Praxisleitfaden IT-Sicherheitskatalog

Anforderungen an die IT für den sicheren Betrieb von Energieversorgungsnetzen

www.bitkom.org

VKU VERBAND KOMMUNALER UNTERNEHMEN e.V.

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
Tel.: 030 27576-0 | Fax: 030 27576-400
bitkom@bitkom.org

www.bitkom.org

und

VKU
Invalidenstraße 91 | 10115 Berlin
Tel.: 030 58580-0 | Fax: 030 58580-101
info@vku.de

www.vku.de

Ansprechpartner Bitkom

Felix Dembski, Bereichsleiter Intelligente Netze und Energie
T 030 27576-204 | f.dembski@bitkom.org

Ansprechpartner VKU

Benjamin Sommer, Referent Informations- und Kommunikationstechnologie
T 030.58580-194 | sommer@vku.de

Verantwortliches Bitkom-Gremium

AG Smart Grids – Projektgruppe IT-Sicherheitskatalog

Verantwortliches Gremium VKU

Ausschuss Netzwirtschaft

Praxisleitfaden IT-Sicherheitskatalog

Anforderungen an die IT für den sicheren Betrieb von Energieversorgungsnetzen

Inhaltsverzeichnis

1 IT-Sicherheitsbestimmungen für Betreiber von Energieversorgungsnetzen 8

Einführung 8

1.1 Gesetzlicher Rahmen für die Sicherheit in Energieversorgungsnetzen 9

1.1.1 Allgemeine Regelungen aus dem Energiewirtschaftsgesetz 9

1.1.2 Der IT-Sicherheitskatalog der BNetzA 10

1.1.3 Zusätzliche Regeln für Betreiber Kritischer Infrastrukturen 12

1.2 Schritte zu einem ISMS nach dem IT-Sicherheitskatalog 14

1.3 Fristen 15

1.4 Ansprechpartner 16

1.5 Exkurs: Anreizregulierung 16

2 Definition des Anwendungsbereichs des ISMS 20

2.1 Richtige Bestimmung des Scope 21

2.2 Grenzen des ISMS 25

2.3 Schnittstellen zur Sicherheitsorganisation außerhalb des Scope 27

2.4 Beteiligte Mitarbeiter 29

2.5 Anwenden des Scope im laufenden ISMS-Projekt 33

2.6 Exkurs: Den Scope – aus Sicht eines Zertifizierers – strukturiert aufsetzen 34

3 Aufwand, Zeit und Personal 38

3.1 Zeit 38

3.1.1 Erfahrungswerte bei der erstmaligen Einführung eines ISMS 38

3.1.2 Aufwand der Implementierung eines ISMS 39

3.1.3 Vom Audit zur Zertifizierung 40

3.2 Personal 41

3.2.1 Ansprechpartner für IT-Sicherheit 42

3.2.2 Weitere Rollen zur Etablierung eines ISMS-Projektes im Unternehmen 43

3.2.3 Weitere Rollen zur Etablierung eines ISMS-Projektes außerhalb des Unternehmens 45

3.3 Zeitplan zum Einsatz des Personals 46

4 Überführung bestehender IT-Sicherheitssysteme in ein Informations-Sicherheits-Management-System (ISMS) 50

4.1 Aktueller Schutz der ITK-Infrastruktur 51

4.2 Überführung von bestehenden IT-Sicherheitssystemen in ein ISMS 52

4.3 Notwendiger Umfang der Dokumentation 53

4.4 Hilfsmittel zur Überführung bestehender IT-Sicherheitssysteme in ein ISMS 54

5 Kooperationsmodelle 58

5.1 Grundsätzliches zur Kooperation 58

5.2 Kooperationsfelder 59

5.3 Kooperationsmodelle 61

5.3.1 Verbund- und Matrixzertifizierungen 62

5.3.2 Zertifizierungsnetzwerke und CrossAudits 63
5.3.3 Die »echte Kooperation« 63
5.3.4 Die »unechte Kooperation« 67
5.3.5 Regionale Verbünde, Dienstleistungsbeziehungen 73
5.4 Exkurs: Externer Informationssicherheitsbeauftragter/Ansprechpartner IT-Sicherheit 75

6 Praxisbeispiele zur Umsetzung 78
6.1 Operationalisierung 78
6.2 Sicherheitsmaßnahmen/zentrale Dienste 79
6.3 Security Monitoring und Protokollierung 82
6.4 Remote-Zugriffe/Fernwartung 83
6.5 Account Management 84
6.6 Anti-Virus/Malware 84
6.7 Patch Management 84
6.8 Backup und Wiederherstellung 85
6.9 Ausfallsicherheit/HA 86

7 Ansprechpartner 88

8 Abkürzungsverzeichnis 91

Verzeichnis der Abbildungen

Abbildung 1: PDCA-Modell für den ISMS-Prozess (nach Quelle: BSI Standard 100-1) 15
Abbildung 2: beispielhafte prozessuale Ansicht des Scope 23
Abbildung 3: Mögliche Technologien, Netzwerke und Personen im potenziellen Scope 24
Abbildung 4: VKU Umfrage Zeitplan ISMS 38
Abbildung 5: VKU Umfrage Personalplanung ISMS 39
Abbildung 6: Beteiligte Rollen beim Aufbau eines ISMS 47
Abbildung 7: Zertifikat bei echter Kooperation 64
Abbildung 8: Unechte Kooperation – Variante 1 69
Abbildung 9: Unechte Kooperation – Variante 2 72
Abbildung 10: Vertikale Zonierung 80
Abbildung 11: Horizontale Zonierung 81

Dieser Praxisleitfaden ist durch die Zusammenarbeit von Mitgliedern des Digitalverbandes Bitkom und des Verbandes Kommunaler Unternehmen e. V. (VKU) entstanden. Er soll Energieversorgungsnetzbetreibern eine erste Orientierung geben, welche Anforderungen durch den im August 2015 durch die Bundesnetzagentur veröffentlichten IT-Sicherheitskatalog auf sie zukommen. Er erläutert die rechtlichen Hintergründe, den Aufbau eines Informationssicherheits-Managementsystems, den zu erwartenden Aufwand, die Überführung bestehender Sicherheitsarchitekturen in die neue Systematik, verschiedene Kooperationsmodelle und Beispiele aus der konkreten technischen Umsetzung. Der Praxisleitfaden kann im Wege der kontinuierlichen Verbesserung zukünftig um weitere Fragen ergänzt werden, die sich bei der Implementierung der Maßnahmen in den Unternehmen ergeben. Der Dank gilt den zahlreichen Bearbeitern aus der Digital- und Energiebranche, die ihr Praxiswissen bei diesem Leitfaden eingebracht haben.

1 IT-Sicherheitsbestimmungen für Betreiber von Energieversorgungsnetzen – Einführung

1 IT-Sicherheitsbestimmungen für Betreiber von Energieversorgungsnetzen

Einführung

Felix Dembski, Bitkom
Benjamin Sommer, VKU
Gerd Niehuis, BTC
Siegmar Merkus, Stadtwerke Krefeld
Andreas Floß, HiSolutions AG

Für Betreiber von Energieversorgungsnetzen und andere Betreiber kritischer Infrastrukturen sind in den letzten Jahren neue gesetzliche Regelungen und Normen bezüglich der Sicherheit ihrer Informations- und Kommunikationstechnik entstanden. Dieser Abschnitt gibt hierzu einen Überblick auch für Nicht-Juristen. Das wichtigste Gesetz ist dabei das IT-Sicherheitsgesetz, das zum 25. Juli 2015 in Kraft getreten ist. Das IT-Sicherheitsgesetz ist ein Artikelgesetz, durch das eine Reihe von Gesetzesänderungen an Einzelgesetzen angestoßen wurde. Zentral sind dabei die Änderungen am BSI-Gesetz. Grundsätzlich adressiert werden Unternehmen aus den Sektoren der Kritischen Infrastruktur, nämlich Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Bundesbehörden. Die einzuhaltenden Vorschriften ergeben sich neben dem BSI-Gesetz jeweils aus den Fachgesetzen der einzelnen Sektoren: Für die Energiebranche etwa aus dem Energiewirtschaftsgesetz und für die Telekommunikationsbranche aus dem Telekommunikations- und dem Telemediengesetz. Entsprechend verstreut können einzelne Regelungen sein. Für die Betreiber von Energieversorgungsnetzen ist vor allem der §11 EnWG von Bedeutung.

Vorgaben für die IT-Sicherheit gelten für Betreiber von Energieversorgungsnetzen ungeachtet der Frage, ob sie zur Kritischen Infrastruktur zählen oder nicht. Wenn sie durch den Gesetzgeber als solche angesehen werden, gelten darüber hinaus Meldepflichten über IT-Sicherheitsvorfälle gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Welche Unternehmen tatsächlich als Kritische Infrastruktur eingestuft werden, wird in einer Rechtsverordnung zum §10 des BSI-Gesetzes festgelegt (»BSI-KRITIS-VO«), die derzeit vom Bundesministerium des Innern erarbeitet und voraussichtlich Ende 2015 vorgelegt wird. In der Rechtsverordnung werden Schwellenwerte für die verschiedenen Branchen aufgestellt, ab denen die besonderen Regelungen für Kritische Infrastrukturen angewendet werden müssen. Es obliegt dann den Unternehmen zu prüfen, ob sie die Schwellenwerte erreichen. Eine offizielle Liste der Unternehmen mit Kritischen Infrastruktur soll es dagegen nicht geben.

1.1 Gesetzlicher Rahmen für die Sicherheit in Energieversorgungsnetzen

Die Sicherheitsvorschriften für Betreiber von Energieversorgungsnetzen ergeben sich aus § 11 des Energiewirtschaftsgesetzes (EnWG). Der erste Absatz enthält dabei allgemeine Vorgaben zum sicheren Betrieb eines Energienetzes, im Absatz 1a folgen die Vorgaben zur IT-Sicherheit. Absatz 1a enthält weiterhin die Ermächtigung für die Bundesnetzagentur (BNetzA) einen Katalog von Sicherheitsanforderungen für Energienetzbetreiber vorzulegen. Dieser Ermächtigung ist die BNetzA am 12.08.2015 nachgekommen. Aus diesem Katalog erwachsen eine Reihe konkreter Verpflichtungen für alle Energienetzbetreiber, die im Rahmen des vorliegenden Leitfadens erläutert werden.

Im Absatz 1c des EnWG werden den Energienetzbetreibern zusätzlich Meldepflichten über IT-Sicherheitsvorfälle gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) auferlegt. Diese gelten jedoch nur für solche Unternehmen, die durch das Bundesinnenministerium in einer Rechtsverordnung nach §10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) als Betreiber Kritischer Infrastrukturen (KRITIS) definiert werden.

Im Folgenden werden die Regelungen für Betreiber von Energieversorgungsnetzen näher erläutert.

1.1.1 Allgemeine Regelungen aus dem Energiewirtschaftsgesetz

Über sämtlichen Vorschriften zur IT-Sicherheit thront die Vorgabe an alle Netzbetreiber, gemäß § 11 Abs. 1 EnWG ein sicheres Energieversorgungsnetz zu betreiben. Konkrete Vorgaben für die IT-Sicherheit lassen sich daraus aber noch nicht ableiten:

1. Betreiber von Energieversorgungsnetzen sind verpflichtet, ein sicheres, zuverlässiges und leistungsfähiges Energieversorgungsnetz diskriminierungsfrei zu betreiben, zu warten und bedarfsgerecht zu optimieren, zu verstärken und auszubauen, soweit es wirtschaftlich zumutbar ist. […]

Was ein sicheres Energieversorgungsnetz im Sinne des Gesetzes mit Blick auf IT-Sicherheit ist, folgt darauf:

2. Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. […]

Das heißt: Netzbetreiber müssen insbesondere die IT-Systeme schützen, die »für einen sicheren Netzbetrieb notwendig sind«. Welche das sein können und was daraus folgt, ist Gegenstand dieses Praxisleitfadens. Vor allem aber schließt sich die Frage an: Bei Einhaltung welcher Vorgaben gilt der Schutz der IT-Systeme als »angemessen«? Dazu heißt es weiter:

> Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen.

»Die Regulierungsbehörde« ist die Bundesnetzagentur. Sie hat am 12. August 2015 einen IT-Sicherheitskatalog vorgelegt, an den sich alle Energienetzbetreiber halten müssen. Die Energiebranche ist dabei eine Ausnahme gegenüber vielen anderen Branchen: Nicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestimmt - wie sonst häufig - die Regeln der IT-Sicherheit, sondern die auch in anderen Fragen der Energieregulierung zuständige Bundesnetzagentur im Benehmen mit dem BSI. Weiter heißt es:

> Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen.

Die IT-Sicherheit muss in einen kontinuierlichen Verbesserungsprozess geführt werden, dessen Ergebnisse routinemäßig überprüft werden. Einmalige Maßnahmen reichen nicht aus.

> Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes liegt vor, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Regulierungsbehörde überprüft werden.

Wer den IT-Sicherheitskatalog einhält und das auch nachweisen kann, der schützt seine IT »angemessen« im Sinne des Gesetzes. Er erfüllt die Anforderungen an einen sicheren Betrieb im Bereich der IT. Ob er das tatsächlich tut, kann die BNetzA überprüfen. Der Netzbetreiber hat nicht die Möglichkeit, stattdessen eigene, aus seiner Sicht angemessene Schutzmaßnahmen, zu ergreifen. Der IT-Sicherheitskatalog stellt den Mindeststandard dar, der einzuhalten ist.

> Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 4 treffen.

Die Bundesnetzagentur kann – wie häufig im Energierecht – ihre Anforderungen noch genauer ausgestalten. Hiervon hat sie bislang keinen Gebrauch gemacht.

1.1.2 Der IT-Sicherheitskatalog der BNetzA

Die Bundesnetzagentur hat entsprechend den Anforderungen des § 11 Abs. 1a EnWG ihren IT-Sicherheitskatalog erarbeitet. Er enthält eigene Regeln für die Informationssicherheit von Energienetzbetreibern.

Das Informationssicherheits-Managementsystem (ISMS)

Das zentrale Element des Katalogs ist die Vorschrift, dass jedes Unternehmen ein Informationssicherheits-Managementsystem (ISMS) aufsetzen und betreiben muss. Dabei handelt es sich

nicht etwa um ein IT-System, das einmal installiert werden muss, sondern ist mit anderen Managementsystemen wie dem Qualitätsmanagement vergleichbar. Die betroffenen Unternehmen werden zum Aufsetzen eines geordneten Prozesses zur Analyse der Anfälligkeit ihre IT-Systeme und in einem zweiten Schritt zur Implementierung von Schutzmaßnamen für mögliche Schwachstellen verpflichtet (»Identifiziere alle Schnittstellen deines Umspannwerkes mit der Außenwelt und bestimme Schutz-, Zugriffs- und Abwehrmaßnahmen für jede einzelne Schnittstelle!«). Die Regeln werden also nicht allgemein vorgegeben, beispielsweise zur Verwendung bestimmter Technologien (nicht: »Benutze Virenscanner!«). Vielmehr muss sich jedes Unternehmen spezifisch mit den individuellen Gegebenheiten beschäftigen und einen Umgang mit möglichen Risiken festlegen. Mehr zum Aufbau eines ISMS siehe unter 1.3.

Der IT-Sicherheitskatalog ist eine auf den ersten Blick neue Systematik des Informationssicherheits-Managements, dessen Elemente auf den zweiten Blick aber bereits vertraut sind. Es handelt sich im Wesentlichen um die Pflicht zum Aufbau und der Zertifizierung eines ISMS gemäß der Norm ISO 27001, wobei die DIN ISO/IEC TR 27019 und weitere Vorgaben aus dem IT-Sicherheitskatalog zu beachten sind. Die ISO 27001 ist eine internationale Norm für Informationssicherheits-Managementsysteme. Dort beschrieben sind die Anforderungen an ein ISMS für ein Unternehmen eines beliebigen Sektors. Die Norm wird für den Energiebereich näher ausgestaltet durch die ISO/IEC TR 27019. Diese Subnorm enthält Leitlinien für ein ISMS im Bereich der Prozesssteuerung und Automatisierungstechnik in der Energieversorgung basierend auf der Norm ISO 27002. Grundlage der ISO IEC TR 27019 war die deutsche DIN SPEC 27009:2012-04.

Das bedeutet, dass im Wesentlichen auf die internationalen Normen der ISO 2700x-Famile zurückgegriffen wird. Diese sind bereits auf die Betreiber von Energieversorgungsnetzen angepasst. Hinzu kommen einige spezifische Vorgaben aus dem IT-Sicherheitskatalog, wie bestimmte Technologien und Risikoeinschätzungen zu behandeln sind. Die Zertifizierung erfolgt dann nicht unmittelbar nach ISO 27001, sondern nach einem Zertifikat »auf Basis von DIN ISO/IEC 27001«, welches die BNetzA mit der deutschen Akkreditierungsstelle (DAkkS) erarbeitet.

Der Netzstrukturplan

Neben der zentralen Forderung nach Einführung eines ISMS enthält der Katalog weitere Vorschriften. Eine davon ist das Aufstellen eines Netzstrukturplans. Dieser soll alle vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten enthalten und jeweils die Technologien und Verbindungen zu anderen Systemen oder Netzen erfassen. Dabei sollen die Kategorien »Leitsystem/Systembetrieb«, »Übertragungstechnik/Kommunikation« und »Sekundär-, Automatisierungs- und Fernwirktechnik« unterschieden werden. Da für die Implementierung eines ISMS ein Überblick über vorhandene Systeme und Komponenten benötigt wird, kann der Netzstrukturplan als Grundlage für die Herleitung des Anwendungsbereichs (Scope) des ISMS dienen (siehe dazu ausführlich Kapitel 2).

Ansprechpartner für IT-Sicherheit

Weiterhin muss jedes Unternehmen gegenüber der BNetzA einen Ansprechpartner für IT-Sicherheit benennen. Dieser soll die Koordination und Kommunikation gegenüber der BNetzA übernehmen. Auf Nachfrage durch die Behörde soll er zu folgenden Themen unverzüglich auskunftsfähig sein:

- Umsetzungsstand und Anforderungen aus dem IT-Sicherheitskatalog
- Aufgetretene Sicherheitsvorfälle sowie Art und Umfang eventuell hierdurch hervorgerufener Auswirkungen
- Ursache aufgetretener Sicherheitsvorfälle sowie Maßnahmen zu deren Behebung und zukünftigen Vermeidung

Bei der Benennung des Ansprechpartners sollen die Netzbetreiber – wo einschlägig – die Vorschriften des Sicherheitsüberprüfungsgesetzes (SÜG) und der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) beachten. Das bedeutet Stand heute, dass nur Ansprechpartner bei den Übertragungsnetzbetreibern gemäß § 10 Abs. 1 Nr. 4 SÜFV einer Sicherheitsüberprüfung unterzogen werden müssen – die Regelung trifft also auf die Verteilnetzbetreiber nicht zu.

1.1.3 Zusätzliche Regeln für Betreiber Kritischer Infrastrukturen

Weitere, über den IT-Sicherheitskatalog hinausgehende Pflichten kommen auf die Netzbetreiber zu, die als Betreiber einer Kritischen Infrastruktur gelten. Das IT-Sicherheitsgesetz hat den Sektor Energie grundsätzlich als Kritische Infrastruktur identifiziert. Allerdings wird nicht jedes kleinste Stadtwerk von den Regelungen erfasst werden. Wen es trifft, wird in einer Rechtsverordnung gemäß § 10 Absatz I BSI-Gesetz festgelegt, die aktuell unter dem Arbeitstitel »BSI-KRITIS-VO« oder kurz KRITIS-Verordnung diskutiert wird. Aus den oben aufgezählten kritischen Sektoren, die durch das BSI-Gesetz berührt sind, sollen insgesamt etwa 2000 Unternehmen als Betreiber Kritischer Infrastrukturen eingestuft werden. Wie viele der knapp 900 Verteilnetzbetreiber Strom und der 700 Verteilnetzbetreiber Gas sich auf die Einstufung als Kritische Infrastruktur mit entsprechenden Pflichten einstellen müssen, ist daher noch schwer abschätzbar. Es ist zu erwarten, dass in der Verordnung mit Größenklassen wie Anzahl der Netzanschlusspunkte, versorgte Einwohner oder Ähnlichem gearbeitet wird. Nach Erscheinen der KRITIS-Verordnung muss jeder Energienetzbetreiber wie auch Unternehmen der anderen betroffenen Sektoren selbst prüfen, ob er unter die dort definierten Schwellenwerte fällt. Eine offizielle Liste der Betreiber Kritischer Infrastrukturen ist nicht geplant.

Meldepflichten

Die so definierten Betreiber Kritischer Infrastrukturen müssen sicherheitsrelevante Vorfälle an das Bundesamt für Sicherheit in der Informationstechnik melden. Im Gegenzug werden sie vom BSI mit einem Lagebild der aktuellen Bedrohungen versorgt. Die Vorschriften hierzu sind sehr verschachtelt. Die entscheidenden Vorschriften finden sich im neu geschaffenen § 11 Abs. 1c EnWG:

3. Betreiber von Energieversorgungsnetzen [...], die [...] als Kritische Infrastruktur bestimmt wurden, haben dem Bundesamt für Sicherheit in der Informationstechnik unverzüglich erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu melden, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes [...] führen können oder bereits geführt haben.

Wer als Betreiber einer Kritischen Infrastruktur klassifiziert wurde, muss also »erhebliche Störungen« der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit seiner informationstechnischen Systeme, Komponenten oder Prozesse an das BSI melden. Von einer erheblichen Störung muss ausgegangen werden, wenn sie zu einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes geführt hat oder führen kann. Die Schwelle ist also sehr niedrig. Es reicht die Möglichkeit der Beeinträchtigung der Funktionsfähigkeit aus. Erst recht gemeldet werden müssen selbstverständlich solche Vorfälle, bei denen tatsächlich die Funktionsfähigkeit beeinträchtigt wurde.

Umfang der Meldung

Zum Umfang der Meldung heißt es wie folgt:

> [...] Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik enthalten. [...]

Hierbei können die Betreiber ein gewisses Maß an Anonymität wahren.

> [...] Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. [...]

Der Name des Betreibers muss also erst genannt werden, wenn es tatsächlich zu einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes kam. Bis zu dieser Schwelle können die Vorfälle auch anonym gemeldet werden.

Einblick in das Lagebild

Die Betreiber Kritischer Infrastrukturen haben dabei nicht bloß Pflichten, sondern ihnen werden auch aktuelle Informationen zur IT-Sicherheitslage vom BSI bereitgestellt. Das sieht eine neue Vorschrift im § 8b Abs. 2 BSI-Gesetz vor. Danach sammelt das BSI die Informationen, die notwendig sind, um Gefahren für die IT-Sicherheit abzuwehren. Es wertet diese Informationen aus, insbesondere auf Sicherheitslücken, Schadprogramme und versuchte Angriffe auf die IT. Daneben analysiert es deren mögliche Auswirkungen auf die Verfügbarkeit der Kritischen Infrastruktur mit der BNetzA und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). So wird ein stets aktuelles Lagebild bezüglich der Sicherheit in der Informationstechnik der Kriti-

schen Infrastrukturen erstellt. Über die so beim BSI erfasste Lage der IT-Sicherheit werden die Betreiber von Kritischen Infrastrukturen dauerhaft und unverzüglich unterrichtet. So sollen die Betreiber Kritischer Infrastrukturen möglichst frühzeitig von Sicherheitslücken und Angriffen erfahren. Die dafür notwendige Kontaktstelle sollen die betroffenen Unternehmen nach § 8b Absatz 3 BSI-Gesetz an das BSI melden. Die Energiebranche ist über den §8c Absatz 3 von der Pflicht zur Einrichtung einer solchen Kontaktstelle ausgenommen. Auch ohne diese Pflicht kann das Informationsangebot des BSI aber von den Unternehmen wahrgenommen werden. Weiterhin können die Informationen über die Teilnahme am Branchenarbeitskreis des UP KRITIS des BSI erhalten werden.

1.2 Schritte zu einem ISMS nach dem IT-Sicherheitskatalog

Der Aufbau eines ISMS erfolgt vereinfacht durch die folgenden Schritte:

1. Festlegung des Anwendungsbereichs (Scope)

Der Anwendungsbereich (Scope) des ISMS wird initial definiert (siehe dazu im Detail Kapitel 2). Es geht um die Frage: Wie weit muss der Anwendungsbereich des ISMS gezogen werden, um einen effektiven Schutz herstellen zu können für die für einen sicheren Netzbetrieb notwendigen Systeme? Hierbei ist besonders der bereits vorgegebene Anwendungsbereich aus dem IT-Sicherheitskatalog einzuhalten. Daraus ist eine Dokumentation zu erstellen, aus der die Geschäftstätigkeit des Unternehmens, die Organisationsstruktur, die Wirtschaftsgüter, die eingesetzten Technologien und so weiter ersichtlich werden.

2. Inventarisieren der Werte (Assets)

In diesem Schritt ist eine Inventarisierung der im Anwendungsbereich enthaltenen Assets unter Nutzung der vorhandenen Datensammlungen vorzunehmen und geeignet zu dokumentieren (zum Aufwand siehe Kapitel 3, zum Verwenden bereits vorhandener Dokumentationen siehe Kapitel 4).

3. Analysieren und Behandeln von Risiken

Es muss ein systematischer Ansatz zur Risikoabschätzung ausgearbeitet werden, dessen Vorgehensmodell auf die Geschäftstätigkeit des Unternehmens angepasst ist. Es muss systematisch die Frage beantwortet werden: »Welche Risiken bestehen für die Assets innerhalb des Anwendungsbereichs des ISMS?« Dabei werden Regelungen und Schutzziele festgelegt, die das ISMS enthält, um die Risiken auf ein akzeptables Niveau zu senken. Ferner werden Kriterien für die Akzeptanz von (Rest-)Risiken bestimmt.

4. Maßnahmen festlegen und umsetzen

Anhand der festgelegten Schutzziele werden risikoorientiert entsprechende Maßnahmen identifiziert und implementiert (Beispiele siehe Kapitel 7).

5. Regelmäßiges Review und kontinuierliche Verbesserung

Damit das ISMS als lebendiger Prozess etabliert wird, ist ein regelmäßiges Überprüfen (Review) der Sicherheitsmaßnahmen notwendig. Mittels Prüfungen der Maßnahmenumsetzungen (Audits) und deren Effektivität wird in einem kontinuierlichen Verbesserungsprozess ein immer höheres Sicherheitsniveau erreicht (siehe PDCA-Modell in Abbildung 1).

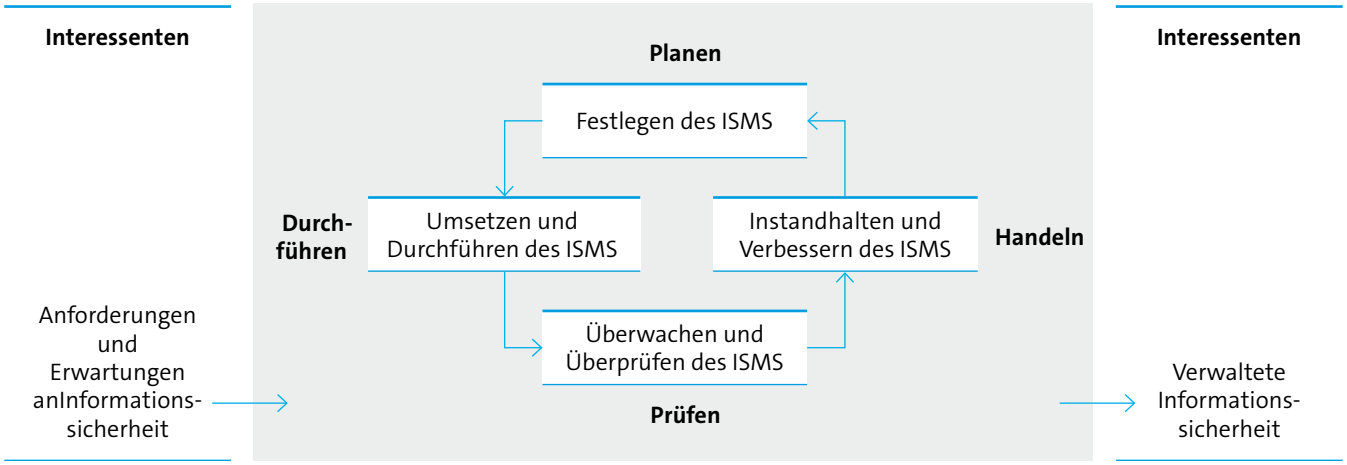


Abbildung 1: PDCA-Modell für den ISMS-Prozess (nach Quelle: BSI Standard 100-1)

1.3 Fristen

Das ISMS als zentrales Element des IT-Sicherheitskatalogs muss bis zum 31.01.2018 eingeführt und durch eine akkreditierte Stelle zertifiziert werden. Grundlage ist dabei die ISO-Norm 27001. Die BNetzA wird durch ein eigens mit der deutschen Akkreditierungsstelle (DAkkS) entwickeltes Zertifikat sicherstellen, dass bei der Implementierung weiterhin der IT-Sicherheitskatalog Berücksichtigung finden muss.

Am kürzesten ist die Frist zur Benennung eines Ansprechpartners für IT-Sicherheit gegenüber der BNetzA. Dieser muss bis zum 30.11.2015 benannt und der BNetzA gemeldet sein.

Für die Meldepflichten von IT-Sicherheitsvorfällen gegenüber dem BSI ist die Veröffentlichung der KRITIS-Verordnung abzuwarten. Nach aktueller Planung soll sie Ende 2015 vorliegen und

Schwellenwerte für die verschiedenen Branchen enthalten, ab denen die Unternehmen als Kritische Infrastrukturen gelten. Nur diese Unternehmen müssen in der Folge IT-Sicherheitsvorfälle aus ihrem Unternehmen an das BSI melden.

1.4 Ansprechpartner

Meldung des Ansprechpartners IT-Sicherheit gegenüber der BNetzA:
IT-Sicherheitskatalog@bnetza.de unter Verwendung des entsprechenden Formulars.

Erste knappe FAQ der BNetzA zum IT-Sicherheitskatalog.

UP KRITIS Branchenarbeitskreise des BSI: www.upkritis.de, upkritis@bsi.bund.de

1.5 Exkurs: Anreizregulierung

Die wichtige Frage nach der Berücksichtigung der Kosten aus dem IT-Sicherheitskatalog bei der Anreizregulierung beurteilt der VKU wie folgt: Da aus den Verpflichtungen des § 11 Absatz 1a EnWG Mehrkosten entstehen, die vom Netzbetreiber nicht beeinflussbar sind, ist es erforderlich, dass diese ungemindert und ohne Zeitverzug in die Erlösobergrenze übernommen werden können. Bislang gibt es dazu jedoch keine Verlautbarungen weder seitens der BNetzA noch des Verordnungsgebers. Im bestehenden Regulierungsregime können die Mehrkosten erst mit einem erheblichen Zeitverzug im Rahmen der Kostenprüfung des Basisjahres anerkannt werden. Der VKU setzt sich seit Langem für eine entsprechende Anpassung der regulatorischen Regelungen ein und fordert die Beseitigung des Zeitverzugs in der Anreizregulierung.

Die Erlösobergrenze kann jährlich um bestimmte Komponenten gem. § 4 ARegV angepasst werden. Dies gilt bislang jedoch nicht für Mehrkosten, die aus den Verpflichtungen des IT-Sicherheitskatalogs entstehen. Dafür, dass die Informationstechnik der Netzbetreiber in der notwendigen Geschwindigkeit und Umfang angepasst wird, entstehen den Unternehmen erhebliche Aufwendungen. Weitere Mehrkosten kommen durch die Einbindung von externen Beratern und Zertifizierern im Rahmen der Umsetzung des IT-Sicherheitskatalogs zustande. Zusätzlich muss der Netzbetreiber von ihm nicht zu vertretende Mehrkosten im Rahmen seiner eichrechtlichen Verpflichtungen in Kauf nehmen.

2 Definition des Anwendungsbereichs des ISMS

2 Definition des Anwendungsbereichs des ISMS

Andreas Makowski, ANMATHO AG
Frank Stoermer, HP

Kernforderung des IT-Sicherheitskatalogs ist die Einführung eine Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001 (ISO 27001). Das Informationssicherheits-Managementsystem gemäß ISO27001 ist ein Managementprozess, der in jedem Unternehmen weitreichende Folgen hat. Je nach bestehendem Organisations- und Sicherheitsniveau, Prozessen und Dokumentationsstand gestaltet ein ISMS das Unternehmen deutlich um. Damit dies auch effektiv und nachhaltig geschieht, müssen einige Basisdokumente vorab definiert werden. Eines dieser Basisdokumente ist der Anwendungsbereich oder Fokus, im Englischen auch Scope genannt. Der Scope hat seinen Ursprung im Projektmanagement: Damit ein Projekt, oder wie in diesem Fall ein Managementsystem, sauber und funktionell implementiert werden kann, muss es einen Fokus haben. Für diesen Fokus werden im späteren Projektverlauf die Ziele und Maßnahmen definiert; Dinge außerhalb des Fokus' sollten nicht oder nur ausnahmsweise behandelt werden. Klar definierte Ziele, Maßnahmen und Grenzen sind die Grundlage für ein erfolgreiches ISMS. Ansonsten läuft ein Unternehmen Gefahr Arbeitspaket um Arbeitspaket, Maßnahme um Maßnahme ohne schlüssige Gesamtstrategie und Orientierung umzusetzen. Angewandt auf Sicherheitsmaßnahmen würden so Lücken gestopft, Konzepte und Richtlinien erstellt und trotzdem wäre das Unternehmen nicht gut geschützt. Solche unschlüssig strukturierten Projekte, die nicht zu einem gelebten ISMS führen, sind nicht selten. Ein solches ISMS würde nicht als laufendes und lebendiges Informationssicherheits-Managementsystem zertifiziert werden. Eine Zertifizierung wird jedoch in Zukunft gesetzliche Pflicht und um dieses Ziel zu erreichen, muss auf das für die Zertifizierung zentrale Basisdokument der ISO27001 besonderer Wert gelegt werden – der Anwendungsbereich oder »Scope«. Weiterhin müssen die zusätzlichen Anforderungen aus dem IT-Sicherheitskatalog berücksichtigt werden, da dieser für die Zertifizierung ebenfalls Berücksichtigung finden wird (siehe Kapitel 1.1.2).

Exkurs Mehrspartenunternehmen

Durch das IT-Sicherheitsgesetz sind neben der Sparte Energie noch die Bereiche Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, sowie das Finanz- und Versicherungswesen betroffen. Viele kommunale Unternehmen sind Mehrspartenunternehmen bei denen neben der Energieversorgung auch die Geschäftsbereiche Wasserversorgung, Telekommunikation und Verkehr existieren. Für die genannten Geschäftsbereiche können laut IT-Sicherheitsgesetz (genauer BSI-Gesetz) so genannte Branchenstandards entwickelt werden, welche die sehr allgemeinen Vorgaben des IT-Sicherheitsgesetzes für die jeweilige Branche spezifizieren. Weiterhin kommt es für die Anwendung der Regelungen des IT-Sicherheitsgesetzes (genauer des BSI-Gesetzes) auf die Ausgestaltung der bereits erwähnten KRITIS-Verordnung an. Da derzeit die Branchenstandards noch nicht vorliegen und weiterhin die KRITIS-Verordnung noch in Arbeit ist, wird in diesem Leitfaden nicht näher auf die Situation der

anderen Branchen eingegangen. Jedes Unternehmen muss aber Überlegungen anstellen, ob es sinnvollerweise das ISMS gleich über mehrere Sparten spannen möchte, um Zeit und Kosten gegenüber Einzelprojekten für jede einzelne Branche zu sparen. Nach derzeitigem Stand, bietet sich eine Zertifizierung nach der ISO 27001 auch für die weiteren Geschäftsbereiche an, da derzeit noch keine speziellen Anforderungen an die Nachweise der Sicherheitsvorkehrungen getroffen wurden. Für die Zukunft kann jedoch nicht ausgeschlossen werden, dass durch das BSI entweder schwächere oder auch strengere Vorschriften an den Nachweis der Sicherheitsmaßnahmen gestellt werden. Eine eindeutige Empfehlung für Mehrspartenunternehmen ist deshalb zum derzeitigen Zeitpunkt nicht möglich.

2.1 Richtige Bestimmung des Scope

Der Scope ist also als Grundstein des ISMS zu betrachten. Alles, was im Scope liegt, wird als relevant für das ISMS und die Informationssicherheit im Unternehmen angesehen. Jedes Objekt (oder auch Asset), d. h. jeder Geschäftswert im Scope muss identifiziert und untersucht werden. Dabei wird ermittelt, welche Auswirkungen es auf die Informationssicherheit hat, wie wahrscheinlich die damit zusammenhängenden Risiken sind und welche Maßnahmen angewendet werden müssen, um das Risiko zu behandeln. Der Scope stellt dadurch auch einen unmittelbaren Zusammenhang zum Gesamtaufwand und zur Qualität des ISMS dar: Ist der Scope zu weit gefasst, müssen mehr Risiken als eigentlich notwendig betrachtet und mit entsprechenden Maßnahmen behandelt werden. Ist der Scope zu eng angesetzt, wurden eventuell Sicherheitsrisiken »ausgeblendet«, was die Effektivität und Plausibilität des ISMS unter Umständen gefährdet. Um diese Gefahr zu minimieren, sollte der Scope nicht als einzelnes Objekt angesehen werden, sondern als Prozess oder Leistungserbringung beschrieben werden. Dies stellt sicher, dass nicht nur Hardware, Systeme oder einzelne Organisationseinheiten betrachtet werden, sondern dass die erbrachte Funktion und die Menschen und Organisationen an allen Schnittstellen in den Vordergrund rücken. Nicht ohne Grund wählt die BNetzA im IT-Sicherheitskatalog für Energienetzbetreiber die Formulierung »alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind« und spricht nicht einfach nur von »Leitstelle, Leittechnik, etc.«

Beginnt man damit, den Scope zu definieren und zu dokumentieren, lohnt es sich gesetzliche und vertragliche Anforderungen zu identifizieren. In unserem konkreten Fall verpflichtet der IT-Sicherheitskatalog für Netzbetreiber, ein ISMS im Sinne der Norm ISO 27001 zu implementieren und zu zertifizieren. Streng genommen müsste man ein ISO 27001 ISMS nur für den Strom- und Gasnetzbetrieb anwenden. In vielen Fällen sind die Energieversorgungsunternehmen auch Wasser- und Abwasserversorger oder Betreiber von ÖPNV und Telekommunikationsnetzen: Allesamt Geschäftszweige, die potenzielle kritische Infrastrukturen (KRITIS) sind, welche aufgrund des IT-Sicherheitsgesetzes abgesichert werden müssten. Das IT-Sicherheitsgesetz, welches in seiner Formulierung wesentlich abstrakter ist, fordert von ihnen zur Absicherung dieser Infrastrukturen unter anderem Sicherheits- und Notfallkonzepte sowie deren Zertifizierung nach einem anerkannten Standard. All diese Anforderungen können bei Miteinbeziehung in den Scope auch

durch das ISO 27001 ISMS erfüllt werden. Hier lohnt es sich also auch im Vorfeld genauer hinzuschauen und den Scope gegebenenfalls auszudehnen, um weitere Anforderungen (zum Beispiel Notfallkonzepte zur Vorlage bei Wirtschaftsprüfern), Verträge (zum Beispiel definierte Verfügbarkeiten in TK-Netzen, Servicelevel Agreement) oder Gesetze (zum Beispiel EnWG, KonTraG, GmbHG, BDSG) zu erfüllen. Allerdings kann hier noch keine Empfehlung zum genauen Vorgehen gegeben werden.

Individuellen Scope bestimmen

Als Grundlage für die Bestimmung des Scope sollte der Netzstrukturplan dienen, der durch den IT-Sicherheitskatalog gefordert ist (siehe Kapitel 1.1.2). In diesen werden wie oben ausgeführt alle vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten aufgeführt (siehe auch Abschnitt IV im IT-Sicherheitskatalog der BNetzA).

Bezüglich des Scope gilt grundsätzlich, dass er individuell ist und für jeden Energienetzbetreiber separat erstellt werden muss. Denn auch wenn viele deutsche Stadtwerke ähnlich sind, die gleiche Software oder das gleiche Leitsystem verwenden: Die damit verbundene Organisation ist oft unterschiedlich, die sie tragenden Prozesse und Technik nur selten gleich. Die risikoorientierte Methodik der ISO 27001 fordert hierbei, dass dafür erst einmal alle Assets des Scopes identifiziert werden müssen, unabhängig davon, ob es sich um IT-Komponenten, Netzwerke, Prozesse, Personen oder Organisationseinheiten handelt. Für den Beginn der Definition des Scope und zur Identifikation der ersten Assets genügen folgende einfache Fragen:

- Ist eine Funktion, ein Geschäftsprozess oder eine Technologie für den wirtschaftlichen Erfolg des Unternehmens unverzichtbar?
- Ist eine Funktion, ein Geschäftsprozess oder eine Technologie für die Handlungsfähigkeit des Unternehmens unverzichtbar?
- Ist eine Funktion, ein Geschäftsprozess oder eine Technologie für ein anderes, im Scope liegendes Asset notwendig?
- Gibt es bereits ein Asset, welches durch konkrete Risiken für eine der drei oben genannten Fragestellungen bedroht ist?

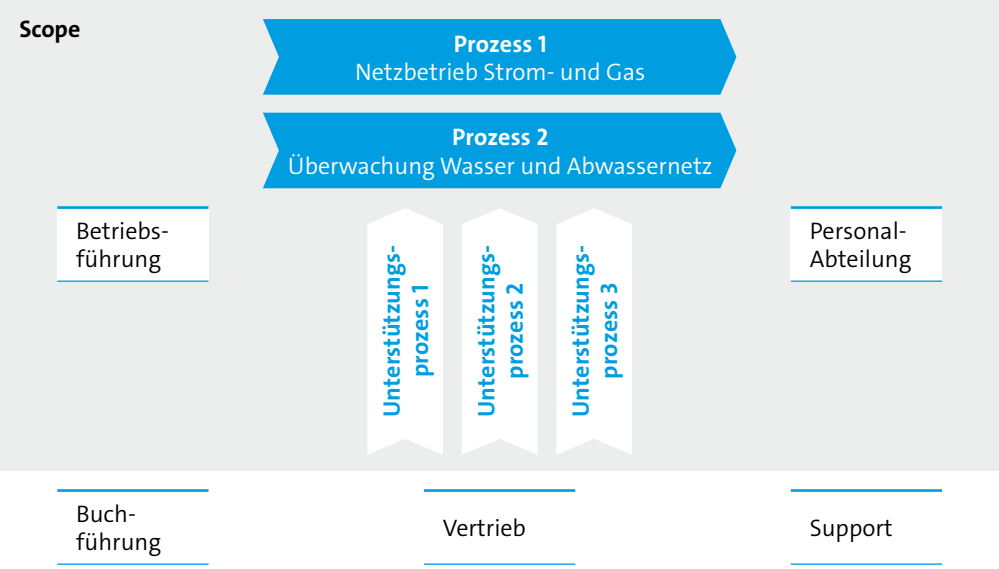


Abbildung 2: Beispielhafte prozessuale Ansicht des Scope

Lautet die Antwort auf eine oder mehrere dieser Fragen »Ja«, gehören die entsprechenden Funktionen, Prozesse, Schnittstellen oder Objekte in den Scope. Ist eine Frage nicht eindeutig zu beantworten, ist die Miteinbeziehung des »unsicheren« Objektes zumindest kritisch zu hinterfragen. Wird ein Prozess oder Objekt ausgegrenzt, sind die Gründe dafür zu belegen und eine Schnittstelle für die zuständige Sicherheitsorganisation des Objektes oder Prozesses zu beschreiben.

Gerade bei Standorten von EVU kann dies den Scope augenscheinlich sehr groß werden lassen, da sich Prozessleitnetze meistens über viele Kilometer erstrecken und in Trafostationen oder Umspannwerken enden. An diesen Grenzpunkten ist die Betrachtung besonders genau durchzuführen – könnte zum Beispiel ein Angreifer durch physikalischen Zugang auf Teile oder gesamte Netzwerke zugreifen, ist dieser weit außerhalb der Organisation stehende Punkt durchaus in den Scope miteinzubeziehen und abzusichern. Die Nutzung von proprietären Protokollen an diesen Punkten gilt hierbei auch nicht als Begründung zum Ausschluss aus dem Scope, schließlich werden aktuell immer mehr Fälle bekannt, in denen Prozessleittechnik von Sachkundigen angegriffen wurde. Dies gilt auch für andere Zugriffe, wie zum Beispiel von Herstellern, Providern und Dienstleistern, aber auch von internen Administratoren oder etwa Reinigungskräften. Obwohl diese Zugriffe selten oder unwahrscheinlich sind, müssen sie als Risiko aufgeführt und bewertet werden. Je nach Bewertung sollte es mit einer oder mehreren organisatorischen oder technischen Maßnahmen aus der ISO 27001 ff. behandelt werden.

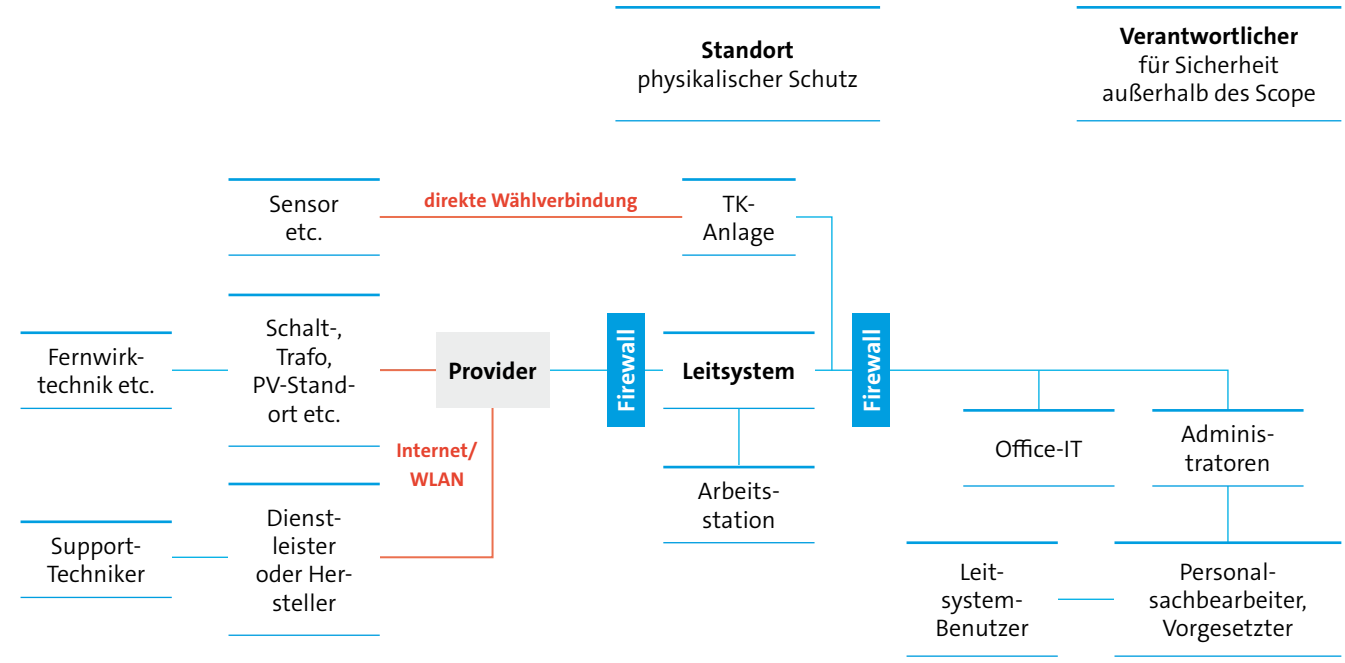


Abbildung 3: Mögliche Technologien, Netzwerke und Personen im potenziellen Scope

Dokumentation des Scope

Die Dokumentation des Scope muss aufgrund der zuvor angeführten Beispiele und ihrer teils enormen Bedeutung umfangreich und möglichst vollständig erfolgen. Obwohl die Beschreibung des Scope natürlich auch erweitert werden kann, lohnt sich bereits im ersten Schritt die Dokumentation der folgenden Punkte:

- **Zweck und Verwendung der Scope-Dokumentation:** Für welche Teile des ISMS ist die saubere Dokumentation des Scope besonders wichtig? Für wen wurde die Definition angefertigt? Meist sollte hier die Informationssicherheitsleitlinie, die Verfahrensbeschreibung des Risikomanagements und die Erklärung der Anwendbarkeit (Statement of Applicability, SOA) angeführt werden (siehe Kapitel 2.5). Weiterhin sollten das Management und die Projektbeteiligten der ISMS-Implementierung als Zielgruppe bzw. Nutzer des Dokuments benannt werden (siehe auch einzubeziehende Instanzen, Kapitel 3).

- **Referenzdokumente:** Welche Dokumente und Anforderungen wirken auf den Scope ein? Dies könnten neben den Normen der ISO2700x-Familie, insb. ISO/IEC TR 27019 auch der IT-Sicherheitskatalog, das EnWG und das IT-Sicherheitsgesetz sein.

- **Beschreibung des Scope als Prozess:** Ein Scope braucht »Fleisch und Blut« (Funktion, Leistung und Menschen). Mit der Beschreibung sollten folgende Fragen beantwortet werden:

- Welche Leistung, welchen Mehrwert erbringt der Scope?
- Welche schützenswerten Informationen enthält er?
- Welche räumlichen, logischen und organisatorischen Grenzen kennzeichnen ihn, und wie wirken sich diese aus?
- Wer ist für die Informationssicherheit im Unternehmen außerhalb seines Geltungsbereichs verantwortlich?
- Gibt es definierte Schnittstellen zu anderen Bereichen oder Organisationen?

Dabei muss bedacht werden, dass die Bezeichnung des Scope nach erfolgreicher Zertifizierung auf dem ausgestellten Zertifikat aufgeführt wird. Eine mögliche Formulierung wäre »Sicherer Betrieb der Steuerungs-, Überwachungs- und Prozessleittechnik des Strom- und Gasnetzes der Stadtwerke XYZ GmbH«

- Die allgemeine Beschreibung sollte um folgende Dokumentationen erweitert werden:
  - Beschreibung der Prozesse und Dienste im Scope
  - Organisationseinheiten, Dienstleister und Personen, die an diesen Prozessen und Diensten maßgeblich beteiligt sind
  - Standorte, Gebäude und Räume, welche für die Prozesse, Dienste und Technik notwendig sind
  - Technische Komponenten, Netzwerke und Infrastruktur
  - Verantwortliche bzw. Eigentümer der vorgenannten Assets
  - Vom Scope ausgeschlossene Bereiche mit der Begründung, warum diese ausgeschlossen wurden

- Der IT-Sicherheitskatalog zwingt zur Anfertigung eines Netzstrukturplans. Dabei handelt es sich um eine Übersicht über die vom Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten mit den anzutreffenden Haupttechnologien und deren Verbindungen. Hierzu sind im IT-Sicherheitskatalog verschiedene Technologiekategorien zur besseren Einordnung aufgelistet. Ebenfalls können bei komplexeren Netzen Gruppen und Teilpläne gebildet werden. Die Strukturanalyse oder der Netzstrukturplan sollten als Auflistung, Tabelle oder Diagramm in aktueller Form vorliegen.

Die nächsten Kapitel widmen sich den Herausforderungen bei der Dokumentation eines einwandfreien und umsetzbaren Scope. Dabei wird besonders darauf eingegangen, wie Grenzen und Schnittstellen definiert werden sollten, welche Mitarbeiter eine Rolle für den Scope spielen und wie der Scope für die weiteren Schritte im ISMS genutzt wird.

2.2 Grenzen des ISMS

Wie oben beschrieben, haben die dokumentierten Grenzen des Scope eine besondere Bedeutung, denn innerhalb dieser Grenzen ist das ISMS anzuwenden (zur besonderen Situation beim Outsourcing und Dienstleistern siehe Kapitel 5). Damit die Sicherheit im ISMS aufrechterhalten

werden kann, darf diese nicht durch vermeidbare, externe Einflussfaktoren gestört werden können. Diese Faktoren müssen deshalb an sinnvollen Grenzen vom Scope getrennt werden. Die Grenzen lassen sich über die Aspekte Zutritt, Zugang/Zugriff und organisatorische Grenzen bestimmen.

Grenzdefinition über Zutritt

In erster Linie kann man durch Zutritt physikalische und räumliche Grenzen definieren. Können die wesentlichen, durch das ISMS zu schützenden Informationen und Systeme durch eine plausible räumliche Trennung abgesichert werden, so kann man diese Trennung (Werksgelände, Gebäude, Räume) in den Scope aufnehmen. In der Risikoanalyse muss dann betrachtet werden, ob die Grenzen überwunden werden und was mögliche Folgen sein können.

Grenzdefinition über Zugang und Zugriff

Beim Zugriff ist es ähnlich, wobei hier primär logische und technische Grenzen definiert werden müssen. In der Regel werden das Netzwerke sein, welche in sich geschlossen einen Verbund von IT-Systemen betreiben. Bedacht werden sollte dabei, dass diese Grenzen häufig durch Technik oder logische Brücken überwunden werden können. So kann ein Leitstellennetz zwar auf einem eigenen Switch oder VLAN isoliert sein, manchmal gibt es aber doch Übergänge durch gemeinsame Coreswitche, Router, Firewalls oder andere Netzwerkbrücken. Potenziell mögliche Remotedesktop-Zugriffe für Administratoren aus dem alltäglichen Unternehmensnetzwerk haben schon in mehreren Situationen für Sicherheitsvorfälle gesorgt. Die Informationssicherheit im Scope wird dann häufig aus den »unsicheren«, nicht durch ein ISMS geschützten Netzwerken kompromittiert – so entsteht eine Bedrohung für das gesamte ISMS. Es sollte also darauf geachtet werden, dass die Grenzübergänge überhaupt adäquaten Schutz bieten. Wenn dies nicht der Fall ist, muss der Scope im Zweifelsfall ausgeweitet werden. Dabei sollte auch das Zusammenwirken von Grenzen berücksichtigt werden, damit die Informationssicherheit nicht kollabiert, falls eine Grenze durchbrochen wird.

Grenzbestimmung über organisatorische Grenzen

Organisatorische Grenzen können sinnvoll sein, weil diese die Verantwortung für die Informationssicherheit auf zusätzliche Schultern verteilen. Ein Beispiel wäre das Ausgrenzen von bestimmten Fachabteilungen, wenn diese tatsächlich keinen Einfluss auf die Informationssicherheit im Geltungsbereich haben. Komplexer ist es wenn Organisationseinheiten einen sekundären Einfluss auf den Scope haben. Dies könnten zum Beispiel Mitarbeiter der Personalabteilung sein, die dafür verantwortlich sind, vertragliche Regelungen mit dem Leitstellenpersonal aufzusetzen, Belehrungen und Schulungsmaßnahmen einzuplanen und bei Einstellung und Entlassungen für die korrekte Aushändigung von Berechtigungen und Schlüsseln verantwortlich sind. Auch die Zusammenarbeit mit Dienstleistern sollte als organisatorische Grenze betrachtet werden, da diese häufig direkt und nicht selten unbemerkt auf sensible Bereiche in Unternehmen zugreifen können. Sei es der Leitsystemhersteller, der sich remote auf das System schaltet, um einen Patch einzuspielen oder die Reinigungskraft, die nicht selten unbeobachtet in den Abendstunden an

einem Systemport etwas anstecken oder abziehen könnte. Sind diese Organisationen oder Personen im Scope berücksichtigt, werden sie als Risiko betrachtet und gegebenenfalls mit einer Maßnahme aus dem Standard behandelt.

Grundsätzlich empfiehlt sich die risikoorientierte Betrachtung aller Objekte, an denen eine Grenze gezogen werden soll. Ist diese Grenze plausibel und mit einer gewissen Wahrscheinlichkeit zu durchbrechen, sollte die Grenze unter Umständen auch um dieses leicht(er) angreifbare und verwundbare Objekt gezogen werden. So macht es etwa mitunter Sinn, den Scope nicht als eine Art »demilitarisierte Zone« zu betreiben, sondern auch die Grenzsysteme zur Office-IT oder zum Internet mit ins ISMS aufzunehmen. Diese aufwändige Betrachtung entfällt, wenn sich ein Unternehmen dazu entscheidet das ISMS unternehmensweit einzuführen. Grenzen des ISMS sind dann die Unternehmensgrenzen, die Zusammenarbeit mit Dienstleistern oder die Informationssicherheit in Projekten sind lediglich Maßnahmen, die umgesetzt werden müssen. Dies kann insbesondere sinnvoll sein, wenn andere Unternehmensteile durch das IT-Sicherheitsgesetz mit ähnlichen Vorgaben konfrontiert ist (siehe Kapitel 2.1).

2.3 Schnittstellen zur Sicherheitsorganisation außerhalb des Scope

Ist ein einwandfreies und funktionelles ISMS abgegrenzt und aufgebaut, ist dies sinnbildlich mit einer Festung vergleichbar. Die Sicherheit der darin liegenden Werte, die Integrität und Verfügbarkeit ist gegeben. Doch Festungen haben, je größer und massiver sie sind, auch einige Nachteile welche auch auf das ISMS übertragbar sind: Durch kluge oder beständige Angriffe sowie Ausspähung und Belagerung können Festungstore geöffnet und auch IT-Sicherheitsmaßnahmen überwunden werden. Nach wie vor brauchen Angriffe auf sensible IT-Infrastrukturen vor allem eines: Zeit. Zeit ist der Faktor, der dem Angreifer immer mehr Erkenntnisse, Vorbereitung und konkrete Angriffswege eröffnet. Dies zeigt, dass die Sicherheit hinter dicken Mauern trügerisch ist, falls man nicht in der Lage ist die Gesamtsituation zu erkennen oder zu beeinflussen. Aus diesem Grund sollten, wie im Folgenden erläutert, Schnittstellen zur Sicherheitsorganisation außerhalb des Scope des ISMS aufgebaut werden.

Schnittstelle Meldepflichten

Eine dieser Schnittstellen wird auch vom IT-Sicherheitsgesetz, genauer dem neuen § 11 Absatz 1c EnWG vorgegeben: die Meldepflicht von Sicherheitsvorfällen. Da viele Energienetzbetreiber ähnlich strukturiert sind und zum Teil die gleichen Systeme verwenden, lohnt sich hier die zentrale Sammlung und Verbreitung von Warnmeldungen, welche durch das BSI geplant ist. Die potenzielle Warnmeldung »Achtung, das System XYZ wurde auf folgende Weise angegriffen; schließen Sie diese Lücke« ist bei rechtzeitigen Reaktionen ein großer Gewinn für die Sicherheit der kritischen Infrastrukturen (siehe Kapitel 1.1.2).

Schnittstelle Unternehmens-IT

Weitere Schnittstellen sind bei Abgrenzungen zur eigenen Unternehmens-IT hin als Pflicht zu betrachten. In der Prozessleittechnik sowie im Hochsicherheitsbereich (zum Beispiel Banken, einzelne Netzbetreiber) wurden die besonders geschützten Netze in der Vergangenheit meist über die unkritische »Büro-IT« angegriffen und aufgebrochen. Denn dort, wo unerfahrene Nutzer in größeren Netzwerken arbeiten welche von wenigen Personen administriert werden, sind Angriffe am einfachsten. Es sollte deshalb eine Schnittstelle zur IT-Sicherheit außerhalb des ISMS aufgebaut und regelmäßig beobachtet werden, ob die Informationssicherheit um das ISMS herum funktionsfähig, leistungsfähig und nach wie vor integer ist. Diese Schnittstelle sollte ein Mitarbeiter oder Partner sein, der für das Thema Informationssicherheit sensibilisiert wurde und so mögliche und echte IT-Sicherheitsvorfälle außerhalb des ISMS erfasst und verarbeitet. Ein regelmäßiger Austausch mit dieser Person oder die Einbeziehung in die Reportingwege dieser Schnittstelle – insbesondere mit Fokus auf bisher erkannte Sicherheitsvorfälle, Schadsoftware und Netzwerkaktivitäten – versetzt das Unternehmen in die Lage, Ausspähversuche und Probeangriffe frühzeitig zu erkennen und gegebenenfalls Vorbereitungen treffen zu können. Weiterhin ermöglicht eine solche Schnittstelle, Sicherheitsvorfälle zu verfolgen und gegebenenfalls Beweise zu sichern, sodass einerseits Angreifer verfolgt und andererseits die genutzten Lücken dokumentiert und geschlossen werden können.

Schnittstelle Objektsicherheit

Eine Schnittstelle zur Unternehmenssicherheit sollte ebenfalls aufgebaut werden, um Einbrüche oder unbefugte Zutritte und Zugriffe auf dem Werksgelände des Unternehmens hinsichtlich eines Angriffs auf die Informationssicherheit zu prüfen. Wurde etwa an Türen mehrfach Alarm ausgelöst oder haben Bewegungsmelder oder Kameras etwas Verdächtiges aufgezeichnet, so kann das ein früher Versuch gewesen sein, die Schutzmaßnahmen zu testen. Sollten bauliche Maßnahmen oder allgemeine Sicherheitsmaßnahmen für den Betrieb des ISMS notwendig sein, können diese direkt von dieser Schnittstelle übernommen werden. An dieser Stelle lohnt es sich auch meist, alle Mitarbeiter zu sensibilisieren und ihnen eine Meldestelle anzubieten, bei der verdächtige Personen und Vorgänge gemeldet werden können. Ein Einbruch im Zusammenhang mit Diebstahl und Vandalismus kann nach erfolgtem Zugriff nur ein Ablenkungsmanöver gewesen sein. Auch wenn sich solche Vorgänge häufig als bedeutungslos erweisen, sind mitdenkende und um Sicherheit besorgte Mitarbeiter eine äußerst sinnvolle Unterstützung für ein effektives ISMS.

Schnittstelle Dienstleister

Eine sehr ausgeprägte Schnittstelle sollte unbedingt auch zu Dienstleistern, Herstellern und Hostern aufgebaut werden. Auch wenn wesentliche Teile des Scopes im Zugriff oder der Verantwortung dieser externen Organisationen liegen, liegt die Verantwortung für die Informationssicherheit im eigenen Unternehmen. Aus diesem Grund ist es also zwingend, vertragliche Regelungen hinsichtlich Vertraulichkeit und Verfügbarkeit der erbrachten Dienstleistung zu treffen. Ein Leitsystemhersteller, welcher sich regelmäßig auf das Leitsystem schaltet sollte somit ein gewisses Informationssicherheitsniveau aufbauen oder nachweisen, damit das ISMS nicht aus

dieser Richtung kompromittiert werden kann. Ein Kommunikationsnetzprovider, welcher die Verbindungen zwischen Leitsystem und Fernwirkgeräten bereitstellt, sollte das notwendige Maß an Informationssicherheit zusichern und auch nachweisen können. Je nachdem, wie viel der kritischen Infrastruktur durch einen Dienstleister betrieben wird, kann sich eine ISO27001 Zertifizierung für diesen beziehungsweise dessen Kunden lohnen. Inzwischen ist diese im Rechenzentrumsbereich und bei Hostern auch schon ein sehr weit verbreitetes Wettbewerbsmerkmal. Kann ein Dienstleister die Zertifizierung nicht vorweisen, müssen von ihm gegebenenfalls einzelne Maßnahmen und Regelungen einfordert und deren kontinuierliche Verbesserung überwacht werden (s. hierzu auch Kapitel 1 und 5.3.5).

Schnittstelle Behörden

Eine Schnittstelle zu Behörden könnte auch sinnvoll sein, damit zum Beispiel Organisationen wie Polizei, Feuerwehr und THW den hohen Schutzbedarf des Unternehmens erkennen. So könnte die Polizei dafür sensibilisiert werden zu reagieren, wenn ein Mann mit Laptop außerhalb der Geschäftszeiten vor dem Werksgelände im Auto sitzt. Die Feuerwehr könnte frühzeitig informieren, wenn ein umgestürzter Baum eine Lücke im Zaun hinterlassen hat. Diese Sensibilisierung sorgt zusätzlich dafür, dass Einbrüche oder Vandalismus an Außenstandorten als Informationssicherheitsvorfälle betrachtet werden können.

In jedem Fall sollte geprüft werden, was außerhalb Ihrer Grenzen und »Grenzübergänge« liegt und ein Kontakt zum jeweiligen Verantwortlichen aufgebaut werden. Obwohl viele Sicherheitsrisiken bestehen und zahllose Angriffsszenarien denkbar sind, haben frühzeitige Erkenntnisse und der Austausch von Informationen schon viele Sicherheitsvorfälle im Keim erstickt.

2.4 Beteiligte Mitarbeiter

Die gelungene Einbindung und das Zusammenwirken der Mitarbeiter bei der Etablierung und der laufenden Umsetzung eines ISMS stellt eines der wesentlichen Erfolgskriterien dar. Die hier geschaffenen Prozesse und Sicherheitsvorkehrungen müssen von allen Mitarbeitern akzeptiert und mitgetragen werden, sonst kommen selbst ausgefeilte Schutzmaßnahmen in der betrieblichen Praxis nicht an, werden in hektischen Situationen außer Acht gelassen, geraten in Vergessenheit oder werden bewusst oder unbewusst umgangen. Entsprechend wichtig ist es, die Informationssicherheit nicht als »Expertenthema« zu betrachten und somit den Kreis der Mitwirkenden im Sinne des Scopes nicht auf die Sicherheits-Rollen zu beschränken. Für die Umsetzung und Akzeptanz ist eine Einbindung vieler Funktionen innerhalb und außerhalb des Unternehmens notwendig, die jeweils zielgruppenspezifisch anzusprechen und einzubeziehen sind.

Rolle der Geschäftsführung

Die Akzeptanz beginnt dabei mit der Geschäftsführung, die letztlich nicht nur die Verantwortung für die Informationssicherheit trägt, sondern auch deren Sinn und Bedeutung für das

Unternehmen erklären und in der täglichen Praxis immer wieder »vorleben« sollte. Entsprechend sollte die Geschäftsführung nicht nur zu Beginn eines solchen Projekts in Erscheinung treten, etwa durch die Verabschiedung der Sicherheitsstrategie oder das Auftreten bei Auftaktveranstaltungen. Auch im Alltag ist die Unterstützung bei Entscheidungen, die für die Mitarbeiter Änderungen oder einen Komfortverlust mit sich bringen, wichtig. Entsprechend haben sich hier Maßnahmen zur gezielten Einbindung und Sensibilisierung von Geschäftsführung und Führungskräften bereits in einem frühen Projekt- und Umsetzungsstadium bewährt.

Ein großer Teil der Projektarbeit und auch die spätere Steuerung der Sicherheitsprozesse wird durch die existierenden und neu geschaffenen Sicherheitsrollen geleistet werden, etwa durch den Ansprechpartner IT-Sicherheit für die BNetzA. Hierbei darf aber im Unternehmen nicht der Eindruck entstehen, dass die Verantwortung für das Thema Sicherheit sich allein auf diese Rollen beschränkt. Die Umsetzungsverantwortung bleibt auch nach Etablierung dieser Rollen bei jedem einzelnen Mitarbeiter im Rahmen seines Verantwortungsbereichs.

Rolle der Betriebsverantwortlichen

Eine der grundsätzlichen Herausforderungen bei der Umsetzung von Informationssicherheit zeigt sich in der Automatisierungstechnik. Eine neue, sich dynamisch weiterentwickelnde IT-Bedrohungslage trifft auf Systeme, die unter gänzlich anderen Voraussetzungen konzipiert und anderen Lebenszyklen unterworfen sind. Entsprechend wichtig ist es für die Sicherheitsrollen im Unternehmen, die Umsetzung von Maßnahmen gemeinsam mit Betriebs- und Anlagen-Verantwortlichen zu planen. Nur so lassen sich mögliche Kommunikations- und Umsetzungsprobleme vermeiden, die sich aus den unterschiedlichen Kenntnissen und Erfahrungen ergeben. Dabei stellt sich möglicherweise heraus, dass bestimmte Sicherheitsmaßnahmen zwar dem Risiko angemessen, aber in der Automatisierungstechnik nicht umsetzbar sind. Auf der anderen Seite sind den Ingenieuren, Technikern und dem Bereitschaftspersonal in den Stationen oft einzelne Sicherheitsrisiken nicht bekannt, die sich aus dem unvorsichtigen Umgang mit IT-Mitteln wie zum Beispiel Wartungs-Notebooks oder mobilen Datenträgern ergeben.

Rolle der Office-IT

Auch das Personal in der Office-IT spielt in der Umsetzung eine wichtige Rolle. Gefragt sind hier beispielsweise die Prozesse im Bereich Benutzer- und Berechtigungsmanagement, dem IT-Service-Management (zum Beispiel Incident- und Change Management) sowie der Beschaffung, Konfiguration und Bereitstellung von Hardware- und Software-Komponenten. Die Durchführung erfolgt teilweise abweichend vom Regelbetrieb in der Office-IT und erfordert somit entsprechende Ausnahmen oder Alternativprozesse und -lösungen, die durch die IT erarbeitet und unterstützt werden müssen. So wird das Benutzermanagement oft dezentral in den Anlagen durchgeführt, um die nötige Ausfallsicherheit zu gewährleisten, aber erfordert möglicherweise trotzdem bei der erstmaligen Einrichtung die Unterstützung der zentralen IT. IT-Software und -Komponenten sind möglicherweise für die Anlagen nur in bestimmten Versionsständen freigegeben, können nicht gemäß der Office-IT-Richtlinien aktualisiert werden und erfordern alternative Sicherheitsmaßnahmen wie zum Beispiel Whitelisting-Lösungen für kritische Systeme.

Rolle der Anwendungsentwicklung

Eine besondere Rolle in der IT spielt die Anwendungsentwicklung. Soweit im Bereich der Prozess-IT auch eigenentwickelte Anwendungen zum Einsatz kommen, ist auch hier spätestens mit der Etablierung eines ISMS neben der Sensibilisierung der Software-Entwickler auf geeignete Prozesse zu achten, um Sicherheitsrisiken möglichst frühzeitig zu minimieren. Dazu gehören Entwicklungsrichtlinien für alle Phasen der Software-Entwicklung sowie der Einsatz von geeigneten Werkzeugen zur statischen und dynamischen Überprüfung von erstelltem Programm-Code. Eine enge Einbindung der Anwendungsentwicklung ist bei der Planung entsprechender Maßnahmen im ISMS unerlässlich.

Gerade im Bereich der Anwendungsentwicklung zeigt sich sehr schnell, dass die bisher beschriebenen Maßnahmen nicht allein auf die internen Mitarbeiter beschränkt sein können. Hier werden Entwicklungsaufgaben oft ausgelagert, sodass sich das ISMS entsprechend auch mit Sicherheitsvorgaben für externe Entwickler befassen muss, um eine durchgängige Betrachtung der Sicherheitsrisiken zu gewährleisten. Gleiches gilt für die Nutzung von Software-Paketen zur Installation im Unternehmen oder durch den Bezug von Software-as-a-Service (SaaS) oder als Cloud-Service. Hier sind im Rahmen des Projektes die Rollen in der IT zu identifizieren, die entsprechende Beschaffungsvorgaben für extern bezogene Software erstellen und den sich ändernden Risiken anpassen können.

Rolle der externen IT-Dienstleister

Auch in den übrigen Bereichen der IT spielt die Auslagerung von IT-Services an externe IT-Dienstleister eine zunehmend wichtige Rolle. Soweit durch eine solche Auslagerung der Scope des ISMS mittel- oder unmittelbar betroffen ist (zum Beispiel durch den externen Betrieb von Arbeitsplätzen oder der Netzwerk-Infrastruktur) sind die Sicherheitsmaßnahmen des Dienstleisters und die von ihm bereitgestellten Rollen mit den Anforderungen des eigenen ISMS abzugleichen und gegebenenfalls vertraglich zu ergänzen. Dies wird in den Fällen, in denen der Dienstleister ebenfalls ein zertifiziertes ISMS betreibt, deutlich erleichtert, aber die Verantwortung für die Sicherheit der bezogenen IT-Dienstleistung bleibt rechtlich weiterhin beim beschaffenden Unternehmen. Je nach Umfang der ausgelagerten Dienstleistung ergeben sich dadurch wiederum zusätzliche Aufwände in der Steuerung und Auditierung des externen Dienstleisters, die durch entsprechende Rollen im Bereich Sicherheit und im Vertrags- bzw. Service-Management erbracht werden müssen.

Rolle des Wartungspersonals

Eine besondere Rolle bei der Einbindung von externen Mitarbeitern in das eigene Sicherheitskonzept spielt bei Prozess-IT-nahen Bereichen häufig das externe Wartungspersonal. Oftmals ist hier im Gegensatz zur Office-IT eine Fremdwartung die zwingende Voraussetzung für die Aufrechterhaltung der herstellerseitigen Gewährleistung für die betreffende Anlage oder Komponente. Umso wichtige ist es, dass diese externen Mitarbeiter ebenso sicherheitsbewusst handeln wie das interne Personal. Dies betrifft sowohl externe Wartungszugänge über VPN- oder andere

Netzwerkverbindungen als auch die Vor-Ort-Wartung. Das heißt beispielsweise konkret, dass Hersteller für seine Wartungstechniker und –Notebooks ein Sicherheitskonzept besitzen sollte, das die Übertragung von Schadsoftware von anderen Einsatzorten oder die ungesicherte Verbindung ins Internet (zum Beispiel zu privaten Zwecken) wirksam verhindert. Gleiches gilt für mitgebrachte mobile Datenträger wie Speichermedien oder USB-Sticks. Im Zweifel sollte den externen Mitarbeitern sichere Technik durch das eigene Unternehmen bereitgestellt werden, bevor diese sich mit unsicheren Geräten wie Laptops mit den sicherheitsrelevanten Schnittstellen verbinden.

Weitere beteiligte Mitarbeiter

Auch außerhalb der IT und IT-naher Dienstleistungen gibt es weitere Unternehmensfunktionen, die bei Planung und Umsetzung eines ISMS berücksichtigt werden sollten. Dazu gehören Bereiche für Haus-, Sicherheits- und Gebäudetechnik, soweit sie den Zugang zu Anlagen innerhalb des Scopes verantworten. Dies ist nicht beschränkt auf die reine Einlasskontrolle, sondern entsprechend der technischen Schutzmaßnahmen wie Zutrittskontrollsysteme, Bewegungsmelder, Video-Überwachung und die allgemeine physische Sicherheit.

Der Personalbereich ist in einigen Situationen mit den neu aufgestellten Sicherheitsanforderungen konfrontiert. So sind die eigenen Prozesse zur Anstellung, Versetzung oder Kündigung dahingehend zu überprüfen, dass die entsprechende Mitteilung zur Bereitstellung aber insbesondere auch dem Entzug von Zutritts- und Zugangsrechten in den betreffenden Unternehmensbereichen zeitnah erfolgt. Gleiches gilt auch für längerfristig tätige externe Mitarbeiter. Auch bei der Einstellung von Personal in diesen Bereichen müssen Mitarbeiter je nach Rolle über das ISMS in Kenntnis gesetzt und für das Thema Informationssicherheit sensibilisiert werden.

Auch das Empfangspersonal und andere Mitarbeiter die mit der Abwicklung von externen Besuchern und Delegationen betreut sind, sollten die entsprechenden Ausweis-, Zugangs- und Verhaltensregeln für verschiedene Unternehmensbereiche kennen und kommunizieren. Hier zeigt sich wieder die Verantwortung jedes einzelnen Mitarbeiters, der beispielsweise unbegleitete Besucher oder solche ohne gültigen Gäste-Ausweis höflich aber bestimmt zum jeweiligen Empfangsbereich begleiten sollte.

2.5 Anwenden des Scope im laufenden ISMS-Projekt

Ist der Scope ausführlich definiert und wie im Kapitel 2.1 bis 2.4 beschrieben dokumentiert, kann in die nächste Projektphase gestartet werden. Der Anwendungsbereich des ISMS nimmt auf die folgenden Aspekte der Dokumentation Einfluss:

- **Die Informationssicherheitsleitlinie** ist die Erklärung des Managements, die Werte und Informationen des Unternehmens mit einem ISMS zu schützen. Die Wirksamkeit des ISMS wird in dieser Managementerklärung auf den Scope beschränkt.

- **Das Risikomanagement** wird erstmals definiert und dokumentiert und behandelt theoretisch alle Assets aus dem Scope. Die Beschreibung der Risikomanagementmethodik sollte auf den Scope referenzieren.

- **Der Netzstrukturplan nach Vorgabe des IT-Sicherheitskatalogs** bietet eine gute Hilfestellung zur initialen Identifikation und Dokumentation der Assets. Er unterstützt dabei, durch das Verfolgen logischer Verknüpfungen zwischen einzelnen Assets alle beteiligten technischen Komponenten zu identifizieren.

- **Das Verzeichnis zur Risikoeinschätzung** ist eine Auflistung aller auf die Assets im Scope einwirkenden Risiken. Es ist eine erweiterte Inventarliste des Geltungsbereichs für das Risikomanagement. Es sollte der Beschreibung der Risikomanagementmethodik angehängt werden. Das Verzeichnis zur Risikobehandlung bezieht sich ebenfalls auf die Assets im Scope und führt diese zwangsläufig auf – mit dem Unterschied, dass in diesem Dokument die Risikobehandlungsmethoden, also die Controls der ISO27001, den Assets zugewiesen werden.

- **Die Erklärung der Anwendbarkeit** (Statement of Applicability, SOA): referenziert nicht direkt auf den Scope, ist aber in starkem Maße von seiner sauberen und vollständigen Dokumentation abhängig. Die Maßnahmen im SOA sollten jedes Asset im Scope mit einer passenden Maßnahme aus dem Risikomanagement abdecken. Hier lohnt sich meist die Querprüfung, um Lücken in der Risikobehandlung zu identifizieren. Anders herum können so auch Maßnahmen identifiziert werden, die keine Wirkung auf den Scope haben und somit faktisch Ressourcenverschwendung wären. Diese Maßnahmen sollten nochmals durch das Risikomanagement betrachtet und neu bewertet werden.

- **Das ISO 27001-Zertifikat auf Basis des IT-Sicherheitskatalogs** weist den Umfang und die Tiefe des ISMS aus. Ist der Scope künstlich klein gehalten, könnte die Wirksamkeit oder die Plausibilität ihres ISMS durch die Öffentlichkeit oder übergeordnete Behörden in Frage gestellt werden.

Exkurs: Den Scope – aus Sicht eines Zertifizierers – strukturiert aufsetzen

Sönke Maseberg, Datenschutz Cert

Ein möglicher Scope könnte lauten »ISMS für die Netzsteuerung«

Ein solcher Scope könnte auf einem ISO 27001-Zertifikat im Sinne des IT-Sicherheitskatalogs als Geltungsbereich angegeben sein, der damit die gesetzlich vorgegebenen Anforderungen erfüllt. Im Rahmen der Auditierung müsste dann festgestellt werden, dass dieser Scope »ISMS für die Netzsteuerung« korrekt auf die entsprechenden Assets des Unternehmens heruntergebrochen wurde, welche für den sicheren Netzbetrieb notwendig sind. Dazu würde sich aus Sicht einer Zertifizierungsstelle der folgende strukturierte Ansatz anbieten:

- Erstellung einer Strukturanalyse, in der alle Komponenten aus dem Unternehmen aufgeführt sind (Ist-Aufnahme der Assets):
  - Standorte, Gebäude, Räume
  - IT-Systeme und Netzkomponenten
  - Anwendungen

Zu verzeichnen sind dabei auch Abhängigkeiten, d. h. zum Beispiel welche Anwendungen auf welchen IT-Systemen/Netzkomponenten betrieben werden und in welchen Räumen/Gebäuden/Standorten. Möglich ist eine Gruppierung, um einen besseren Überblick herzustellen; dazu bieten sich auch Netzwerkpläne an.

- Klassifikation der Komponenten dahingehend, ob diese »für einen sicheren Netzbetrieb notwendig sind« sind. Dazu bietet sich folgende Klassen an:
  - »enforcing« für unabdingbar notwendige Komponenten: die Komponenten können einen Einfluss auf die Netzfahrweise haben (unmittelbar oder mittelbar durch Bereitstellung von Daten)
  - »supporting« für Komponenten, die zwar auf den ersten Blick klar dem Netz zugeordnet sind, aber tatsächlich auch nicht mittelbar die Netzfahrweise beeinflussen können
  - »non-interfering« für Komponenten, die offensichtlich keinen Einfluss auf die Netzfahrweise haben können

Der Scope setzt sich damit zusammen aus allen Komponenten, die als »enforcing« klassifiziert wurden. Die Abgrenzung zu anderen Komponenten wird durch klare Schnittstellen zu »supporting«-Komponenten beschrieben. Dieser strukturierte Ansatz stellt nur eine Möglichkeit dar, den Scope und die Assets des Scopes abzubilden. Selbstverständlich sind auch andere Lösungen denkbar.

3 Aufwand, Zeit und Personal

3 Aufwand, Zeit und Personal

Dirk Wegner, Applied Security
Steffen Heyde, Secunet
Markus Werckmeister, DQS
Michael Niehenke, items

3.1 Zeit

3.1.1 Erfahrungswerte bei der erstmaligen Einführung eines ISMS

Der VKU hat im Jahr 2015 eine Umfrage zur IT-Sicherheit bei seinen Mitgliedern durchgeführt. Die Ergebnisse zeigen, dass die teilnehmenden Unternehmen für die Einführung eines ISMS sehr unterschiedliche Zeitrahmen einplanen. Während gut die Hälfte der Befragten von einem Umsetzungszeitraum von unter zwei Jahren ausgeht, rechnen die verbleibenden 45 Prozent mit zwei oder mehr Jahren. Die Frist zur Umsetzung laut dem IT-Sicherheitskatalog wurde von ursprünglich einem Jahr, nach Stellungnahme des VKU und anderer Verbände, auf knapp zwei-einhalb Jahre verlängert. Frist zum Nachweis des Zertifikats des ISMS ist nun der 31.01.2018. Damit sollte zumindest die Mehrheit der Unternehmen den Zeitplan einhalten können.

Zeitplan
Wie lang wird der Zeitraum von der Planung bis zur vollständigen Einführng der ISMS voraussichtlich in etwa sein?

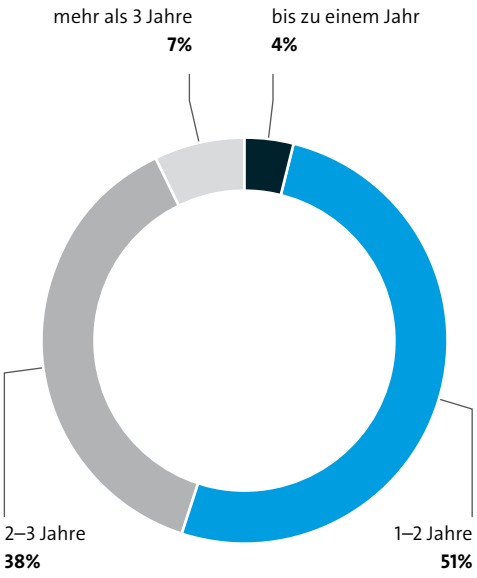


Abbildung 4: VKU Umfrage Zeitplan ISMS

Voraussetzung ist natürlich, dass die Unternehmen nun mit der Umsetzung der Maßnahmen beginnen. Gerade größere Unternehmen sollten etwas mehr Zeit einplanen, da Projekte hier mehr Beteiligte haben und deshalb häufig etwas länger dauern. Bezüglich des eingesetzten Personals für die Umsetzung rechnen die Unternehmen im Mittel mit 3,7 Stellen, die für die Einführungsphase des ISMS gebraucht werden sowie 1,6 Stellen für den laufenden Betrieb.

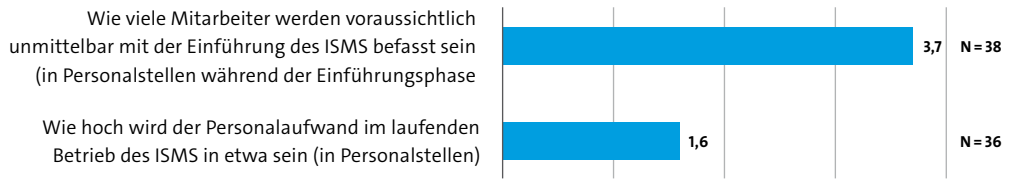


Abbildung 5: VKU Umfrage Personalplanung ISMS

Weitere interessante Ergebnisse können Sie über den VKU beziehen.

3.1.2 Aufwand der Implementierung eines ISMS

Wie die Umfrage gezeigt hat, sind der Aufwand und damit die Umsetzungszeiträume zur Implementierung eines ISMS sehr verschieden. Eine allgemeine Darstellung des Aufwandes für die Etablierung eines ISMS kann deshalb nicht dargestellt werden. Der Aufwand hängt stark von verschiedenen Faktoren ab:

- Umfang des zu betrachtenden Anwendungsbereiches (siehe auch Kapitel 2)
- Anzahl der involvierten Personen und Bereiche im Unternehmen (siehe Kapitel 3.2)
- Umfang und Qualität der bereits umgesetzten IT-Sicherheitsmaßnahmen
- Umfang und Qualität der bestehenden Dokumentation (siehe Kapitel 4)
- Umfang des vorhandenen unternehmensweiten Risikomanagements
- Beschaffenheit und Heterogenität der IT-Landschaft
- Vorarbeiten, die gegebenenfalls im Rahmen des Umwelt- und des Qualitätsmanagement wiederverwendet werden können
- Qualität der Berater

Eine hohe Priorisierung des Projektes durch die Geschäftsführung ist ein weiterer wesentlicher Faktor für die Zeitdauer der erstmaligen Umsetzung. Nur wenn die Geschäftsführung hinter dem Projekt steht und die Mitarbeiter für die Umsetzung der Aufgaben mindestens teilweise von operativen Aufgaben freistellt, kann die Umsetzung eines solchen Projekts in kürzerer Zeit gelingen. Die wesentlichen weiteren Erfolgsfaktoren für eine erfolgreiche und zügige Einführung eines ISMS sind:

- Richtlinien, Ziele und Aktivitäten müssen den geschäftlichen Anforderungen und Bedürfnissen sowie der Organisationskultur entsprechen.
- Die konkrete Anwendung eines kontinuierlichen Verbesserungsprozesses, zum Beispiel mit Hilfe des PDCA-Zyklus, muss nachweisbar sein oder nachweisbar gemacht werden.
- Im betrieblichen Alltag der Organisation muss ein gutes Verständnis für Informationssicherheit und ein Bewusstsein für relevante Risiken vorhanden sein.
- Durch angemessene Ausbildungs- und Trainingsmaßnahmen muss das vorhandene Sicherheitsbewusstsein erhalten und bei Bedarf verbessert werden.
- Das Anwenden und Befolgen von Leitlinien, Richtlinien und anderen ISMS-Elementen des organisationseigenen Regelwerks darf nicht nur auf dem Papier, sondern muss in der Realität passieren.
- Informationssicherheit sollte innerhalb der Organisation aktiv vermarktet werden.
- Es müssen genügend Ressourcen für den Aufbau und Betrieb des ISMS zur Verfügung stehen.

Für ein mittleres Stadtwerk (150 bis 200 Mitarbeiter) können im Allgemeinen etwa 1 bis 2 Jahre veranschlagt werden. Für große Netzbetreiber können dagegen eher 2 Jahre oder mehr angesetzt werden (siehe auch Kapitel 3.1).

Folgende Aufwände könnten/sollten getrennt betrachtet werden:
- Einführungsaufwand für Awareness-Schaffung und -Beibehaltung von Führungskräften und Mitarbeitern zur Änderung des Verhaltens im Umgang mit klassifizierten Dokumenten (Information Assets)
- Aufwand jeweils für Analyse/Planung, Einführung, Betrieb und Aufrechterhaltung des ISMS

3.1.3 Vom Audit zur Zertifizierung

Auf dem Weg zur Zertifizierung des ISMS müssen mehrere Audits durchlaufen werden. Die Planung und Durchführung von Audits (intern oder extern) von Managementsystemen wird in der ISO 19011 generell beschrieben und ist unabhängig vom zu Grunde gelegten Regelwerk. In der Norm sind neben dem Auditprozess auch die Qualifikationsanforderungen an die Auditoren festgelegt. Im Falle eines ISMS müssen Zertifizierungsorganisationen die Anforderungen der ISO/IEC 27006 zur Zertifizierung eines ISMS erfüllen, wenn sie über eine Akkreditierung der nationalen Akkreditierungsstelle Deutsche Akkreditierungsstelle GmbH (DAkkS) verfügen wollen.

Die Anzahl der Audittage wird in Abhängigkeit der nachfolgenden Faktoren gemäß der Tabellen A und C der ISO/IEC 27006 ermittelt:
- Umfang des ISMS Geltungsbereiches, IT-Systeme und der betroffenen Information Assets
- Komplexität des ISMS (zum Beispiel Kritikalität der IT-Systeme, Risiken/Bedrohungen gemäß Annex A)
- Anzahl der Mitarbeiter und Standorte
- Art der Geschäftstätigkeit und weitere Geschäftsanforderungen/Gesetze
- Art und Vielfältigkeit der eingesetzten Technologie bei den implementierten Informationssicherheits-Controls

- Grad des Outsourcings von Informationssicherheits-Controls

Die so ermittelten Audittage verteilen sich auf zwei Schritte (Stagen) der Zertifizierung:

Stage 1 (ehemals Systemanalyse): Prüfung der ISMS-Dokumentation auf Normkonformität und Vollständigkeit, Prüfung der vollständigen Erfassung und Klassifizierung der Information Assets und IT-Systeme, Ermittlung des Komplexitätsgrades (Prozesse, IT-Systeme, Organisation), Prüfung der Risikoidentifikation und -bewertung, Ableitung eines Auditplanes. Zusammenfassend ausgedrückt: Es wird geprüft, ob die Beschreibung und Dokumentation des ISMS (z. B. Informationssicherheits-Prozesse, Informationssicherheitsleitlinien) nach den Vorgaben der Norm erfolgt sind.

Stage 2 (ehemals Systemaudit): Prüfung der normkonformen Umsetzung der ISMS-Vorgaben, Bewertung der Wirksamkeit des ISMS mit all seinen Komponenten (beispielsweise Management Review, Interne Audits, PDCA-Zyklus, Informationssicherheits-Kennzahlen, Informationssicherheits-Zielerreichung, etc.), Bewertung der Wirksamkeit der Informationssicherheits-Controls. Vereinfacht dargestellt wird geprüft, ob das, was in der Dokumentation des ISMS vorgegeben ist, auch der Norm entsprechend umgesetzt wurde.

Um mit dem Stage 1 Audit beginnen zu können, müssen die oben genannten ISMS-Komponenten vorhanden sein. Nach erfolgreichem Abschluss des Stage-1-Audits kann das Stage-2-Audit geplant werden. Dazwischen sollte ein angemessener Zeitraum liegen der ausreichend ist, festgestellte Lücken zu schließen. Um Stage 2 erfolgreich zu durchlaufen sollten u. a. die internen Audits und das Management Review in einem signifikantem Umfang und Reifegrad vorliegen.

Im Folgejahr nach der Erstzertifizierung erfolgt das 1. und nach einem weiteren Jahr das 2. Überwachungsaudit, welche jeweils vom Umfang geringer sind, als im Erstzertifizierungsaudit. Diese Umfänge sind auch in der ISO/IEC 27006 festgelegt.

Optional gibt es die Möglichkeit des Voraudits, in denen der Reifegrad entlang des Projektfortschrittes neutral bewertet wird und Zertifizierungsrisiken frühzeitig adressiert werden können.

3.2 Personal

In diesem Abschnitt wird behandelt, welche Stellen oder Personen im Unternehmen bei der Umsetzung der Vorgaben aus dem IT-Sicherheitskatalog und dem IT-Sicherheitsgesetz eingebunden und welche Rollen neu geschaffen werden müssen. Dieser Abschnitt ist nicht zu verwechseln mit Kapitel 2.4, in dem beschrieben wird, welche Personalgruppen bei der richtigen Bestimmung des Scopes bedacht werden müssen. Dieser Abschnitt beschreibt dagegen das notwendige Personal für die Einführung des ISMS.

Die grundlegende Verantwortung für die Informationssicherheit trägt wie oben beschrieben die Geschäftsführung. Deshalb muss die Geschäftsführung in das Projekt verantwortlich eingebunden werden und das Projekt initiieren und auch führen. Sie wird gegebenenfalls auch haftbar gemacht, wenn aufgrund unzureichender Schutzvorkehrungen Dritte geschädigt werden. Die Delegation von Aufgaben und die Formulierung spezieller Zuständigkeiten wie im Weiteren erläutert, sind wichtige Voraussetzungen dafür, Informationssicherheit als wesentliche Aufgabe in einem Unternehmen zu verankern. Hierdurch wird jedoch die Geschäftsführung nicht von ihrer Grundverantwortung entbunden. Das Aufsetzen eines ISMS ist ein wesentliches Projekt des gesamten Unternehmens. Dies gilt auch für die Fortführung des ISMS nach der Initialisierung und dem ersten Audit.

Der Erfolg von Einführung und Betrieb eines wirksamen ISMS hängt ganz wesentlich von der Managementunterstützung ab. Deshalb wird auch im ISO 27001 Standard ein Schwerpunkt auf die Unterstützung des Managements gelegt.

3.2.1 Ansprechpartner für IT-Sicherheit

Die Bestellung eines Ansprechpartners für IT-Sicherheit ist gemäß IT-Sicherheitskatalog der BNetzA verpflichtend. Seine Aufgaben umfassen laut dem Katalog, gegenüber der BNetzA zu folgenden Punkten unverzüglich Auskunft geben zu können:

- Zum Umsetzungsstand der Anforderungen aus dem IT-Sicherheitskatalog
- Zu aufgetretenen Sicherheitsvorfällen sowie der Art und des Umfangs etwaiger hierdurch hervorgerufener Auswirkungen
- Zur Ursache aufgetretener Sicherheitsvorfälle sowie zu Maßnahmen zu deren Behebung und zukünftigen Vermeidung

Der Ansprechpartner kann bei einem externen Unternehmen beschäftigt sein, muss in jedem Fall aber eng in die Prozesse des betroffenen Unternehmens eingebunden sein und mit den Fachkollegen im engen Austausch stehen. Zum Zeitpunkt der Anfrage sollte er entsprechend schon informiert sein und falls erforderlich direkt an denjenigen Mitarbeiter verweisen können, der detaillierte Informationen zur Anfrage liefern kann.

Es ist gute Praxis im Unternehmen eine Person als IT-Sicherheitsbeauftragten zu benennen, der Einführung und Betrieb des ISMS operativ verantwortet. Diese Rolle ist zwar nicht gesetzlich vorgeschrieben, es bietet sich jedoch an, eine zentrale Stelle mit dem Aufgabengebiet Informationssicherheit zu betrauen. Wenn die Person auch nach Einführung des ISMS im Unternehmen bleibt und nicht nur zur Initialisierung beauftragt ist, kann es sinnvoll sein die Funktion mit derjenigen des Ansprechpartners für die BNetzA zu verbinden, da sie den oben genannten Anforderungen gut entspricht. Die Person kann im Unternehmen folgende Aufgaben wahrnehmen:

- den Informationssicherheitsprozess steuern und bei allen damit zusammenhängenden Aufgaben mitwirken
- die Unternehmensleitung bei der Weiterentwicklung der verbindlichen Regelungen zur Informationssicherheit unterstützen

- die Realisierung für Informationssicherheitsmaßnahmen initiieren und überprüfen
- Informationssicherheitsmaßnahmen mit dem Datenschutzbeauftragten abstimmen
- die Eignung und Wirksamkeit von Sicherheitsmaßnahmen durch jährliche interne Audits prüfen
- der Unternehmensleitung über den Status Quo der Informationssicherheit berichten
- sicherheitsrelevante Projekte begleiten
- Informationssicherheitsvorfälle untersuchen
- Sensibilisierungs- und Schulungsmaßnahmen durchführen.

Gleichzeitig kann der IT-Sicherheitsbeauftragte auch zentraler Ansprechpartner bei Sicherheitsvorfällen für das BSI sein, wobei diese Rolle für Energienetzbetreiber im Gegensatz zu Betreibern Kritischer Infrastrukturen aus anderen Branchen nicht explizit vorgeschrieben ist (siehe auch 1.1.3). Die Verschmelzung von Informationssicherheitsbeauftragten und Ansprechpartner für die BNetzA muss vom Unternehmen individuell geprüft werden. Da der Ansprechpartner gegenüber der BNetzA aber unverzüglich zu Sicherheitsvorfällen auskunftspflichtig ist, muss in jedem Fall ein enger Austausch zwischen den Rollen bestehen (für einen externen IT-Sicherheitsbeauftragten siehe Kapitel 5.4).

3.2.2 Weitere Rollen zur Etablierung eines ISMS-Projektes im Unternehmen

Neben dem Ansprechpartner für IT-Sicherheit können nach unternehmensindividueller Prüfung weitere Rollen eingeführt oder einbezogen werden, um das Projekt zur Etablierung eines ISMS optimal umsetzen zu können. Im Folgenden werden diese möglichen Rollen kurz dargestellt. Diese sollten zum Auftakt des Projektes und dann später punktuell zu einzelnen Aufgaben innerhalb des Projektes einbezogen werden. Sollten diese Funktionen nicht dediziert in dem jeweiligen Unternehmen existieren, können auch Personen hinzugezogen werden, die die Aufgaben der jeweiligen Rolle wahrnehmen. Es kann auch sein, dass mehrere Personen im Unternehmen vorhanden sind, die die jeweilige Rolle für unterschiedliche Bereiche (zum Beispiel Innen- und Außenanlagen) innehaben. Gerade bei kleineren Unternehmen können einzelne Mitarbeiter auch mehrere Rollen innehaben.

Datenschutzbeauftragter

Der Datenschutzbeauftragte hat auf die Einhaltung des Bundesdatenschutzgesetzes (BDSG) sowie anderer Vorschriften, die den Datenschutz betreffen, hinzuwirken. Eine wesentliche Voraussetzung zur Wahrung des Datenschutzes ist die Gewährleistung der Datensicherheit. Dadurch ergibt sich in der Praxis eine breite Überschneidung der Bereiche Datenschutz und Informationssicherheit. Die Unterschiede resultieren nur aus den unterschiedlichen Blickwinkeln. Während der Datenschutz ausschließlich auf personenbezogene Daten abzielt, bezieht sich die Informationssicherheit auf alle Daten, die für das Unternehmen einen Wert darstellen. Mit denselben Sicherheitsmaßnahmen können also sowohl Anforderungen des Datenschutzes als auch der Informationssicherheit erfüllt werden. Eine enge Zusammenarbeit zwischen den

Bereichen Informationssicherheit und Datenschutz sollte daher sichergestellt werden, um Redundanzen zu vermeiden bzw. Synergieeffekte zu nutzen.

Allerdings gibt es neben den Überschneidungen der beiden Bereiche auch Felder, in denen Informationssicherheit und Datenschutz in einen Interessenkonflikt geraten können. Etwa ist das langfristige und umfangreiche Speichern von Protokolldaten zu Anmeldeinformationen aus Sicht der Informationssicherheit für die Untersuchung zukünftiger Sicherheitsvorfälle gewünscht. Allerdings handelt es sich bei den Protokolldaten auch um personenbezogene Daten. Damit ist eine Speicherung aus Datenschutzsicht im Hinblick auf Zweckgebundenheit und Datensparsamkeit kritisch zu prüfen.

Risiko-Manager

Das Risikomanagement (Enterprise Risk Management) ist ein wesentlicher Bestandteil eines ISMS. Falls bereits ein strukturiertes Risikomanagement im Unternehmen existiert, sollte sichergestellt werden, dass das ISMS mit dem vorhandenen Risikomanagement ausreichend verzahnt wird. Denn jedes IT-Risiko stellt auch ein Unternehmensrisiko dar.

Der Risiko-Manager fungiert als zentrale und unabhängige Stelle zur Beurteilung bzw. Kontrolle von Risiken, Risikoansammlungen (»Risiko Cluster«) und risikoorientierten Sachverhalten. Außerdem versorgt er die Geschäftsführung mit Informationen über Geschäftsrisiken und unterstützt Fachbereiche und Geschäftsführung in Fragen des Risikomanagements. Falls bereits ein Risiko-Manager im Unternehmen benannt ist, sollte dieser im Projekt zur Einführung eines ISMS hinzugezogen werden, sodass auch Risiken, die durch die Informationsverarbeitung entstehen, bewertet werden können.

Personal-Verantwortlicher

Die Personalabteilung koordiniert Prozesse für die Personalverwaltung, zum Beispiel bei Ein- und Austritt oder Versetzung von Personal. Diese Prozesse haben auch direkten Einfluss auf die IT-Systeme, wenn der entsprechende Mitarbeiter diese Systeme in seiner Tätigkeit verwenden muss oder musste. Zusätzlich ist das Personal je nach Tätigkeit auch für die Umsetzung der Sicherheitskonzepte zu schulen. Hier ist die Personalabteilung Schnittstelle und kann das Projekt unterstützen.

IT-Leiter

Je nach Unternehmen vertritt der IT-Leiter in der Regel die IT-Systeme der Office-IT und die Umsetzung IT-bezogener Prozesse. Er sollte an der Identifizierung und gegebenenfalls Absicherung der Schnittstellen zu den Systemen der Prozess-IT hinzugezogen werden und seine Mitarbeiter motivieren, die Umsetzung des ISMS zu unterstützen.

Facility-Verantwortlicher

Der Facility-Manager ist unter anderem verantwortlich für Gebäude, Zutrittskontrollanlagen, Netzersatzanlagen und Notfall-Pläne. Viele damit verbundenen Prozesse und Systemkomponenten haben Einfluss auch auf die IT-bezogenen Einrichtungen im Unternehmen und damit auch auf das ISMS. Ein Beispiel ist die Zutrittsverwaltung und –Kontrolle des Rechenzentrums. Eine Einbindung des Verantwortlichen ist deshalb mit einzuplanen.

Verantwortlicher für Umwelt-Management

Ist bereits ein Umwelt-Management-Verfahren nach ISO 14000 etabliert, können die Berichtsprozesse gegebenenfalls angepasst wiederverwendet werden. Eine möglichst frühe Absprache mit dem Verantwortlichen ist daher ratsam.

Verantwortlicher für Qualitätsmanagement

Existiert ein Qualitätsmanagement-Prozess nach ISO 9001, sind bereits Prozesse etabliert die gegebenenfalls auch im Rahmen eines ISMS in angepasster Form wiederverwendet werden. Die Verantwortlichen können nach Erfahrungen mit der Umsetzung befragt und nach der Best-Practice-Umsetzung im Unternehmen befragt werden. Zur Verwendung bereits vorhandener Dokumentation siehe auch Kapitel 4.

Arbeitssicherheitsingenieur

Um Risiken, die im Zusammenhang mit der Kopplung zwischen IT-Sicherheit und Arbeitssicherheit entstehen können, aufnehmen und bewerten zu können, sollten die Verantwortlichen für die Arbeitssicherheit im Projekt eingebunden werden.

3.2.3 Weitere Rollen zur Etablierung eines ISMS-Projektes außerhalb des Unternehmens

Ausgelagerte Bereiche

Unternehmensaufgaben können unter Umständen an weitere Unternehmen vergeben sein (zum Beispiel RZ-Betrieb). Diese Unternehmen sind entsprechend den jeweiligen Aufgaben mit in das Projekt einzubeziehen, wenn deren Erfüllung die Bereiche substanziell beeinträchtigen können, die im Rahmen des ISMS-Scope betrachtet werden müssen.

Berater zum Aufsetzen eine ISMS

Je nach Ausstattung mit fachkundigem Personal ist es gegebenenfalls angezeigt, erfahrene Berater zur Etablierung eines ISMS hinzuziehen. Dies ermöglicht ein effiziente Projektdurchfüh-

rung und eine schnelle Klärung von audit-bezogenen Fragestellungen, ohne dass der Auditor im Vorfeld angesprochen werden muss.

Lieferanten

Die Hersteller wesentlicher Systemkomponenten sollten einbezogen werden, wenn die jeweiligen Komponenten Bestandteil des Audits sind. Dies betrifft beispielsweise geprüfte Härtungskonzepte oder Konfigurationen, die die IT-Sicherheitsfunktionen der Lösung betreffen.

Externe Dienstleister

Die externen Dienstleister, die ausgelagerte Dienste im Sinne der Erfüllung der Aufgabe wahrnehmen, müssen einbezogen werden, wenn die jeweiligen Dienste Bestandteil des Audits sind. Dies betrifft beispielsweise Sicherheitsdienstleistungen wie die Überwachung des Firmengeländes und der Gebäude aber auch IT-Dienstleistungen, die durch externe Betreiber zur Verfügung gestellt werden.

Qualifizierte Auditoren

Die Auditoren sollten im Projekt möglichst früh ausgewählt werden und in der Lage sein, ihre Expertise nachzuweisen. So besteht die Möglichkeit, auch den Auditor im Projekt direkt einzubeziehen, um Audit-spezifische Fragestellungen kurzfristig zu klären. Auch sollte eine Zeitplanung aufgesetzt werden, sodass das Audit zur geplanten Zeit auch von Seiten des Auditors aus umgesetzt werden kann.

3.3 Zeitplan zum Einsatz des Personals

Nicht jede Rolle muss bei jedem Prozess innerhalb der Einführung und Zertifizierung eines ISMS beteiligt sein. In der nachfolgenden Zuordnung sieht man einen beispielhaften groben Plan hinsichtlich der Beteiligung der einzelnen Rollen in Prozessen des ISMS.

Rolle – ISMS-Phase	Initiali-sierung	IST-Aufnahme/ Scoping	Implemen-tierung	Vor-Audit	Audit	Re-Audit
Geschäftsführer	■					
IT-Sicherheitsbeauftragter	■	■	■	■	■	■
Berater zum Aufsetzen eine ISMS	■	■	■	■	■	■
Auditor				■	■	■
Revision	■	■	■			
IT-Leiter	■	■	■	■	■	■
Leiter Netzsteuerung	■	■	■	■	■	■
Arbeitssicherheitsingenieur		■	■			
Verantwortlicher für Qualitätsmangement		■	■			
Verantwortlicher für Umwelt-Management		■	■			
Facility-Verantwortlicher		■	■			
Personal-Verantwortlicher		■	■			
Risiko-Manager (Enterprise Risk Management)	■	■	■	■	■	■
Datenschutzbeauftrager		■	■			
Personal-Verantwortlicher		■	■			
Lieferanten		■	■			
Externe Dienstleister		■	■	■	■	■

■ beteiligt ■ ggf. beteiligt, wenn nötig

Abbildung 6: Beteiligte Rollen beim Aufbau eines ISMS

4 Überführung bestehender IT-Sicherheitssysteme in ein Informations-Sicherheits-Management-System (ISMS)

4 Überführung bestehender IT-Sicherheitssysteme in ein Informations-Sicherheits-Management-System (ISMS)

Gerd Niehuis, BTC
Dieter Behrendt, Netz Lübeck GmbH
Thomas Gronenwald, Dominik Goergen, admeritia GmbH

Die geforderte Einrichtung eines ISMS für Systeme, die für den sicheren Netzbetrieb notwendig sind, ist eine herausfordernde Aufgabe für die Energienetzbetreiber. Daher sollten bereits vorhandenen Systeme des Netzbetreibers wie zum Beispiel Organisationsstrukturen sowie Prozesse und Dokumentationen soweit möglich genutzt und gegebenenfalls angepasst werden, um einen Teil der Anforderungen aus dem IT-Sicherheitskatalog an das ISMS mit vergleichsweise geringen Aufwänden zu erfüllen.

Managementsysteme bieten den Unternehmen den Vorteil, dass die an sie gestellten Anforderungen in funktionierende Prozesse strukturiert und zielgerichtet erfüllt werden. Durch die Verwendung von Standards und Normen erfolgt die Umsetzung in der Regel koordinierter, effizienter und sicherer als wenn diese Systeme nicht existierten und sind zudem überprüf- und belegbar. Zumeist erfordern Managementsysteme folgendes Vorgehen:

- Erstellung und Verbreitung von Leitlinien
- Zuordnung der Zuständigkeiten
- Schulung der Mitarbeiter
- Erarbeitung von Anweisungen und Dokumentationen
- Durchführung von Audits
- Kontinuierliche Verbesserung

In einigen Unternehmen der Energieversorgung sind zudem bereits Integrierte Managementsysteme (IMS) eingerichtet. Diese umfassen Methoden und Instrumente zur Einhaltung von Anforderungen aus verschiedenen Bereichen in einer einheitlichen Struktur. Die Mitarbeiter derartig aufgestellter Unternehmen sind mit der Beachtung aufgestellter Regeln, der Zuweisung von Verantwortung, den regelmäßigen Schulungen sowie der wiederkehrenden Auditierung bereits vertraut. Somit lassen sich hier Ressourcen bündeln und Synergien nutzen.

Ein Managementsystem für Informationssicherheit (ISMS) kann dann mit deutlich reduziertem Aufwand umgesetzt werden. Zudem verbessert ein funktionierendes Sicherheitsmanagement in der Praxis die Informationssicherheit oftmals nachhaltiger, da nur durch dieses die Wirksamkeit der Investitionen in die Sicherheitstechnik über den Zeitverlauf aufrechterhalten wird.

4.1 Aktueller Schutz der ITK-Infrastruktur

Damit Netzbetreiber ihrer Verpflichtung der allgemeinen Versorgungssicherheit nachkommen können, wurden in vielen Fällen bereits Prozesse und Handlungsanweisungen für bestimmte Bereiche etabliert. Diese sollten zu Beginn des Implementierungsprozesses des ISMS gesammelt und daraufhin geprüft werden, inwieweit sie auch in einem ISMS nach dem IT-Sicherheitskatalog Verwendung finden können. Von Interesse können hier alle Regeln und Dokumentationen sein, die ITK-Systeme vor unbefugten Zugriff schützen, stabil und ausfallsicher machen sollen oder dem Schutz von personenbezogenen Daten dienen. Zusätzlich nützlich können bereits vorhandene Regeln und Dokumentationen zum Schutz vor menschlichem Fehlverhalten, technischem Versagen, organisatorischen Mängeln oder höherer Gewalt sein. Dazu könnten die nachfolgenden Bereiche gehören:

Räumliche Sicherheit

Bereits im ersten Energiewirtschaftsgesetz aus dem Jahre 1935 verlangte der Gesetzgeber den Betrieb einer sicheren und zuverlässigen Versorgung. Versorgungseinrichtungen wurden daher stets nach dem aktuellen Stand der Technik gebaut, vor Umwelteinflüssen gesichert und vor unzulässigen Übergriffen geschützt. Sicherheitsrelevante Betriebsmittel sind meist Video- oder anderweitig überwacht.

Kommunikationswege

Bereits aus Gründen der Zuverlässigkeit unterhalten Netzbetreiber eigene Informationsnetze. Zudem sind wichtige Verbindungen i. d. R. redundant ausgelegt. Die Beschaltung und Entstörung der Informationsverbindungen erfolgt überwiegend durch eigenes Personal.

Dokumentationssysteme

Nur mit einer umfangreichen Dokumentation der Kommunikationswege, verbauten Betriebsmitteln und deren Parametrierungen sind Netzbetreiber in der Lage, schnell auf Störungen reagieren zu können. Dokumentierte Vereinbarungen mit Lieferanten gehören ebenso zum Standard wie der Kontakt zu Behörden (zum Beispiel bei Störungen der Versorgung mit Strom oder Gas).

Anweisungs- und Informationssysteme

Unternehmen besitzen oft eine Vielzahl von Regeln, in denen die internen und externen Prozesse beschrieben sind. Diese sind zum Beispiel Geschäftsanweisungen, Betriebsvereinbarungen, Verhaltensregeln, Organisations-, Verfahrens- und Arbeitsanweisungen. Durch die zunehmende Digitalisierung der Prozesse, existieren bereits viele Anweisungen zur Verwendung digitaler Hilfsmittel wie PCs, Smartphones, Laptops, Handhelds oder USB-Sticks.

Schulungssystem

Die Qualifizierung der Mitarbeiter im Rahmen von Aus- und Weiterbildungsprogrammen, sowie die strikte Terminierung und Überwachung von Pflichtschulungen, sollte in den meisten Netzbetrieben bereits eingerichtet sein.

Zugangssystem

Zum Schutz der Gelände, Gebäude und Räume werden häufig bereits elektronische Schließsysteme verbaut. Diese lassen nicht nur eine differenzierte Zugangsregelung zu, sondern ermöglichen auch eine Dokumentation der erfolgten Schließungen. Die Zuordnung oder der Entzug von Zugangsrechten ist jederzeit möglich.

Risiko

Das Aufspüren betrieblicher Risiken, deren Bewertung und deren Eingrenzung ist bei vielen Netzbetreibern üblich. Teilweise ist auch die für die Einschätzung von IT-Risiken erforderliche fundierte Methode, die imstande ist reproduzierbare und nachvollziehbare Ergebnisse zu generieren, bereits vorhanden. Des Weiteren existiert mitunter eine Schnittstelle vom IT-Risikomanagement zum Gesamtunternehmensrisikomanagement.

Personal

Die Verpflichtung des Personals auf die Wahrung von Betriebsgeheimnissen und die Einhaltung von Verhaltensregeln, sind in einigen Unternehmen bereits über ein Compliance Management-System sichergestellt.

Organisation

Die Definition und Übertragung von Zuständigkeiten sowie Pflichten und Verantwortlichkeiten sind in den meisten Unternehmen der Energieversorgung gängige Praxis. Vorhanden sind dementsprechend meist Funktions- oder Rollenbeschreibungen, Überwachungsprozesse sowie Organigramme.

4.2 Überführung von bestehenden IT-Sicherheitssystemen in ein ISMS

In einem Informationssicherheits-Managementsystem (ISMS) wird die IT-Sicherheit für einen definierten Anwendungsbereich geplant und kontrolliert (siehe dazu Kapitel 2). Sofern Prozessdokumentationen, Richtlinien und Handlungsanweisungen bereits vorhanden sind, können diese in ein ISMS überführt werden. Vorab sind die Unterlagen auf Vollständigkeit und Aktualität

zu prüfen und gegebenenfalls an die Anforderungen des ISMS anzupassen, sofern sie diese nicht bereits erfüllen.

Zumindest für die nachfolgend aufgeführten Systeme sollten die vorhandenen Dokumentationen und Prozesse gesammelt und untersucht werden, ob sie sich für eine Überführung in das neue ISMS eignen.

Industrial Control Systems

Zum automatisierten Messen, Steuern und Regeln von Abläufen, beispielsweise zur Automation von Prozessen und zur Überwachung von großen industriellen Produktionssystemen, kommen in vielen Bereichen sogenannte Industrial Control Systems (ICS) zum Einsatz. Diese finden häufig in der produzierenden Industrie aber auch in der Energiewirtschaft Verwendung. Im Gegensatz zur Office-IT werden ICS über längere Zeiträume mit quasi gleicher Anwendersoftware betrieben. Änderungen finden im Rahmen vorprojektierter Möglichkeiten wie zum Beispiel Änderung von Reglern, Parametern oder Grenzwerten statt. Die Installation von Patches erfolgt, soweit überhaupt verfügbar, in sehr geringem Umfang.

Systeme zur Bereitstellung von Messdaten

Im Hinblick auf die Netzsteuerung können aber auch TK- und EDV-Systeme im Netz betroffen sein, die selbst zwar nicht direkt Teil der Netzsteuerung, aber an dieser mittelbar beteiligt sind. Darunter fallen zum Beispiel Messeinrichtungen an Trafo- oder Netzkoppelstationen, welche durch die Bereitstellung von (Mess-) Daten einen indirekten Einfluss auf die Netzsteuerung haben.

4.3 Notwendiger Umfang der Dokumentation

Die nachfolgende Liste zeigt die Bereiche, die in jedem Fall in den Geltungsbereich des IT-Sicherheitskatalogs fallen. Hier sollte zuerst geprüft werden, ob bereits entsprechende Dokumentationen im Unternehmen existieren, die gegebenenfalls bei der Erstellung des ISMS genutzt werden können (Quelle: IT-Sicherheitskatalog, Tabelle 2, S. 11 ff.):

- Leitsysteme und Systembetrieb

Alle zentralisierten Systeme, die der Netzsteuerung oder -überwachung dienen, sowie die hierzu notwendigen unterstützenden IT-Systeme, Anwendungen und zentralen Infrastrukturen.
Beispiele:

- Zentrale Netzleit- und Netzführungssysteme
- Zentrale Messwerterfassungssysteme
- Systeme zur Überwachung und Steuerung von Netzspeichern
- Datenarchivierungssysteme
- Zentrale Parametrier-, Konfigurations- und Programmiersysteme

Weiterhin sollten die für den Betrieb der oben genannten Systeme notwendigen unterstützenden Systeme erfasst werden.

- Übertragungstechnik/Kommunikation

Die in der Netzsteuerung zur Kommunikation eingesetzte Übertragungs-, Telekommunikations- und Netzwerktechnik. Beispiele:
- Router, Switches und Firewalls
- Übertragungstechnische Netzelemente
- Zentrale Management- und Überwachungssysteme der Übertragungs-, Telekommunikations- und Netzwerktechnik
- Kommunikationsendgeräte
- Funksysteme
- Sekundär-, Automatisierungs- und Fernwirktechnik

Die prozessnahe Steuerungs- und Automatisierungstechnik, die zugehörigen Schutz- und Sicherheitssysteme sowie fernwirktechnische Komponenten. Hierzu gehören insbesondere die Technik in den dezentralen Stationen sowie die Automatisierungstechnik in Netzspeicheranlagen. Beispiele:
- Steuerungs- und Automatisierungskomponenten
- Leit- und Feldgeräte
- Controller und SPS inklusive digitaler Sensor- und Aktorelemente (Steuerung)
- Schutzgeräte und Sicherheitskomponenten
- Fernwirkgeräte
- Mess- und Zählvorrichtungen.

Die umfangreiche Dokumentation wird benötigt, um eine valide Planungsgrundlage für die Umsetzung von Sicherheitsmaßnahmen zu erhalten. Existieren nicht dokumentierte Bereiche, so werden die implementierten Sicherheitsmaßnahmen durch deren Nichtberücksichtigung im schlimmsten Fall unwirksam. Des Weiteren ist diese Dokumentation Basis für Überwachungs- und Verbesserungsprozesse (siehe auch Kapitel 1.2.) da durch sie auftretende Fehler oder Schwachstellen nachvollziehbar gemacht werden.

4.4 Hilfsmittel zur Überführung bestehender IT-Sicherheitssysteme in ein ISMS

Das »ICS-Security-Kompendium« des BSI enthält in Kapitel 5 »Best Practice Guide für Betreiber« einen Überblick über einige architektonische, technische und organisatorische Best Practices für die Betreiber von ICS. Diese Best Practices stellen eine Sammlung von sinnvollen Maßnahmen dar, welche sich zum einen in der Praxis bewährt haben und sich zum anderen aus den vorhandenen Standards ISO 27000/IT-Grundschutz, IEC 62443 und VDI 2182 ableiten lassen. Diese Normen sind zu den Best Practices in Bezug gesetzt. In der Tabelle 6 des Kompendiums erfolgt eine

Gegenüberstellung der Best Practices mit IEC 62443, VDI/VDE 2182, NERC CIP und DHS Best Practices. In der Tabelle 7 erfolgt eine »Gegenüberstellung der Best Practices mit IT-Grundschutz und ISO 27001«. Es bietet damit einen guten Startpunkt zum Umgang mit ICS.

Dies ermöglicht, sich auf erprobte Verfahrensweisen zu berufen und Sicherheitsmaßnahmen demgemäß umzusetzen. Alternativ können eigene Lösungsansätze, die die Anforderungen der DIN/ISO IEC 27001:2015-03 erfüllen, entwickelt werden. Der Aufwand sowie mögliche Fehler dabei können durch die Anwendung der aufgeführten Best Practices vermieden werden. Die hier genannten Zuordnungen erleichtern darüber hinaus die Auswahl dieser Maßnahmenempfehlungen erheblich, da erkenntlich ist zur Erfüllung welcher Anforderungen der Norm diese geeignet sind.

5 Kooperations-modelle

5 Kooperationsmodelle

Christian Westerkamp, ANMATHO AG
Rudolf Gurland, T-Systems
Sven Kuse, Smart Optimo
Michael Rose, DREWAG NETZ

5.1 Grundsätzliches zur Kooperation

Durch die gesetzliche Einführungs- und Zertifizierungspflicht des ISMS sowie die relativ kurzen Umsetzungsfristen sehen sich besonders kleinere und mittlere Stadtwerke einem erheblichen zeitlichen und finanziellen Druck ausgesetzt. Zugleich haben heute die meisten Versorgungsunternehmen bereits Sicherheitsregeln zur Verfügbarkeit, Integrität und Vertraulichkeit implementiert. Auch wenn diese nicht immer nach dem IT-Sicherheitskatalog bzw. der DIN ISO/IEC 27001 ausgerichtet sind, stehen die Unternehmen so bei diesen Prozessen nicht ganz am Anfang (siehe dazu auch Kapitel 4). Dementsprechend wird bei ähnlich organisierten Netzbetreibern vermehrt die Frage nach der Möglichkeit des Aufbaus eines ISMS und seiner Zertifizierung im Verbund gestellt, um so Synergien realisieren zu können.

Probates und durchaus erfolgreiches Mittel zur Kostensenkung, Effektivitätssteigerung und Prozessoptimierung sind in der Energiebranche bereits seit einigen Jahren Kooperationen. Gerade Stadtwerke in regionaler Nähe sowie Netzbetreiber mit Konzernstrukturen haben auf diesem Gebiet bereits Erfahrungen sammeln können.

Man sollte sich hinsichtlich einer angestrebten Kooperation jedoch bewusst sein, dass ein ISMS-Projekt zum überwiegenden Teil individuelle organisatorische und prozessuale Komponenten beinhaltet, die gegebenenfalls auch durch individuelle Maßnahmen flankiert werden müssen. Dort aber, wo sich IT-Infrastruktur, Aufbau- und Ablauforganisation mehrerer Netzbetreiber harmonisieren lassen oder diese es bereits sind, ist ein gemeinsamer Weg zur Implementierung eines ISMS möglich und es lassen sich durchaus Synergien realisieren.

Die Wegstrecke zur Umsetzung eines ISMS wird durch eine Kooperation aber nicht unbedingt einfacher. Neben den »harten« (Verträge, Kosten) sind auch die »weichen« Faktoren einer solchen Zweckgemeinschaft nicht zu vernachlässigen. Die kooperierenden Werke müssen in ihrer Mentalität, Arbeitsweise, ihren Management- und Projektfähigkeiten sowie ihrem Engagement zusammenpassen und funktionieren. Etwaige Dissonanzen können das Projekt leicht konterkarieren und schnell dazu führen, dass sich beabsichtigte Synergien eher in einen Antagonismus umwandeln. Letztlich muss jedes Unternehmen die Prozesse zur Erstellung des ISMS selbst durchlaufen. Es ist nicht vorgesehen, dass faktisch ein Unternehmen als Lokomotive die anderen mitzieht.

Eine finale Zertifizierung im Verbund ist darüber hinaus nach Beschluss der DakkS (Deutsche Akkreditierungsstelle) vom 20.01.2015 nur noch sehr eingeschränkt möglich. Nachfolgend werden einzelne Möglichkeiten der Kooperation aufgezeigt.

5.2 Kooperationsfelder

Im Rahmen der rechtlichen Anforderungen an die Unternehmen ist es sinnvoll, Synergien zu erschließen und Verfahren und Vorgehensweisen zu erarbeiten, die eine Vergleichbarkeit und Austauschbarkeit der Ergebnisse fördert. Sie können helfen, die Kosten der Konformität mit den gesetzlichen Anforderungen und der Zertifizierung zu reduzieren und Redundanzen in den Aufwänden zu vermeiden. Im Wesentlichen gibt es drei Kooperationsfelder, in denen solche Modelle Anwendung finden können: Ressourcen, Prozesse und Information.

Ressourcen

Beim Aufbau der notwendigen Rollen und Strukturen können die Unternehmen auf verschiedene Weise miteinander kooperieren. Vielfach können Dienstleistungen entweder selbst erbracht, von Externen eingekauft oder im kooperativen Betrieb mit anderen genutzt werden. Kooperationsmöglichkeiten ergeben sich beispielsweise bei folgenden Rollen:

- **Ansprechpartner IT-Sicherheit/ISMS Beauftragter/IT-Sicherheitsbeauftragter (ISB):** Die Einführung der Rolle des Ansprechpartners für IT-Sicherheit wird durch den IT-Sicherheitskatalog vorgegeben (siehe Kapitel 2.4 und Seite 14 ff. im IT-Sicherheitskatalog). Hier ist eine Kooperation nur möglich, wenn die Unternehmen und die betroffenen Mitarbeiter in sehr engem Austausch sind, da sonst die Anforderungen an den Ansprechpartner nicht eingehalten werden können (siehe Kapitel 3.2.1). Wird daneben jedoch zusätzlich auf einen externen IT-Sicherheitsbeauftragten zurückgegriffen, so können Netzbetreiber hierbei kooperieren.

- **Sicherheitsorganisation:** Alle Aspekte eines sicheren und überwachten IT-Betriebes wie zum Beispiel der Betrieb eines Cert (Computer Emergency Response Team) kann als Service eines IT-Sicherheitsdienstleisters eingekauft werden und muss nicht in jedem Unternehmen aufgebaut werden. Auch der Aufbau eines Security Operation Center (SOC), das den Betrieb kontinuierlich überwacht, kann als Service eingekauft werden.

- **Zentrale Meldestelle:** Der Betrieb einer gemeinsam getragenen Zentralen Meldestelle zu den Aufsichtsbehörden– BSI (Bundesamt für Sicherheit in der Informationstechnik) und BNetzA (Bundesnetzagentur) ist denkbar. So eine gemeinsame Stelle wird auch als »single point of contact« bezeichnet.

- **Zertifizierer und Auditoren:** Die Beauftragung von Zertifizierern und Auditoren kann gemeinsam von Unternehmen der Branche in Angriff genommen werden um so die branchenspezifische Ausprägung sicher zu stellen. Dies umfasst zum einen die Auditierung durch einen externen Auditor, als auch die zukünftigen internen Pre- Audits und Kontrollmaßnahmen (siehe dazu auch 5.3.2).

Prozesse

Ähneln sich Unternehmen bei ihren Prozessen, dann können sie durch verteilte Arbeiten und durch punktuelle Kooperation zu schnelleren und vergleichbaren Ergebnissen gelangen. Praktisch kann die Beschreibung der notwendigen Prozesse durch die gemeinsame Entwicklung von Vorgehensweisen (Templates) beschleunigt und gefördert werden. Die Etablierung von Management Support in der Einführungsphase und darüber hinaus für die zu beschreibenden Rollen und Prozesse wird erleichtert. Langfristig kann der Aufbau eines brancheninternen Zertifizierungsnetzwerkes und Durchführung von Cross Audits durch geschulte Mitarbeiter (Auditoren bei den Netzbetreibern) in der Phase der zyklischen Überprüfung und Wiederholung der Audits implementiert werden.

Information

Durch den Austausch von Informationen kann die Wirksamkeit der Maßnahmen eines ISMS erhöht werden und häufig eine schnellere Reaktion auf Störfälle erfolgen. Die Bereitstellung von Best Practices und Erfahrungen kann einen »Knowledge Pool« generieren, der so durch einzelne Unternehmen nicht oder nur weniger umfassend aufgebaut und gepflegt werden könnte. Wenn die Daten entsprechend anonymisiert werden, können selbst Informationen und Erfahrungen bereitgestellt werden, die Unternehmen normalerweise nicht direkt ihren Marktbegleitern offenbaren würden. Die Erstellung eines gemeinsamen Lagebildes zur Informationssicherheit ermöglicht eine bessere Gefährdungsbewertung und Erstellung von Risikoanalysen, die nicht unternehmens-, sondern branchenspezifisch sind.

Aus den skizzierten Kooperationsfeldern lassen sich aus dem IT-Sicherheitskatalog sowie der ISO 2700x-Familie mit ihren entsprechenden Regelwerken und Akkreditierungsanforderungen als Kooperationsschwerpunkte die folgenden Punkte ableiten:

- ISMS-Aufbau
  Ein ISMS-Projekt kann aufgrund seines modularen Aufbaus kooperativ angegangen werden. Da viele Vorgehensweisen bei der Implementierung eines ISMS generisch sind und sich die IT-Infrastruktur, die Aufbau- und Ablauforganisation vieler Stadtwerke ähneln, ist ein gemeinsamer Weg zur Implementierung eines ISMS möglich und es lassen sich bei erfolgreichen Projekten deutliche Synergien realisieren.

- Kontakt-/Meldestelle
  Unternehmen mit der Branche Wasser/Abwasser haben, sofern sie von der KRITIS-Verordnung erfasst werden (siehe Kapitel 2), nach dem IT-Sicherheitsgesetz dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Kontaktstelle mitzuteilen. »Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind.« (IT-Sicherheitsgesetz, § 8b Abs. 3). Auch für Betreiber von Energienetzen kann die Einrichtung einer Kontaktstelle sinnvoll sein, da darüber auch Informationen über die Sicherheitslage vom BSI an die Unternehmen fließen. Das IT-Sicherheitsgesetz sieht ausdrücklich eine gemeinsame Kontaktstelle gegenüber dem BSI vor,

wenn die Betreiber kritischer Infrastrukturen dem gleichen Sektor angehören (so genannter single point of contact - SPOC).

- Gruppenzertifizierung
  Eine sogenannte Matrix- oder Gruppenzertifizierung nach ISO 27001 kann nach Beschluss der DakkS vom 20.01.2015 (Beschluss-Nr: 01/2015) nur noch unter bestimmten Voraussetzungen für gesellschaftsrechtlich miteinander verbundene Unternehmen stattfinden. Bei dieser Konstellation werden Verbünde als Organisationen mit einem einheitlichen Managementsystem und verschiedenen Standorten und/oder verschiedenen rechtlich eigenständigen Unternehmenseinheiten definiert. Hierbei werden die Verbundwerke stichprobenartig auditiert. Bei erfolgreichem Bestehen wird ein sogenanntes Verbundzertifikat erteilt, siehe dazu auch Kapitel 5.3.1.

- Überwachungsaudits
  Die Sicherheitsmaßnahmen müssen regelmäßig auf ihre Erfüllung überprüft werden. Das ISMS setzt wiederkehrende interne und externe Audits voraus. Durch den langfristigen Aufbau eines Zertifizierungsnetzwerkes und der Durchführung von Cross Audits durch geschulte Mitarbeiter können personelle und finanzielle Ressourcen eingespart und die Sicherheit in den teilnehmenden Unternehmen erhöht werden.

- Voraudit
  Es besteht grundsätzlich immer die Möglichkeit, vor einer ISO27001-Auditierung, ein Voraudit durchführen zu lassen. Gegenstand eines Voraudits können zum Beispiel die prinzipielle Überprüfung der Zertifizierungsreife oder die Einübung der Mitarbeiter im ISMS des Netzbetreibers auf eine reale Auditsituation sein. Ob die Option eines Voraudits sinnvoll ist und welche Inhalte empfehlenswert sind, ergibt sich erst im Verlauf einer Projektierung der Einführung eines ISMS. Der Aufwand eines Voraudits kann bis zu einem Drittel einer ISO27001-Auditierung betragen. Wenn solche Voraudits wechselseitig von kooperierenden Unternehmen durchgeführt werden, die bereits zertifiziert sind, können Kosten gespart werden.

Mögliche Kooperationsmodelle werden im Folgenden erläutert.

5.3 Kooperationsmodelle

Nachfolgend werden einige Kooperationsmöglichkeiten und –modelle dargestellt, die für die Planung und Einführung eines ISMS und die Schaffung der Zertifizierungsfähigkeit eines Netzbetreibers betrachtet werden sollten und die sich zum Teil bereits in der Praxis als umsetzbar herauskristallisiert haben.

5.3.1 Verbund- und Matrixzertifizierungen

Verbund- und Matrixzertifizierungen sind in der industriellen Praxis nicht ungewöhnlich, so zum Beispiel im Geltungsbereich der ISO 9001 (Qualitätssicherung), der ISO 14001 (Umweltmanagement) und der OHSAS 18001 (Arbeitsschutz).

Für eine Matrixzertifizierung schließen sich mehrere Unternehmen mit der gleichen Unternehmensausrichtung zusammen. Die beteiligten Unternehmen richten sich beispielsweise für eine ISO 9001-Zertifizierung an einem einheitlichen Qualitätsmanagement-System aus. Der Aufbau und die Ablauforganisation aller beteiligten Unternehmen orientieren sich an gemeinsamen Qualitätszielen und einer einheitlichen Qualitätspolitik, die in einer Qualitätsmanagement-Dokumentation unternehmens- und standortübergreifend beschrieben wird. Sofern lokale Verfahrens- und Arbeitsanweisungen notwendig sind, werden diese dabei dem zentralen Qualitätsmanagement-System untergeordnet. Zur Auditierung des Qualitätsmanagement-Systems ist es nicht erforderlich, alle beteiligen Standorte oder Unternehmen zu prüfen, In einem Stichprobenverfahren werden nur einzelne Unternehmen oder Standorte geprüft. Zusätzlich werden Auditberichte, Korrekturmaßnahmen und Eigenbewertung des Qualitätsmanagement-Systems durch die beteiligten Verbundmitglieder zur Prüfung zur Verfügung gestellt. Jedes Unternehmen erhält ein eigenes Zertifikat, auch wenn das Unternehmen nicht direkt Prüfungsobjekt im Zertifizierungsaudit war. Auch anschließende Überwachungs-Audits können so in verbundenen Unternehmen angewendet werden. Die Aufwands- und Kostenvorteile sind offensichtlich, allerdings muss das Verfahren in dieser Form seitens der Trägergemeinschaft für Akkreditierungen (DakkS, Deutsche Akkredierungsstelle) nach der jeweiligen Norm vorgesehen und freigegeben sein.

Die DakkS hat mit Beschluss vom 20.01.2015 klargestellt, dass

> *»ein Verbund mehrerer einzelner voneinander unabhängiger und eigenverantwortlich agierender Organisationen, die sich einer externen Organisation bedienen, um ein Managementsystem zu entwickeln, einzuführen und aufrechtzuerhalten, […] keine ›Organisation mit mehreren Standorten‹ im Sinne von IAF MD1:2007 darstellt und […] deshalb auch nicht gemäß Stichprobenverfahren auditiert, zertifiziert und überwacht werden kann […] Es handelt sich (hier) vielmehr um einen Verbund mehrerer selbstständiger Organisationen, die jeweils einzeln zertifiziert und entsprechend (jährlich) überwacht werden müssen.«*

Das bedeutet, dass der letzte und entscheidende Schritt der Zertifizierung nicht gemeinsam gegangen werden kann.

Darüber hinaus liegen im Geltungsbereich der ISO 2700x-Familie bislang wenig Erfahrungen mit dieser Art der Zertifizierung vor und als Regeloption ist es, anders als bei der Qualitätssicherung, nicht etabliert und wird von den meisten Auditoren abgelehnt.

Für Querverbundsunternehmen bietet sich die Matrixzertifizierung an, wenn verschiedene Sparten mit unterschiedlichen Anforderungen und Scopes zertifiziert werden sollen (siehe dazu auch Kapitel 2).

5.3.2 Zertifizierungsnetzwerke und CrossAudits

Aus dem Umfeld der Behörden, die dem Umsetzungsplan Bund für die Einführung des BSI Grundschutz folgen, ist die Bildung von Zertifizierungsnetzwerken bekannt. Das wesentliche Prinzip dabei ist die interne Ausbildung von Auditoren und die Bildung von Zertifizierungsgruppen, in denen sich mehrere Einrichtungen zusammenschließen und sich wechselseitig auditieren. Voraussetzung dafür ist hinreichendes geschultes Personal, das diese Tätigkeit übernehmen kann und gleichzeitig intern die Einführung und die Zertifizierungsvorbereitung für die eigene Organisation übernehmen kann. Der Aufbau eines Zertifizierungsnetzwerkes wird durch die Möglichkeit der Durchführung von Überprüfungsaudits und internen Assessments im Rahmen des PDCA-Zyklus (Plan, Do, Check, Act) deutlich attraktiver, da in der Phase nach der Einführung wesentlich geringere externe Aufwände entstehen und das branchenspezifische Know-how mit einfließen kann. Auf der andere Seite stehen hier hohe Personalaufwände in den Mitgliedsunternehmen, die in kleineren und mittleren Netzbetreibern in der Regel nicht kontinuierlich zu tragen sind, sodass ein externer Zertifizierungspartner hinzugezogen werden muss. Grundsätzlich muss der Auditor unabhängig sein und darf nicht gleichzeitig die Zertifizierungsvoraussetzungen im Unternehmen schaffen. Er darf also nicht das durch ihn selbst konzipierte ISMS auditieren. In bestehenden Verbünden und Arbeitsgemeinschaften der Netzbetreiber sollte der Aufbau eines Zertifizierungsnetzwerks thematisiert und als Option betrachtet werden. Im Falle einer Entscheidung zur Errichtung eines Netzwerks sollte dies bereits in der Konzeptionsphase durch einen Dienstleister begleitet werden, der sowohl mit den Anforderungen des Aufbaus eines ISMS und im Besonderen die Anforderungen aus dem IT Sicherheitskatalog vertraut ist. Weiterhin sollte dieser als Auditor eine Zertifizierung vorbereiten können und entsprechende Erfahrung darin mitbringen.

5.3.3 Die »echte Kooperation«

Von einer »echten Kooperation« wird gesprochen, wenn sich mehrere Netzbetreiber gesellschaftsrechtlich miteinander »verbinden« wollen (oder dies bereits getan haben). Dies kann beispielsweise die Gründung einer gemeinsamen Betreiber-, Netz- oder Rechenzentrumsgesellschaft sein.

Die nachfolgende Grafik zeigt folgendes Modell: Mehrere Netzbetreiber – alle in regionaler Nähe befindlich – beabsichtigen eine neue gemeinsame Rechenzentrumsgesellschaft (zum Beispiel in Form einer GmbH) zu gründen. Aus politischen und ökonomischen Erwägungen soll dort auch die gemeinsame Netzleitstelle implementiert werden, welche nach erfolgreichem Aufbau den Netzbetrieb für alle beteiligten Gesellschaften gewährleistet.

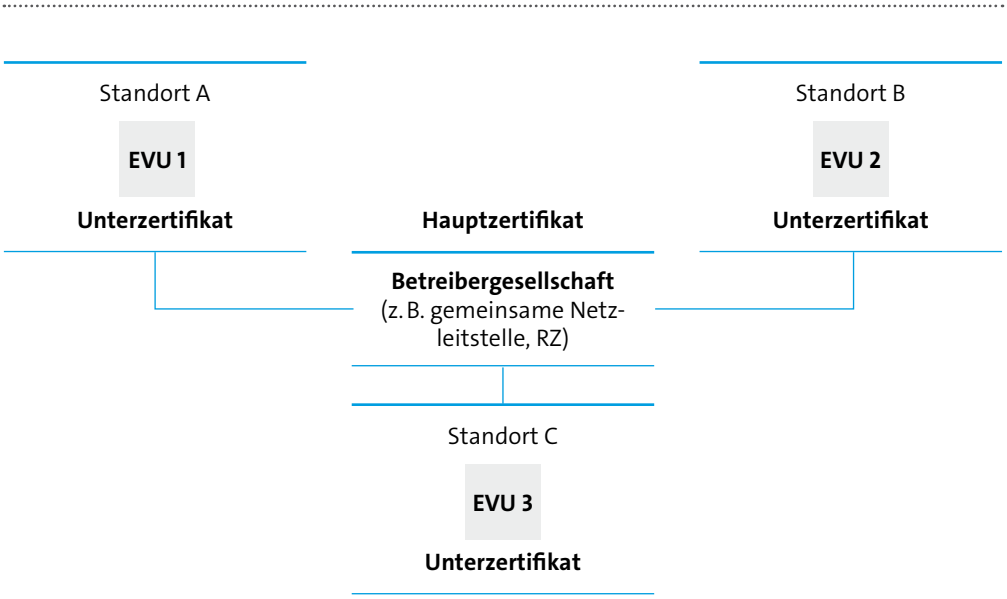


Abbildung 7: Zertifikat bei echter Kooperation

- Bei Gründung einer gemeinsamen Gesellschaft sind sämtliche Prozesse völlig neu zu gestalten; dementsprechend kann von Beginn an eine direkte Ausrichtung der Prozesse auf Grundlage der ISO 27001 erfolgen.

- Die Gesellschafterwerke müssen lediglich leichte Anpassungen hinsichtlich eines einheitlichen Managementsystems vornehmen und – abhängig vom Scoping des ISMS (siehe Kapitel 2) – gegebenenfalls kritische Schnittstellen betrachten.

- Im Hinblick auf die Zertifizierung bietet sich hier die einzige Möglichkeit einer sogenannten Gruppenzertifizierung, da es sich hier um eine Organisation mit einem »Netzwerk an lokalen Geschäfts- oder Zweigstellen« handelt. Die Betreibergesellschaft wird hier zum (Haupt-)Zertifikatsnehmer, die Gesellschafterwerke werden als einzelne Standorte betrachtet. Das Zertifizierungsaudit erfolgt bei der Betreibergesellschaft, die Standorte werden nur stichprobenartig auditiert. Die Betreibergesellschaft erhält nach erfolgreicher Zertifizierung das Hauptzertifikat, die Gesellschafterwerke Unterzertifikate, die der gesetzlichen Anforderung vollumfänglich genügen.

Dadurch entstehen einerseits deutlich geringere Ressourcenaufwände beim ISMS-Aufbau und dem IT-Sicherheitsbeauftragten andererseits erheblich weniger Kosten bei der Zertifizierung sowie für die nachgelagerten Überwachungsaudits. Sämtliche Kosten können gleichmäßig (oder nach Gesellschaftsanteilen gestaffelt) auf alle beteiligten Werke umgelegt werden.

Nachteile

- Der gesetzliche geforderte ISMS-Aufbau und die Zertifizierung werden nicht ausschlaggebend für die gemeinsame Gründung einer Gesellschaft sein; vielmehr ist eine weitreichende gesellschaftsrechtliche Verbindung wohl eher vorgelagerten wirtschaftlichen und politischen Erwägungen geschuldet.

- Die Entschlussfassung zur Gründung einer gemeinsamen Gesellschaft ist häufig ein langwieriger Prozess, der u. a. auch mit gegenteiligen politischen Interessen behaftet sein kann (bspw. Zusammenführung von Assets). Dadurch kann es zu deutlichen Zeitverzögerungen kommen – auch hinsichtlich der geforderten Umsetzungsfristen aus dem IT-Sicherheitskatalog.

- Es ist fraglich, ob die aus diesem Kooperationsmodell zu realisierenden Synergien nicht durch die Kosten für die Gründung der gemeinsamen Gesellschaft aufgezehrt werden.

Exkurs – Gruppenzertifizierung für echte Kooperation

Wie bereits zuvor erwähnt, besteht im Falle einer echten Kooperation die einzige Möglichkeit einer Matrix- bzw. Gruppenzertifizierung des ISMS nach ISO 27001 – wenn das ISMS als einheitliches Managementsystem betrieben werden soll.

Die Zertifizierung des ISMS erfolgt entsprechend der für den ISO 27000-Standard veröffentlichten Regelwerke und Akkreditierungsanforderungen IAF MD1:2007 (abrufbar unter www.dakks.de). Darin enthalten sind spezifische Vorgaben für die Zertifizierung von Einzelunternehmen und die Zertifizierung an mehreren Standorten nach einem Stichprobenverfahren, sowie Vorgaben für zu erbringende Zeitaufwände, die Stichprobengröße, das Auswahlverfahren und vieles mehr.

Für eine Gruppenzertifizierung müssen die Verbundwerke zwingend nachfolgend (auszugsweise) skizzierte Grundvoraussetzungen erfüllen:

- Bei der beabsichtigten Zertifizierung der kooperierenden Netzbetreiber muss ein Netzbetreiber gegenüber der ausgewählten Zertifizierungsgesellschaft als alleiniger Vertragspartner auftreten und wird damit für das zu zertifizierende ISMS gesamtverantwortlicher Zertifikatsnehmer.

- Alle kooperierenden Netzbetreiber müssen ihre Tätigkeiten in ähnlicher Weise (zum Beispiel vergleichbare Technologien, gleiche Produkte) durchführen.

- In allen Fragen des ISMS haben die kooperierenden Netzbetreiber die Führungsrolle des Zertifikatsnehmers anzuerkennen und sind Bestandteil einer zentralen (jährlichen) Managementbewertung.

- Es muss ein zentraler ISMS-Beauftragter der obersten Leitung für alle beteiligten Netzbetreiber benannt werden.

- Es muss ein gemeinsames ISMS und eine gemeinsame Dokumentation für die ganze Gruppe vorliegen. Die Dokumentation darf nur durch den Zertifikatsnehmer geändert werden.

- Es ist zulässig, lokale Unterschiede durch Variationen allgemein definierter Verfahren des ISMS zu berücksichtigen oder diese zum Beispiel zu ergänzen. Derartige Änderungen an der ISMS-Dokumentation müssen aber mit dem Zertifikatsnehmer abgestimmt sein und dürfen nur lokale Prozesse betreffen.

- Die beteiligten Netzbetreiber müssen gegenüber dem Zertifikatsnehmer eine schriftliche Verpflichtungserklärung zu zuvor genannten Statuten abgeben. Diese Erklärung muss spätestens zur Zertifizierung durch die jeweilige Zertifizierungsgesellschaft eingesehen werden können.

- Das ISMS muss vor Zertifizierungsbeginn bei allen beteiligten Netzbetreibern implementiert sein.

- Das ISMS muss bei allen beteiligten Netzbetreibern intern auditiert sein, die Planung der internen Audits und die Auswertung der Ergebnisse erfolgt zentral durch den Zertifikatsnehmer

- Korrekturmaßnahmen müssen vom Zertifikatsnehmer veranlasst und deren Durchführung von ihm überwacht werden.

Vorteile

Vorteil ist, dass nicht alle kooperierenden Netzbetreiber bei einem Zertifizierungsaudit begutachtet werden müssen, sondern dies nur stichprobenartig erfolgt (Zertifizierungsaufwand je Netzbetreiber liegt erfahrungsgemäß bei ca. 20–30 Prozent). Jeder kooperierende Netzbetreiber bekommt ein eigenes Zertifikat, auch wenn es nicht im Zertifizierungsaudit geprüft wurde. Die Kosten der Zertifizierung fallen dementsprechend geringer aus und können über alle kooperierenden Netzbetreiber gleichmäßig verteilt werden.

Nachteile

Risikoentscheidungen müssen innerhalb eines jeden Netzbetreiber getroffen werden, Eskalationsprozesse enden somit bei der jeweiligen Netzbetreiber-Leitungsebene. Außerdem müssen die beteiligten Netzbetreiber eine gemeinsame IT-Sicherheitsorganisation (Rollen, Berichtswege, Reporting) haben. Weiterhin können unternehmensübergreifende Risikoentscheidungen nur durch eine übergreifende zentrale Leitung getroffen werden. Der Eskalationsprozess ist ebenfalls übergreifend über eine gemeinsame zentrale Leitung organisiert. Das einzelne Unternehmen ist damit in seiner Handlungsfähigkeit eingeschränkt und auf die anderen Unternehmen im Verbund angewiesen.

Im Geltungsbereich der ISO 27000er Reihe liegen bislang wenige Erfahrungen mit dieser Art der Zertifizierung vor und die Grundvoraussetzungen für eine Gruppenzertifizierung sind wie beschrieben hoch. Bei einer Entscheidung für ein derartiges Vorgehen sollten sich die kooperie-

renden Netzbetreiber immer die Sinnhaftigkeit und Machbarkeit in Bezug auf die Zertifizierung vor Augen halten. Möglicherweise avisierte Kostenersparnisse können durch anhaltende Unstimmigkeiten und das Nichteinhalten der Voraussetzungen für eine Gruppenzertifizierung die ISMS-Einführung scheitern lassen.

Bei einer Gruppenzertifizierung gilt zudem die Regel des gemeinsamen Bestehens der Zertifizierung. Sofern nur ein beteiligter Netzbetreiber eine Schlechtleistung erbracht hat und bei der Zertifizierung durchfällt, gilt die gesamte Zertifizierung des ISMS für die Kooperation als nicht bestanden und es muss diese (mit erhöhten Kosten und deutlichem Zeitverzug) wiederholt werden.

5.3.4 Die »unechte Kooperation«

Zur Hebung von Synergien ist die Bildung einer echten Kooperation nicht zwingend notwendig. Ausreichend ist hierfür auch eine so genannte »unechte Kooperation« (ohne gesellschaftsrechtliche Verbindung), bei der sich Energienetzbetreiber zum Zweck des Aufbaus und gegebenenfalls der Zertifizierung eines ISMS zusammenfinden. Eine unechte Kooperation kann dabei – je nach individueller Zielsetzung – in zwei Varianten vollzogen werden.

Variante 1 – Gemeinsame und individuelle Vorgehensweise

Ein ISMS-Projekt besteht aus mehreren Komponenten. Dabei gibt es zwei Basis-Komponenten, welche die Grundlagen für ein ISMS bilden: 1. Die IT-Sicherheitsstrategie (Leitlinien, Richtlinien, Scope), sowie 2. der Aufbau einer IT-Sicherheitsorganisation und der seitens der ISO 27001 geforderten Implementierung eines nachhaltigen Sensibilisierungssystems für die Unternehmensführung und die Mitarbeiter (sog. Security Awareness). Die Basis-Komponenten sind generisch und können für alle beteiligten Unternehmen im Verbund gleich gestaltet werden.

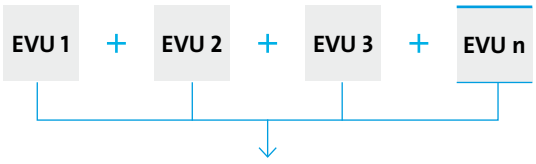
Mittels gemeinsamer Workshops erarbeiten die Projektbeteiligten der einzelnen Netzbetreiber die notwendigen Inhalte und Anforderungen aus den gesetzlichen Vorgaben und der ISO 27001. Der Austausch der einzelnen Projektbeteiligten zu etwaigen bereits vorhandenen Dokumenten in den Verbundwerken (wie zum Beispiel Leit- oder Richtlinien) und die Vorgabe von standardkonformen und zertifizierungserprobten Templates können Ressourcen sparen.

Das Rad muss bei der ISMS-Basis nicht immer mühevoll neu erfunden werden. Wenn beispielsweise ein Verbundwerk bereits eine gut ausformulierte Richtlinie zum Mobile Device Management besitzt, kann diese durchaus von den übrigen Verbundwerken übernommen werden. Das Motto »copy and paste« ist hier also durchaus erwünscht.

Es ist ratsam, die Workshops von externen Fachexperten, die sich mit den Anforderungen und Strukturen der ISO 27001 sowie dem Ablauf eines Zertifizierungsaudits und den Ansprüchen der Auditoren auskennen, vorbereiten, moderieren und begleiten zu lassen. Sonst kann sich die Situation ergeben, dass sich Energienetzbetreiber mit der in Eigenregie erstellten IT-Sicherheits-

dokumentation auf der sicheren Seite wähnen, diese einer ISO 27001-konformen Überprüfung allerdings nicht standhalten.

Je nach Zielsetzung des Verbunds können die beteiligten Netzbetreiber die weiteren Projekt-Phasen entweder alleine oder aber auch gemeinsam verfolgen. Es darf bei dieser Entscheidung jedenfalls nicht unterschätzt werden, dass jeder Netzbetreiber individuelle organisatorische und prozessuale Bestandteile hat, die gegebenenfalls durch individuelle Maßnahmen flankiert werden müssen.



Im Verbund mittels gemeinsamer Workshops

Phase 1 – ISMS-Basis

Komponente 1
Kick-off

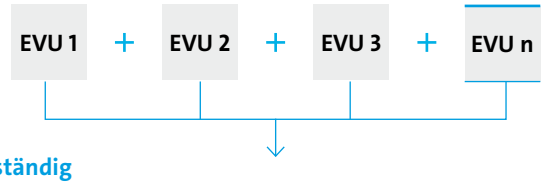
Bestandteile

- Vermittlung von Grundlagen und Anforderungen aus dem IT-Sicherheitsgesetz und IT-Sicherheitskatalog
- Vorstellung der Umsetzungsvorgaben und Controls aus ISO/IEC 27001, 27002, 270019
- Anforderungsvermittlung an eine erfolgreiche Zertifizierung
- Vorgehensweise zur Implementierung des ISMS
- Definition des Scopes
- Analyse von Harmonisierungsmöglichkeiten und Synergie mit bestehenden Prozessen
- Ziel- und Meileinsteindefinition
- Formulierung von Arbeitspaketen
- Aufbau und Koordination der Projektplanung

Komponente 2
ISMS-Strategie & Organsiation

Bestandteile

- Ausrichtung der IS-Strategie an gesetzlichen Vorgaben, Geschäftsprozessen und ISO/IEC 27001
- Implementierung von ISMS-Rollen
- Implementierung eines revisionssicheren Dokumentationssystems mit Struktur und Vorlagen aus ISO/IEC 27001, 27002
- Aufbau und Durchführung eines nachhaltigen Sensibilisierungssystems für Führungskräfte und Mitarbeiter mit stetig aktualsierten Inhalten aus der IT-Sicherheit
- Aufbau und Einführung von qualitätssichernden Maßnahmen und Prozessen zur Revision von IS-Ereignissen und Dokumentation



Jedes Werk eigenständig

Phase 2 – ISMS-Individuell

Komponente 3
IT-Sicherheitscheck

Bestandteile

- IST-Analyse
- Erstellung Netzstrukturplan
- Schutzbedarfsfeststellung und Risikobetrachtung
- Soll-Aufstellung gem. ISO/IEC 27002, 27019
- Gap-Analyse
- Zustandsbericht
- Handlungsempfehlungen

Komponente 4
ISMS-Einführung

Bestandteile

- Erstellung ISMS-Gesamtkonzept gem. Anforderungen des IT-Sicherheits-Checks
- Erstellung von Einzel-/Teilkonzepten gem. zutreffender Controls aus ISO/IEC 27002
- Validierung und Dokumentation des Gesamtkonzepts
- Übergabe von Umsetzungsvorgaben an Fachabteilungen

Phase 3 – Zertifizierung

Komponente 5
Audit & Zertifizierung

Bestandteile

- Durchführung Zertifizierungsaudit
- Zertifikatsverleihung
- Durchführung Überwachungsaudits in den nächsten zwei Folgejahren
- Übergabe von Beanstandungen in den KVP des ISMS

Phase 4 – Nachhaltigkeit

Komponente 6
Nachhaltigkeit

Bestandteile

- Überprüfung des ISMS-Umsetzungsstatus
- Durchführung Voraudits
- Abstimmung von Folgeaufgaben mit dem ISB

Abbildung 8: Unechte Kooperation – Variante 1

Die dargestellte Variante 1 beinhaltet hier die Entscheidung für einen individuellen Projektfortgang für jedes einzelne Netzbetreiber sowie eine eigenständige Zertifizierung des ISMS, da eine Gruppenzertifizierung nach Beschluss der DAkkS hier nicht mehr möglich ist (vgl. nachfolgende Grafik).

Vorteile

- Synergien lassen sich durch die gemeinsame Nutzung bereits vorhandener Richtlinien, Dokumente und Organisationsstrukturen realisieren.
- Ressourceneinsparungen im Hinblick auf Zeit, Personal und Kosten sind durch gemeinsames Erarbeiten der ISMS-Basis möglich.
- Die Anleitung durch versierte und praxiserfahrene externe Fachexperten garantiert ein zielführendes Vorgehen.
- Die Kostenverteilung erfolgt für die gemeinsamen Workshops gleichmäßig über alle beteiligten Netzbetreiber.
- Das ISMS-Kernprojekt, seine spezifische Umsetzung sowie die Verantwortung für die Zertifizierung bleiben bei dieser Variante bei den einzelnen Netzbetreibern.
- Das Thema IT-Sicherheit ist bei den Mitarbeitern nach einer solchen Umsetzung stärker verinnerlicht, als wenn die Umsetzung extern geleitet wird.

Nachteil

Es besteht die Gefahr, dass durch ein unterschiedliches Engagement der Teilnehmer die Erarbeitung der ISMS-Basis-Struktur nur auf Wenige verteilt wird. Dies kann zu einer Erhöhung der Arbeitsbelastung bei einzelnen Werken und demnach dort zu einer deutlich erhöhten Ressourcenbelastung führen.

Variante 2 – Coaching-Workshops

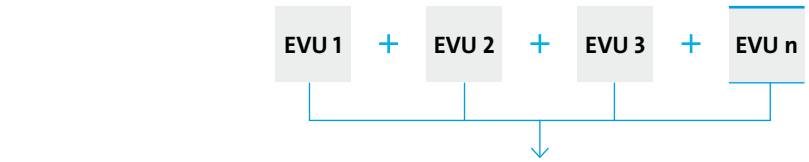
Entscheidet man sich dafür – anders als in Variante 1 – sämtliche Phasen des ISMS-Projekts vollständig im Verbund anzugehen und möchte man die Projektinhalte mit einem Minimum an externer Unterstützung erarbeiten, um weitere Kosten zu sparen, bietet sich die zweite Variante mit Coaching-Workshops an.

Bestandteil der jeweiligen Coaching-Workshops ist die Vermittlung von Basis- und Expertenwissen, Projekterfahrungen sowie die Anleitung zur korrekten Konzeption, Planung und Gestaltung von ISMS-Komponenten durch externe Fachexperten. Die Anleitung zur Umsetzung der beschriebenen Punkte erfolgt hierbei stets anhand von Praxisbeispielen und Norm- und Standardgerechten Vorlagen.

Grundsätzlich sind alle Coaching-Workshops in der Art aufgebaut, dass sie durch Fragenkataloge vorbereitet und mit klaren Arbeitspaketen nachbereitet werden. Dabei können die Workshopteilnehmer außerhalb der Workshops auf Nachfrage von einem ISMS-Coach, einem ISMS-Implementierer und/oder einem ISMS-Auditor begleitet werden. Fachliche und inhaltliche Fragen können so jederzeit an die externen Fachexperten gestellt werden.

Aufgrund des beabsichtigten Einsparfaktors sollte man sich jedoch vergegenwärtigen, dass dieses Vorgehen nicht die Erstellung oder Formulierung von Richtlinien, Konzepten und umfassenden Handlungsempfehlungen durch die externen Fachexperten beinhalten kann. Diese Form des Coachings ist daher in hohem Maße vom Mitwirken der Workshopteilnehmer abhängig und setzt die gewissenhafte Vor- und Nachbereitung seitens der Workshopteilnehmer voraus.

Um eine zügige Bearbeitung der Inhalte der Coaching-Workshops und eine fundierte Inhaltsvermittlung sicherzustellen, sollte die Teilnehmerzahl der in der nachfolgenden Grafik plakativ dargestellten Workshops die Marke von etwa 10 Personen nicht übersteigen.



Im Verbund mittels gemeinsamer Coaching-Workshops

	Komponente 1 Kick-off	Komponente 2 ISMS-Strategie & Organsiation
Phase 1	**Kick-off I**	**IS-Strategie**
	Kick-off II	**Schulung ISB**
		Organisation I
		Awareness Basis
		ISMS-Dokumentation
		Organisation II
		Organisation III
		Organisation IV
		Awareness Pro
	Komponente 3 IT-Sicherheitscheck	**Komponente 4** ISMS-Einführung
Phase 2	**IT-Security-Check**	**Gesamtkonzept**
		Einzelkonzepte I
		Einzelkonzepte I
	Komponente 5 Audit-& zertifizierung	**Komponente 6** Nachhaltigkeit
Phase 3 & 4	**Zertifizierungsvorbereitung**	**Gestaltung Nachhaltigkeit**

Abbildung 9: Unechte Kooperation – Variante 2

Vorteile

- Die Vorteile entsprechen zunächst denen der Variante 1.
- Durch ein vollständig arbeitsteiliges Vorgehen zum Aufbau und zur Implementation des ISMS sind Synergien realisierbar und Ressourceneinsparungen möglich.

Nachteile

- Auf individuelle Fragestellungen, Ausrichtungen und Konstellationen der einzelnen Netzbetreiber kann nur in einem sehr geringen Maße eingegangen werden. Es ist ein hohes Maß an Eigenarbeit gefordert.

- Der Erfolg des gesamten ISMS-Projekts ist vom Mitwirken der Workshopteilnehmer abhängig und setzt die gewissenhafte Vor- und Nachbereitung seitens der Workshopteilnehmer voraus. Auch hier besteht die Gefahr einer Erhöhung der Arbeitsbelastung bei einzelnen und einer erhöhten Ressourcenbelastung hinsichtlich Personal und Kosten.

5.3.5 Regionale Verbünde, Dienstleistungsbeziehungen

In der heutigen Strom- und Gasnetzbetreiberlandschaft sind Dienstleistungsbeziehungen häufig anzutreffen. Beispielsweise werden zentrale Bereiche der Netzführung von kleineren Stadtwerken an größere Unternehmen mit vorhandenem Leitsystem ausgelagert. Ein anderes Beispiel sind IT-Dienstleistungen (RZ-Betrieb, Applikationsbetrieb usw.), die häufig von spezialisierten IT-Unternehmen für viele Unternehmen mit Schwerpunkt Energiewirtschaft erbracht werden. Diese Konstellationen sind bei der Zertifizierung der Netzbetreiber entsprechend zu beachten. Es müssen im Rahmen des ISMS entsprechende Vorgaben an die Dienstleister formuliert und in Verträgen festgeschrieben werden.

Grundsätzlich ist es für das zu zertifizierende Unternehmen von Bedeutung, welche Anforderungen sich an den Dienstleister richten, ob und wie dieser die Anforderungen umsetzt und in welcher Form ein Nachweis und eine Kontrolle (Audit) erfolgen können. Dabei lassen sich folgende Szenarien unterscheiden:

Dienstleister ist nicht nach ISO/IEC 27001 zertifiziert

In diesem Fall muss der zu zertifizierende Netzbetreiber die sich nach Inventarisierung und Risikoanalyse ergebenden umzusetzenden Maßnahmen an den Dienstleister richten. Damit eine Inventarisierung und Risikoanalyse möglich ist, müssen alle erforderlichen Informationen vom Dienstleister zur Verfügung gestellt werden.

Die Umsetzung der Maßnahmen muss vom Dienstleister nachgewiesen und vom Dienstleistungsnehmer in internen und externen Audits kontrolliert werden. Insbesondere bei großen Dienstleistern kann die Bereitstellung der (teilweise vertraulichen) Informationen und die Vor-Ort-Kontrolle aufwändig sein.

Die erforderlichen Rechte des Dienstleistungsnehmers sollten möglichst bereits im Dienstleistungsvertrag entsprechend formuliert werden. Falls das nicht möglich ist, können einzelne Sicherheitsanforderungen (Maßnahmen) aufgestellt und deren Umsetzung vom Dienstleister ggfs. schriftlich versichert werden.

Der Dienstleister ist nach ISO/IEC 27001 zertifiziert

Ein bestehendes ISO27001-Zertifikat des Dienstleisters kann unter bestimmten Voraussetzungen die erforderlichen Tätigkeiten für das zu zertifizierende Unternehmen vereinfachen. Zielstellung ist dabei, die Prüfung des Dienstleisters bei der Auditierung des Dienstleistungsnehmers zu sparen, da bereits ein Audit durchgeführt und durch das Zertifikat bestätigt wurde.

Da eine ISO27001-Zertifizierung mit Spielräumen verbunden ist (beispielsweise kann der Dienstleister den Geltungsbereich selber definieren und Risiken nach eigenem Ermessen akzeptieren), ist ein Zertifikat alleine allerdings nicht ausreichend für die Zertifizierung des Dienstleistungsnehmers/Auftraggebers.

Der Dienstleistungsnehmer muss prüfen,

- ob der Geltungsbereich des Dienstleisterzertifikates den Geltungsbereich des Dienstleistungsnehmers abdeckt. Hierfür muss der Dienstleister die Geltungsbereichsbeschreibung bereitstellen.
- welche Sicherheitsmaßnahmen nicht umgesetzt worden sind sowie ob (Rest-) Risiken beim Dienstleister bestehen, die der Dienstleistungsnehmer ggfs. nicht bereit ist zu tragen.

Bei einem zertifizierten Dienstleister ist weiterhin zu beachten, dass dieser sein Zertifikat auch aberkannt bekommen kann oder dass mit der Zeit neue, nicht tragbare (Rest-) Risiken entstehen. In diesem Fall droht auch der Verlust der Zertifizierung beim Dienstleistungsnehmer. Daher sollten entsprechende Vorsichtsmaßnahmen getroffen werden um entweder den Dienstleister umgehend zu wechseln oder die Überprüfung des Dienstleisters wie im vorigen Abschnitt beschrieben durch das eigene Unternehmen durchführen zu können.

Den Dienstleistern kommt die Aufgabe zu, die jeweiligen Zertifizierungsanforderungen gegebenenfalls mehrerer Dienstleistungsnehmer unter einen Hut zu bringen. Konkurrierende Anforderungen und nicht harmonisierende technische Konzepte sollten idealerweise vermieden werden. Idealerweise sollten Energienetzbetreiber mit einem gemeinsamen Dienstleister ähnliche Sicherheits- und technische Konzepte entwickeln. Daraus ergibt sich die Empfehlung, dass die Kunden ein und desselben Dienstleisters für die Zertifizierung möglichst eine Kooperation bilden sollten. Dies bietet darüber hinaus auch entsprechende Synergiepotenziale bei Gefährdungs-, Maßnahmenlisten usw., die einmal entwickelt, in ähnlicher Form von mehreren Netzbetreibern verwendet werden können. Durch diese Art der Kooperation lassen sich konkurrierende Maßnahmen im Ansatz weitestgehend vermeiden und es bieten sich maximale Synergiepotenziale. Beispielsweise könnten sich alle Unternehmen der Kooperation auf einen gemeinsamen Auditor verständigen und Audits würden im Idealfall in wesentlichen Bereichen für die Zertifizierung mehrerer Netzbetreiber nur einmal durchgeführt.

5.4 Exkurs: Externer Informationssicherheitsbeauftragter/ Ansprechpartner IT-Sicherheit

In der Praxis ist in Unternehmen im Bereich der IT-Sicherheit vermehrt eine finanzielle, personelle und/oder zeitliche Ressourcenknappheit festzustellen. Häufig werden interne IT-Administratoren zusätzlich zu ihren eigentlichen Aufgaben zum IT-Sicherheitsbeauftragten berufen. Dies führt häufig zu einer Überlastung des Mitarbeiters sowie zu prozessualen Engpässen.

Unter Berücksichtigung von Effizienz und Effektivität kann es zweckmäßig sein – ähnlich wie bei einem externen Datenschutzbeauftragten – die Funktion des Informationssicherheitsbeauftragten nicht durch einen eigenen Mitarbeiter zu besetzen, sondern auf die Dienstleistung eines geeigneten und qualifizierten externen Informationssicherheitsbeauftragten zurückzugreifen.

Der BSI Standard 100-2 gibt sehr grob das Anforderungsprofil an einen Informationssicherheitsbeauftragten vor. Hiernach soll dieser detaillierte IT-Fachkenntnisse und Kenntnisse im Projektmanagement besitzen. Diese Fähigkeiten werden zur Bewältigung dieser Rolle jedoch nicht ausreichend sein. Die Vorteile eines externen Informationssicherheitsbeauftragten können sein:

- Es handelt sich um zertifizierte Experten, die aktuelles Fachwissen zur IT-Sicherheit in der Energie- und weiteren KRITIS-Branchen mitbringen
- Entlastung eigener Ressourcen bei kalkulierbaren Kosten
- Gewährleistung von Unabhängigkeit und Neutralität, sodass die Kontrollfunktion im Unternehmen optimal wahrgenommen werden kann (zum Beispiel objektive Beurteilung der Sicherheitslage)
- Nutzung von Synergien bei IT-Sicherheit und Datenschutz, da beiderseitiges Know-how vorhanden

Der Ansprechpartner für IT-Sicherheit gegenüber der BNetzA wie auch der IT-Sicherheitsbeauftragte können auch intern beauftragt werden. Der Ansprechpartner muss dabei zwingend im Unternehmen im aktuellen Tagesgeschäft der kritischen Bereiche des Unternehmens fest eingebunden sein (siehe Kapitel 3.2.1).

6 Praxisbeispiele zur Umsetzung

6 Praxisbeispiele zur Umsetzung

Thomas Gronenwald, Heiko Rudolph, Dominik Goergen, admeritia GmbH
Andreas Schmid, ROHDE & SCHWARZ SIT GmbH

Beispiele und Erfahrungen bei der technischen Umsetzung nach Einführung ISMS.

6.1 Operationalisierung

Mit Fertigstellung des Risikobehandlungsplans gilt es die notwendigen, technischen Maßnahmen umzusetzen. Dabei spricht man in der Regel von der Operationalisierung des ISMS. Ziel dabei ist es ein technisch wirksames ISMS zu erhalten. Der Risikobehandlungsplan beschreibt dabei die identifizierten Risiken und den Umgang damit. Er dient darüber hinaus als Instrument zur Steuerung der Umsetzungsreihenfolge der technischen Maßnahmen.

Die Operationalisierung eines ISMS im Kontext des IT-Sicherheitskatalogs und darüber hinaus in der Netz- und Prozessleittechnik, unterscheidet sich stark zu der Operationalisierung herkömmlicher, also klassischer ITK. Der maßgebliche Unterschied ist, dass die folgenden Rahmenbedingungen der Netz- und Prozessleittechnik schon ab einem relativ frühen Zeitpunkt für die Umsetzung berücksichtigt werden müssen:

- Lange Lebenszyklen der Leittechnik, ihrer Komponenten und stützenden ITK-Systeme von bis zu 20 Jahren
- Damit verbundene vertragliche Konstellationen mit den Anlagenerrichtern und –integratoren mitsamt Service Level Agreements, die einen Eingriff in die ITK-Verbünde und Anlagen der Netz- und Prozessleittechnik nicht immer einfach ermöglichen
- 24/7-Betrieb der Netz- und Prozessleittechnik in Verbindung mit relativ kurzen Revisionszeiten

Diese Rahmenbedingungen machen es erforderlich, die auf Basis des Risikobehandlungsplans umzusetzenden Maßnahmen früh zu planen und zu konzipieren. Dies ist alleine schon deshalb notwendig, um die jeweilige Betriebsorganisation zu berücksichtigen, da eine weitere gängige Rahmenbedingung ist, dass die Netz- und Prozessleittechnik in der Regel aufgrund des Automatisierungsgrades über wenige personelle Ressourcen verfügt. Durch den Rationalisierungsdruck der vergangenen Perioden ist der Personalbestand innerhalb der Netzleittechnik sukzessive reduziert worden. Für die zusätzlichen Anforderungen und Aufgaben, die im Rahmen eines ISMS nun aufkommen, sind deshalb häufig nicht ausreichend personelle Kapazitäten vorhanden.
Des Weiteren ist das in der Netzleitung tätige Personal meist nicht im Detail mit den Themengebieten Cyber Security und der klassischen ITK vertraut. Diese Problematik lässt sich teilweise durch die Übertagung von Aufgabengebieten auf die Büro- oder Corporate IT lösen. Mitunter lassen sich so auch Synergieeffekte erzeugen, da die Nutzung von bereits bestehender Infrastruktur und vorhanden Wissensbeständen ermöglicht wird.

Dabei darf die Autarkie der Netz- und Prozessleittechnik freilich nicht aus den Augen verloren werden. Dies muss umfassend in einem Betriebsregime durch Betriebsprozesse organisiert werden und in die Regelungsdokumente insbesondere hinsichtlich der Verantwortlichkeiten einfließen. Dabei sind insbesondere die verantwortlichen Rollen sowie gegebenenfalls die Anlagenerrichter und -integratoren für die Netz- und Prozessleittechnik aktiv einzubeziehen. Auf Grundlage der vorliegenden technischen Gegebenheiten ist es notwendig, die relevanten Regelungsdokumente, insbesondere Richtlinien und Verfahren sowie Anweisungen darauf abzustimmen. Somit beugt man der Gefahr vor, Regelungsdokumente zu erstellen, die später auf die faktischen technischen Gegebenheiten hin angepasst werden müssen und aufgrund dessen womöglich nicht implementiert werden können, wie es in der Praxis häufiger vorkommt.

Für ein gut operationalisiertes ISMS sind ferner die Sicherheits-, Änderungs- und Entwicklungsprozesse von herausragender Bedeutung. Hierbei ist vor allem auf eine ausreichende Prozessreife und Revisionssicherheit zu achten.

Es ist somit unabdingbar, für ein technisch wirksames ISMS, welches den Effekt haben soll, das technische Sicherheitsniveau faktisch zu erhöhen, die technische Umsetzung frühzeitig zu planen und iterativ in das ISMS einfließen zu lassen. Geschieht die Implementierung eines ISMS klassisch im Top-Down Ansatz, d. h. Ausgestaltung auf der Managementebene und Transport der Anforderungen als Vorgaben an die operativ tätigen Mitarbeiter, so ist es insbesondere im Bereich der Prozess- oder Netzleittechnik zwingend anzuraten, bei der ISMS-Ausgestaltung auf ein Gegenstromverfahren zu setzen. Dies bedeutet, dass nach Möglichkeit das operativ tätige Personal frühzeitig und umfassend bei der Gestaltung des ISMS als solches miteinbezogen werden sollte. Dieses Vorgehen hat den Vorteil, dass Probleme bei der operativen Umsetzung von Vorgaben bereits in der Planungs- und Entstehungsphase aufgedeckt und behoben werden können. Treten diese Probleme erst später zutage, so ist deren Beseitigung im Allgemeinen mit einem größeren Aufwand verbunden als dies bei dem hier dargestellten Gegenstromverfahren der Fall ist.

6.2 Sicherheitsmaßnahmen/zentrale Dienste

Um ein ISMS zu operationalisieren, sind geeignete Sicherheitsmaßnahmen zu betrachten und umzusetzen. Hierzu werden technische Sicherheitsmaßnahmen wie Beispielsweise Viren- und Patchmanagement-Lösungen zu so genannten »zentralen Diensten« zusammengefasst. Dazu werden diese Dienste in einem vertikalen und horizontalen Zonenmodell (siehe Kapitel 7.3 Netzwerkzonierung) für eine bidirektionale Kommunikation aller relevanten und technologieübergreifenden Assets über definierte Security Gateways zentral bereitgestellt. Die ausgewählten Sicherheitsmaßnahmen werden dabei gemäß Defense-in-Depth-Prinzip mehrstufig angeboten und können anforderungsgerecht in bestehende Infrastrukturen integriert werden. Das Defense-in-Depth- Prinzip beschreibt dabei den Aufbau von mehreren, parallel betriebenen Sicherheitsmechanismen zur Erhöhung der Sicherheit. So können nicht nur Synergie- und Kosteneinsparungspotenziale erreicht, sondern auch die in der Praxis häufige Anforderung an eine autarke oder

abgegrenzte Standortverwaltung umgesetzt werden. Das wesentliche Ziel der zentralen Dienste ist es jedoch, die Assets gegen Bedrohungen angemessen zu schützen und die Auswirkungen von Bedrohungen auf den Betrieb zu minimieren, bzw. diesen auch bei etwaigen Sicherheitsvorfällen aufrechtzuerhalten. Die technischen Sicherheitsmaßnahmen sind dabei gemäß einer Schutzbedarfsfeststellung angemessen auszuwählen. Systembetreiber erhalten hierdurch wichtige Werkzeuge zur Absicherung und Aufrechterhaltung des Produktionsbetriebes. Gleichzeitig sorgt dies für ein zentrales Management mit abgestuften Administrationsmöglichkeiten.

Die Dienste können zudem in ein Managementkonzept gefasst werden, das eine zentrale Verwaltung mit abgestufter, delegierter Administration kombiniert.

Generell wird die Isolation von schutzbedürftigen Gütern (Assets) zum Schutz derselben Defense-in-Depth-Strategien empfohlen. Die Grundlage des Ansatzes bildet ein Zonenmodell. Dieses Modell schützt kritische und sensible Automatisierungsprozesse vor unberechtigten Zugriffen aus nicht vertrauenswürdigen Netzwerksegmenten. Das Zonenmodell basiert dabei in der Regel auf sechs Zonen, welche bestimmte Funktionen übernehmen und die Systeme nach differenziertem Schutzbedarf klassifiziert aufnehmen.

So werden kritische Steuerungs- und Automatisierungssysteme ausschließlich in den Zonen 1 und 2 angeordnet und über geeignete Security Gateways von anderen Zonen separiert.

Die Zone mit dem höchsten Schutzbedarf definiert die Sicherheitsmaßnahmen nach dem Maximum-Prinzip, dem Kumulations- oder dem Verteilungseffekt gemäß der durchgeführten Schutzbedarfsfeststellung. Erfüllt ein Asset diese Voraussetzungen nicht, wird eine eigenständige Subzone mit Sicherheitsmaßnahmen gebildet, die von der übergeordneten Zone vererbt werden. Eine Zone kann dabei mehrere Subzonen beinhalten.

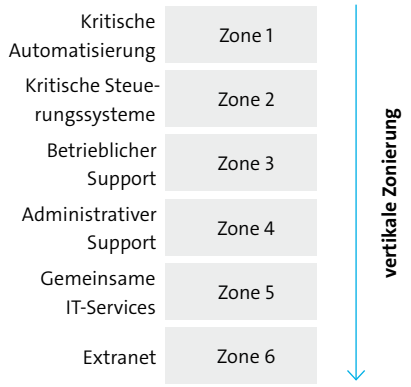


Abbildung 10: Vertikale Zonierung

Eine horizontale Zonierung segmentiert das Netzwerk territorial. So können unterschiedliche Standorte mit differenzierten Schutzbedarfen betrieben werden.

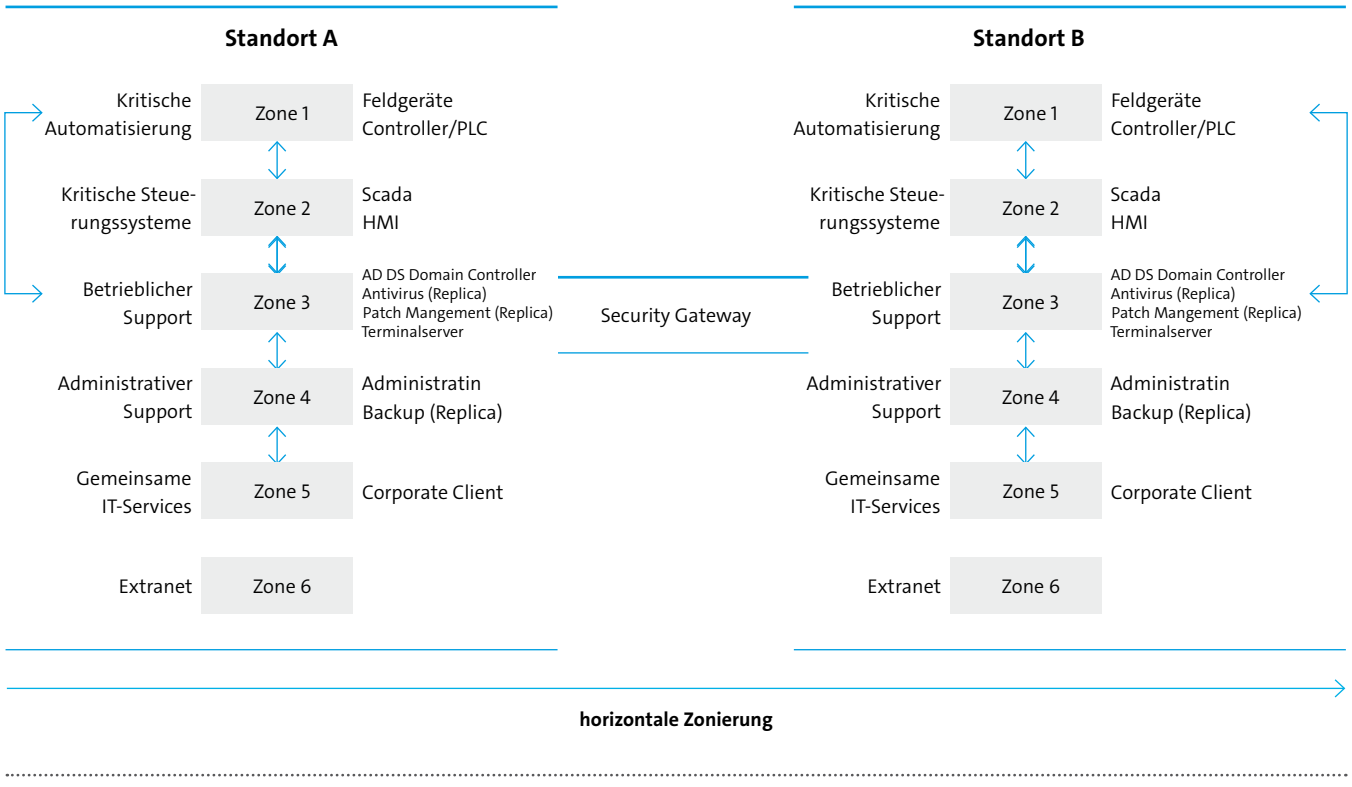


Abbildung 11: Horizontale Zonierung

Hierfür notwendige Kommunikationswege und Schnittstellen werden über bereitgestellte Security Gateways realisiert. Die zonenübergreifende Kommunikation erfolgt über sichere, geschützte und definierte Kommunikationskanäle. Diese Transferzonen werden technisch durch »demilitarisierte Zonen« realisiert, welche nach dem »Least Privilege-Prinzip« aufgebaut sind. Informationen können dabei bidirektional ausgetauscht werden. Dies erlaubt einen sicheren Zugriff zu Wartungs- und Konfigurationsarbeiten als auch den Zugriff zwecks Datenauswertung/-erfassung, zum Beispiel aus dem Bürokommunikations- oder anderen Netzen. Ein Zugriff kann hierfür über Terminaldienste organisiert werden. Somit ist ein direkter Zugriff auf vernetzte Automatisierungssysteme ausgeschlossen und ausschließlich über Transferzonen möglich. Die Kommunikationskanäle sind sodann, wenn machbar immer mit einer Ende-zu-Ende-Verschlüsselung zu versehen. Alternativ können die jeweiligen Zonenübergänge über einzelne VPN-Tunnel realisiert werden.

Um den größtmöglichen Schutz der einzelnen Zonen zu erhalten, sollten ausschließlich die notwendigsten Kommunikationsbeziehungen zwischen den einzelnen Assets zugelassen und

freigeschaltet werden. Hierzu sind geeignete Whitelisting-Konzepte zu erarbeiten und technisch wirksam umzusetzen.

Das Whitelisting-Konzept ist dabei so eng zu fassen, wie es die technischen Gegebenheiten zulassen, idealerweise werden Applikations-Filter eingesetzt, die die entsprechenden Anwendungen feingranular erkennen können. Port-Filterung kann zusätzlich stattfinden, ist aber alleinig nicht als ausreichend anzusehen.

Darüber hinaus können weitere Security Gateways an den Zonenübergängen platziert werden.

6.3 Security Monitoring und Protokollierung

Um mit geeigneten Maßnahmen, Sicherheitsvorfällen entgegenwirken oder aber diese überhaupt zeitnah erkennen zu können, sind geeignete Security Monitoring und Protokollierungslösungen zu etablieren. Praxiserprobt sind dabei Lösungen, die vollständig an die Anforderungen und Bedürfnisse der Betreiber von Energieversorgungsnetzen angepasst werden können.

Handelsübliche, sogenannte out-of-the-box-Lösungen (OOTB) sind dabei aufgrund Ihrer Inflexibilität, nur bedingt zu empfehlen.

Eines der Hauptziele ist es darüber hinaus, mittels einer konsolidierten Verwaltungsoberfläche alle relevanten Informationen und Meldungen auf einen Blick zu erhalten und diese bewerten zu können. Unterschiedliche Lösungen für verschiedene Typen von Systemen und Komponenten haben sich in der Praxis als nicht effektiv bewehrt und sollten vermieden werden. Vielmehr ist auch hier ein zentrales und ganzheitliches Konzept anzustreben. Durch einzelne Satellitensysteme, kombiniert mit einem geeigneten Zonenmodel (Netzwerkzonierung) können sodann auch dort Informationen gesammelt werden, wo es bislang keine Kommunikationsverbindungen gab. Des Weiteren können damit, mittels vorab definierter Schwellwerte, sodann auch automatisierte Alarmierungen ausgelöst und das Fachpersonal informiert werden.

Neben einem Security Monitoring und der dazugehörigen Protokollierung empfiehlt es sich außerdem ein Sicherheitsinformations- und Ereignis-Management (SIEM) zu etablieren, welches sicherheitsrelevante Informationen zentral erfasst, korreliert und mit eigener Intelligenz in Echtzeit bewertet. So können gezielte Angriffe frühzeitig erkannt und mit entsprechenden Maßnahmen dem Angriff entgegengewirkt werden.

Auch hier haben sich Lösungen erprobt, die vollständig an die Anforderungen und Bedürfnisse der Betreiber von Energieversorgungsnetzen angepasst werden können.

Ergänzt werden diese durch geeignete Frühwarnsysteme zur Erkennung und zur Verhinderung von Angriffen. Hier empfiehlt sich in der Praxis der Einsatz von Intrusion-Prevention (IPS) und Intrusion-Detection-Systemen (IDS), welche Anomalien und Angriffe auf Leittechnikebene inter-

pretieren und verarbeiten können. Dazu muss das IPS/IDS in der Lage sein unterschiedlichste Signaturen, beispielsweise für Modbus TCP oder Siemens S7, verarbeiten zu können.

6.4 Remote-Zugriffe/Fernwartung

Fernwartungs- oder Remotezugriffe sind generell auf das notwendigste zu beschränken. Ist ein Fernwartungszugang unumgänglich, sollte dieser zentralisiert bereitgestellt und mit geeigneten Sicherheitsmaßnahmen versehen werden. Auf mehrere, unterschiedliche Einzellösungen sollte hingegen aufgrund der erhöhten Angriffsfläche und Komplexität verzichtet werden.

Grundsätzlich empfiehlt sich die Implementierung einer mehrstufigen Firewall-Infrastruktur. Hierbei wird eingehender und ausgehender Datenverkehr nicht nur durch eine, sondern zugleich mehrere unterschiedliche Firewalls geprüft. Dabei bietet es sich an zugleich auch unterschiedliche Hersteller (dual Vendor) und Technologien einzusetzen.

Darüber hinaus sollten alle Fernzugriffe mittels personalisierten Benutzerkonten stattfinden und vorab durch einen definierten Freigabeprozess aktiviert und nach erfolgter Wartung auch wieder deaktiviert werden.

Dauerhaft freigeschaltete Benutzerkonten sollten zu jederzeit vermieden werden. Neue Bedrohungen, Risiken und Sicherheitsanfälligkeiten unterstreichen zudem die Anforderung an eine starke Authentifizierung. Hier sollten ausschließlich Zwei-Faktor- Authentifizierungen (2FA) zum Einsatz kommen, die den Zugriff auf sensible Zonen schützt und die Identitäten von Benutzern sicherstellt.

Zudem sollte alle Benutzeraktivitäten mit geeigneten technischen Maßnahmen überwacht und protokolliert werden. Hierzu sind technische Lösungen für ein Security Monitoring bzw. eine Protokollierung zu etablieren.

Der Fernzugriff sollte ausschließlich über geeignete SSL-VPN-Lösungen in Kombination mit Terminaldiensten oder sogenannten Sprungsystemen erfolgen. Direktzugriffe (Site-to-Site-VPN) auf einzelne Systeme sollten zwingend vermieden werden.

Für das transferieren von Dateien empfehlen sich sogenannte Datendrehscheiben. Dabei können Daten in einer demilitarisierten Zone abgelegt und in einer anderen Zone abgerufen werden. Ein direkter Transfer ist hierbei zu keiner Zeit möglich. Darüber hinaus können mehrere Prüfinstanzen vorgeschaltet werden, sodass sichergestellt werden kann, dass bspw. kein Schadcode transportiert wird.

6.5 Account Management

Immer häufiger werden Automatisierungs-, Prozesssteuerungs- und -leitsysteme mit Verzeichnisdiensten insbesondere auf dem Windows Betriebssystem integriert. Die Möglichkeit, eine zentrale Benutzer- und Passwortverwaltung innerhalb von Domänen zu nutzen, wird häufig nicht ergriffen und so die Anforderungen des Access Control verfehlt.

Empfehlenswert bei der technischen Umsetzung sind auch hier mehrstufige Domänenmodelle. Domänenmodelle basierend auf einzelnen Domänen gelten hingegen aus Redundanz- und Sicherheitsaspekten als bedenklich und sollten in der Praxis vermeiden werden. Modelle mit mehr als einer Domäne hingegen können den Sicherheitsanforderungen der Verfügbarkeit und Autarkie gerecht werden. In solchen Szenarien spricht man von »parent- und child domain«-Domainmodellen. Ferner wird so eine hierarchische, delegierte Administration auf Grundlage des »Least Privilege-Prinzips« etabliert und möglich.

6.6 Anti-Virus/Malware

Eine eng mit den Anlagenerrichtern und -integratoren konzipierte, geprüfte und freigegebene Virenschutzlösung wird über eine mehrstufige Infrastruktur bereitgestellt. Bei der Konzeptionierung und Implementierung der Lösung sind insbesondere Scan-Ausnahmen, gestaffelte Signatur-Updates, sowie Tests und Early-Adopter-Strategien (frühzeitiger Anwender, repräsentative Testgruppen) zu berücksichtigen.

Auch hier wird die Mehrstufigkeit durch sogenannte Parent- und Child-Instanzen gelöst. Hierbei wird die Parent-Instanz über definierte Zonenschnittstellen mit den an den Standorten integrierten Lösungen verbunden. Hierdurch kann eine zentrale, aber dennoch autarke Bereitstellung von Virenschutzlösungen gewährleistet werden. Dabei werden neue Virensignaturen zentral heruntergeladen, getestet und für die weitere Nutzung vertikal und horizontal an den jeweiligen Standorten bereitgestellt. Die Freigabe der Virensignatur obliegt dann dem jeweiligen Fachbereich selber.

Somit entfällt das Infektionsrisiko durch manuelle Downloads und das manuelle unregelmäßige Einspielen von Virensignaturen auf den Endgeräten. Eine direkte Schnittstelle zum Internet ist nicht notwendig und sollte zwingend vermeiden werden. Über geeignete Transfer- und Sicherheitszonen (siehe Zonenmodell), wird ein direkter Zugriff auf kritische Anlagenbereiche in der Praxis, praktisch ausgeschlossen.

6.7 Patch Management

Ein geregeltes Patch Management sollte auf klaren, vorab definierten und mit den Herstellern abgestimmten, Prozessen basieren.

Diese müssen zwingend mindestens die Identifikation, Bewertung, das Testen und einen detaillierten Freigabeprozess beinhalten. Auch hier empfiehlt sich die Bereitstellung als zentraler Dienst.

So werden Anlagenbetreibern die Aktualisierungen über standardkonforme Patchmanagement-Prozesse und über sichere, verschlüsselte Kanäle für die vertikalen Zonen zur Verfügung gestellt.

Ein manuelles Einspielen von Sicherheitsaktualisierungen per Wechseldatenträger, welches zumeist als erhebliches Sicherheitsrisiko gilt, entfällt somit.

Darüber hinaus kann der Patchlevel der Systeme in den vertikalen als auch von zentraler Stelle aus in den horizontalen Zonen beobachtet und bedarfsweise nachgesteuert werden. Eine zentrale Installation von Updates, sollte jedoch ausgeschlossen werden. Vielmehr sollte auch hier die Entscheidungsgewalt beim jeweiligen Fachbereich etabliert werden, um eine grundsätzliche Autarkie zu gewährleisten.

Neben Betriebssystemkomponenten, sollten jedoch auch alle Netzwerkkomponenten wie Switches, Router, Firewalls u.v.m. in den Patch Management-Prozess eingebunden und regelmäßig aktualisiert werden. Darüber hinaus sind zudem alle Anwendungen von Drittanbietern mit aufzunehmen. Um die Angriffsfläche zu minimieren, sollte jedoch darauf geachtet werden, so wenig zusätzliche Anwendungen wie möglich zu nutzen. Ist dies nicht ohne weiteres machbar, sollte ein zentralisiertes Terminalserverkonzept in Betracht gezogen werden.

6.8 Backup und Wiederherstellung

Die richtige Backup-Methode muss je nach Anwendungsfall bzw. System gewählt werden. In der Regel ist eine Kombination aus folgenden drei Methoden empfehlenswert:

- Inkrementelles Backup
- Differentielles Backup
- Vollbackup/Image-oder Snapshot-Verfahren

Auch sind Fallunterscheidungen je nach eingesetzter Technologie vorzunehmen. Wird beispielsweise eine Virtualisierung der Hardware vorgenommen, so sind andere Backup-Methoden gegebenenfalls noch zu berücksichtigen. Bei Datenbank- und Echtzeitsystemen sollten Sie in der Regel jedoch auf ein Image- oder Snapshot-Verfahren verzichten, da hierdurch ein erhöhtes Risiko eines Datenverlustes besteht.

Generell müssen sämtliche Backup-Methoden kompatibel zu den festgelegten Sicherheitsanforderungen und Kritikalitäten bezüglich der maximal tolerierbaren Ausfallzeit (mtA) sein. Ebenso sollten wichtige Hardwarekomponenten jederzeit vorgehalten werden umso bei einem Hardwareausfall, auch eine Wiederherstellung vornehmen zu können.

Durch mehrstufige Backup-Konzepte, welche über das Zonenmodel in die zentralen Dienste eingegliedert werden, können anforderungsgerechte Wiederherstellungsprozesse realisiert und etabliert werden.

6.9 Ausfallsicherheit/HA

Die Verfügbarkeit von kritischen Geschäftsprozessen hängt oft von der Funktion eines zentralen Servers oder einer zentralen Komponente ab. Je mehr Prozesse auf einem Server oder dieser Komponente laufen, desto ausfallsicherer muss dieser sein. Kritische Komponenten sollten daher in der Regel redundant ausgelegt und in unterschiedlichen Gebäuden, Räumen und Brandabschnitten betrieben werden. Kann ein Ausfall prinzipiell toleriert werden, sind zumindest geeignete und erprobte Backup-Strategien zu nutzen um ein System in kurzer Zeit wiederherstellen zu können.

Die Wiederherstellung des Gesamtsystems kann in der Praxis jedoch erhebliche Zeit in Anspruch nehmen. Neben der Vorhaltung von Ersatzteilen sollten zusätzlich folgende Möglichkeiten zur Steigerung der Verfügbarkeit eingesetzt werden:

- Cold-Standby

- Cold Standby wird in der Regel als Verhaltensweise redundanter Komponenten (bspw. Ersatzserver) in einem IT-Verbund definiert. Bei einem Ausfall einer Komponente wird dabei nicht automatisiert wie beim Hot Standby die Ersatzkomponente aktiviert, sondern diese wird manuell durch eine Fachkraft in Betrieb genommen. Diese Vorgehensweise inkludiert eine unvermeidbare Ausfallzeit, daher ist diese Methode in der Regel nicht für Anwendungen gedacht, die eine hohe Verfügbarkeit (24x7) benötigen. Im Umkehrschluss ist diese Variante jedoch kostengünstiger.

- Hot-Standby
  - Beim Hot Standby übernimmt dagegen sofort ein anderes System die Funktion der ausfallenden Komponente. Diese Hochverfügbarkeit führt entsprechend zu höheren Kosten.

- Cluster
  - Load balanced Cluster
    - Load balanced Cluster werden eingesetzt, um den Anforderungen an eine Rechenlastverteilung auf mehrere Systeme gerecht zu werden. Einsatzgebiete sind in der Regel Umgebungen mit hohen Anforderungen an die zu erbringende Computer- oder Systemleistung.

- Failover Cluster
  - Failover Cluster werden zur Steigerung der Verfügbarkeit bzw. zum Erreichen einer besseren Ausfallsicherheit eingesetzt. Im Fehlerfall kann ein sogenannter gesunder Cluster-Knoten die auf dem fehlerhaften Cluster-Knoten, laufenden Dienste übernehmen.

Jede einzelne dieser Möglichkeiten bietet ein unterschiedliches Niveau an Verfügbarkeit und ist in der Regel auch mit unterschiedlichen Kosten verbunden. Anhand einer vorab definierten Risikoeinschätzungsmethodik, sollten hier gemäß der Risikoeinschätzung geeignete Maßnahmen umgesetzt werden.

7 Ansprechpartner

Mitwirkende Unternehmen	Kontakt
admeritia GmbH	Heiko Rudolph Gladbacher Straße 3 | 40764 Langenfeld T +49 2173 20363-0 | heiko.rudolph@admeritia.de www.admeritia.de
ANMATHO AG	Dipl.-Kfm. Christian Westerkamp, LL.M. (Mitglied der Geschäftsleitung) Winterhuder Weg 8 | 22085 Hamburg T +49 40 2294719-0 | info@anmatho.de www.anmatho.de
Applied Security GmbH	Dirk Wegner Einsteinstraße 2a | 63868 Großwallstadt T +49 6022 26338-0 | kontakt@apsec.de www.apsec.de
Bitkom **Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.**	Felix Dembski Albrechtstraße 10 | 10117 Berlin T +49 30 27576-0 | bitkom@bitkom.org www.bitkom.org
BTC Business Technology Consulting AG	Gerd Niehuis, Informationssicherheit Escherweg 5 | 26121 Oldenburg T + 49 441 3612-1203 | gerd.niehuis@btc-ag.com www.btc-ag.com
datenschutz cert GmbH	Dr. Sönke Maseberg Konsul-Smidt-Straße 88a | 28217 Bremen T + 49 421 696632-50 | office@datenschutz-cert.de www.datenschutz-cert.de
DREWAG NETZ	Michael Rose Rosenstraße 32 | 01067 Dresden T +49 351 20585-6773 | Michael_Rose@Drewag-Netz.de www.drewag-netz.de
DQS GmbH, Deutsche Gesellschaft zur Zertifizierung von Managementsystemen	Markus Werckmeister August-Schanz-Straße 21 | 60433 Frankfurt am Main T +49 69 95427-477 | bdit@dqs.de www.dqs.de
Hewlett-Packard GmbH	Enterprise Security Services Jürgen Seiter Herrenberger Straße 140 | 71034 Böblingen T +49 7031 14-6541 | Juergen.seiter@hp.com www.hp.com/enterprise/security
HiSolutions AG	Andreas Salm Bouchéstraße 12 | 12435 Berlin T +49 30 533289-0 | info@hisolutions.com www.hisolutions.com
items GmbH	Michael Niehenke Hafenweg 7 | 48155 Münster T +49 251 6945-6123 | m.niehenke@itemsnet.de www.itemsnet.de

Mitwirkende Unternehmen	Kontakt
NBB Netzgesellschaft Berlin-Brandenburg mbH & Co. KG	Robert Schmidt, Gruppenleiter Leitwarte/Dispatchin An der Spandauer Brücke 10 | 10178 Berlin T +49 30 81876-1332 | robert.schmidt@nbb-netzgesell-schaft.de www.nbb-netzgesellschaft.de
Netz Lübeck	Dieter Behrendt Geniner Straße 80 | 23560 Lübeck Briefpost 23533 Lübeck T +49 451 888-2440 | dieter.behrendt@netz-luebeck.de www.netz-luebeck.de
regio iT GmbH	Bernhard Barz Lombardenstraße 24 | 52070 Aachen T +49 241 41359-9626 | bernhard.barz@regioit.de www.regioit.de
RheinEnergie AG	Hans-Jürgen Ramm, Gruppenleiter Parkgürtel 24 | 50823 Köln T +49 221 178-4831 | h.ramm@rheinenergie.com www.rheinenergie.com
ROHDE & SCHWARZ SIT GmbH	Andreas Schmid, Senior Consultant Network & IT Security Am Studio 3 | 12489 Berlin T +49 30 65884-223 | info.sit@rohde-schwarz.com www.sit.rohde-schwarz.com
secunet Security Networks AG	Steffen Heyde Alt-Moabit 96 | 10115 Berlin T +49 201 5454-2025 | steffen.heyde@secunet.com www.secunet.com
smartOPTIMO GmbH & Co. KG	Sven Kuse Luisenstraße 20 | 49074 Osnabrück T +49 541 600680-11 | info@smartoptimo.de www.smartoptimo.de
Stromnetz Hamburg GmbH	Robert Strade, Leiter Betriebsorganisation Überseering 12 | 22297 Hamburg T +49 40 49202-8681 | robert.strade@stromnetz-hamburg.de www.stromnetz-hamburg.de
SWK STADTWERKE KREFELD AG	Siegmar Merkus, Leiter IT-Service St. Töniser Straße 124 | 47804 Krefeld siegmar.merkus@swk.de TM +49 160 90653175 | T +49 2151 98-2355 www.swk.de
T-Systems International GmbH	Business Unit Cyber Security security-info@t-systems.com www.t-systems.de
TÜV Süd Management Service GmbH	Ridlerstraße 65 | 80339 München T +49 89 50084-801 www.tuev-sued.de
VKU **Verband kommunaler Unternehmen e. V.**	Benjamin Sommer Invalidenstraße 91 | 10115 Berlin T +49 30 58580-0 | info@vku.de www.vku.de

8 Abkürzungsverzeichnis

Abkürzung	Tabellenkopf
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik,
CERT	Computer Emergency Response Team – Gruppe von IT-Sicherheitsfachleuten, die bei einem konkreten IT-Sicherheitsvorfall tätig wird
DAkkS	Nationale Akkreditierungsstelle Deutschlands, überprüft faktisch die Prüfer. Stellen, die die Konformität mit Normen, Zertifizierungen, etc. bewerten (z. B. TÜV), müssen ihrerseits bei der DakkS registriert sein und werden von ihr geprüft, um eine einheitliche Qualität der Prüfer sicherzustellen.
ICS	Industrial Control System: Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse
IS Controls	Im Anhang A der ISO 27001 beschriebene Maßnahmen, mit identifizierten Risiken umzugehen
IDS	Intrusion detection system – System zum Erkennen von Eindringlingen in ein IT-System
IPS	Intrusion Prevention System – System zum Verhindern des Eindringens Fremder in IT-Systeme
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization, Internationale Standardisierungs-organisation und Herausgeberin der ISO 27001-Normenfamilie für Informations-Sicherheitsmanagement
ISO 2700x-Familie	Serie von Normen für Informationssicherheits-Managementsysteme
IT-Grundschutz	Informationssicherheitsmanagement Systematik des BSI
ITK	Informations- und Kommunikationstechnologie
Scope	Individuell definierter Anwendungsbereich des ISMS
SOA	Statement of Applicability, »Erklärung zur Anwendbarkeit«, listet die ergriffenen grundsätzlichen Maßnahmen zur Risikobehandlung aus Anhang A der ISO 27001 auf und erlaubt so auch deren Überprüfung
UP KRITIS	Öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen beim BSI, unterhält diverse Branchen- und Themen-Arbeitskreise
VKU	Verband Kommunaler Unternehmen e. V.
VPN	Virtual Private Network
Whitelisting	»weiße Liste«, Verfahren, bei dem eine Liste mit den ausschließlich vertrauenswürdigen Elementen (Personen, Unternehmen oder Programme) angelegt wird. Nur die Interaktion mit den Elementen auf dieser Liste wird technisch erlaubt.

Bitkom vertritt mehr als 2.300 Unternehmen der digitalen Wirtschaft, davon gut 1.500 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom