Deloitte.

IT-Sicherheitskatalog der BNetzA
Informationssicherheit bei Netzbetreibern

Die Energiewirtschaft wird zunehmend „digital". Netzbetreiber sind bereits heute und zukünftig noch stärker auf IKT-Lösungen zur erfolgreichen Bewältigung der Energiewende angewiesen. Doch mit neuen IKT-basierten Prozessen, zunehmender Vernetzung der Business- und Prozess-IT sowie mit dem Zuwachs der Datenmenge wachsen auch die Risiken für die Unternehmen.

Die jüngsten Probleme und Sicherheitsvorfälle zeigen, dass die Gefahr durch Nichtverfügbarkeit, Manipulation oder Diebstahl von Informationen bereits heute präsent ist. Es ist zu erwarten, dass diese Bedrohung zukünftig zunehmen wird.

Beispiele von bekannt gewordenen Vorfällen

- 2012 setzten Unbekannte mit einem DDoS-Angriff die Webseiten und die E-Mail-Infrastruktur eines deutschen ÜNBs außer Betrieb.
- 2013 bestand eine konkrete Netzausfallgefahr in österreichischen und deutschen Netzen durch einen fehlgeleiteten Steuerbefehl eines deutschen Energieversorgers.
- 2014 wurden 1.000 Smart Meters von eigenen Mitarbeitern eines Stromversorgers unbemerkt so manipuliert, dass sie einen zu niedrigen Stromverbrauch erfassten und damit Stromdiebstahl ermöglichten.

Insbesondere im Bereich der kritischen Infrastrukturen kann eine fehlende Informationssicherheit erhebliche ökonomische bzw. gesellschaftliche Schäden auslösen. Dies erklärt auch die Brisanz des Themas für Netzbetreiber.

Mit der Verabschiedung des IT-Sicherheitskatalogs der BNetzA werden Netzbetreiber zur Implementierung eines ISMS verpflichtet.

Informationssicherheit im Fokus der BNetzA

Mit dem Entwurf des „IT-Sicherheitskataloges" der Bundesnetzagentur (BNetzA) liegt derzeit ein relevantes Regelwerk zur Sicherstellung der Informationssicherheit bei Netzbetreibern vor. Er basiert auf § 11 Absatz 1a EnWG und umfasst vorrangig Maßnahmen zum Schutz der IKT im Bereich der Netzsteuerung. Eine zentrale Forderung ist die Einführung und anschließende Zertifizierung eines Informationssicherheits-Managementsystems (ISMS) gemäß ISO/IEC 27001. Die Verabschiedung des Kataloges wird Mitte 2015 erwartet.

Zusätzlich wurde am 12. Juni 2015 das neue IT-Sicherheitsgesetz verabschiedet, das die betroffenen Unternehmen der kritischen Infrastruktur verpflichtet, einen sog. Grundschutz einzuführen und bei Angriffen einer noch zu definierenden Meldepflicht nachzukommen. Der „ IT-Sicherheitskatalog" der BNetzA konkretisiert die Anforderungen an Netzbetreiber und verpflichtet die betroffenen Unternehmen zum zügigen Handeln. Bei all dem steht die oberste Managementebene der Netzgesellschaften in der Verantwortung und der Verpflichtung, den Aufbau und Betrieb eines wirksamen und wirtschaftlichen ISMS durch entsprechende strategische, ressourcenbezogene und organisatorische Entscheidungen sicherzustellen.

Spezifika eines ISMS für Netzbetreiber

In Anlehnung an den „IT-Sicherheitskatalog" der BNetzA sind die Schutzziele

- Verfügbarkeit der zu schützenden Systeme und Daten
- Integrität der verarbeiteten Systeme und Informationen
- Vertraulichkeit der mit den betrachteten Systemen verarbeiteten Information

von zentraler Bedeutung. Damit rücken mindestens die Systeme in den Fokus, welche die Fahrweise des Netzes mittelbar oder unmittelbar beeinflussen und die Versorgungssicherheit tangieren. Hierzu zählen z.B.:

- Leitsysteme und der Systembetrieb
- Übertragungs-, Telekommunikations- und Netzwerktechnik
- Sekundär-, Automatisierungs- und Fernwirktechnik

Die BNetzA ordnet ihrerseits alle Systeme der Netzsteuerung in die „hohe" bis „sehr hohe" Schutzbedarfskategorie ein.

Um die ISO/IEC 27001 auf die spezifischen Systeme der Netzbetreiber zu adaptieren und eine Zertifizierung zu ermöglichen, stehen die Netzbetreiber vor enormen Herausforderungen. Denn welche Maßnahmen zu ergreifen sind, wird zunächst nicht vorgegeben. Festzuhalten bleibt hierzu nur, dass es in den Verantwortungsbereich des Netzbetreibers fällt, angemessene und dem Stand der Technik entsprechende Schutzmaßnahmen zur Erfüllung der Schutzziele bzw. Gewährleistung der Versorgungssicherheit zu treffen. Im Schadensfall ist der Netzbetreiber in der Nachweispflicht, dass er ausreichend effektive und angemessene Maßnahmen getroffen hat.

In einem ISMS für Netzbetreiber genießt grundsätzlich das Schutzziel der Verfügbarkeit der Systeme und Daten hohe Priorität und wird sich daher in Schutzniveaus und den entsprechenden Schutzmaßnahmen widerspiegeln. Zudem unterscheidet sich die technische Systemlandschaft des Netzbetreibers in ihren Sicherheitsanforderungen von herkömmlichen IT-Umgebungen deutlich. So sind bei der Netzsteuerung häufig „Altsysteme" mit lückenhafter Sicherheitsarchitektur im Einsatz und nicht selten hat der Systemhersteller den Support bereits eingestellt. Prozessnahe IT-Systeme sind zudem eng auf die jeweilige Hardware ausgerichtet und bieten eingeschränkte Möglichkeiten zur Erweiterung um Sicherheitskomponenten.

Allgemein bekannte Standardlösungen für IT-Sicherheit sind daher bei Netzbetreibern häufig nicht anwendbar oder ermöglichen kein ausreichendes Schutzniveau. So werden die Standardmaßnahmen wie Einsatz von Firewalls, Virenschutzprogrammen und Berechtigungsverwaltung bei Weitem nicht ausreichen. Weitere technische Maßnahmen wie „Härtung" der Systeme, Einsatz von Whitelists, Verschlüsselung, Netzwerksegmentierung etc. sind unbedingt in den Lösungsansatz aufzunehmen. Organisatorische Maßnahmen gehören ebenfalls dazu und müssen für die Umgebung des Netzbetreibers angepasst und eingeführt werden. Hierzu zählen die Konzepte für das Vorfallsmanagement, für Not- und Krisenfälle, aber auch das Trainings- und Awareness-Programm für alle Mitarbeiter, damit die Unternehmen bspw. auch Social-Engineering-Angriffen entgegen treten können.

Nicht zuletzt aus diesem Grund ist ein netzbetreiberspezifisches und individuell ausgerichtetes ISMS auszugestalten. Dabei soll die Zertifizierung nach ISO/IEC 27001 lediglich einen Mindeststandard beim jeweiligen ISMS sicherstellen. Voraussetzung hierfür sind zwei Aspekte: Zum einen bedarf es eines tiefen Verständnisses zu den Funktionalitäten der Prozess-IT. Zum anderen muss die Kenntnis zum „Stand der Technik" für wirksame Schutzmaßnahmen in ausreichendem Maße vorliegen. Das richtige Zusammenspiel dieser beiden Komponenten ist ausschlaggebend für die erfolgreiche Einführung, den Betrieb und die regelmäßige Anpassung des ISMS und damit die Umsetzung der Anforderungen des „IT-Sicherheitskatalogs".

Abb. 1 – Regulatorischer Rahmen und Richtlinien

Nationale Gesetzgebung	• IT-Sicherheitsgesetz • Bundesdatenschutzgesetz • Energiewirtschaftsgesetz
Regulatorischer Rahmen (BNetzA)	• IT-Sicherheitskatalog (noch nicht verabschiedet)
Normen und Standards	• ISO/IEC 27001 • BSI IT Grundschutzkatalog • Weitere Normen z.B. von NIST
Sonstige Rahmenwerke und Whitepapers	• BDEW Whitepaper zu Anforderungen an sichere Steuerung- und TK-Systeme • ENISA Guidelines for Security measures for Smart Grids • Weitere Rahmenwerke z.B. von NIST, ITIL und CobiT

Unsere Leistungen

Angesichts der in Kürze erwarteten Verabschiedung des „IT-Sicherheitskataloges“ und damit zusammenhängenden Verpflichtung zur Einführung eines ISMS ist es für Netzbetreiber jetzt notwendig, sich mit den an sie gerichteten Anforderungen auseinanderzusetzen, Lösungsansätze aufzuarbeiten und die Umsetzung zu starten.

Sehr gerne unterstützen wir Sie bei den Herausforderungen des ISMS. Hierfür steht Ihnen ein erfahrenes und interdisziplinäres Team aus Spezialisten unserer Energy & Resources Practice und der Cyber Risk Services Practice zur Verfügung.

Unsere Vorgehensweise bei der Entwicklung und Einführung Ihres ISMS orientiert sich an den Vorgaben der ISO/IEC 27001, dem vorgeschlagenen Vorgehen im „IT-Sicherheitskatalog“ und den Standards des BSI sowie Umsetzungsempfehlungen des BDEW. In Abb. 2 ist unsere Vorgehensweise in fünf Schritten skizziert.

1. Set-up festlegen: Zunächst grenzen wir den Geltungsbereich, die Sicherheits- und Schutzziele sowie die wesentlichen Rollen und Verantwortlichkeiten ab.
2. Ist-Analyse durchführen: Anschließend analysieren und kategorisieren wir die vorhandenen Assets. Hierbei erfolgt die Einordnung in Schutzbedarfskategorien, die die Basis zur Ableitung des Umfangs an Schutzmaßen bilden.
3. Maßnahmen konzipieren: Für die jeweiligen Assets bzw. Systeme konzipieren wir Maßnahmen, die sowohl IT-technische als auch organisatorische Aspekte berücksichtigen. Weiterhin erstellen wir den Maßnahmenkatalog und helfen bei der Priorisierung zur Umsetzung.
4. Maßnahmen umsetzen: Wir implementieren und dokumentieren die Sicherheitsorganisation und die Managementprozesse. Weiterhin schulen wir die betroffenen Mitarbeiter zur operativen Umsetzung des ISMS-Konzeptes.
5. Regelmäßiger Health Check: Wir unterstützen bei der Festlegung und Durchführung eines Review-Programms. Die Ergebnisse fließen wiederum in die Verbesserung des ISMS ein.

Als Kunde profitieren Sie bei der Implementierung eines ISMS von der Branchenerfahrung unserer Berater, die in zahlreichen Projekten zu unterschiedlichsten Themen bei Netzbetreibern (Asset-Management, Systemführung, Netzwirtschaft usw.) Erfahrungen und Wissen aufgebaut haben. Wir haben in einer Vielzahl von Projekten bereits unsere Expertise in der Konzeption und Umsetzung von ISMS in komplexen Organisationen bewiesen. Wir sind weltweit einer der führenden Anbieter hierfür. Kontaktieren Sie uns – gerne stellen wir Ihnen unsere Erfahrung mit der Einführung von Informationssicherheits-Managementsystemen dar.

Als Kunde profitieren Sie bei der Implementierung eines ISMS von der Branchenerfahrung unserer Berater.

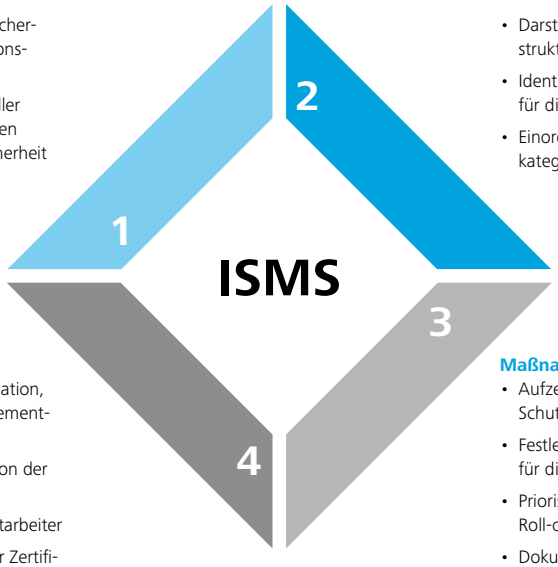
Abb. 2 – Vorgehen zur Einführung eines ISMS bei Netzbetreibern

Set-up festlegen

- Festlegung des Geltungsbereiches des ISMS
- Festlegung der Informationssicherheitspolitik und der Informationssicherheitsziele
- Definition und Verankerung aller Rollen und Verantwortlichkeiten im Bezug auf Informationssicherheit

Ist-Analyse durchführen

- Identifikation organisationseigener Assets im Sinne des BNetzA-Kataloges
- Darstellung der Assets in einem Netzstrukturplan
- Identifizierung der Gefährdungsarten für die jeweiligen Assets
- Einordnung der Assets in Schutzbedarfskategorien



Maßnahmen umsetzen

- Aufbau der Sicherheitsorganisation, Implementierung von Managementprozessen
- Umsetzung und Dokumentation der Sicherheitsmaßnahmen
- Schulungsmaßnahmen für Mitarbeiter
- Vorbereitungsmaßnahmen zur Zertifizierung

Maßnahmen konzipieren

- Aufzeigen der jeweils angemessensten Schutzmaßnahme (Stand der Technik)
- Festlegung der konkreten Maßnahmen für die Systeme
- Priorisierung der Maßnahmen für den Roll-out
- Dokumentation der Maßnahmen

Regelmäßiger Health Check

- Durchführung von regelmäßigen Prüfungen zur Wirksamkeit des ISMS (z.B. jährlich)
- Überprüfung der Umsetzung von bereits festgelegten Optimierungsmaßnahmen
- Erkennen von weiteren Optimierungspotenzialen unter Berücksichtigung von IT-Weiterentwicklungen und Veränderungen bei den Sicherheitsstandards

Ihre Ansprechpartner

Für mehr Informationen

Dr. Andreas Langer
Director Energy & Resources
Tel: +49 (0)69 75695 6512
anlanger@deloitte.de

Peter Wirnsperger
Partner Cyber Risk Services
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Artur Borger
Senior Consultant Energy & Resources
Tel: +49 (0)30 25468 7049
arborger@deloitte.de

Für weitere Informationen besuchen Sie unsere Webseite www.deloitte.com/de

Stand 2/2016