Implementieren und Zertifizieren von IT-Sicherheitsmanagementsystemen nach ISO 27001 in der Energiewirtschaft

Stefan Loubichi

Abstract

Implementation and certification of IT security management systems according to ISO 27001 in the energy industry

After the WannaCry attack on the 12th of May 2017 as the biggest cyber attack in history or the attack on the Ukrainian electricity network on the 23rd of December, 2015, we know that there is no industry that is safe from cyber attacks. In 2015 the government of the Federal Republic of Germany has defined with the IT security act and the critical infrastructures regulation how IT critical industries like the power industry must address the IT related risks and how this must be proved. For this purpose, enterprises of the energy industry must implement a management system according to the ISO 27001 in conjunction with the governmental IT security catalogue of the energy industry. This management system has to be audited annually by independent certification bodies with auditors approved for the energy industries. This article provides answers on how to implement the management systems, what to consider during the process of certification and the benefits of such a management system.

Am Freitag, den 12. Mai 2017 begann die bislang weltweit größte Cyber-Attacke der Geschichte. Innerhalb von nur 3 Tagen waren bereits mindestens 220.000 Computer in 150 Ländern betroffen und jeder kennt jetzt WannaCry. Wieder einmal zahlten viele Unternehmen die Erpressungsgelder. Gott sei Dank wurde dieser Angriff jedoch „nur“ von Kriminellen ausgeführt. Je mehr diese Angriffe aber öffentlich werden, desto größer wird die Gefahr, dass diese IT-Spezialisten irgendwann nicht von Kriminellen, sondern von politisch motivierten Fanatikern engagiert werden. Da wir alle den Thriller „Black Out“ gelesen haben, wissen wir, wie Menschen auf einen länger andauernden Ausfall der Stromversorgung reagieren. Auch wenn wir (im Expertenkreis) wissen, dass die Ursachen eines Stromausfalles -wie er in Black Out beschrieben ist- so nicht auftreten können, so stellt sich natürlich die Frage, wie sicher sind wir vorbereitet gegen IT-Attacken in der Energiewirtschaft.

Gott sei Dank gibt es nur zwei Dinge auf Erden, die sicher sind: der Tod und Steuerzahlungen. Und natürlich der Mythos der sicheren IT-Strukturen in der Energiewirtschaft. Aber werfen wir einmal einen Blick hinter diesen Mythos.

Grundmuster eines Angriffs auf ein Stromnetz

Vergegenwärtigen wir uns hierzu einmal das Grundmuster von Hackerangriffen auf Stromnetze, wie diese nahezu „mustergültig“ am 23.12.2015 in der Ukraine in Ivano-Frankivsk ausgeführt wurden:

Stufe 1 – Targeting:

Gesucht werden Organisationen, welche sich durch einen hohen Automatisierungsgrad sowie eine große Remote-Steuerung auszeichnen.

Stufe 2 – Eindringen in das Netzwerk der Verwaltung:

Mit Crimeware wie BlackEnergy versehene Office Dokumente werden an die Verwaltungsmitarbeitenden übersandt. Unter irgendwelchen Vorwänden wird der Mitarbeitende aufgefordert, Makros im Dokument zu aktivieren, um die Lesbarkeit der Dokumente zu ermöglichen. Hierdurch ist dem Angreifer ein Eindringen in das fremde Netz möglich, indem er die Malware installiert. Dies geschieht in der Regel mindestens sechs Monate vor dem Angriff.

Stufe 3 – Benutzerrechte:

Durch die Malware werden Netzzugangsrechte ausgespäht und es werden Netzwerke mit hohen Benutzerrechten generiert. Mittels VPN Technik wird jetzt aus der Verwaltungsumgebung die IT-Umgebung der Leittechnik ausspioniert.

Stufe 4 – Übernahme der Leittechnik:

Mittels Malware-Clients oder mittels Remote-Administrationstools wird die Leittechnik übernommen.

Stufe 5 – Der eigentliche Angriff:

- Übernahme der Kontrollen der Leitwartenrechner zu einem günstigen Zeitpunkt (z.B. Schichtwechsel)
- Aussperrung der Leitwarten-Mitarbeitenden aus dem System
- Remote-Abkopplung von Verteilernetzen oder Umspannstationen

Autor

Prof. h.c.(IUK) PhDr. Dipl.-Kfm./ Dipl.-Vw. Stefan Loubichi
rps training & consulting GmbH
Andreaskloster 16
50667 Köln, Deutschland

– Installation von Schadsoftware auf dem Leitwartenrechner sowie Löschung relevanter Systemdateien auf dem Leitwartenrechner
– Denial-of-Service-Angriffe auf die Callcenter der Energieunternehmen, damit die Kommunikation zum Energieunternehmen de facto nicht möglich wird und eine große Verwirrung entsteht.

Wer wissen möchte, wie dies in der Ukraine konkret vor sich ging, hier die Quellen zum Nachlesen:
– https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
– https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Gefährdungspotentiale bei Energieerzeugern

Jetzt werden sich vielleicht die Energieerzeuger denken: Tja, die Netzbetreiber, aber wir sind anders. Anders vielleicht, aber wirklich weniger gefährdet?

Mythos „Air Gap"

Unter einem Air Gap versteht man ein vom restlichen Internet physisch abgetrenntes Netzwerk. Also kann in ein derart vernetztes System nichts eindringen, oder doch? Im April 2016 fanden sich auf einem System, das 2008 in Block B des KKW Gundremmingen installiert wurde und auf dem die Protokolle der Brennelement-Lademaschine verarbeitet und visualisiert werden sowie im Büro-Netz des KKWs die 2008/2009 verbreiteten Würmer Conficker und Ramnit. Es ist sehr wahrscheinlich, dass die Schadsoftware über USB-Sticks eingespielt wurde. Es stellt sich jedoch nicht nur die Frage, wieso die USB Ports offen waren, sondern wieso das Antiviren-System des Jahres 2016 sieben Jahre alte Schadsoftware nicht erkannte.

Mythos „Sichere SCADA Systeme"

www.shodan.io durchforstet das Internet nach öffentlich zugänglichen Geräten, also auch auf SCADA-Systeme. Positiv gesehen leistet SHODAN uns allen hiermit einen guten Dienst, indem aufgezeigt wird, welche anfälligen Systeme es gibt. Negativ betrachtet erleichtert es aber Kriminellen, die kritischen SCADA Systeme zu finden. Über shodan.io waren zum Beispiel bis vor kurzem die mit dem Internet verbundenen französischen Kraftwerke zu finden. Wer Zugang zu SCADA Systemen findet, kann diese in der Regel aber nicht nur kontrollieren, sondern diese auch modifizieren und manipulieren. Dies ist der IT-kritische Super-Gau nicht nur für Energieerzeuger, sondern für alle Nutzer von SCADA-Systemen, d.h. der kompletten Industrie. Nicht vergessen werden darf hierbei, dass diese Anfälligkeit mit Industrie 4.0 ein noch nie dagewesenes Gefährdungspotential erreichen wird.

Hinzu kommt, dass die laut dem aktuellen BSI Lagebericht eingesetzten Angriffsmethoden und -mittel immer vielfältiger werden:
– Schadsoftware
– Ransomware
– Social Engineering
– Advanced Persistent Threats
– Spam
– Botnetze
– DDoS
– Drive-by-Exploits und Exploit-Kits
– Identitätsdiebstahl
– Seitenkanalangriffe

[Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf;jsessionid=B1AF45C9BD3A80DBE9146BF7AA36526D.1_cid360?__blob=publicationFile&v=5]

Die Antwort der Bundesregierung auf die Bedrohung

2011 hat die Bundesregierung mit der Cybersicherheitsstrategie den Grundstein für mehr Sicherheit im Cyberraum gelegt. Die digitale Agenda des Jahres 2014 bereitete daraufhin den Weg für das im Juli 2015 in Kraft getretene IT-Sichergesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme), welches im Bereich der kritischen IT-Infrastrukturen (Energie- und Wasserversorgung, Gesundheitswesen, Finanzwesen, Telekommunikation u.a.) dafür sorgt, dass ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen nicht auftritt. Die 1. Verordnung zur Bestimmung kritischer Infrastrukturen (Kritis-VO) trat hiernach am 3. Mai 2016 in Kraft. Die 2. Verordnung wird im Frühjahr 2017 in Kraft treten.

Eine Pflicht zur Umsetzung der IT-Sicherheit nach dem Stand der Technik sowie eine Pflicht zur Überprüfung der Absicherung durch Dritte im Rahmen eines Audits ist durch § 11 EnWG durch den IT-Sicherheitskatalog vorgeschrieben. Abhängig von verschiedenen Kriterien betritt diese Pflicht:
– Energieversorgungsnetze
– Energieanlagen
– Genehmigungsinhaber nach §§ 6,7 oder 9 AtomG

Die Pflicht zur Einhaltung von IT-Sicherheitsstandards, zu denen Betreiber Kritischer Infrastrukturen mit dem IT-Sicherheitsgesetz verpflichtet werden, besteht zwei Jahre nach Inkrafttreten der Verordnung, aus der der Kreis der konkret Betroffenen ermittelt werden kann.

Prüfungsgrundlagen

Die Prüfungen werden im Rahmen von Zertifizierungsverfahren durchgeführt, d.h. die Zertifizierungen werden „nur" von Zertifizierungsgesellschaften durchgeführt, welche von der Deutschen Akkreditierungsgesellschaft DAkkS (Infos unter www.dakks.de) vorher akkreditiert sind. Grundlage hierfür ist die ISO/IEC 17021-1:2015.

Bei der Prüfung der Unternehmen des Energiesektors wenden die akkreditierten Zertifizierungsgesellschaften folgende Normen an:
– ***ISO 27001:2013*** (eigentliche Zertifizierungsgrundlage)
– ***ISO 27006:2015*** (Besondere Anforderungen für Zertifizierungsgesellschaften, die Informationssicherheitsmanagementsysteme (ISMS) zertifizieren
– ***ISO TR 27019*** (Leitfaden für das ISM von Steuerungssystemen der Energieversorgung auf Grundlage der ISO 27002
– ***ISO 19011:2011*** (Leitfaden zur Durchführung von internen und externen Audits

Von elementarer Bedeutung ist es in diesem Zusammenhang, dass man zumindest die relevanten Normkapitel der ISO 27001 kennen muss:

Kapitel 04: Kontext der Organisation
Kapitel 05: Führung
Kapitel 06: Planung
Kapitel 07: Unterstützung
Kapitel 08: Betrieb
Kapitel 09: Bewertung der Leistung
Kapitel 10: Verbesserung

Anforderungen an Auditoren, Auditdauer und Auditumfang:

Neben den „Standardanforderungen" an Auditoren verlangt Abschnitt 7.1 der ISO 27006:2015 weitere Anforderungen, welche die Auditoren im Rahmen einer von der Bundesnetzagentur anerkannten Schulung zu den Grundlagen der Energieversorgung mit Strom und Gas erlernen. Diese Schulung dauert sechs Tage und umfasst mindestens die nachfolgenden Themen:
– Rechtliche Rahmenbedingungen und Anforderungen in der Energiewirtschaft
– Technische Grundlagen der Strom- und Gasversorgung
– Grundlagen für den Netzbetrieb
– Netzsteuerung, Dispatching
– IT-Kritische Infrastrukturen für den Netzbetrieb-Scope des ISMS nach dem IT Sicherheitskatalog

Ein Auditverfahren besteht aus einer Erstzertifizierung, einem ersten Überwachungsaudit nach (spätestens) zwölf Monaten und einem zweiten Überwachungsaudit nach (circa) vierundzwanzig Monaten. Durch das so genannte Rezertifizierungsverfahren nach (circa) 36 Monaten erfolgt dann ein weiterer dreijähriger Zertifizierungszyklus.

Für die Auditdauer gelten die Vorgaben von Anhang B der ISO/IEC 27006:2015. Dabei ist die Formel zur Ermittlung der Auditdauer gemäß ISO/IEC 27006:2015 Anhang B.3.4 auf die besondere Situation des KRITIS Betreiber im Energiesektor abzustellen. In Abweichung zu ISO 27006:2015 ist eine Reduzierung der Auditdauer um maximal 10 Prozent zulässig. Die Standarddauer für die Erstzertifizierung ist aus dem nachfolgenden Auszug aus der folgenden Tabelle zu entnehmen:

VZÄ	Audit-tage	VZÄ	Audit-tage
1 bis 10	5	176 bis 275	14
11 bis 15	6	276 bis 425	15
16 bis 25	7	426 bis 625	16,5
26 bis 45	8,5	626 bis 875	17,5
46 bis 65	10	876 bis 1175	18,5
66 bis 85	11	1.176 bis 1.550	19,5
86 bis 125	12	1.551 bis 2.025	21
126 bis 175	13	2.026 bis 2.675	22

Hinweise: VZÄ = Mitarbeiter-Vollzeitäquivalente; ein Audittag umfasst eine reine Auditzeit von acht Zeitstunden (ohne Pausen und eventuelle Fahrzeiten)

Die Anzahl der zu auditierenden Standorte bestimmt sich wie folgt aus Abschnitt 9.1.5.1. der ISO/IEC 27006:2015:

Erstzertifizierung:
Quadratwurzel aller Standorte

Überwachungsaudit:
Quadratwurzel aller Standorte x 0,6

Rezertifizierungsaudit:
Quadratwurzel aller Standorte x 0,8

Stationen eines Auditverfahrens

Alles beginnt mit der Auswahl der „richtigen“ Zertifizierungsgesellschaft und des richtigen leitenden Auditors.

Hieran schließt sich die Auditplanung an, d.h. die organisatorische Abstimmung zwischen KRITIS – Betreiber und dem Lead-Auditor der Zertifizierungsgesellschaft. Im Rahmen der Auditplanung werden abgestimmt:

- Geltungsbereich
- Termine
- Interviewpartner
- Standorte
- Prüfbereiche

Das Erstzertifizierungsaudit besteht aus einem Audit der Stufe 1 sowie einem Audit der Stufe 2, bei allen weiteren Auditformen entfällt i.d.R. Stufe 1.

Das Audit der Stufe 1 hat folgende Ziele:

- Auditierung der Managementsystemdokumentation
- Beurteilung standortspezifischer Bedingungen
- Statusbewertung des Kunden
- Informationsabstimung zum Geltungsbereich, der Prozesse, der Standorte, gesetzlicher und behördlicher Aspekte etc.
- Zuteilung der Ressourcen für Stufe 2
- Schwerpunktbildung für das Audit der Stufe 2
- Beurteilung der Managementsystembewertung und des internen Audits

Zum Ende der Auditstufe 1 wird dem Kunden in einer Abschlussbesprechung mitgeteilt, ob es mit Stufe 2 weitergehen kann oder nicht.

Das Audit der Stufe 2 hat das Ziel, die Umsetzung einschließlich der Wirksamkeit des Managementsystems zu bewerten. Hierzu setzen die Auditoren Auditchecklisten ein, mit denen Normforderung und Umsetzung in der Realität verglichen werden. Es empfiehlt sich, diese Auditchecklisten im Vorhinein von der Zertifizierungsgesellschaft anzufordern, um die Denkart des Zertifizierers zu kennen.

Im Rahmen des Audits kann es dann natürlich vorkommen, dass Normanforderung und Umsetzung nicht übereinstimmen. In der Regel wird dann vom Lead-Auditor eine Empfehlung gegeben oder eine Feststellung (in der Regel in der Klassifizierung als Einzelabweichung oder Abweichung) getroffen. Der Kunde muss nun eine Ursachenanalyse betreiben, eine Korrekturmaßnahme ableiten sowie durchführen und die Zertifizierungsgesellschaft muss die Wirksamkeit der Korrekturmaßnahme abschließend bewerten.

So wie zu Beginn des Audits eine Eröffnungsbesprechung durchgeführt wird, wird zum Ende des Audits eine Abschlussbesprechung durchgeführt.

Ein weit verbreiteter Irrglaube besteht darin, dass im Rahmen der Abschlussbesprechung vom Lead-Auditor mitgeteilt wird, ob das Auditergebnis mit positiv endete oder nicht. Der Lead-Auditor übersendet jedoch die Unterlagen zusammen mit seiner Empfehlung an den Zertifizierungsausschuss der Zertifizierungsgesellschaft, welcher dann nach Sichtung aller Unterlagen und ggf. nach Rücksprache mit dem Kunden entscheidet, ob der Empfehlung des leitenden Auditors gefolgt werden kann oder nicht.

Obwohl die Auditoren bei ihren Feststellungen in der Regel sehr sorgfältig arbeiten, kann es durchaus vorkommen, dass die Kundenorganisation eine andere Sichtweise hat und man sich auf der Abschlussbesprechung nicht auf eine gemeinsame Bewertung einigen kann. In solchen Fällen hat der KRITIS Betreiber dann natürlich die Möglichkeit, sich im Rahmen einer Beschwerde an die Zertifizierungsgesellschaft zu wenden.

Implementierung des ISMS – Basis für die erfolgreiche Zertifizierung:

Beratungsgesellschaften im Business der Implementierung von zertifizierungsfähigen Managementsystemen leben in der Regel davon, dass diese ihre StandardberaterInnen haben, welche wissen, was an Nachweisen in einem Zertifizierungsverfahren erforderlich ist, so dass diese von Woche zu Woche „erfolgreich“ Unternehmen der verschiedensten Branchen durch eine Zertifizierung bewegen können. Bis dato war dies zweifelsfrei so, gleichwohl ist jetzt durch den fachspezifischen IT-Sicherheitskatalog und den Leitfaden für die Energiewirtschaft, d.h. die ISO TR 27019, Bewegung ins Spiel gekommen. Und durch die Anforderungen der Energiewirtschaft an die AuditorInnen müssen die BeraterInnen damit rechnen, dass AuditorInnen in den ISO 27001 Audits der Energiewirtschaft sitzen, die tatsächlich Ahnung von der Materie haben. Aus diesem Grunde sind Unternehmen der Energiewirtschaft gut beraten, sich keine Low-Cost-BeraterInnen ohne Bezug zur Energiewirtschaft einzukaufen, sondern BeraterInnen, die auch hinreichendes Fachwissen aus der Energiebranche mitbringen. Nur hierdurch ist sichergestellt, dass die Implementierung des ISMS – Systems nach ISO 27001 auch nachhaltig zu einer erfolgreichen Zertifizierung führt. Und auch von BeraterInnen, die kostengünstige Standarddokumentationen für die Energiewirtschaft im Bereich der ISO 27001 anbieten, sollte dringend Abstand gehalten werden, denn hier ist die Energiewirtschaft viel zu komplex.

Eine gern gestellte Frage in diesem Zusammenhang besteht natürlich darin, ob es eine Faustregel dafür gibt, wie lange man zur Implementierung eines ISMS benötigt und ob es hierzu einen Strukturplan oder einen Meilensteinplan gibt. Frage 1 ist aus den bisherigen Erfahrungswerten relativ leicht damit zu beantworten, dass von der Entscheidung der obersten Leitung eines Energieunternehmens bis zur erfolgreichen Erstzertifizierung in der Regel (mindestens) 12 Monate liegen.

Als Meilensteine der Implementierung kann man sich an dem nachfolgen Zeitraster orientieren:

<u>Monat 01:</u>
Kick-Off-Veranstaltung zur Erläuterung des Vorhabens
Festlegung des Anwendungsbereiches des Managementsystems
Schulung der zukünftigen ISMS Beauftragten/ISMS-Auditoren
IST-Analyse mittels Fragebögen, die sich orientieren an ISO 27002, ISO TR 27019 und dem IT-Sicherheitskatalog

<u>Monat 02:</u>
Rollen, Verantwortungen und Befugnisse in der Organisation verifizieren und modifizieren
Kontext der Organisation in Bezug auf die ISO 27001 festlegen
Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Festlegung von Politik und Vision
Verifizierung von Ressourcen, Kompetenz und Bewusstsein
Informationssicherheitsziele und Planung zu deren Erreichung

Monat 03:
Bewertung der betrieblichen Planung und Steuerung
Risiko- und Chancenmanagement
Informationssicherheitsrisikobeurteilung und -behandlung
Festlegung der erforderlichen dokumentierten Informationen
Managementsystemdokumentation erstellen

Monat 08:
Managementsystemdokumentation freigeben
Interne Audits durchführen (System, Prozess, Produkt)
Nichtkonformitäten, Korrekturmaßnahmen und fortlaufende Verbesserung realisieren

Monat 10:
Managementbewertung durchführen

Monat 11:
Simulation eines externen Audits

Monat 12:
Externes Audit durch Zertifizierungsstelle

Theoretisch kann man den Prozess auch schneller erfolgreich abgeschlossen haben, theoretisch kann man aber auch ein ganzes Leben lang auf Kaffee, Tee und Zucker verzichten.

Was für einen Nutzen hat die Implementierung eines ISMS letztlich für ein Unternehmen der Energiewirtschaft:

Implementierung und Zertifizierung von Managementsystemen kosten Geld und kein Unternehmen der Welt gibt gerne Geld aus. Betrachten wir also den Return on Invest, d.h. welchen Nutzen hat ein Unternehmen der Energiewirtschaft durch dieses Managementsystem:

- Erfüllung der gesetzlichen Anforderungen des IT-Sicherheitsgesetzes sowie Vermeidung von Bußgeldern
- Klar definierte Abläufe und Rollen im Bereich der Informationssicherheit
- Reduktion der Risiken im operativen Business, da ein operativer Ausfall in der Regel existenzbedrohend ist
- Vermeidung bzw. Reduktion strafrechtlicher Konsequenzen für die verantwortlichen Führungskräfte

Diese Nutzen sollten in der Regel die Kosten übertreffen. Sollte der Invest hierfür nicht vorhanden sein, so stellt sich per se die Frage, ob das entsprechende Unternehmen wirklich mittelfristig überlebensfähig ist und keine Gefahr für die Energieversorgung unserer Gesellschaft darstellt.

Nehmen Sie zudem gerne das Angebot des Simulatorzentrums zur Teilnahme an einer kostenlosen Info-Veranstaltung am 28. Juni 2017 zum Thema

Implementierung von Managementsystemen nach ISO27001 für Kritis-Betreiber der Energiewirtschaft

an. Verschaffen Sie sich Planungssicherheit und erhalten Sie wertvolle Praxistipps, um Ihr ISMS-Projekt erfolgreich zum Abschluss zu bringen und die Sicherheit Ihrer IT nachhaltig zu verbessern.

Gerne können Sie sich über einen der folgenden Links noch einmal über die Inhalte informieren und sich bei Interesse direkt dort registrieren.

www.vgb.org/it_sicherheitsgesetzt_infoveranstaltung.html
simulatorzentrum.de/2017/03/28/infoveranstaltung-it-sicherheit

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), u.a. IT-Personalzertifizierungen von Microsoft (MCSE, MCDBA, MCSD), Cisco, Novell sowie CompTIA, mehr als zehn Jahre Erfahrung in der Energiewirtschaft, u.a. für die Gas- und Ölindustrie im Nahen Osten, in der Pipeline- und Messtechnik in Kanada und den Niederlanden sowie mehrjähriger leitender Auditor für die Zertifizierung der Kraftwerksschule und des Simulatorzentrums (KSG / GfS).