Schulungsangebote 2018

Zur Implementierung / Zertifizierung des IT-Sicherheitskataloges nach § 11 Abs. 1b EnWG

für
Erzeugungsanlagen
im Sinne von
Anhang 1, Teil 3 Nr. 1.1.1
Kritis-Verordnung
sowie Gasspeicher
im Sinne von
Anhang 1, Teil 3 Nr. 2.1.2
Kritis-Verordnung

Gender-Erklärung

Zur besseren Lesbarkeit werden in unseren Veröffentlichungen personenbezogene Bezeichnungen, die sich zugleich auf Frauen und Männer beziehen, generell nur in der im Deutschen üblichen männlichen Form angeführt, also z.B. „Teilnehmer“ statt „TeilnehmerInnen“ oder „Teilnehmerinnen und Teilnehmer“.

Dies soll weder eine Geschlechterdiskriminierung noch eine Verletzung des Gleichheitsgrundsatzes bedeuten.

INHALT

„Für das Können gibt es nur einen Beweis: Das Tun"

Marie von Ebner-Eschenbach
(1830-1916)

Gemäß dieses Leitmottos werden unsere Maßnahmen nur von Fachkräften durchgeführt, welche

1. nicht nur über eine herausragende fachliche Qualifizierung verfügen
2. über eine moderne pädagogische Qualifizierung und Erfahrung in der Erwachsenenbildung verfügen
3. praktische Erfahrung im speziellen Seminarthema haben

VORWORT

Mit dem Entwurf des IT Sicherheitskatalogs im Januar 2018 hat das letzte Kapitel in Sachen Implementierung und Zertifizierung für Unternehmen der Energiewirtschaft begonnen. Die Betreiber der Energieanlagen müssen nunmehr 18 Monate nach Inkrafttreten des IT Sicherheitskataloges eine erfolgreiche Zertifizierung nachweisen. Bis Ende Februar 2018 sind Kommentierungen zum Entwurf möglich und mit einer offiziellen Inkraftsetzung des IT-Sicherheitskataloges wird derzeit nach Ostern 2018 gerechnet.

Dabei müssen nicht nur die Normen:

- ISO/IEC 27001
- ISO/IEC 27002
- TR ISO/IEC 27019

nachgewiesen werden, sondern auch:

Anhang A des VGB Standards VGB – S – 175

sowie der

IT – Sicherheitskatalog nach § 11 Absatz 1b EnWG

Betreiber von Kernkraftwerken sind nur dann von der Zertifizierung ausgenommen, wenn sie die SEWD IT Richtlinie erfolgreich nachweisen können.

Nach derzeitigem Stand des Entwurfs des IT-Sicherheitskataloges sind hierbei folgende Fristen zu beachten:

1. Zum Nachweis darüber, dass die Anforderungen des IT-Sicherheitskataloges umgesetzt wurden, hat der Anlagenbetreiber der Netzagentur 1,5 Jahre nach Veröffentlichung des IT-Sicherheitskataloges den Abschluss des Zertifizierungsverfahrens durch Vorlage einer Kopie des Zertifikates mitzuteilen.
2. Der Ansprechpartner IT-Sicherheit sowie seine Kontaktdaten sind der BNetzA innerhalb von 2 Monaten nach Veröffentlichung des IT- Sicherheitskatalogs mitzuteilen.

Die Zertifizierungsverfahren der Netz- und Gasbetreiber nach dem IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG, welche eigentlich alle bis 31. Januar 2018 positiv abgeschlossen sein sollten, haben dabei gezeigt, dass es gut geschulter Mitarbeiter*innen und einer guten Beratung bedarf, um die Fristen einzuhalten.

Mit unserer Erfahrung und unserer Kompetenz wollen wir Ihnen helfen, das Zertifizierungsverfahren innerhalb der von der Bundesnetzagentur gesetzten Frist erfolgreich zu realisieren.

EINFÜHRUNG

INFORMATIONSSICHERHEIT NACH ISO/IEC 27001:2017

für Energieerzeuger nach § 11 Absatz 1b EnWG

ZIEL

Sie lernen die wichtigen theoretischen Grundlagen der Informationssicherheit gemäß Normenreihe ISO/IEC 27000 ff. sowie den IT-Sicherheitskatalog für Erzeuger (§ 11 Abs. 1b EnWG) kennen.

ZIELGRUPPE

Führungskräfte, Security-Verantwortliche, Sicherheitsberater, Mitarbeitende der Leit-stelle sowie der ITK.

ZUGANGSVORAUSSETZUNG

Keine

DATEN UND FAKTEN

Dauer	1 Tag
Termine	27.04.2018 07.06.2018
Zeit	9.00 - 17.00 Uhr
Teilnehmer	min. 4 - max. 25
Gebühren	750,00 € zzgl. MwSt.

SEMINARINHALT

- Einführung Informationssicherheits-management
- Überblick über die ISO/IEC 27000 ff. Normenfamilie
- Mindestanforderungen nach ISO/IEC 27001
- Empfehlungen und Leitlinien der ISO/IEC 27002
- Anforderungen des IT-Sicherheits-kataloges nach § 11 Abs. 1b EnWG
- Ablauf eines Zertifizierungsver-fahrens gemäß IT-Sicherheitskatalog in Verbindung mit ISO/IEC 27001

ZERTIFIKATSERWERB (optional)

Multiple-Choice Prüfung in Deutsch

Dauer 45 min, 30 Fragen, zum Bestehen der Prüfung müssen 60% der Fragen richtig beantwortet sein.

QUALIFIZIERUNG
INFORMATIONSSICHERHEITSMANAGE-MENTBEAUFTRAGTER

für Energieerzeuger nach § 11 Absatz 1b EnWG

ZIEL

Sie lernen die Planung, Implementierung, Aufrechterhaltung sowie Verbesserung eines ISMS auf der Basis von ISO/IEC 27001 und IT-Sicherheitskatalog für Erzeuger kennen.

ZIELGRUPPE

Personen, die im Unternehmen als Ansprechpartner IT-Sicherheit und/oder als ISMS-Beauftragte tätig sein möchten.

ZUGANGSVORAUSSETZUNG

ISMS Grundkenntnisse
(zum Beispiel durch Besuch des Seminars 2018-I.1)

DATEN UND FAKTEN

Dauer	5 Tage
Termine	09.07.2018 - 13.07.2018 08.10.2018 - 12.10.2018
Zeit	9.00 - 17.00 Uhr
Teilnehmer	min. 4 - max. 25
Gebühren	2.250,00 € zzgl. MwSt.

SEMINARINHALT

- Gesetzesgrundlagen IT-Sicherheit
- Behördliche Umsetzungshilfen IT-Sicherheit
- ISMS Dokumentation nach ISO/IEC 27001:2017
- Zusatzanforderungen nach ISO/IEC 27002 und ISO/IEC 27019
- Empfehlungen und Leitlinien der ISO/IEC 27002
- Anforderungen des IT-Sicherheits-kataloges nach § 11 Abs. 1b EnWG
- Aufbau einer zertifizierungsfähigen Dokumentation
- Implementierung eines Informations-sicherheitsmanagementsystems

ZERTIFIKATSERWERB (optional)

Multiple-Choice Prüfung in Deutsch

Dauer 90 min, 60 Fragen, zum Bestehen der Prüfung müssen 60% der Fragen richtig beantwortet sein.

Qualifizierung

AUDITOR FÜR INFORMATIONSSICHERHEITSMANAGEMENTSYSTEME

für Energieerzeuger nach § 11 Absatz 1b EnWG

ZIEL

Sie lernen die Planung, Implementierung, Aufrechterhaltung sowie Verbesserung eines ISMS auf der Basis von ISO/IEC 27001 und IT-Sicherheitskatalog für Erzeuger kennen.

ZIELGRUPPE

Führungskräfte, Security-Verantwortliche, Sicherheitsberater, Mitarbeitende der Leit-stelle sowie der ITK.

ZUGANGSVORAUSSETZUNG

Keine

DATEN UND FAKTEN

Dauer	5 Tage
Termine	20.08.2018 - 24.08.2018 26.11.2018 - 30.11.2018
Zeit	9.00 - 17.00 Uhr
Teilnehmer	min. 4 - max. 25
Gebühren	2.250,00 € zzgl. MwSt.

SEMINARINHALT

- Beherrschen der ISO 19011 sowie der relevanten Bereiche von ISO/IEC 17021, ISO/IEC 27006 und ISO/IEC 27007
- Aufrechterhaltung der Kompetenz von Auditoren
- Soziale Kompetenzen für Auditoren
- Erstellen von Auditplänen sowie das Planen von Audits
- Checklisten zur Durchführung von Audits
- Durchführung von Audits
- Feststellungen in Audits, Korrekturmaßnahmen, Nachverfolgung
- Erstellung von Auditberichten

ZERTIFIKATSERWERB (optional)

Multiple-Choice Prüfung in Deutsch

Dauer 90 min, 60 Fragen, zum Bestehen der Prüfung müssen 60% der Fragen richtig beantwortet sein.

WER · WIE · WO

DOZENT

Prof. h.c. (IUK)
PhDr. Dipl.-Kfm./
Dipl.-Vw.
Stefan Loubichi

international langjährig erfahrener Berater, Dozent sowie Lead-Auditor, mehr als 10 Jahre Erfahrung in der Energiewirtschaft

METHODEN

Vortrag mit Plenumsdiskussion; Plenumsarbeiten; Vertiefung durch praktische Beispiele; Einzel- und Gruppenarbeit.

LEHRGANGSMATERIALIEN

Nach verbindlicher Seminarbestätigung mailen wir Ihnen die Lehrgangsmaterialien in digitaler Form vorab zur Vorbereitung zu.

VERANSTALTUNGSORT

Simulatorzentrum
Deilbachtal 173
45257 Essen

Gerne führen wir alle Schulungsangebote auch als In-House-Schulungen bei Ihnen durch.

Des Weiteren bieten wir auch individuelle Workshops zur Implementierung des ISMS – Systems an und bieten Ihnen auch eine Beratung bis zur Zertifizierung Ihres Unternehmens an.

HINTERGRUNDWISSEN ZUM IT-SICHERHEITSKATALOG

mit freundlicher Unterstützung des VGB POWERTECH

IT-Sicherheitskatalog nach § 11 Absatz 1b EnWG – Was jetzt getan werden muss!

Stefan Loubichi

Abstract

Kurzfassung Überschrift

With the draft of the IT-security catalogue in January 2018 the last chapter in implementing and certifying for companies in the energy industry has begun. The operator of energy plants has to demonstrate successful certification within 18 months after the IT standard had been put into force.

Not only ISO/IEC 27001, ISO/IEC 27002 and TR ISO/IEC 27019 must be proven, but also the appendix A of the VGB standard VGB S – 175. Nuclear power plants are only exempt from certification, if they can successfully prove the adaption of the SEWD IT directive.

Protection goals, risk objectives and risk handling are just as important to this IT security standard as protection zones are.

Unfortunately, neither the conformity assessment program for carrying out audits nor the requirements for auditors are currently clearly defined, so that there are also unknown quantities here.

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.(IUK) PhDr. Dipl.-Kfm./Dipl.-Vw. Stefan Loubichi
International experienced lead auditor for managementsystems (ISO 27001, ISO 14001, ISO 9001, OHSAS 18001, ISO 26000), more than ten years international experience (Germany, Middle East, P.R. China, European Union, South America) in the energy industry as well as lead auditor in the field of certifying Kraftwerksschule Essen or Simulator Centrum Essen (GfS mbH / KSG mbH), Deutschland

Hinweis

Dieser Aufsatz befasst sich mit dem Entwurf des IT-Sicherheitskataloges nach § 11 Absatz 1b EnWG. Obgleich noch Kommentierungen bis Ende Februar 2018 möglich sein werden, ist aus Erfahrungen davon auszugehen, dass so gut wie keine wesentlichen Änderungen mehr eintreten werden, so dass der IT-Sicherheitskatalog für Betreiber nach Ostern 2018 aller Voraussicht nach veröffentlicht wird, so dass dann die entsprechenden Umsetzungsfristen beginnen werden.

IT Sicherheitsanforderungen in der Energiewirtschaft

Bezüglich der IT-Sicherheitsanforderungen in der Energiewirtschaft sind derzeit die folgenden vier Blöcke in Deutschland zu berücksichtigen:

IT-Sicherheitsgesetz

- in Kraft getreten am 25.7.2015
- definiert IT-Sicherheitsmindeststandards für Betreiber Kritischer Infrastrukturen (KRITIS)
- legt Meldepflichten für erhebliche IT-Sicherheitsvorfälle für KRITIS-Betreiber fest

EU-NIS Richtlinie

[EU-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit]

- im August 2016 als EU-Richtlinie in Kraft (2016/1148)
- in Deutschland per Gesetz am 29.6.2017 als Umsetzungsgesetz in Kraft getreten (BGBl Jahrgang 2017, Teil I Nr. 40)

Marktkommunikationsregegularien

gekennzeichnet durch:

- EDI@Energy Kommunikationsrichtlinie
- EDI@Energy Übertragungswegregelungen
- erhöhte Anforderungen im Zielmodell

Digitalisierungsgesetz zur Energiewende

charakterisiert durch:

- Maßnahmen nach dem Stand der Technik für „berechtigte Stellen“ (§ 49 I MsbG)
- BSI TR und Schutzprofile für Smart Meter
- ISMS für Smart-Meter Gateway Admins

Die letzte wesentliche, bis dato noch nicht hinreichend definierte Regelung zur IT-Sicherheit in der Energiewirtschaft war der IT-Sicherheitskatalog für Betreiber von Energieanlagen.

EnWG und KritisV

Als gesetzliche Grundlage hierfür ist § 11 Abs. 1b EnWG anzusehen: Hiernach haben Betreiber von Energieanlagen, welche als Kritische Infrastruktur bestimmt sind und an ein Energieversorgungsnetz angeschlossen sind, innerhalb einer von der BNetzA festgelegten Frist einen angemessenen Schutz gegen Bedrohungen für elektronische Datenverarbeitungssysteme und TK-Systeme zu gewährleisten.

Wer diese Erfordernisse zu erfüllen hat, ist durch die BSI Kritis Verordnung, respektive durch den Anhang 1 Anlagenkategorien und Schwellenwerte im Sektor Energie bestimmt. Gemäß der letzten Änderung vom 21.06.2017 sind derzeit folgende Aspekte besonders relevant:

Erzeugungsanlage im Sinne von Anhang 1, Teil 3, Nr. 1.1.1 Kritis-V

Definition:

Anlage im Sinne des § 3 Nr. 18c EnWG in der jeweils geltenden Fassung

Berechnungsformel zur Ermittlung des Schwellenwertes:

Der Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs von 3.735 kWh pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500.000 versorgten Personen wie folgt zu berechnen:

3.700 GWh/Jahr ≈
7.375 kWh/Jahr x 500.000

Die durchschnittliche elektrische Arbeit zur Versorgung von 500.000 Personen im Jahr entspricht einer installierten Netto-Nennleistung von:

420 MW ≈ (3.700 GWh/Jahr) / (8.760 h/Jahr)

Gasspeicher im Sinne von Anhang 1, Teil 3, Nr. 2.1.2 Kritis-V

Definition:

Gasspeicher im Sinne des § 3 Nr. 31 EnWG in der jeweils geltenden Fassung

Berechnungsformel zur Ermittlung des Schwellenwertes:

Der Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs von 10.380 kWh pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500.000 versorgten Personen wie folgt berechnet:

5.190 GWh/Jahr =
10.380 kWh/Jahr x 500.000

Zoneneinteilung der ITK Strukturen

Bevor über eine Schutzzielerreichung gesprochen werden kann, ist es von Rele-

vanz, eine Einteilung der ITK-Strukturen der Betreiber von Energieanlagen nach folgendem 6 Zonen Schema vorzunehmen, wobei im Rahmen der Zoneneinteilung nicht eine Netzsegmentierung vorgenommen wird, sondern eine Klassifizierung von Anwendungen, Systemen und Komponenten einer Energieanlage bezüglich ihrer Bedeutung für einen sicheren Anlagenbetrieb:

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, Netz-dienstleistungen 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

Nachzuweisende Schutzziele

Im Rahmen des IT-Sicherheitskatalogs nach § 11 Absatz 1b EnWG werden folgende Ziele zu berücksichtigen sein:

Allgemeine Schutzziele

Die allgemeinen Schutzziele sind wie folgt im Entwurf des IT-Sicherheitskataloges charakterisiert:
- Sicherstellung der Verfügbarkeit der zu schützenden Systeme und Daten
- Integritätssicherstellung der verarbeiteten Informationen und Systeme
- Gewährleistung der Vertraulichkeit mit den betrachteten Systemen verarbeiteten Informationen

In einer Trivialdefinition seien die vorstehend bezeichneten Ziele wie folgt im Sinne der BNetzA 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

Spezielle Schutzziele

Für Energieerzeugungsanlage sind (derzeit) folgende besondere Schutzziele festgelegt:
- 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 Gasspeicher sind (derzeit) folgende besonderen Schutzziele festgelegt

- Bereitstellung von Speicherkapazität entsprechend den kommunizierten Anweisungen des Dispatchings 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.

Risikoeinschätzung /-behandlung

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.

Risikoeinschätzung

Eine Risikoeinschätzung ist im Rahmen der Schadenskategorien:
- kritisch
- hoch
- mäßig
- gering

für alle erfassten Anwendungen, Systeme und Komponenten vorzunehmen.

Im Rahmen der Einstufung der Schadenskategorien sollten zumindest die nachfolgenden Kriterien berücksichtigt werden:
- Beeinträchtigung der Versorgungs-sicherheit
- Einschränkung der Energielieferung
- Betroffener Bevölkerungsanteil
- Gefährdung für Leib und Leben
- Gefährdung für Datensicherheit und Datenschutz durch Offenlegung oder Manipulation
- Finanzielle Auswirkungen

Als Ursachen sind in diesem Zusammenhang in Betracht zu ziehen:

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

Nichtvorsätzliche Gefährdungsursachen:
- 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!

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 speziell:
  Ermittelte Risiken dürfen nicht akzeptiert werden. Maßnahmen zur Risikobehandlung sind hier zumindest soweit umzusetzen, dass lediglich ein als gering zu bewertendes Restrisiko verbleibt.
- Zone 1-3 i.V.m. Zone 4-6:
  Bei Anwendungen, Systeme 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.

Auf den nachfolgenden selbsterklärenden Passus des IT-Sicherheitskataloges wird ob seiner Relevanz verwiesen:

„Sofern Anwendungen, Systeme und Komponenten, die den Zonen 1 bis 3 zugeordnet sind, mit Anwendungen, Systemen und Komponenten aus den Zonen 4 bis 6 Informationen austauschen, die für den sicheren Anlagenbetrieb benötigt werden, ist sicherzustellen, dass Verfügbarkeit, Integrität und Vertraulichkeit der Informationen gewahrt bleiben. Der Schutzbedarf dieser Informationen richtet sich nach dem Schutzbedarf der Anwendungen, Systeme und Komponenten in der Zone mit der jeweils höheren Bedeutung für den sicheren Anlagenbetrieb."

Managementsystemanforderungen

Genauso wie die Kritis-Netzbetreiber sind die Kritis-Anlagenbetreiber verpflichtet, die Informationssicherheitsmanagementsystem- Konformität mit den Anforderungen des IT-Sicherheitskatalogs durch ein Zertifikat einer für die Zertifizierung des IT-Sicherheitskatalogs bei der Deutschen Akkreditierungsstelle (DAkkS) akkreditierten unabhängigen Zertifizierungsstelle zu belegen.

Per se wird er hier erst einmal verpflichtet sein, eine Konformität zu den nachfolgenden Normen nachzuweisen:
- DIN ISO/IEC 27001
- DIN ISO/IEC 27002
- DIN ISO/IEC 27019

Für Betreiber von Erzeugungsanlagen gilt darüber hinaus die Verpflichtung, die Anforderungen des Anhangs A des VGB Standard IT-Sicherheit für Erzeugungs-anlagen (VGB-S-175) zu erfüllen.

Explizit wird in dem IT-Sicherheitskatalog auch auf die DIN ISO/IEC TR 27019 „ISMS- Leitfaden von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 verwiesen. Dies bedeutet, dass die zusätzlichen Spezifika von den Anlagebetreibern zu implementieren und von den Zertifizierungsstellen zu prüfen sind.

Zusätzliche Anforderungen der TR 27019 gibt es derzeit in den nachfolgenden Bereichen:
- 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

Für die Zertifizierung der Anlagenbetreiber durch externe Dritte kommt diesen Punkten in mehrfacher Hinsicht eine besondere Bedeutung zu.

Ansprechpartner für IT-Sicherheit

Wie die Netzbetreiber müssen auch die Anlagenbetreiber einen qualifizierten Ansprechpartner IT-Sicherheit gegenüber der Bundesnetzagentur benennen. Diese Person muss gegenüber der Bundesnetzagentur stets Auskunft über folgende Punkte geben können:
- Umsetzungsstand der Anforderungen aus dem vorliegenden IT-Sicherheitskatalog
- Aufgetretene Sicherheitsvorfälle sowie Art und Umfang hierdurch hervorgerufener Auswirkungen (insbesondere in solchen Fällen, die gemäß § 11 Absatz 1c EnWG eine Meldepflicht des Betreibers gegenüber dem BSI auslösen)

– Ursache aufgetretener Sicherheitsvorfälle sowie Maßnahmen zu deren Behebung und zukünftigen Vermeidung

Beispiele für meldepflichtige erhebliche Störungen wären zum Beispiel:
– Neuartige oder außergewöhnliche IT-Störungen
– Gezielte Angriffe
– Neue Modi Operandi
– Vorfälle, die nur mit deutlich erhöhtem Ressourcenaufwand bewältigt werden können

Voraussichtliche Umsetzungsfristen

– Zum Nachweis darüber, dass die Anforderungen des IT-Sicherheitskataloges umgesetzt wurden, hat der Anlagenbetreiber der Netzagentur 1,5 Jahre nach Veröffentlichung des IT-Sicherheitskataloges den Abschluss des Zertifizierungsverfahrens durch Vorlage einer Kopie des Zertifikates mitzuteilen.
– Der Ansprechpartner IT-Sicherheit sowie seine Kontaktdaten sind der BNetzA innerhalb von 2 Monaten nach Veröffentlichung des IT- Sicherheitskatalogs mitzuteilen.

4 Phasen-Konzept zur erfolgreichen zertifizierungsreifen Umsetzung

Für viele Anlagenbetreiber stellt sich nun die Frage: Was ist zu tun bis zur Zertifizierung?

Die Antwort kann natürlich nur unternehmensspezifisch sein, gleichwohl wird hier auf das nachstehende -bereits bei Netzbetreibern erfolgreiche- 4 Phasen Konzept verwiesen:

Ist Aufnahme
– Festlegung des Scopes
– Technische und organisatorische GAP-Analyse
– Auswertung der Analyse

Vorphase zur Implementierung
– Erstellung / Aktualisierung der Assets
– Zoneneinteilung
– Durchführung der Risikoeinschätzung
– Festlegung der Risikobehandlung
– Erstellung der SoA

Implementierung
– Implementierung der technischen Maßnahmen
– Implementierung der organisatorischen Maßnahmen
– Anfertigung der Dokumentation
– Durchführung von intensiven Schulungen für alle relevanten Personen

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 Monate benötigen.

Sonderregelungen für Anlagen nach § 7 I AtomG

Zum guten Schluss sei noch darauf verwiesen, dass es ein Irrglaube ist, dass Anlagen nach § 7 I AtomG per se von allem ausgeschlossen sind.

Hierzu sei aus dem derzeitigen Entwurf des IT-Sicherheitskataloges zitiert:

„Für die IT-Sicherheit von Anlagen nach § 7 Absatz 1 des Atomgesetzes besteht mit der „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)“ bereits ein anlagenspezifisches Regelwerk, dessen Schutzziele die kerntechnische Sicherheit gewährleisten sollen. Die IT-Sicherheit von Anlagen nach § 7 Absatz 1 des Atomgesetzes muss sich nach § 11 Absatz 1b Satz 1 EnWG jedoch auch an ihrer Bedeutung für den sicheren Netzbetrieb und damit für die allgemeine Versorgungssicherheit orientieren.

Betreiber von Anlagen nach § 7 Absatz 1 des Atomgesetzes sind daher verpflichtet, im Rahmen der Schutzbedarfsfeststellung gemäß SEWD-Richtlinie IT auch die unter B./II./1. genannten besonderen Schutzziele für Erzeugungsanlagen bei der Zuordnung der schutzbedürftigen Anwendungen, Systeme und Komponenten zu den IT-Schutzbedarfsklassen zu berücksichtigen. Diese besonderen Schutzziele sind nachrangig zum Schutzziel der atomaren Sicherheit zu behandeln.

Sofern die besonderen Schutzziele für Erzeugungsanlagen bei der Schutzbedarfsfeststellung berücksichtigt werden, führt die Umsetzung der SEWD-Richtlinie IT zu einem IT-technischen Schutzniveau, welches mit dem in § 11 Abs. 1b S. 1 EnWG geforderten Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind, vergleichbar ist.

Ein angemessener Schutz des Betriebs von Energieanlagen im Sinne von § 11 Absatz 1b Satz 1 EnWG liegt daher für Anlagen nach § 7 Absatz 1 des Atomgesetzes vor, wenn diese den Anforderungen der SEWD-Richtlinie IT entsprechen und bei deren Umsetzung auch die besonderen Schutzziele gemäß Abschnitt B./II./1. berücksichtigen.

Zum Nachweis der Erfüllung der Anforderungen haben Betreiber von Anlagen nach § 7 Absatz 1 des Atomgesetzes erstmalig bis zum 30.06.2019 der Bundesnetzagentur eine Bestätigung der für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden der Länder vorzulegen, aus der hervorgeht, dass die Anforderungen der SEWD-Richtlinie IT vom Betreiber eingehalten werden. Darüber hinaus haben die Betreiber eine verbindliche, von der Geschäftsführung unterzeichnete Erklärung abzugeben, dass auch die besonderen Schutzziele für Erzeugungsanlagen gemäß Abschnitt B./II./1. bei der Schutzbedarfsfeststellung berücksichtigt wurden. Der Nachweis der Erfüllung der Anforderungen ist jeweils zum 30.06. eines jeden Jahres erneut zu erbringen.“

Aspekte der Dritt-Zertifizierung des IT-Sicherheitskataloges

Ein besonderer Flaschenhals zur Umsetzung des IT-Sicherheitskataloges nach § 11 Absatz 1b EnWG wird aller Voraussicht wie bei den KRITIS-Netzbetreibern und ihrem IT-Sicherheitskatalog nach § 11 Absatz 1a EnWG die Zertifizierung durch von der DAkkS akkreditierte Zertifizierer sein.

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 Konformitätsbewertungs-programm festgelegt werden, dass die zu erfüllenden Parameter zur Auditdurchführung sowie Zusatzanforderungen für Auditoren (noch) festlegt. Auch dies ist noch nicht geschehen.

Abschließendes Fazit

Es ist der Welt der Märchen zuzuordnen, dass die vom IT-Sicherheitskatalog nach § 11 Absatz 1b EnWG betroffenen KRITIS – Anlagenbetreuer unverhältnismäßig lange vor der Implementierung und Zertifizierung geschützt wurden. Vergleicht man diesen IT-Sicherheitskatalog mit dem IT-Sicherheitskatalog für Netzbetreiber so fällt nicht nur auf, dass er umfangreicher ist, sondern dass auch zusätzliche Drittanforderungen wie der VGB Standard IT-Sicherheit für Erzeugungsanlagen (VGB-S-175) integriert wurden. Eine Implementierung sowie eine erfolgreiche Zertifizierung wird deshalb nur mit erheblicher Anstrengung in der von der Bundesnetzagentur gesetzten Frist möglich sein.

Autor

Prof. h.c.(IUK) PhDr. Dipl.-Kfm./Dipl.-Vw. Stefan Loubichi, international erfahrener leitender Auditor für Managementsysteme (ISO 27001, ISO 14001, ISO9001, OHSAS 18001, ISO 26000), 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).

NOCH FRAGEN?

Sollten Sie noch Fragen zu unseren maßgeschneiderten Schulungsangeboten haben, so freuen wir uns diese zeitnah in einem persönlichen Gespräch zu beantworten.

IHR ANSPRECHPARTNER

Peter Lasch
Produktmanager
Marketing und Vertrieb
Telefon 0201 4862-169 · Telefax 0201 4862-156
E-Mail p.lasch@ksg-gfs.de

Informationen über Ihren nach DIN EN ISO 9001:2015 zertifizierten Schulungsanbieter:

KSG Kraftwerks-Simulator-Gesellschaft mbH
Deilbachtal 173
45257 Essen

erhalten Sie im Internet unter www.simulatorzentrum.de

RECHTLICHE HINWEISE

1. Diese Broschüre stellt ein Angebot zum Abschluss eines Vertrages zur Lehrgangsteilnahme im Rahmen der oben genannten Parameter dar. Sie können dieses Vertragsangebot im Rahmen aller laut BGB möglichen Formen annehmen. Hiernach erhalten Sie von uns eine Anmeldebestätigung, die zugleich die schriftliche Bestätigung des zustande gekommenen Lehrgangsvertrags darstellt. Aus Verbraucherschutzgründen verzichten wir auf allgemeine Geschäftsbedingungen.
2. Eine Kündigung ist bis 14 Tage vor Starttermin kostenfrei möglich. Hiernach fallen Stornogebühren in Höhe von 80% an.

KSG Kraftwerks-Simulator-Gesellschaft mbH
Deilbachtal 173 · 45257 Essen
Telefon 0201 4862-0 · Telefax 0201 4862-298
www.simulatorzentrum.de

Zertifiziert nach
DIN EN ISO 9001

Titelbild |© stockWERK fotolia.com

03|2018