ew
Magazin für die Energiewirtschaft
www.ew-magazin.de
SONDERDRUCK (Nr. 7401) aus 2017 (Jg. 116), Heft 3, S. 60-63

IT-Sicherheitskatalog

Stromnetz Hamburg erhält ISMS-Zertifizierung

von Andreas Krause und Robert Strade, Stromnetz Hamburg GmbH;
Michael Pietsch und Dr. Herbert Slomski, Consulectra Unternehmensberatung GmbH

IT-Sicherheitskatalog

Stromnetz Hamburg erhält ISMS-Zertifizierung

Die Stromnetz Hamburg GmbH hat ein Informationssicherheitsmanagementsystem unter Berücksichtigung des IT-Sicherheitskatalogs der Bundesnetzagentur eingeführt und das Einführungsprojekt mit der Zertifizierung abgeschlossen.

Eine Kernforderung in dem im August 2015 von der Bundesnetzagentur (BNetzA) veröffentlichten IT-Sicherheitskatalog gemäß § 11 (1a) des Energiewirtschaftsgesetzes ist die Einführung eines Informationssicherheitsmanagementsystems (ISMS) nach DIN ISO/IEC 27001 sowie die Zertifizierung durch eine unabhängige hierfür zugelassene Stelle. Zusätzlich sind durch die Norm DIN ISO/IEC TR 27019 (DIN SPEC 27019) erweiterte Anforderungen um Besonderheiten im Bereich der Prozesssteuerung der Energieversorgung umzusetzen und ein Netzstrukturplan zu erstellen. Der Netzbetreiber ist verpflichtet, die Konformität seines ISMS mit den Anforderungen des IT-Sicherheitskatalogs bis zum 31. Januar 2018 durch ein Zertifikat von einer bei der Deutschen Akkreditierungsstelle (DAkkS) akkreditierten Stelle nachzuweisen.

Mit dem im November 2016 erfolgreich durchgeführten Zertifizierungsaudit für das eingeführte ISMS ist die Stromnetz Hamburg GmbH (SNH) einer der ersten Netzbetreiber in Deutschland, die eine Zertifizierung ihres ISMS konform zum IT-Sicherheitskatalog erhalten. Der Zertifizierung ging ein für alle Beteiligte anstrengendes und anspruchsvolles Projekt voraus, das zwar mit der Zertifizierung einen Abschluss findet, der aber nur als Zwischenetappe gesehen werden kann, denn die Etablierung eines ISMS bedeutet weiterhin eine permanente Beschäftigung mit dem Thema Informationssicherheit.

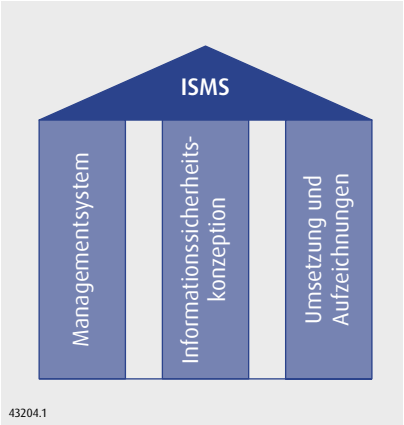

Bild 1: Aufgabenbereiche als Säulen des ISMS

Projektübersicht

Das Projekt zur Einführung eines ISMS bei SNH wurde bereits Anfang 2015 begonnen, als absehbar war, dass der IT-Sicherheitskatalog durch die BNetzA veröffentlicht wird. Das Projekt bestand zunächst aus den Teilprojekten zur Einführung des ISMS und der Erstellung der Informationssicherheitshandbücher und Richtlinien für den Bereich Netzführung. Ende 2015 wurde entschieden, den Geltungsbereich des ISMS so zu erweitern, dass auch der Bereich Metering einbezogen wird, der aufgrund des angekündigten Gesetzes zur Digitalisierung der Energiewende für den Betrieb der Smart-Meter-Gatewayadministration ebenfalls ein ISMS etablieren muss. Das neu implementierte Teilprojekt umfasste die beiden neuen Geltungsbereiche Smart-Meter-Gatewayadministration und den Betrieb einer Zertifizierungsstelle (Sub Certification Authority, Sub-CA) zur Vergabe von Zertifikaten und Schlüsseln für die verschlüsselte und sichere Datenübertragung im Rahmen der Smart-Metering-Public-Key-Infrastruktur.

Ein wichtiges Element des ISMS ist die systematische Risikobewertung der Informationswerte.

Durch die Synchronisierung dieser Vorhaben konnten vor allem im Bereich des Managementsystems deutliche Synergien erzielt werden, während die Sicherheitskonzeptionen jeweils ihre systemspezifischen Schwerpunkte hatten. Entsprechend wurde die ISMS-Organisation mit einem übergeordneten ISMS-Verantwortlichen und einem ISMS-Beauftragten sowie Informationssicherheitsbeauftragte für die einzelnen Geltungsbereiche Netzführung, Smart-Meter-Gatewayadministration und Sub-CA aufgebaut.

Für eine erfolgreiche Einführung eines ISMS sind drei Aufgabenbereiche zu betrachten, die als die Säulen des ISMS dargestellt werden können und gleichermaßen wichtig sind (*Bild 1*):

- Managementsystem
- Informationssicherheitskonzeption
- Umsetzung und Aufzeichnungen.

Managementsystem

Das grundsätzliche Vorgehen für den Aufbau und die Etablierung des Managementsystems ist in *Bild 2* dargestellt. Ausgangspunkte sind die mit der Unternehmensleitung abgestimmte ISMS-Leitlinie, die festgelegte ISMS-Organisation und der definierte Geltungsbereich des ISMS.

Ein wichtiges Element des ISMS ist die systematische Risikobewertung der Informationswerte. Im Rahmen der Risikoanalyse werden die Assets und Informationswerte des Geltungsbereichs bezüglich der möglichen Bedrohungen analysiert und bewertet. Zur Begegnung der ermittelten Risiken werden Maßnahmen aus dem Anhang der ISO/IEC 27001 und aus der ISO/IEC 27019 ausgewählt, die angewendet werden sollen, um das Risiko zu reduzieren. Dies wird in der Erklärung zur Anwendbarkeit (Statement of Applicability, SoA) dokumentiert. In einem Risikobehandlungsplan werden die konkreten Maßnahmen dokumentiert, die innerhalb eines festgelegten Zeitplans

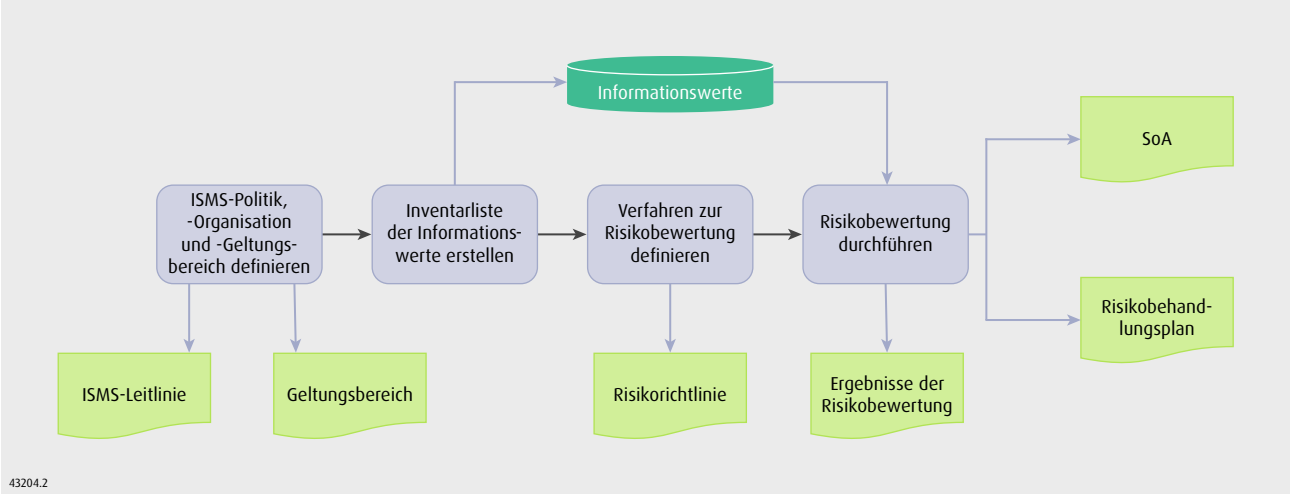

Bild 2. Risikomanagement als wichtiges Element eines ISMS

zur Reduzierung des Risikos umgesetzt werden sollen. Die Risikobewertung wird entsprechend der Vorgaben der erstellten Risikorichtlinie regelmäßig (mindestens jährlich) durchgeführt, um sicherzustellen, dass die Risikobewertung geänderte Rahmenbedingungen berücksichtigt.

Weitere Aspekte zur Unterstützung des kontinuierlichen Verbesserungsprozesses bestehen in der Definition von Kennzahlen (Key Performance Indicator, KPI), mit denen die Erreichung der definierten Informationssicherheitsziele gemessen und überwacht werden können, sowie interne und externe Audits und die Bewertung durch das Management (*Bild 3*). Alle festgestellten Nichtkonformitäten und Verbesserungsmöglichkeiten werden in einer entsprechenden Liste strukturiert erfasst und durch die jeweils benannten Verantwortlichen bearbeitet. Für den Umgang mit Informationssicherheitsvorfällen sind eine Meldestelle und ein entsprechender Prozess eingerichtet. Ein ebenfalls sehr wichtiger Punkt für eine Etablierung eines ISMS ist die Schulung und Sensibilisierung der Mitarbeiter. Nur entsprechend sensibilisierte Mitarbeiter können dafür sorgen, dass die vorgegebenen Regeln zur Informationssicherheit eingehalten und Abweichungen erkannt und behoben werden können. Zusammengefasst sind mindestens die in *Tafel 1* aufgelisteten Dokumente beziehungsweise Beschreibungen im Rahmen des Managementsystems zu erstellen beziehungsweise bereitzustellen.

Der SNH kam beim Aufbau des ISMS zugute, dass bereits andere Managementsysteme wie Qualitäts-, Umwelt- und Energiemanagementsysteme im Rahmen eines integrierten Managementsystems etabliert waren und so teilweise auf vorhandene Prozessbeschreibungen und Richtlinien zurückgegriffen werden konnte. Dennoch bedeutete es für alle Beteiligte viel Arbeit, das ISMS für die Geltungsbereiche zu etablieren und zum Leben zu erwecken.

Informationssicherheitskonzeption

Für die Beschreibung der Informationssicherheitskonzeption konnte zwar teilweise auf vorhandene Richtlinien und Dokumentationen zurückgegriffen werden, da die SNH bereits in der Vergangenheit großen Wert auf die Informationssicherheit gelegt hatte. Dennoch entstand auch hier nicht unerheblicher Aufwand, die Informationssicherheitshandbücher, Richtlinien und Arbeitsanweisungen an die Anforderungen der Normen anzu-

Plichtdokumente
■ ISMS-Leitlinie
■ ISMS-Geltungsbereich
■ ISMS-Organisation und -Verantwortung
■ Risikorichtlinie mit Beschreibung der Methode der Risikobewertung
■ Risikobewertungsberichte
■ Erklärung zur Anwendbarkeit (SoA)
■ Risikobehandlungsplan
■ Informationssicherheitsziele und Beschreibung der Verfahren zur Messung des KPI
■ Schulungskonzept
■ Verfahren zur Lenkung dokumentierter Informationen
■ Verfahren zum Umgang mit Korrektur- und Vorbeugemaßnahmen
■ Auditberichte von internen Audits
■ Berichte von Managementbewertungen

Tafel 1. Plichtdokumente für das Managementsystem

Informationssicherheitskonzeption
■ Personalsicherheit
■ Verwaltung und Nutzung von Werten
■ Klassifizierung von Informationen
■ Handhabung von Datenträgern
■ Zugangssteuerung zu Systemen und Benutzerverwaltung
■ Zutrittssicherheit für Räume und Gebäude
■ Sicherheit von Geräten und Betriebsmitteln
■ Änderungsmanagement und Betriebssicherheit von Systemen
■ Netzwerksicherheit und sichere Informationsübertragung
■ kryptographische Maßnahmen
■ Lieferantenbeziehungen und Verträge
■ Verfahrensbeschreibung zum Umgang mit Informationssicherheitsvorfällen
■ Notfallmanagement
■ Netzstrukturplan

Tafel 2. Themenbereiche im Rahmen der Informationssicherheitskonzeption

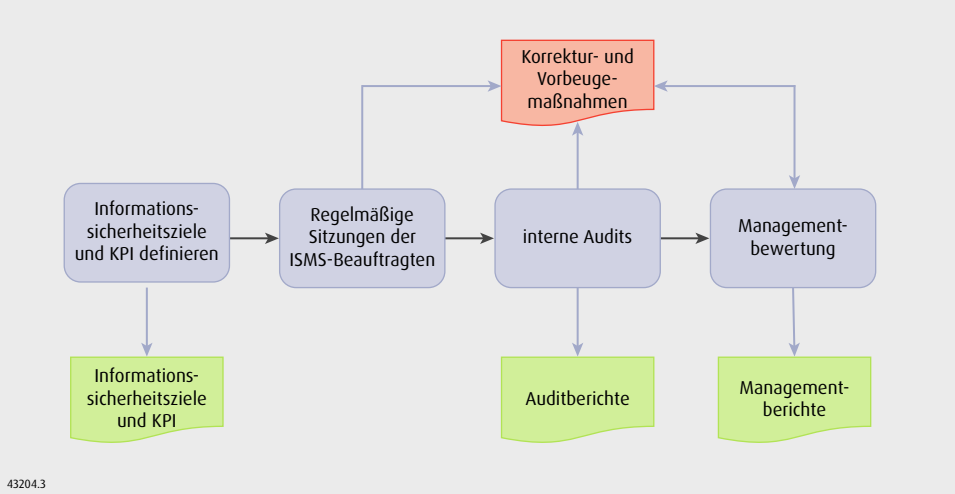

Bild 3. Elemente des kontinuierlichen Verbesserungsprozesses

passen beziehungsweise neu zu erstellen. Konkret bedeutete das, dass jeweils Antworten auf die rund 150 anwendbaren Maßnahmen aus den Normen ISO/IEC 27002 und ISO/IEC 27019 gefunden werden mussten.

Des Weiteren gehörte dazu auch die Entwicklung des Netzstrukturplans, der die vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten mit den jeweiligen Haupttechnologien und deren Verbindungen strukturiert darstellt. Zusammengefasst sind im Rahmen der Informationssicherheitskonzeption mindestens die in *Tafel 2* dargestellten Themenbereiche zu behandeln.

Umsetzung und Aufzeichnungen

Die Systeme rund um das Netzleitsystem bei der SNH genügten bereits in der Vergangenheit einem hohen Standard der Informationssicherheit. Um nachzuweisen, dass die in den Richtlinien und Arbeitsanweisungen vorgegebenen Regeln auch eingehalten und umgesetzt werden, sind entsprechende Aufzeichnungen und Dokumentationen erforderlich. Dazu gehören unter anderem:

- die Vergabe von Zugangsberechtigungen
- Protokolle von Anwenderaktivitäten
- Aufzeichnungen von Sicherheitsvorfällen
- durchgeführte Schulungsmaßnahmen
- Korrektur- und Vorbeugemaßnahmen
- Messungen der KPI.

Internes Audit

Im Vorfeld des Zertifizierungsaudits wurde ein internes Audit durch einen externen Auditor durchgeführt. Dadurch wurde sichergestellt, dass das ISMS mit einem neutralen Blick begutachtet wurde. Dabei wurden einige Schwachstellen aufgedeckt, die bis zum Zertifizierungsaudit noch behoben werden konnten.

Zertifizierungsaudit

Alle genannten Aufgabenbereiche sind im Rahmen des Zertifizierungsaudits durch die Datenschutz Cert GmbH ausführlich geprüft worden. Das Zertifizierungsaudit gliederte sich in eine Dokumentenprüfung (Stufe 1) und eine Prüfung der Umsetzung (Stufe 2), bei der detailliert die Umsetzung der Sicherheitsvorgaben in den IT-Systemen sowie das Managementsystem geprüft wurden.

Es hat sich gezeigt, dass die SNH gut aufgestellt waren und das Audit erfolgreich bestanden haben. Das ISMS-Einführungsprojekt wurde mit Unterstützung der Consulectra Unternehmensberatung GmbH durchgeführt. Dazu sagt Gero Boomgaarden, Geschäftsbereichsleiter Netzbetrieb und ISMS-Verantwortlicher der SNH: »Ein Beratungsunternehmen kann zwar einen gewissen Anteil der Arbeiten übernehmen; dennoch sollte der Aufwand im Unternehmen selbst nicht unterschätzt werden, denn ein ISMS lebt davon, dass die Mitarbeiter des Unternehmens die Prozesse und Regelwerke verinnerlichen und aktiv in ihren Arbeitsprozess aufnehmen.«

Andreas Krause, Leitstellensysteme und ISMS-Beauftragter, Stromnetz Hamburg GmbH, Hamburg

Robert Strade, Fachbereichsleiter Betriebsorganisation und Projektleiter Einführung ISMS, Stromnetz Hamburg GmbH, Hamburg

Michael Pietsch, Projektleiter, Consulectra Unternehmensberatung GmbH, Hamburg

Dr. **Herbert Slomski**, Projektleiter, Consulectra Unternehmensberatung GmbH, Hamburg

>> andreas.krause@stromnetz-hamburg.de
robert.strade@stromnetz-hamburg.de
m.pietsch@consulectra.de
h.slomski@consulectra.de

>> www.stromnetz-hamburg.de
www.consulectra.de