Der finale Countdown des IT-Sicherheitskataloges nach § 11 Absatz 1b EnWG

Stefan Loubichi

Abstract

The final countdown of the IT security catalogue according to § Section 11 paragraph 1b EnWG

With the IT-security catalogue issued in December 2018, the last chapter of implementing and certifying companies in the energy industry has begun. The operators of energy plants have to demonstrate successful certification until March 31, 2021. .

Not only the IT-security catalogue according to § 11 Ib EnWG must be proven, but also ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27019. Nuclear power plants are only exempt from certification, if they can successfully prove the adaption of the SEWD IT directive.

In this essay, we first show you who is really affected. Compared to the draft, there have been some significant changes. Another important change to the draft is, that appendix A of the Standard VGB-S-175 is no longer binding. As well the BDEW whitepaper is not binding.

Protection goals, risk objectives and risk handling are just as important to this IT security standard as protection zones are. All these concepts are discussed in this paper.

Unfortunately, the conformity assessment program for carrying out audits is currently not clearly defined. Thanks to the ISO/IEC 27006 and the experiences gained from the audits according to the security catalogue of § 11 Abs. 1a EnWG, it is nonetheless possible to predict how the audit will be like. The question of which evidence will be presented when in the audits is also discussed in this essay.

Furthermore, we present you a project plan for the implementation of the IT-security catalogue according to § 11 Ib EnWG in a period of 12 to 18 months.

All the before mentioned facts lead to the estimation that the implementation of the IT catalog will be a major but manageable challenge.

Autor

Prof. h.c. PhDr. Dipl.-Kfm./Dipl.-Vw. Stefan Loubichi
International experienced lead auditor for management systems
Kraftwerksschule Essen and Simulator Centre Essen (GfS mbH/KSG mbH), Essen, Deutschland

Mit dem im Dezember 2018 veröffentlichten IT Sicherheitskatalog hat das letzte Kapitel in Sachen Implementierung und Zertifizierung für Unternehmen der Energiewirtschaft begonnen. Die Betreiber der Energieanlagen müssen bis zum 31. März 2021 eine erfolgreiche Zertifizierung nachweisen.

Dabei muss nicht nur der IT-Sicherheitskatalog nach § 11 Ib EnWG nachgewiesen werden, sondern auch die Normen ISO/IEC 27001, ISO/IEC 27002 sowie ISO/IEC 27019. Betreiber von Kernkraftwerken sind nur dann von der Zertifizierung ausgenommen, wenn sie die SEWD IT-Richtlinie (Störmaßnahmen oder sonstige Einwirkungen Dritter) erfolgreich nachweisen können.

In diesem Aufsatz zeigen wir Ihnen erst einmal, wer wirklich betroffen ist. Schließlich gab es hier im Vergleich zum Entwurf einige bedeutsame Änderungen. Eine weitere wichtige Veränderung besteht darin, dass der Anhang A des Standards VGB-S-175 nicht mehr verbindlich ist. Auch ist das entsprechende BDEW-Whitepaper (Bundesverband der Energie- und Wasserwirtschaft e. V.) entgegen Erwartungen einiger Protagonisten nicht als verbindlich erklärt worden.

Schutzziele, Risikoziele und Risikobehandlung sind in dem IT Sicherheitskatalog dabei genauso von Bedeutung wie Schutzzonen. All die zugehörigen Konzepte werden in diesem Aufsatz vorgestellt.

Leider ist derzeit das Konformitätsbewertungsprogramm zur Durchführung von Audits nicht eindeutig definiert. Dank der ISO/IEC 27006 und den Erfahrungen aus den Audits nach dem IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG ist aber vorsehbar, wie die Auditdurchführung sein wird. Die Frage, welche Nachweise wann in den Audits zu präsentieren sein werden, wird in diesem Aufsatz ebenfalls erörtert.

Des Weiteren stellen wir Ihnen einen Projektplan vor, mit dem Sie den IT-Sicherheitskatalog nach § 11 Abs. 1b EnWG („Energiewirtschaftsgesetz“; Gesetz über die Elektrizitäts- und Gasversorgung) in einem Zeitraum von 12 bis 18 Monaten implementieren können.

Alle diese vorstehend genannten Fakten führen dazu, dass die Umsetzung des IT-Sicherheitskataloges zu einer großen, aber bewältigbaren Herausforderung wird.

Die Fristen

Beginnen wir erst einmal mit den Fristen, welche von den Betreibern der Energieanlagen einzuhalten sind. Hier sind drei Fristen zu nennen und zu kennen:

28.02.2019:

Bis dahin ist ein/e Ansprechpartner/-in IT-Sicherheit inkl. Kommunikationsdaten an die nachfolgende E-Mail-Adresse zu melden: it-sicherheitskatalog@bnetza.de

Gemäß den Erfahrungen des IT-Sicherheitskataloges nach § 11 Abs. 1a EnWG sei darauf verwiesen, dass die Bundesnetzagentur die „ständige“ Erreichbarkeit auch (periodisch) überprüft.

30.06.2019:

Betreiber von Anlagen nach § 7 Abs. 1 AtG haben bis zu o.g. Zeitpunkt gegenüber der Bundesnetzagentur vorzulegen:

- Eine von der zuständigen Landesbehörde ausgestellte Bestätigung, dass die Schutzziele der SEWD Richtlinie IT eingehalten werden.
- Eine von der Geschäftsführung unterzeichnete Erklärung, dass auch die besonderen Schutzziele für Erzeugungsanlagen (B./II.1./1.) berücksichtigt (!) wurden.

Diese Nachweise sind jedoch nicht nur einmalig zum 30.06.2019, sondern jährlich zum Stichtag einzureichen.

31.03.2021:

Gegenüber der Bundesnetzagentur haben Betreiber von Energieanlagen, welche die Schwellenwerte laut BSI-KritisV (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz) erreichen oder überschreiten, durch Vorlage einer Kopie des Zertifikats einer von der DAkkS (Deutsche Akkreditierungsstelle GmbH) akkreditierten Zertifizierungsgesellschaft nachzuweisen, dass die Anforderungen des IT-Sicherheitskataloges nach § 11 Abs. 1b EnWG nachgewiesen sind. Auf die jährlichen Audits sei an dieser Stelle verwiesen.

Es sei an dieser Stelle auch darauf verwiesen, dass es nicht zutreffend ist, wonach ein Zertifikat nach ISO/IEC 27001 äquivalent hierzu sei oder dass Betreiber bei einem derartigen Zertifizierungsverfahren automatisch auch ein ISO/IEC 27001 Zertifikat erhalten.

Die Einzelheiten der Auditdurchführung sind der letzte fehlende Mosaikstein. Derzeit erarbeiten Deutsche Akkreditierungsstelle und Bundesnetzagentur ein entsprechendes Konformitätsbewertungsprogramm, welches sich aller Voraussicht nach an das Konformitätsbewertungsprogramm nach § 11 Abs. 1a EnWG anlehnen wird.

(Ausschließlicher) Herr der operativen Zertifizierungsverfahren wird die Deutsche Akkreditierungsstelle sein. Die Bundesnetzagentur wird hier keine Aktien im Spiel haben.

Wer ist betroffen?

Während im Entwurf des IT-Sicherheitskatalog vom Januar 2018 In Kapitel II des IT-Sicherheitskataloges nur auf:

- Erzeugungsanlagen gemäß Anhang 1, Teil 3 Nr.1.1.1 BSI-KritisV
- Gasspeicher gemäß Anlage 1, Teil 3 Nr. 2.1.2 BSI-KritisV

referenziert wurde, wird in der jetzt verabschiedeten Version des IT-Sicherheitskatalog Bezug genommen auf:

- Erzeugungsanlagen (Anhang 1, Teil 3 Nr. 1.1.1)
- Erzeugungsanlagen mit Wärmeauskopplung – KWK-Anlage (Anhang 1 Teil 3 Nr. 1.1.2)
- Dezentrale Energieerzeugungsanlagen (Anhang 1 Teil 3 Nr. 1.1.3)
- Speicheranlagen (Anhang 1 Teil 3 Nr. 1.1.4)
- Gasförderanlagen (Anhang 1 Teil 3 Nr. 2.1.1)
- Gasspeicher (Anhang 1 Teil 3 Nr. 2.1.2)

Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung sind jedoch bei Überschreiten des Schwellwertes der installierten Netto-Nennleistung (elektrisch) in Höhe von 420 MW nicht von der Zertifizierungspflicht befreit, sondern müssen sich nach § 8a BSI-Gesetz prüfen lassen.

Bemessungskriterium bei den Anlagen Nr. 1.1.1, 1.1.3 und 1.1.4 ist die installierte Netto-Nennleistung (elektrisch) in MW, bei 1.1.2 ist dies die direkt mit der Wärmeauskopplung verbundene elektrische Wirkleistung bei Wärmenennleistung ohne Kondensationsanteil. Der Schwellenwert bei den Anlagen Nr. 1.1.1 bis 1.1.4 ist jeweils 420 MW.

Bemessungskriterium bei Anlagen nach Nr. 2.1.1 ist die Energie des geförderten Gases in GWh/Jahr, bei 2.1.2 ist dies die entnommene Arbeit in GWh/Jahr. Schwellenwert ist in beiden Fällen 5.190 GWh/Jahr.

Aufgrund der besonderen Unkenntnis sei hier nochmals auf folgende wichtige Aspekte aus Anhang 1, Teil 1 der BSI-KritisV verwiesen:

- Eine Anlage gilt zum 1.4. des Kalenderjahres, das auf das Kalenderjahr folgt, in dem der Schwellenwert erstmals erreicht oder überschritten wurde, als Kritische Infrastruktur (Anhang 1, Teil 1, Nr. 2)
- Bei installierter Netto-Nennleistung ist auf den rechtlich und tatsächlich möglichen Betriebsumfang der durch denselben Betreiber betriebenen Anlage abzustellen (Anhang 1, Teil 1 Nr. 5). Gerade bei den erneuerbaren Energien ist dieser Sachverhalt von besonderer Relevanz.
- Von einer gemeinsamen Anlage, die als kritische Infrastruktur zu betrachten ist, spricht man, wenn ein enger räumlicher und betrieblicher Zusammenhang gegeben ist, d.h. wenn die Anlagen
  - auf demselben Betriebsgelände liegen
  - mit gemeinsamen Betriebseinrichtungen verbunden sind
  - einem vergleichbaren technischen Zweck dienen
  - unter gemeinsamer Leitung stehen.

Des Weiteren wurde bereits in der (im Energiesektor) teilweise nicht hinreichend zur Kenntnis genommenen ersten Verordnung zur Änderung der BSI-KritisV vom 21.6.2017 bzgl. der Anlagentypen auf folgende gesetzlichen Definitionen verwiesen:

- Erzeugungsanlagen:
  § 3 Nr. 18c Energiewirtschaftsgesetz
- Erzeugungsanlagen mit Wärmeauskopplung – KWK-Anlage:
  § 2 Nr. 14 Kraft-Wärme-Kopplungsgesetz
- Dezentrale Energieerzeugungsanlagen:
  § 3 Nr. 11 Energiewirtschaftsgesetz
- Gasspeicher:
  § 3 Nr. 31 Energiewirtschaftsgesetz

Die Definition der beiden anderen Anlagetypen erfolgte ohne Gesetzesnennung wie folgt:

Speicheranlage
Anlage zur Speicherung von elektrischer Energie
Gasförderanlage
Anlage zur Förderung von Erdgas aus einer Bohrung

Schutzziele

Allgemeine Schutzziele:

Die allgemeinen Schutzziele sind wie folgt im IT-Sicherheitskatalog definiert:

- Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten
- Integritätssicherstellung der verarbeiteten Informationen und Systeme
- Gewährleistung der Vertraulichkeit der mit den betrachteten Systemen verarbeiteten Informationen

In einer Trivialdefinition seien die vorstehend bezeichneten Ziele wie folgt im Sinne der Bundesnetzagentur definiert:

Verfügbarkeit = Die zu schützenden Systeme und Daten sind auf Verlangen einer berechtigten Einheit zugänglich und nutzbar zu machen.

Integrität = Richtigkeit und Vollständigkeit der verarbeiteten Daten sowie die korrekte Funktionsweise der Systeme

Vertraulichkeit = Schutz der Systeme und Daten vor unberechtigtem Zugriff durch Personen oder Prozesse

In diesem Kontext werden im Zertifizierungsverfahren natürlich die Redundanzen von ITK-Systemen (Informations- und Kommunikationstechnik) als auch die Funktionalität der Sicherungssysteme von ITK-Systeme geprüft werden müssen!

Besondere Schutzziele:

Für Erzeugungsanlagen (Anlagen im Sinne von Anhang 1, Teil 3 Nr. 1.1.1 bis 1.1.4 BSI-KritisV) sind folgende besondere Schutzziele festgelegt (Hier gab es im Vergleich zum Entwurf keinerlei Veränderungen):

- Bereitstellung von elektrischer Leistung entsprechend den kommunizierten Fahrplänen und vertraglichen Verpflichtungen im Rahmen der Maßnahmen gemäß § 13 Abs. 1 EnWG.
- Bereitstellung von elektrischer Leistung entsprechend der Anforderung des Übertragungsnetzbetreibers gemäß § 13 Abs. 2 EnWG und der Anforderung des Verteilnetzbetreibers gemäß § 13 Abs. 2 i. V. m. § 14 Abs. 1 EnWG.
- Bereitstellung von elektrischer Leistung zur Deckung des lebenswichtigen Bedarfs an Elektrizität entsprechend den Verfügungen des Lastverteilers gemäß § 1 Abs. 1 Nr. 1 Elektrizitätssicherungsverordnung i. V. m. § 1 Abs. 1 Energiesicherungsgesetz.
- Gewährleistung der Schwarzstartfähigkeit, sofern technisch möglich und vertraglich mit dem Übertragungsnetzbetreiber vereinbart, sowie die Unterstützung des Übertragungsnetzbetreibers beim Netzwiederaufbau.

Für Gasförderanlagen und Gasspeicher sind (Anlagen im Sinne von Anhang 1, Teil 3 Nr. 2.1.1 bis 2.1.2 BSI-KritisV) folgende besonderen Schutzziele festgelegt:

- Bereitstellung von Ausspeiseleistung bzw. Speicherkapazität entsprechend den kommunizierten der Speichernutzer und Ein- und Ausspeisung von Gasmengen entsprechend den vertraglichen Verpflichtungen im Rahmen der Maßnahmen gemäß § 16 Abs. 1 EnWG.
- Ein- und Ausspeisung von Gasmengen entsprechend den Anforderungen des Fernleitungsnetzbetreibers gemäß § 16 Abs. 2 EnWG und den Anforderungen des Verteilernetzbetreibers gemäß § 16 Abs. 2 i. V. m. § 16a EnWG.

– Ein- und Ausspeisung von Gasmengen zur Deckung des lebenswichtigen Bedarfs an Gas entsprechend den Verfügungen des Lastverteilers gemäß § 1 Abs. 1 Nr. 1 Gassicherungsverordnung i. V. m. § 1 Abs. 1 Energiesicherungsgesetz.

Das Zonenkonzept

Das (im Vergleich zum Entwurf gleichgebliebene) Zonenkonzept fordert, dass:
– Anwendungen,
– Systeme und
– Komponenten

in sechs verschiedene Zone eingeteilt werden, die eine unterschiedliche Bedeutung für einen sicheren Anlagenbetrieb haben. Dies setzt jedoch als erstes voraus, dass alle Elemente, d.h. auch Büro- und Verwaltungsinformationssysteme erst einmal erfasst werden müssen. Gerade bei verschiedenen SAP-Systemen ist es nämlich stets interessant zu sehen, wer letztlich doch wohin zugreifen kann.

Es findet sich im IT-Sicherheitskatalog kein explizites Verbot dahingehend, dass eine Zusammenfassung von Entitäten zu Gruppen nicht zulässig wäre, wobei natürlich sichergestellt sein müsste, dass eine Kennzeichnung und Rückverfolgbarkeit aller Entitäten einer Gruppe durch entsprechende Festlegungsmerkmale möglich wäre.

Nun zu den einzelnen Zonen:

ZONE 1:

-> zwingend notwendig für den sicheren Betrieb; relevante Aspekte:
– Fokus auf Verfügbarkeit des Systems bzw. der Funktionalität und auf die Integrität der Messungen und Signale zum Schutz von Menschen, Anlage und Umwelt
– Manipulation von Daten führt direkt zu Auswirkungen auf die angesteuerte Anlage
– Keine Ausfalltoleranz – Anlage schaltet sich bei Fehlfunktionen umgehend ab

ZONE 2:

-> dauerhaft notwendig für den Betrieb der Energieanlage; relevante Aspekte;
– Fokus auf Integrität der Messungen, Signale und Daten und der Verfügbarkeit des Systems bzw. der Funktion
– Manipulation der Daten kann indirekt zu falschen Bedienhandlungen führen
– Ausfalltoleranz: wenige Minuten bis eine Stunde – Anlage kann kurzfristig mit erhöhtem personellen Einsatz zur manuellen Überprüfung von Funktionalitäten, zur manuellen Steuerung oder Hand-Nachrechnung von Werten ohne Beeinträchtigung von Menschen, Anlage und Umwelt weiter betrieben werden

ZONE 3:

-> notwendig für den effizienten Betrieb der Energieanlage sowie zur Erfüllung der gesetzlichen Anforderungen; relevante Aspekte:
– Fokus auf Integrität der Daten
– Manipulation der Daten kann indirekt Auswirkungen auf die optimale Fahrweise der betriebenen Anlagen haben (Wirtschaftlichkeit, Umweltverträglichkeit, Verschleiß) und zu Rückwirkungen auf den sicheren Netzbetrieb führen
– Ausfalltoleranz: wenige Stunden – Anlage fährt mit reduziertem Wirkungsgrad, Netzdienstleistungen entfallen, Daten der Energieanlage sind extern nicht verfügbar, Instandhaltung ist erschwert oder nicht mehr möglich

ZONE 4:

-> bedingt notwendig für den kontinuierlichen Betrieb der Energieanlage; relevante Aspekte:
– Schutzbedarf dieser Systeme muss spezifisch ermittelt werden.
– Ausfalltoleranz: wenige Tage – sicherer Anlagenbetrieb bei Ausfall weiterhin möglich

ZONE 5:

-> notwendig für die organisatorischen Prozesse der Energieanlage; relevante Aspekte:
– Schutzbedarf dieser Systeme muss spezifisch ermittelt werden
– Ausfalltoleranz: eine Woche – sicherer Anlagenbetrieb bei Ausfall weiterhin möglich

ZONE 6:

-> bedingt notwendig für die Organisation der Prozesse der Energieanlage; relevante Aspekte:
– Schutzbedarf dieser Systeme muss spezifisch ermittelt werden
– Ausfalltoleranz: eine Woche – sicherer Anlagenbetrieb bei Ausfall weiterhin möglich

Für den Fall, dass es Anwendungen, Systeme und Komponenten gibt, welche mehreren Zonen zugeordnet werden können, so ist die für den sicheren Anlagenbetrieb bedeutsamere Zone die ausschlaggebende Zone.

Ausdrücklich wird darauf verwiesen, dass im IT-Sicherheitskatalog zwar auf das Zonenschaubild gemäß VGB Standard S 175 „IT-Sicherheit für Energieanlagen“ referenziert wird. Dieses Schaubild soll jedoch nur einen Anhaltspunkt für die Zoneneinteilung geben. Die exakten Kriterien finden sich ausschließlich in der textualen Fassung des IT-Sicherheitskataloges nach § 11 Ib EnWG.

Aus der Erfahrung aus dem Netzbereich sei darauf verwiesen, dass auch im Bereich des § 11 Ib EnWG hinsichtlich der Segmentierung von Geräten, Anwendungen und Netzen große Herausforderungen in den folgenden Bereichen liegen werden:
– Trennung von Office und Produktion
– Trennung von Anlagen-Subnetzen
– Zonenübergänge
– Funktechnologien
– Fernzugriffe
– Kryptographie
– Public-Key-Infrastrukturen (PKI)
– Kontrolle der Netzkommunikation

Sicherheitsanforderungen

Folgende Sicherheitsanforderungskategorien werden im IT-Sicherheitskatalog nach § 11 Abs. 1b EnWG benannt:
– Informationssicherheitsmanagementsystem
– Sicherheitskategorien und Maßnahmen
– Ordnungsgemäßer Betrieb der betroffenen ITK-Systeme
– Risikoeinschätzung
– Risikobehandlung
– Ansprechpartner/-in IT-Sicherheit

Informationssicherheitsmanagement system/Sicherheitskategorien und Maßnahmen:

In D.I. des IT-Sicherheitskataloges wird explizit verlangt, dass für Anwendungen, Systemen und Komponenten der Zonen 1-3 ein Informationssicherheitsmanagementsystem nach der High Level Structure Norm ISO/IEC 27001 implementiert sein muss. Eine Zertifizierung auch nach ISO/IEC 27001 ist nicht verlangt. Da viele Anlagenbetreiber bereits Managementsysteme nach den anderen High Level Structure Managementsystemen wie z.B. ISO 9001, ISO 14001 oder ISO 45001 haben, ist dies nicht so schwierig und im Rahmen eines integrierten Managementsystems zu realisieren.

Die Referenzmaßnahmenziele und -maßnahmen (=„Controls“) des normativen Anhangs A der ISO/IEC 27001 müssen bei jedem Unternehmen im Rahmen der SoA auf Anwendung geprüft werden. Wenn bestimmte Controls nicht anwendbar sind, so muss dies nachweisbar begründet werden.

In D.II des IT-Sicherheitskataloges ist festgelegt, dass bei der Implementierung des Informationssicherheitsmanagementsystems die nachfolgenden Normen berücksichtigt werden müssen:

ISO/IEC 27002: Leitfaden für Informationssicherheitsmaßnahmen

ISO/IEC 27019: Informationssicherheitsmaßnahmen für die Energieversorgung

In der ISO/IEC 27002 wird für jedes Control des normativen Anhangs A der ISO/IEC 27001 eine Anleitung zur Umsetzung sowie weitere Informationen gegeben.

In der ISO/IEC 27019 wird für jedes Control, welches für Energieversorger besondere Aspekte enthält, zusätzliche Umsetzungsanleitungen gegeben.

Wendet man wirklich stringent eine Kaskadierung von Anhang A der ISO/IEC 27001,

ISO/IEC 27002 und ISO/IEC 27019 an, so kann man bei der Umsetzung und Nachweisführung der vermeintlich so problematischen 114 Controls eigentlich keine sehr großen Fehler begehen.

Aus den Erfahrungswerten der Auditierung gemäß des IT-Sicherheitskataloges für Netzbetreiber (§ 11 Abs. 1a EnWG) sei darauf verwiesen, dass oftmals die speziellen Aspekte der Informationssicherheitsmanagementsysteme für Energieversorger, d.h. die ISO/IEC 27019, nur unzureichend berücksichtigt wurden. Aus diesem Grunde nachstehend eine Übersicht über diese Zusatzanforderungen:

- 6.1.6 Kontakt zu Behörden
- 6.1.7 Kontakt zu speziellen Interessengruppen
- 6.2.1 Identifizierung von Sicherheit im Umgang mit externen Mitarbeitern
- 6.2.2 Adressieren von Sicherheit im Umgang mit Kunden
- 6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten
- 7.1.1 Inventar der organisations-eigenen Werte (Assets)
- 7.1.2 Eigentum von organisations- eigenen Werten (Assets)
- 7.2.1 Regelung die Klassifizierung von Informationen
- 8.1.2 Sicherheitsüberprüfung
- 8.1.3 Arbeitsvertragsklauseln
- 8.1.1 Aufgaben und Verantwortlichkeiten
- 9.1 Sicherheitsbereiche
- 9.1.1 Sicherheitszonen
- 9.1.2 Zutrittskontrolle
- 9.1.7 Sichern von Leitstellen
- 9.1.8 Sicherung von Technikräumen
- 9.1.9 Sicherung von Außenstandorten
- 9.2.1 Platzierung und Schutz von Betriebsmitteln
- 9.2.2 Unterstützende Versorgungseinrichtung
- 9.2.3 Sicherheit der Verkabelung
- 9.3 Sicherheit in Räumlichkeiten Dritter
- 9.3.1 Betriebseinrichtung in Bereichen anderer Energieversorger
- 9.3.2 Betriebseinrichtung beim Kunden vor Ort
- 9.3.3 Gekoppelte Steuerungs- und Kommunikationssysteme
- 10.1 Verfahren und Verantwortlichkeiten
- 10.1.1 Dokumentierte Betriebsprozesse
- 10.1.4 Trennung von Entwicklungs-, Test- und Produktiveinrichtung
- 10.2.1 Integrität und Verfügbarkeit von Funktionen der Betriebssicherheit
- 10.4.1 Maßnahmen gegen Schadsoftware
- 10.4.2 Schutz vor mobiler Software (mobile Agenten)
- 10.6.3 Sicherung der Prozessdatenkommunikation
- 10.10 Überwachung
- 10.10.1 Auditprotokolle
- 10.10.6 Zeitsynchronisation
- 11.1 Geschäftsanforderungen für die Zugangskontrolle
- 11.1.1 Leitlinie zur Zugangskontrolle
- 11.3 Benutzerverantwortung
- 11.3.1 Passwortverwendung
- 11.4.5 Trennung in Netzen
- 11.4.8 Logische Anbindung von externen Prozesssteuerungssystemen
- 11.5 Zugriffskontrolle auf Betriebssysteme
- 11.5.1 Benutzeridentifikation und Authentisierung
- 11.5.5 Session Time-Out
- 12.1 Sicherheitsanforderungen von Informationssystemen
- 12.1.1 Analyse und Spezifikation von Sicherheitsanforderungen
- 12.4 Sicherheit von Systemdateien
- 12.4.1 Kontrolle von Software im Betrieb
- 14 Sicherstellung des Geschäftsbetriebs (BCM)
- 14.1. Informationssicherheitsaspekte beim BCM
- 14.1.1 Einbeziehung der Informationssicherheit in den BCM Prozess
- 14.2.1 Notfall-Kommunikation Maßnahme
- 15.1 Einhaltung gesetzlicher Vorgaben
- 15.1.1 Identifikation der anwendbaren Gesetze

Interessant ist sicherlich der nachfolgende Satz in D.II. des IT-Sicherheitskataloges: „Die Bundesnetzagentur behält sich vor, etwaige Anpassungen der genannten DIN-Normen in Bezug auf ihre Anwendbarkeit in regelmäßigen Abständen zu überprüfen.“ Die Bundesagentur hat in Bezug auf DIN-Normen jedoch nicht mehr, aber auch nicht weniger Rechte und Möglichkeiten wie jeder Bundesbürger/jede Bundesbürgerin, welche sich in Normierungsprozesse der DIN einbringen möchte.

Eine sehr wichtige Änderung in Bezug zum Entwurf des IT-Sicherheitskataloges ist die Frage, inwieweit der VGB-Standard „IT-Sicherheit für Erzeugungsanlagen (VGB-S-175) zu berücksichtigen ist. In der jetzigen Fassung des IT-Sicherheitskataloges hat sich die Verbform verändert.

In Normen und Gesetzen bezeichnet die Verbform:

„müssen“ eine Anforderung

„sollen“ eine Empfehlung (Nur bei untypischen Fällen“ darf entgegen der Empfehlung gehandelt werden

„dürfen“ eine Erlaubnis

„können“ eine Möglichkeit oder eine Fähigkeit

In der jetzigen Fassung des IT-Sicherheitskataloges heißt es jetzt nur noch, dass der VGB Standard Hilfestellung bei der Umsetzung des Informationssicherheitsmanagementsystems geben KANN. Es kann im Zertifizierungsverfahren somit nicht verlangt werden, dass ein Energieversorger den Nachweis erbringen muss, dass er VGB S 175 berücksichtigt hat. Dies gilt auch für das BDEW/OE – Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“, welches ebenfalls nicht nachweislich umgesetzt sein muss.

Ordnungsgemäßer Betrieb der betroffenen ITK-Systeme:

In D.III finden sich im Vergleich zum Entwurf nur redaktionelle Änderungen: Zu erfüllen sind folgende Anforderungen:

- Sicherstellung, dass der Betrieb der ITK-Systeme ordnungsgemäß erfolgt
- Bewertung der Risiken durch ITK-basierte Angriffe und Behandlung der Risiken durch geeignete Maßnahmen

Die Forderung der Bundesnetzagentur, dass technische Störungen der ITK-Systeme zu jeder Zeit erkannt und behoben werden können ist mehr frommer Wunsch denn realisierbar. Gemäß den Erfahrungen des Bundesamtes in der Sicherheitstechnik werden Angriffe oftmals erst nach Monaten erkannt. Verwiesen sei in diesem Falle zum Beispiel auf den erfolgreichen Angriff stattlicher Hacker auf den Deutschen Bundestag.

Risikoeinschätzung:

Analog zu den KRITIS relevanten Netzbetreibern müssen auch die Anlagenbetreiber sowohl eine Risikoeinschätzung (gemäß Normelement 6.1.2 der ISO/UEC 27001:2017) als auch eine Risikobehandlung (gemäß Normelement 6.1.3 der ISO/IEC 27001:2017) nachweisen.

Eine Risikoeinschätzung ist im Rahmen der Schadenskategorien:

- kritisch
- hoch
- mäßig
- gering

für alle erfassten Anwendungen, Systeme und Komponenten vorzunehmen.

Bei allen Anwendungen, Systemen und Komponenten, die für einen sicheren Anlagenbetrieb notwendig sind, ist per se mindestens von einer Einstufung in die Kategorie hoch auszugehen. Abweichungen hiervon sind stets ausführlich zu begründen und zu dokumentieren.

Folgende Kriterien müssen bei der Risikoeinschätzung mindestens berücksichtigt werden:

- Beeinträchtigung der Aufgabenerfüllung in Hinblick auf Einschränkung der Energielieferung und Versorgungsfreiheit
- Gefährdung für Leib und Leben
- Gefährdung für Datensicherheit und Datenschutz durch Offenlegung bzw. Manipulation
- finanzielle Auswirkungen

Im Entwurf des IT-Sicherheitskataloges wurde noch auf den betroffenen Bevölkerungsteil abgestellt, hiervon findet sich in der endgültigen Fassung nichts mehr.

Bei der Risikoeinschätzung sind wiederum folgende Faktoren [mindestens] zu berücksichtigen

I. Vorsätzliche Handlungen:
- gezielte IT-Angriffe
- Computer-Viren, Schadsoftware
- Abhören der Kommunikation
- Diebstahl von Rechnern etc.

II. Nichtvorsätzliche Gefährdungen:
- Elementare Gefährdungen
- Höhere Gewalt
- organisatorische Mängel
- menschliche Fehlhandlungen
- technisches Versagen
- Versagen oder Beeinträchtigung anderer für die Anlagensteuerung relevanter Infrastrukturen und externer Dienstleistungen
- Ungezielte Angriffe und Irrläufer von Schadsoftware

Eine Risikoeinschätzung nach ISO/IEC 27005 oder ISO 31000 wird nach wie vor nicht verlangt. Es wird lediglich hierauf verwiesen.

Risikobehandlung:

Die Risikobehandlung korreliert mit der Zoneneinteilung der Anwendungen, Systeme und Komponenten:
- Zone 1-3 allgemein:
  Es sind stets angemessene und geeignete Maßnahmen der Risikobehandlung im Sinne des Normelementes 6.1.3 der ISO/IEC 27001:2017 zu treffen.
- Zone 1-3:
  Für alle Anwendungen, Systemen und Komponenten der Zonen 1 bis 3 sind angemessene und geeignete Maßnahmen zur Risikoreduktion zu treffen.
- Zone 1 speziell:
  Ermittelte Risiken dürfen nicht akzeptiert werden. Maßnahmen zur Risikobehandlung sind hier zumindest soweit umzusetzen, bis lediglich ein als gering zu bewertendes Restrisiko verbleibt. Das Risikoniveau setzt sich dabei aus Schadenskategorie und Eintrittswahrscheinlichkeit zusammen.
- Zone 1-3 i.V.m. Zone 4-6:
  Bei Anwendungen, Systemen und Komponenten der Zonen 1-3, welche Informationen mit Zone 4-6 austauschen, welche für den sicheren Anlagenbetrieb benötigt werden, ist sicherzustellen, dass die allgemeinen Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit der Informationen gewahrt bleiben.

Eine Maßnahme ist im Sinne des IT-Sicherheitskatalog dann als angemessen anzusehen, wenn sie dem allgemein anerkannten Stand der Technik entspricht. Von Relevanz ist hier sicherlich die Formulierung in § 8a BSI-Gesetz, die wie folgt wiedergegeben wird:

„Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur steht."

Was Stand der Technik ist, wurde bereits im Grundsatzurteil des Bundesverfassungsgerichtes aus dem Jahr 1978 in Sachen des Schnellen Brüters in Kalkar festgehalten [BverfGE 49,86]: Der Stand der Technik ist mehr als die allgemein anerkannten Regeln der Technik, aber weniger als der Stand der Wissenschaft und Forschung. Dieser Sachverhalt wird jedoch oft von Zertifizierungsgesellschaften verkannt.

In Hinblick auf die Energieerzeuger, welche regenerative Quellen nutzen ist, sind in diesem Zusammenhang die folgenden Gesetze ausdrücklich zu beachten:
- § 9 EEG 2017 (Gesetz für den Ausbau erneuerbarer Energien)
- § 14 EEG
- § 20 EEG 2017

Der IT-Sicherheitskatalog verweist jedoch ausdrücklich darauf, dass es den Fall geben kann, dass auf den Stand der Technik nicht immer zurückgegriffen werden kann. Während es in Hinblick auf den IT-Bereich in der Regel einfach(er) ist, den Stand der Technik einzuhalten, so ist dies bei der Langlebigkeit der OT nicht immer der Fall. Für diesen Fall muss belegt werden, dass die jeweiligen ITK-Schutzziele dennoch erreicht werden können.

Ansprechpartner IT-Sicherheit:

Seit Inkrafttreten des IT-Sicherheitsgesetzes waren/sind kritische Infrastrukturen gemäß § 8a BSI-Gesetz verpflichtet, beim Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Kontaktstelle zu registrieren, über die der Betreiber dem BSI ITK-Störungen gemäß § 11 Abs. 1c EnWG meldet.

Hiervon zu unterscheiden ist die im IT-Sicherheitskatalog ausgesprochene Forderung, dass Betreiber gegenüber der Bundesnetzagentur eine/n Ansprechpartner für IT-Sicherheit (und eine Stellvertretung) benennen müssen, der/die stets unverzüglich Auskunft zu folgenden Punkten geben kann:
- Umsetzungsstand der Anforderungen aus dem IT-Sicherheitskatalog
- aufgetretene Sicherheitsvorfälle sowie Art und Umfang ggf. hervorgerufener Auswirkungen
- Ursache aufgetretener Sicherheitsvorfälle sowie Maßnahmen zu deren Behebung und zukünftigen Vermeidung

Somit kann es durchaus vorkommen, dass Meldungen sowohl gegenüber der Bundesnetzagentur als auch gegenüber dem Bundesamt für Sicherheit in der Informationstechnologie erfolgen müssen.

Auf die abweichenden Regelungen für Anlagen nach § 7 Absatz 1 des Atomgesetzes im Geltungsbereich des IT-Sicherheitskataloges wird nur insoweit eingegangen, als dass bereits durch die Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherheitskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT) bereits ein anlagenspezifisches Regelwerk vorliegt, dessen Schutzziele die kerntechnische Sicherheit bis dato gewährleistet haben.

Phasen-Konzept zur erfolgreichen zertifizierungsreifen Umsetzung

Spätestens seit der Veröffentlichung des Entwurfes des IT-Sicherheitskataloges im Januar 2018, d.h. vor 12 Monaten, haben viele Energieerzeuger mit der Implementierung begonnen. Es war in diesem Zusammenhang auch bereits logisch und vorhersehbar, dass man mit der Implementierung eines Informationssicherheitsmanagementsystems nach ISO/IEC 27001 in Verbindung mit ISO/IEC 27002 und ISO/IEC 27019 nichts falsch machen konnte und dass hierdurch bereits die Hauptarbeit getan sein würde.

Ausgehend von den Erfahrungen der Implementierung und Zertifizierung von Informationssicherheitsmanagementsystemen gemäß des IT-Sicherheitskataloges nach § 11 Abs. 1a EnWG und den Erfahrungen der Implementierung und Zertifizierung von Informationssicherheitsmanagementsystemen nach ISO/IEC 27001 in Verbindung mit ISO/IEC 27002 und ISO/IEC 27019 bei Energieerzeugern sei auf den nachfolgenden Projektplan zur Implementierung eines ISMS-Systems nach dem IT-Sicherheitskatalog gemäß § 11 Abs. 1b EnWG als gangbare Option verwiesen:

I. Ist-Aufnahme:
- Festlegung des Scopes
- Technische und organisatorische GAP-Analyse
- Auswertung der Analyse

II. Vorphase zur Implementierung:
- Erstellung/Aktualisierung der Assets
- Zoneneinteilung
- Durchführung der Risikoeinschätzung
- Festlegung der Risikobehandlung
- Erstellung der SoA

III. Implementierung:
- Implementierung der technischen Maßnahmen
- Implementierung der organisatorischen Maßnahmen
- Anfertigung der Dokumentation
- Durchführung von intensiven Schulungen für alle relevanten Personen

IV. Internes Audit/Vorbereitung auf das externe Audit:
- Überprüfung der implementierten technischen Maßnahmen
- Überprüfung der implementierten organisatorischen Maßnahmen

– Durchführung eines internen Audits
– Nichtkonformitäten, Korrekturen und kontinuierliche Verbesserung
– Erstellung des Managementreviews

Hierfür werden die Anlagenbetreiber in der Regel 12-18 Monate benötigen.

Es wird darauf verwiesen, dass es natürlich viele weitere Möglichkeiten der Implementierung gibt.

Aspekte der Dritt-Zertifizierung des IT-Sicherheitskataloges

Auch wenn mit der ISO/IEC 27006 eine spezielle Norm für die Auditierung von ISO 27001 Managementsystemen existiert, so wird aufgrund des IT-Sicherheitskataloges nach § 11 Absatz 1b EnWG von der BNetzA und der DAkkS ein Konformitätsbewertungsprogramm festgelegt werden, dass die zu erfüllenden Parameter zur Auditdurchführung sowie Zusatzanforderungen für Auditoren (noch) festlegt.

Es wird aus den Vergangenheitserfahrungswerten eine Zertifizierung gemäß nachfolgendem Schema erwartet:

Phase 0: Vor dem Audit der Stufe 1

Vor dem Audit müssen gegenüber der KBS mindestens folgende Nachweise präsentiert werden:
– Zertifizierungsantrag
– Geltungsbereich
– Informationssysteme im Geltungsbereich inkl. Kategorisierung und Signifikanz
– Organigramm
– Liste der Werte mit Angabe des Risikos
– Erklärung zur Anwendbarkeit (SOA)
– Vollzeitäquivalente im Geltungsbereich
– Standorte im Geltungsbereich
– Unternehmensbeschreibung

Hinweis:

Außer den Punkten 3., 5. und 6. müssten die anderen Punkte bei anderen Bezugsnormen auch angegeben werden

Phase 1: Audit der Stufe 1

Im Rahmen des Audits der Stufe 1 sind zumindest folgende Nachweise für die KBS vorzuhalten:
– MS Handbuch nebst allen mitgeltenden Dokumenten
– Dokumentation in Sachen Kontext der Organisation
– Dokumentation in Sachen Risikobewertung und -behandlung
– Prozesslandkarte
– Netzstrukturplan
– Verantwortlichkeitsmatrix
– Liste der Werte mit entsprechender Klassifizierung und Bewertung
– Managementbewertung
– Interner Auditbericht

Hinweise:

Außer dem Punkt 7. müssten die anderen Punkte bei anderen Bezugsnormen auch angegeben werden.

In Stufe 1 des Audits muss im Übrigen auf jeden Fall beschrieben sein, wann Bereiche mit hohem Risiko in den drei Audits eines Zertifizierungsaudits (Erstzertifizierung/ Rezertifizierung, 1. Überwachungsaudit, 2. Überwachungsaudit) auditiert werden sollen.

Wichtig ist in diesem Zusammenhang auch zu wissen, was die Zielsetzungsschwerpunkte des Audits der Stufe 1 sein werden:
– Bewertung es MS-Dokumentation
– Überprüfung der Erklärung zur Anwendbarkeit in Bezug auf Vollständigkeit und Korrektheit
– Bewertung des Standortes und der standortspezifischen Bedingungen
– Bewertung des Kontextes
– Verifizierung der Risikobewertung und -behandlung
– Bewertung der Informationssicherheitspolitik und -ziele
– Einhaltung der gesetzlichen und behördlichen Aspekte

Phase 2: Audit der Stufe 2

Vergegenwärtigen wir uns an dieser Stelle, was ein Audit der Stufe 2 unbedingt abgeprüft haben muss:
– Führungsrolle und das Engagement für die Informationssicherheitspolitik und die Ziele der Informationssicherheit;
– die in ISO/IEC 27001 aufgeführten Dokumentationsanforderungen;
– Bewertung der mit der Informationssicherheit verbundenen Risiken, und dass die Bewertungen in regelmäßigen Abständen wiederholt gültige und vergleichbare Ergebnisse liefern;
– Festlegung von Kontrollzielen und Kontrollen auf der Grundlage der Informationssicherheitsrisikobewertung und -behandlung;
– die Leistung der Informationssicherheit und die Wirksamkeit des ISMS unter Berücksichtigung der Ziele der Informationssicherheit;
– Korrespondenz zwischen den er-mittelten Kontrollen, der „Erklärung zur Anwendbarkeit“ und den Ergebnissen der Informationssicherheitsrisikobewertung und -behandlung sowie der Informationspolitik und -ziele;
– Durchführung von Kontrollen (siehe Anhang D ISO/IEC 27006), unter Berücksichtigung des externen und internen Kontexts und der damit verbundenen Risiken, Überwachung, Messung und Analyse von Prozessen und Kontrollen der Informationssicherheit, um festzustellen, ob die Kontrollen umgesetzt und im Einklang der Sicherheitsziele stehen;
– Programme, Prozesse, Verfahren, Aufzeichnungen, interne Audits und Überprüfungen der Effektivität des ISMS, um sicherzustellen, dass diese auf Top-Managemententscheidungen und die Informationspolitik und -ziele zurückführbar sind.

Als wesentliche Mindestreferenzdokumente sind im Audit der Stufe 2 mindestens einzusehen/vorzulegen:
– Beschreibung des Geltungsbereiches
– Sicherheitspolitik
– Richtlinie zur Risikoanalyse
– Richtlinie zur Risikobehandlung
– Erklärung zur Anwendbarkeit
– Sicherheitsziele
– Richtlinie zur Kompetenzsicherstellung aller relevanten Mitarbeiter
– Dokumentenlenkung
– Risikoanalyse
– Risikobehandlungsplan
– Richtlinie zu Messungen und Monitoring
– Richtlinie für interne Audits
– Bericht zum internen Audit
– Richtlinie zur Managementbewertung
– Bericht zur Managementbewertung
– Richtlinie zum Umgang mit Nichtkonformitäten
– Richtlinie zum Umgang mit mobilen Geräten
– Richtlinie zum Umgang mit Teleworking
– Richtlinie zum Umgang mit Werten
– Richtlinie zur Zugangskontrolle
– Richtlinie zur Kryptographie
– Richtlinie zum aufgeräumten Schreibtisch
– relevante Arbeitsanweisungen
– Richtlinie zur Datensicherung
– Richtlinie zu Vertraulichkeitsvereinbarungen
– Richtlinie zur sicheren Entwicklung
– Richtlinie zur Härtung von Systemen
– Richtlinie zum Umgang mit Lieferanten
– Richtlinie zum Umgang mit Sicherheitsvorfällen
– Notfallkonzept
– Liste aller relevanten vertraglichen und gesetzlichen Anforderungen

In Anlehnung an 78 SD 001 (Einstufung von Abweichungen), die bei der Akkreditierung von Konformitätsbewertungsstellen zwingend anzuwenden ist, hat sich folgende Klassifizierung bei Feststellungen in Audits festgesetzt:

Kritische Abweichung:
– Abweichung von einer Normforderung oder anderweitig festgelegten Anforderung, die ein falsches Ergebnis der Konformitätsbewertung verursacht bzw. verursachen kann.
– Abweichung, die die grundlegende Wirksamkeit des QM-Systems in Frage stellt.
– Wiederholtes Auftreten einer nicht kritischen Abweichung zur gleichen Normforderung

Nicht-kritische Abweichung:

Abweichung von einer Normforderung oder anderweitig festgelegten Anforderung, von der keine unmittelbare Auswirkung auf das Ergebnis der Konformitätsbewertung der Konformitätsbewertungsstelle zu erwarten ist und die die grundlegende Wirksamkeit des QM-Systems nicht in Frage stellt.

Referenzen

IT-Sicherheitsgesetz, in Kraft getreten am 25.7.2017, §§ 8a und 8b BSI-Gesetz, BSI – Kritisverordnung vom 22.04.2016, §§ 11 (1a) und 11 (1b).

VO (EG) Nr. 765/2008, Akkreditierungsstellengesetz, DAkkS Dokument 71 SD 0 001 „Allgemeine Regeln zur Akkreditierung von Konformitätsbewertungsstellen.

71 SD 6 013, 71 SD 6 014, 71 SD 6 015, 71 SD 6 016, 71 SD 6 039, 71 SD 6 056.

78 SD 001 Einstufung von Abweichungen.

DIN EN ISO/IEC 17021-1: Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren – Teil 1: Anforderungen.

DIN EN ISO 19011: Leitfaden zur Auditierung von Managementsystemen.

DIN EN ISO/IEC 27001:2017 Informationssicherheitsmanagementsysteme – Anforderungen.

DIN EN ISO/IEC 27000:2017 Informationssicherheitsmanagementsysteme - Überblick und Terminologie.

DIN EN ISO/IEC 27002:2017 Leitfaden für Informationssicherheitsmaßnahmen.

ISO/IEC 27015:2018 Information technology – Security techniques – Information security risk management.

ISO/IEC 27006:2015 Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheitsmanagementsystemen anbieten.

ISO/IEC 27019:2017 Informationssicherheitsmaßnahmen für die Energieversorgung.

VGB S 175 VGB Standard „IT Security for Generating Plants“.

BDEW Whitepaper/OE Whitepaper Anforderungen an sichre Steuerungs- und Telekommunikationssysteme, Version 2.0 Mai 2018.

ISO 31000:2018 Risk management – Guidelines.

TeleTrusT Handreichung zum Stand der Technik in der IT-Sicherheit.

BSI TR-01202, BSI TR-01202 Kryptographische Verfahren: Teil 1 Empfehlungen und Schlüssellängen, Teil 2 Verwendung von TLS, Teil 3 Verwendung von IPsec und IKEv2, Teil 4 Verwendung von SSH.

BSI TR-3103 Sicheres WLAN: Teil 1 Sicherheitsmechanismen, Teil 2 WLAN Sicherheitskonzept, Teil 3a Auswahl von Auswahlkriterien für WLAN-Systeme, Teil 3b Prüfkriterien für WLAN-Systeme.

BSI TR-3108 Sicherer E-Mail-Transport.

BSI TR-3109 Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb.

BSI TL-02103 Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf.

BSI TR-03138 Richtlinie Ersetzendes Scannen

Energiewirtschaftsgesetz.

Erneuerbare-Energien-Gesetz.

DIN EN ISO/IEC 27037:2016 Leitfaden für die Identifikation, Mitnahme, Sicherung und Erhaltung digitaler Beweismittel.

DIN 66399-1:2012 Vernichtung von Datenträgern Teil1: Grundlagen und Begriffe.

DIN 66399-2:2012 Vernichtung von Datenträgern Teil2: Anforderungen an Maschinen zur Vernichtung von Datenträger.

DIN SPEC 66399-03:2013 Vernichtung von Datenträgern Teil3: Prozess der Datenträgervernichtung.

Autor

Prof. h.c. PhDr. Dipl.-Kfm./Dipl.-Vw. Stefan Loubichi, international erfahrener leitender Auditor für Managementsysteme (ISO 27001, ISO 14001, ISO9001, ISO 45001, ISO 26000), Prüfer nach § 8a BSI-Gesetz sowie nach dem IT-Sicherheitskatalog, mehr als zehn Jahre Erfahrung (Deutschland, Naher Osten, Europäische Union, VR China, Südamerika) in der Energiewirtschaft sowie mehrjähriger leitender Auditor für die Zertifizierung der Kraftwerksschule und des Simulatorzentrums (KSG/GfS)