigung von Ausschlüssen und Grenzen, Umgang mit den (externen) Schnittstellen

Schnittstellen zur Sicherheitsorganisation außerhalb des Scopes

- IS-Verantwortung außerhalb des Scopes
- Identifikation der externen Schnittstellen (technisch, organisatorisch)
- Schnittstellen als Risiken -
- Risikoanalysen bei Schnittstellen mit hohem Schutzbedarf
- Umgang mit Risiken; Scope ausdehnen oder Risiken isolieren?

Beteiligte Mitarbeiter

- Leistungserbringung des Scopes - Mitarbeiter im Scope
- Externe Mitarbeiter, Partner, Stellen
- Weitere Beteiligte im Unternehmen

Übertragung des Scope in die SOA

- Plausibilität beim Vergleich von Scope und SOA
- Möglichst keine Punkte in der SOA, welche im Scope nicht betrachtet wurden

Aus ISO 27019 (Din Spek 27009)

Einleitung

Diese Spezifikation definiert auf Basis des Standards DIN ISO/IEC 27002:2008-09 „Leitfaden für das Informationssicherheits-Management“ Umsetzungsanleitungen zur Realisierung von Informationssicherheits-Maßnahmen im Rahmen eines Informationssicherheits-Managements für Prozesssteuerungssysteme der Energieversorgung. Das Ziel dieser Arbeit ist die Erweiterung der ISO/IEC 27000-Standards auf den Bereich der Prozessleit- und Automatisierungstechnik der Energieversorgung, um die Implementierung eines einheitlichen Informationssicherheits-Managementsystems (ISMS) auf Basis des Standards DIN ISO/IEC 27001 für das gesamte Unternehmen, von der Geschäfts- bis hin zu Prozessebene, zu ermöglichen.

Im Fokus der Anwendung dieses Standards sind Systeme und Netzwerke zur Steuerung und Überwachung von Erzeugung, Übertragung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen. Dies umfasst die Leit- und Automatisierungssysteme, die Schutz- und Safetysysteme sowie die Messtechnik inklusive der zugehörigen Kommunikations- und Fernwirktechnik. Diese Systeme werden im Folgenden unter dem vereinfachten Oberbegriff „Prozesssteuerungssysteme“ zusammengefasst.

...

1 Anwendungsbereich

Der Anwendungsbereich dieser Spezifikation umfasst die Systeme der Prozesssteuerung der Energieversorgung die zur Steuerung und Überwachung von Erzeugung, Übertragung, Speicherung und Verteilung von Strom, Gas und Wärme in Kombination mit der Steuerung von unterstützenden Prozessen dienen. Dies umfasst insbesondere die folgenden Systeme, Anwendungen und Komponenten:

- die gesamte IT-gestützte zentrale und dezentrale Prozess-, Leit-, Automatisierungs- und Überwachungstechnik sowie die für ihren Betrieb genutzten IT-Systeme, wie z. B. Programmier- und Parametriergeräte;
- Digitale Steuerungs- und Automatisierungskomponenten wie Leit- und Feldgeräte, Controller oder SPSen inklusive digitaler Sensor- und Aktorelemente;
- alle weiteren in der Prozesstechnik genutzten unterstützenden IT-Systeme, sei es für ergänzende Aufgaben der Visualisierung und Steuerung, zur Überwachung oder zur Archivierung und Dokumentation;
- die gesamte in der Prozesstechnik zur IT-Kommunikation eingesetzte Netzwerk-, Telemetrie-, Fernwirk- und Fernsteuertechnik;
- Digitale Mess- und Zählvorrichtungen, z. B. zur Verbrauchs- und Emmissionswerterfassung;
- Digitale Schutz- und Safetysysteme, z. B. Schutzgeräte oder Maschinenschutzkomponenten;
- verteilte Komponenten zukünftiger Smart-Grid-Umgebungen;
- alle Programme und Anwendungen, die auf den vorgenannten Systemen eingesetzt werden;
  Nicht im Geltungsbereich dieser Spezifikation ist die konventionelle bzw. klassische Prozesstechnik d.h. nicht- digitale, rein elektromechanische oder elektronische Überwachungs- und Prozesssteuerungssysteme.

Telekommunikationssysteme und die Nachrichtentechnik, die im Umfeld der Prozesssteuerung eingesetzt werden, sind ebenfalls nicht im direkten Anwendungsbereich dieser Spezifikation. Sie werden durch den Standard ISO/IEC 27011 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002:2005 abgedeckt. Anwendern dieser Spezifikation wird empfohlen, die dort definierten Maßnahmenempfehlungen für die im Umfeld der Prozesssteuerung eingesetzten Telekommunikations- und Nachrichtentechniksysteme umzusetzen.

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