ISO 27001 – praxisorientierte Umsetzungsschritte für einen sicheren Netzbetrieb

Selten stand die Energiewirtschaft durch die Energiewende vor so hohen Anforderungen wie in den letzten Jahren und ein Nachlassen des Änderungsdruckes ist aktuell nicht zu erwarten. Vielfältige dezentrale Einspeisungen mit unstetiger Erzeugung, Engpässe in den Netzkapazitäten, neue Geschäftsmodelle und gesetzliche Vorgaben setzen vernetzte und intelligente IT-Systeme als Basis für eine zukünftige sichere Energieversorgung voraus.

Werden aktuell Themen wie Smart Metering und eMobilisierung umgesetzt, stehen mit Industrie 4.0 schon die nächsten in den Startlöchern. Einhergehend mit diesem Trend verschärfen sich die Anforderungen an die IT-Sicherheit, nicht nur aus Sicht der Infrastruktur. Auch die Zunahme professioneller Einbrüche durch Malware mit Viren, Trojanern, Würmern, Spyware und vielen weiteren Möglichkeiten in Netzwerken, Servern und Steuerungseinheiten sowie ein mangelndes Bewusstsein seitens der Mitarbeiter sind in punkto Sicherheit zu berücksichtigen. Die Liste der Fälle, in denen bekannte Sicherheitslücken für gezielte Übergriffe auf kritische Infrastrukturen ausgenutzt bzw. diese durch sonstige Malware gefährdet wurden, wird zunehmend länger. Genannt seien hier der Ausfall eines Hochofens in Deutschland mit einem beträchtlichen Schaden und Stuxnet zur Manipulation der eingesetzten Steuerungstechnik. Weitere Veröffentlichungen und Live-Präsentationen machen deutlich, wie einfach in ausgesuchten Fällen der Zugriff auf die Versorgungsinfrastruktur ist.

Studien belegen die gravierenden Folgen bei einem Ausfall der kritischen Infrastrukturen. Um dieser Gefahr zu begegnen, hat der Gesetzgeber die Anforderungen an einen sicheren Netzbetrieb definiert, der mit der Einführung eines an die Branchenspezifika angepassten Informations-Sicherheits-Managementsystem (ISMS) nach ISO 27001 gegeben ist.

Laut Gesetzgebung müssen Betreiber durch geeignete IT-Sicherheitsmaßnahmen dafür sorgen, dass die als kritisch eingestuften Infrastrukturen nicht durch interne oder externe Bedrohungen gestört werden. Zudem sind sicherheitsrelevante Zwischenfälle meldepflichtig.

IT-Sicherheitskatalog veröffentlicht

Die Bundesnetzagentur hat aufbauend auf dem im Juli 2015 verabschiedeten IT-Sicherheitsgesetz einen IT-Sicherheitskatalog (***Bild 1***) veröffentlicht, der die Unternehmen zur Umsetzung IT-sicherheitstechnischer Mindeststandards und zur Einführung eines ISMS gemäß ISO 27001 verpflichtet. Bezieht sich der IT-Sicherheitskatalog speziell auf IT- und TK-Systeme, so adressiert die ISO 27001 alle Aspekte zur Informationssicherheit einschließlich der Risikoanalysen und der organisatorischen Einbettung im Unternehmen.

Die Unternehmen haben zwei Jahre Zeit, ein den gesetzlichen Anforderungen entsprechendes Informations-Sicherheits-Management-System einzuführen und zertifizieren zu

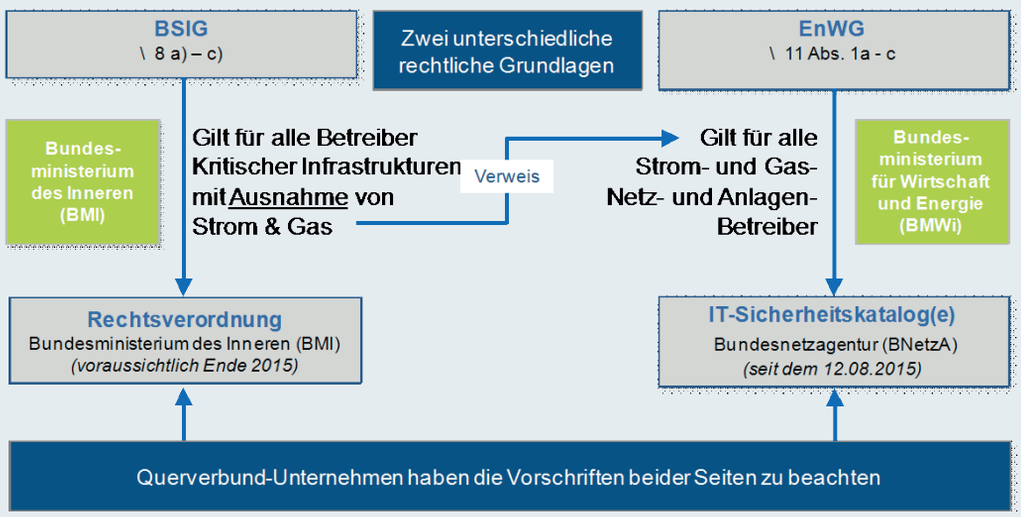

***Bild 1**: Neben einer Rechtsverordnung des BMI, die Ende 2015 erscheinen soll, hat die Bundesnetzagentur einen IT-Sicherheitskatalog für Netzbetreiber veröffentlicht*

lassen. Unternehmen, die sich nicht daran halten, drohen erhebliche Bußgelder je Einzelverstoß, die im Wiederholungsfall ansteigen können.
Entsprechende Rechtsverordnungen für die nichtregulierten Netzbetreiber werden zum Jahreswechsel erwartet.
Die Unterscheidung zwischen regulierten und nicht regulierten Bereichen stellt klassische Querverbundunternehmen vor die Aufgabe, ein harmonisiertes und rechtskonformes ISMS zu definieren und einzuführen.
Hierzu bietet sich in einem ersten Schritt eine Voranalyse an, in der zum einen ein einheitlicher Wissenstand zu den Themen IT-Sicherheitsgesetz und IT-Sicherheitskatalog geschaffen wird und die daraus resultierenden konkreten Anforderungen an das Unternehmen definiert werden. Zum anderen wird der Geltungsbereich des einzuführenden ISMS (Festlegung der zu betrachtenden Sparten und kritischen Infrastrukturen, nur technische oder auch kaufmännische Systeme, gegebenenfalls abweichender Geltungsbereich zur Zertifizierung, etc.) festgelegt.
Da erfahrungsgemäß in vielen Unternehmen schon IT-sicherheitsrelevante Maßnahmen umgesetzt wurden, muss in einem weiteren Schritt der Reifegrad und hieraus abgeleitet der Handlungsbedarf bestimmt werden. Dieser Arbeitsschritt setzt ein hohes Maß an methodischem und inhaltlichem Wissen voraus, da hier die Weichen für ein später zertifizierungsfähiges System gestellt werden.

Daran anschließend startet die operative Projektarbeit zur Einführung eines ISMS entsprechend den getroffenen Festlegungen (***Bild 2***). Deutlich werden hier die verschiedenen Zielrichtungen und Untersuchungsbereiche, die mit einer erfolgreichen ISMS-Einführung verbunden sind. Die Bearbeitung erfolgt in Workshops, in denen die individuellen Strukturen der Unternehmen für die ISMS-Einführung adaptiert und die entsprechenden Regelwerke und Prozessvorgaben festgelegt werden. Neben der Dokumentation erfolgt die sukzessive Einführung durch Informationsveranstaltungen und prozessbegleitende Schritte. Abschließend werden die Ergebnisse nochmals gegen die Vorgaben überprüft, um ggf. offene Fragestellungen und ausstehende Detailfestlegungen abschließend umzusetzen.
Jedes definierte System ist nur so gut, wie es in den Unternehmen gelebt wird. Wir empfehlen, die Einführung und den Betrieb des ISMS regelmäßig und vor den jeweiligen Zertifizierungen zu überprüfen. Dieses erfolgt anhand definierter Leitlinien und Prozessvorgaben, aber auch in der Umsetzung vorgegebener Maßnahmen und dem Umgang mit der sicherheitskritischen Infrastruktur. Hier bietet sich neben der rein formalen Begleitung der Aufbau von Szenarien und die Durchführung von Penetrationstests an, anhand derer das ISMS geprüft und ggf. nachgesteuert werden kann.

***Bild 2**: Zielrichtungen und Untersuchungsbereiche, die mit einer erfolgreichen Einführung eines Information Security Management Systems (ISMS) verbunden sind*

Zertifikat in Arbeit

Derzeit erarbeitet die Bundesnetzagentur gemeinsam mit der Deutschen Akkreditierungsstelle (DAkkS) ein eigenes Zertifikat. Das Zertifikat wird im Wesentlichen auf dem bereits existierenden Zertifikat bzw. Zertifizierungsschema zur ISO/IEC 27001 basieren und dieses um die zusätzlichen Anforderungen des IT-Sicherheitskatalogs ergänzen. Des Weiteren soll der Anwendungsbereich (Scope) spezifiziert werden, um sicherzustellen, dass zumindest die für einen sicheren Netzbetrieb notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme von der Zertifizierung erfasst sind.

Bereits bestehende Zertifizierungen nach ISO/IEC 27001, BSI Grundschutz usw. sind nicht ausreichend, um die Erfüllung der Anforderungen des IT-Sicherheitskatalogs nachzuweisen.

Zusammenfassend ist zu sagen, dass die Einführung eines ISMS vor dem Hintergrund der Zunahme externer Bedrohungen und der Digitalisierung auf Seiten der Netzbetreiber unabhängig von den gesetzlichen Vorgaben sinnvoll und notwendig ist. Letztere führen zu einem Umsetzungszwang bei einer Vielzahl von Vorgaben, Definitionen und aktuell noch offenen Fragestellungen. Um hier einen möglichst guten Überblick und Einstieg in die notwendigen Projektschritte zu erhalten, bietet Fichtner IT Consulting ein ISMS-Kompendium zur

- Festlegung des Geltungs-/Anwendungsbereichs des ISMS (inkl. Schutzbedarfsermittlung),
- Einleitung der notwendigen organisatorischen Maßnahmen und Sicherstellung der erforderlichen Rahmenparameter,
- Einrichtung des geforderten Sicherheitsprozesses

an.

Mit diesem Leitfaden (***Bild 3***) lassen sich mit überschaubarem Aufwand die operativen Handlungsbedarfe, die aus der Umsetzung der Anforderungen des IT-Sicherheitskataloges und des IT-Sicherheitsgesetzes resultieren, frühzeitig identifizieren und bewerten, um so eine ausreichende Planungssicherheit zu erlangen.

***Bild 3**: ISMS-Handbuch*

Unerlässlich ist auf jeden Fall, eine ISMS-Einführung mit Augenmaß auf die Bedrohungssituation und die spezifischen Aufgaben und Abläufe des jeweiligen Netzbetreibers umzusetzen.

AUTOR

HEIKO WISSEL
Fichtner Consulting AG, Stuttgart
Tel. +49 711 8995-1484
heiko.wissel@fit.fichtner.de