Zertifizierungsanforderungen an Smart Meter Betreiber

Tobias Goldschmidt

HiSolutions AG
goldschmidt@hisolutions.com

Zusammenfassung

Die Wettbewerbs- und Überlebensfähigkeit von Unternehmen ist in hohem Maße von der Informationstechnologie (IT) abhängig. Um die notwendige Handlungsfähigkeit aufrecht zu erhalten, verlangt es einen sicheren und verlässlichen IT-Betrieb, welcher gerade im Umfeld der Energieversorgung und -messung durch zahlreiche Vorschriften und Gesetze zunehmend reglementiert wird. Dies erfordert die Ausrichtung der IT-Systeme auf Sicherheit und Verlässlichkeit sowie den Aufbau einer klar strukturierten IT-Organisation, welche die gewünschten Leistungen über definierte Prozesse zur Verfügung stellt. Standardisierte Verfahren wie IT-Grundschutz vom Bundesamt für Sicherheit in der Informationstechnik (BSI) und ISO/IEC TR 27019 beschreiben eine solche Herangehensweise durch das Definieren von spezifischen Anforderungen an Unternehmen im Umfeld der Energieversorgung und -messung, welche bereits im Systemdesign, aber auch im Systembetrieb zu berücksichtigen sind. Der Artikel fasst die unterschiedlichen Anforderungen der Standards zusammen und zeigt Wege zur Integration dieser in ein zertifizierungsreifes Informationssicherheitsmanagementsystem (ISMS) im Smart Metering Umfeld auf.

1 Einleitung

Die Leistungsfähigkeit von Systemen in der Informations- und Kommunikationstechnologie (IKT) hat sich um Größenordnungen erhöht. Gleichzeitig ist die Komplexität, Dynamik und Leistungsfähigkeit von Systemen in der IKT signifikant gestiegen. Gründe hierfür sind unter anderem die zunehmende Integration bestehender Systeme in neue sowie das Hinzufügen neuer Funktionalitäten, ohne die Wechselwirkung mit bereits bestehenden Komponenten vollständig zu verstehen. Der Aufbau einer klar strukturierten IT-Organisation, welche die gewünschten Leistungen über definierte Prozesse zur Verfügung stellt und somit einen sicheren und verlässlichen IT-Betrieb garantiert, wird im Umfeld der Energieversorgung und -messung von Vorschriften und Gesetzen gefordert. Standards wie der ISO/IEC 27001 „Informationssicherheits-Managementsysteme - Anforderungen“ erleichtert die Definition und Einführung solcher Sicherheitsprozesse, sind jedoch zu abstrakt, um die Unternehmen im Umfeld der Energieversorgung und -messung gezielt zu unterstützen. Grund hierfür ist insbesondere die Tatsache, dass der Standard primär auf den klassischen IT-Betrieb bzw. typische IT-Systeme des Back-Office einer Institution abzielt. Besondere Einsatzszenarien sollen mehr und mehr durch weitere Standards in der ISO 27000 Familie berücksichtigt werden.

Der vorliegende Artikel untergliedert sich in ein Anforderungsteil, definiert durch diverse Standards und Richtlinien im Smart Meter Umfeld sowie ein Integrationsteil zur Aufnahme der Anforderungen in den Aufbau und Betrieb eines ISMS nach IT-Grundschutz.

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 315-325.

2 Anforderungen im Smart Meter Umfeld

Die Industrie ihrerseits hat die Problematik des Fehlens von Vorgaben im Umfeld der Energieversorgung und -messung erkannt und entwickelte 2013 den internationalen Standard ISO/IEC TR 27019 „Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002“. Dieser erweitert die Vorgaben des ISO/IEC 27002 „Leitfaden für das Informationssicherheits-Management“, der Umsetzungshilfe zum Standard ISO/IEC 27001 dahingehend, dass die branchenspezifischen Anforderungen an Unternehmen der Energieversorgung und -messung, bereits im Systemdesign, aber auch im Systembetrieb berücksichtigt werden können. Im Vergleich mit herkömmlichen IT-Umgebungen bestehen grundsätzlich signifikante Unterschiede bezüglich der Risiken und Chancen Informationssicherheit bei Entwicklung, Betrieb, Instandhaltung, Wartung und dem Einsatzumfeld von Prozesssteuerungssystemen sicherzustellen. Hinzu kommt, dass die Prozesstechnik häufig ein integraler Bestandteil von kritischen Infrastrukturen ist und somit zwingend für deren sicheren und störungsfreien Betrieb funktionieren muss. [ISOT13]

Für die reine Produktebene erarbeitete das BSI zwei Common Criteria Schutzprofile sowie eine Technische Richtlinie (TR) für die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway), um ein einheitliches technisches Sicherheitsniveau zu definieren. Die Technische Richtlinie TR-03109 beschreibt die zu erfüllenden Anforderungen an Funktionalität, Interoperabilität und Sicherheit von Komponenten im Umfeld des Smart Metering. Die Richtlinie bildet ein übergeordnetes Dachdokument und stellt eine Prüfgrundlage für die Erfüllung der Anforderungen speziell für Smart Meter Gateways (SMGW) dar. Um die Interoperabilität der in einem Smart Metering-System vorhandenen Komponenten zu gewährleisten, werden innerhalb der (Unter-)Richtlinien konkrete technische Anforderungen (z.B. im Bereich Kryptographie und Public Key Infrastrukturen (PKI)) an ein intelligentes Messsystem (z.B. hinsichtlich dem Sicherheitsmodul) einschließlich deren Testspezifikationen definiert. [BSIT13a]

Sämtliche Zertifizierungsanforderungen im Smart Meter Umfeld lassen sich in produktspezifische Anforderungen sowie Anforderungen an den Betrieb unterteilen.

Die Technische Richtlinie BSI TR-03109 fasst sämtliche Anforderungen für den zertifizierungsreifen Betrieb eines SMGW zusammen. Abbildung 1 stellt in einer aggregierten Übersicht die Verzahnungen der unterschiedlichsten Anforderungen hierfür zusammenfassend dar. Farblich gekennzeichnete Richtlinien befinden sich derzeit in der Planungs- bzw. bereits in der Abstimmungsphase, sind jedoch noch nicht final erschienen.

Das SMGW verfügt über ein internes Sicherheitsmodul, welches kryptographische Operationen sowie einen sicheren Schlüssel- und Zertifikatsspeicher zur Verfügung stellt. Das SMGW übernimmt

- die Speicherung der aus dem Lokalen Metrologischen Netz (LMN) empfangenen Messwerte,
- die Verarbeitung dieser gemäß konfigurierter Regelwerke sowie
- die Versendung der verarbeiteten Messwerte an berechtigte Marktteilnehmer im Weitverkehrsnetz (WAN).

Die gesammelten Messwerte können durch das SMGW sternförmig an die Adressaten im Weitverkehrsnetz direkt verteilt oder indirekt über einen bestimmten Teilnehmer verbreitet werden.

Zusätzlich bietet das SMGW Funktionen für Nutzer und Techniker, damit diese Verbrauchsdaten und Systeminformationen abrufen oder steuerbare Energieverbraucher (z.B. Waschmaschine) und Energieerzeuger (z.B. Photovoltaik-Anlage) bequem ansprechen können.

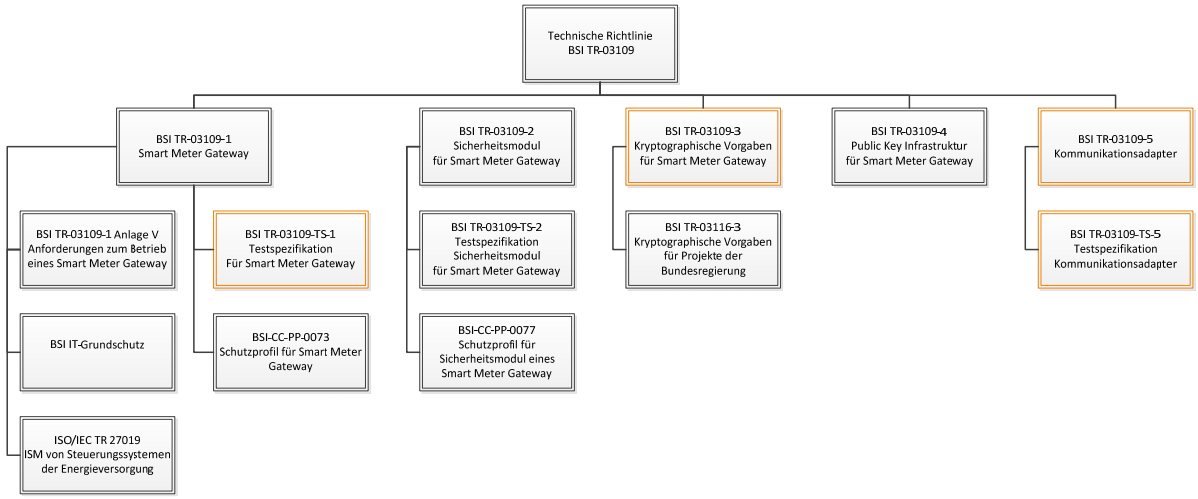

Abb. 1: Anforderungen zum zertifizierungsreifen Betrieb des Smart Meter Gateways

Darüber hinaus erfüllt es die Aufgaben einer Firewall und separiert die angebundenen Netze voneinander. Personenbezogene Messwerte werden, basierend auf den vertraglich vereinbarten Regelungen, nur an berechtigte Parteien versendet. Das SMGW stellt dadurch den Datenschutz sowie die Datensicherheit für den Nutzer sicher.

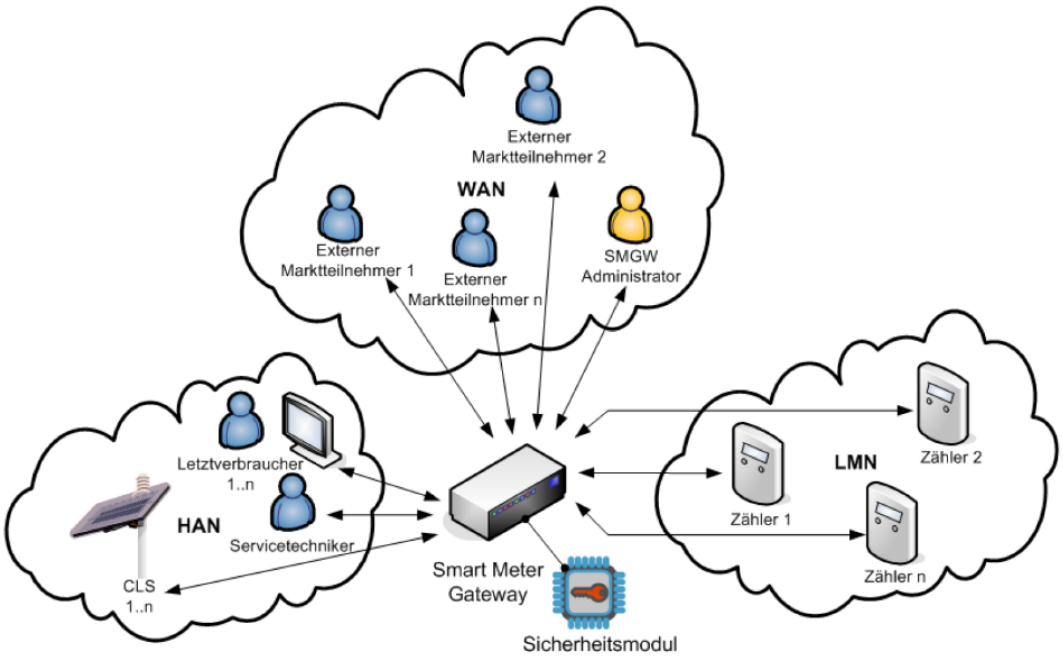

Abb. 2: Einsatzumgebung des Smart Meter Gateways [BSIT13b]

Ein SMGW muss somit mindestens drei physische Schnittstellen bereitstellen, welche in Abbildung 2 im Überblick dargestellt werden:

1. Im Local Metrological Network (LMN) kommuniziert das SMGW mit den angebundenen Zählern für Strom, Gas, Wasser und Wärme eines oder mehrerer Nutzer (Letztverbraucher). Die Zähler kommunizieren ihre Messwerte über das LMN an das SMGW.

2. Im Wide Area Network (WAN) kommuniziert das SMGW mit den externen Marktteilnehmern sowie dem SMGW Administrator.
3. Im Home Area Network (Heimnetz – HAN) kommuniziert das SMGW mit den Controllable Local Systems (steuerbare Energieverbraucher und Energieerzeuger – CLS) und fungiert dabei als Proxy-Server. Das SMGW ermöglicht zusätzlich die Kommunikation von lokalen Geräten des Heimnetzes über das Weitverkehrsnetz mit autorisierten Teilnehmern.

Im Folgenden werden den einzelnen Komponenten des SMGW sowie dessen Kommunikationsschnittstellen den hierfür anforderungsgebenden Standards und Richtlinien zugeordnet. Hierfür listet Tabelle 1 die in Abbildung 1 referenzierten Standards und Richtlinien konkret nach ihrem Einsatzgebiet auf.

Tab. 1: Überblick – Relevante Standards und Richtlinien im Smart Meter Umfeld

Standard / Richtlinie	Beschreibung
BSI TR-03109	Anforderungen an die Funktionalität, Interoperabilität und Sicherheit der Komponenten im Umfeld des Smart Metering
BSI TR-03109-1	SMGW – Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems
BSI TR-03109-TS-1	Testspezifikation – Prüfgrundlage zur Evaluierung und anschließenden TR-Zertifizierung des SMGW Hinweis: Dokument befindet sich in der Vorbereitungsphase
BSI-CC-PP-0073	Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen
BSI IT-Grundschutz	BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
ISO/IEC TR 27019	Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002
BSI TR-03109-2	SMGW – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls
BSI TR-03109-TS-2	Testspezifikation – Prüfgrundlage zur Evaluierung und anschließenden TR-Zertifizierung des Sicherheitsmoduls des SMGW Hinweis: Dokument befindet sich in der Vorbereitungsphase
BSI-CC-PP-0077	Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen
BSI TR-03109-3	Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen Hinweis: Dokument befindet sich in der Abstimmungsphase
BSI TR-03116-3	Kryptographische Vorgaben für Projekte der Bundesregierung
BSI TR-03109-4	Smart Metering PKI – Public Key Infrastruktur für SMGW
BSI TR-03109-5	Kommunikationsadapter Hinweis: Dokument befindet sich in der Planungsphase
BSI TR-03109-TS-5	Testspezifikation für Kommunikationsadapter Hinweis: Dokument befindet sich in der Planungsphase

2.1 Technische Richtlinie BSI TR-03109-1

Die Technische Richtlinie BSI TR-03109-1 beschreibt die Anforderungen, welche die Komponenten im Smart Meter Umfeld hinsichtlich Funktionalität, Interoperabilität und Informationssicherheit erfüllen muss.

Dabei wird das Common Criteria Schutzprofil referenziert und derart ergänzt, indem die funktionalen Sicherheitsanforderungen an das SMGW und dessen Einsatzumgebung um Vorgaben an Kommunikationsprotokolle, Tarif- und Auswertungsprofile sowie kryptographische Verfahren erweitert werden. Dabei richtet sich die Technische Richtlinie BSI TR 03109-1 vorwiegend an Hersteller von SMGW. [BSIT13b]

BSI TR-03109 Anlage V - Anforderungen zum Betrieb beim Administrator

Die Anlage V der Technischen Richtlinie BSI TR-03109-1 fordert von jedem SMGW Betreiber die Implementation, das Betreiben sowie das Dokumentieren eines ISMS nach ISO/IEC 27001 auf Basis IT-Grundschutz. Zusätzlich müssen die Standards DIN 27009 sowie ISO/IEC TR 27019 berücksichtigt werden, soweit die dort aufgeführten Maßnahmen hinsichtlich der Aufgaben und Betriebsprozesse des SMGW Betreibers anwendbar sind. Zur Erfüllung dieser Anforderungen muss der BSI IT-Grundschutz, hier speziell die BSI IT-Grundschutz-Vorgehensweise nach BSI Standard 100-2 sowie die BSI IT-Grundschutz-Kataloge, angewendet werden. Für Risikoanalysen kann die Methodik nach BSI Standard 100-3 verwendet werden, sie muss jedoch mindestens dem Rahmenwerk eines etablierten Standards folgen. [BSII08a], [BSII08b]

2.1.1 Common Criteria Schutzprofil BSI-CC-PP-0073

Das Common Criteria Schutzprofil BSI-CC-PP-0073 soll die Gewährleistung von Datenschutz und Datensicherheit sicherstellen.

Basierend auf einer Bedrohungsanalyse für den sicheren und datenschutzfreundlichen Betrieb, legt das Common Criteria Schutzprofil erforderliche Mindestsicherheitsanforderungen fest. SMGW müssen auf dieser Basis geprüft werden und erhalten anschließend ein Zertifikat als verbindlichen Nachweis über die Erfüllung der Schutzziele. Zur Gewährleistung von Interoperabilität und der technischen Umsetzung der Mindestsicherheitsanforderungen des Schutzprofils hat das BSI zusätzliche Vorgaben in der Technischen Richtlinie BSI TR-03109 fixiert.

2.1.2 BSI IT-Grundschutz

Das BSI beschreibt im Standard 100-2 eine Methodik zum Identifizieren und Umsetzen von Sicherheitsmaßnahmen der IT. Ziel ist das Erreichen eines mittleren und angemessenen Schutzniveaus für IT-Systeme. Zur Erreichung des Ziels empfiehlt der IT-Grundschutz technische, infrastrukturelle, organisatorische und personelle Maßnahmen. SMGW Betreiber müssen das systematische Vorgehen bei der Absicherung ihrer IT-Systeme, im Rahmen des Aufbaus eines ISMS, gegen Gefährdungen der IT-Sicherheit mit einem Zertifikat ISO/IEC 27001 auf Basis von IT-Grundschutz nachweisen. Unterstützend hierfür stellt das BSI IT-Grundschutz-Kataloge (Sammlung von Dokumenten, unterteilt in Bausteine, Gefährdungen und Maßnahmen) zur Verfügung, welche die schrittweise Einführung und Umsetzung eines ISMS detailliert erläutert. [BSII08a]

Smart Meter Betreiber müssen den Betrieb eines ISMS über ein Zertifikat ISO 27001 auf der Basis IT-Grundschutz nachweisen. Smart Meter Hersteller müssen den Betrieb eines ISMS über ein Sicherheitskonzept, erstellt nach den Vorgaben des IT-Grundschutz, nachweisen.

2.1.3 ISO/IEC TR 27019

Der Standard ISO/IEC TR 27019 fokussiert Systeme und Netzwerke zur Steuerung und Überwachung von Anlagen, deren Ziel und Zweck die Erzeugung, Übertragung und Verteilung von Strom, Gas sowie Wärme ist. Hierbei werden auch Systeme berücksichtigt, die sich mit der Steuerung unterstützender Prozesse befassen. Diese umfassen Leit- und Automatisierungssysteme, Schutz- und Safetysysteme sowie die Messtechnik inklusive der zugehörigen Kommunikations- und Fernwirktechnik. [DINS12]

2.2 Technische Richtlinie BSI TR-03109-2

Die Technische Richtlinie BSI TR-03109-2 spezifiziert die Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls für das SMGW. Hierzu beschreibt die Richtlinie konkret den Lebenszyklus des Sicherheitsmoduls inklusive der jeweils wesentlichen Aufgaben, der beteiligten Rollen und des relevanten Schlüssel- und Zertifikatsmaterials. Zusätzlich werden die Spezifikation des File- und Objektsystems, die Zugriffsregeln und das Kommandosets des Sicherheitsmoduls detailliert erläutert. Sicherheitstechnische Anforderungen an das Sicherheitsmodul selbst werden durch das Common Criteria Schutzprofil BSI-CC-PP-0077 festgelegt. [BSIT13c]

2.2.1 Common Criteria Schutzprofil BSI-CC-PP-0077

Das Common Criteria Schutzprofil BSI-CC-PP-0077 schreibt die geeignete Erfassung der Sicherheitsfunktionalität des Sicherheitsmoduls des SMGW vor. Dies beinhaltet die kryptographische Absicherung der Kommunikationsflüsse zwischen dem SMGW, den übrigen Komponenten sowie den beteiligten Parteien des Smart-Metering-Systems. Das hierfür verantwortliche Sicherheitsmodul dient als sicherer Speicher für das erforderliche Schlüsselmaterial. Zusätzlich stellt das Sicherheitsmodul die Kernroutinen für Signaturerstellung und -prüfung, Schlüsselgenerierung, Schlüsselaushandlung sowie Zufallszahlengenerierung für das SMGW bereit. [BSIP13b]

2.3 Technische Richtlinie BSI TR-03109-3

Die Technische Richtlinie BSI TR-03109-3 beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in der Infrastruktur von Messsystemen im Energiesektor. Die Richtlinie selbst befindet sich derzeit noch in der Abstimmungsphase und verweist daher auf die Technische Richtlinie BSI TR-03116-3. [BSIT13d]

2.3.1 Technische Richtlinie BSI TR-03116-3

Die Technische Richtlinie BSI TR-03109-4 gibt verbindlich die einzusetzenden kryptographischen Verfahren sowie die zu verwendenden Schlüssellängen für die Absicherung der Infrastruktur von intelligenten Messsystemen im Energiesektor vor. Diese Vorgaben basieren auf Prognosen über die Sicherheit der verwendeten kryptographischen Verfahren und Schlüssellängen über einen Zeitraum von 6 Jahren. [BSIT14]

2.4 Technische Richtlinie BSI TR-03109-4

Die Technische Richtlinie BSI TR-03109-4 spezifiziert die Architektur sowie die Mindestanforderungen an die Interoperabilität und Sicherheit der Smart Metering - Public Key Infrastruktur (SM-PKI), mit der die Authentizität der bei der Kommunikation eingesetzten öffentlichen

Schlüssel der Kommunikationspartner auf Weitverkehrsnetz-Ebene sichergestellt wird. Der Authentizitätsnachweis der Schlüssel wird über digitale Zertifikate aus der SM-PKI realisiert. Zertifikate werden dabei ausschließlich für die Schlüssel von Maschinen ausgestellt. [BSIT13e]

3 Aufbau eines ISMS nach BSI IT-Grundschutz

SMGW sowie das interne Sicherheitsmodul werden gemäß Common Criteria mit EAL4+ in einer überaus hohen Vertrauenswürdigkeitsklasse, aufgrund von Datenschutz sowie sämtlichen Aspekten der Versorgungssicherheit, geprüft. Damit dieses hohe Maß an Sicherheit auch für die Betreiber von SMGW gilt, fordert der Anhang V der technischen Richtlinie TR-03109-1 [BSIT13b], dass der SMGW Betreiber ein ISMS nach ISO/IEC 27001 implementieren, betreiben und dokumentieren muss. Ergänzend dazu müssen die Standards DIN 27009 sowie ISO/IEC TR 27019 berücksichtigt werden, soweit die dort definierten Maßnahmen auf die Aufgaben und Betriebsprozesse des SMGW Betreibers anwendbar sind.

Die IT-Grundschutz-Vorgehensweise (vgl. [BSII08a]) beschreibt einen Anwendungsansatz für die Etablierung und Aufrechterhaltung eines ISMS auf der IT-Grundschutz-Methodik und den IT-Grundschutz-Katalogen. Grundlage für den zertifizierungsfähigen Betrieb eines ISMS konform den Vorgaben des IT-Grundschutz, ist die Erstellung eines Sicherheitskonzepts, welches die folgenden acht Schritte der Grundschutzvorgehensweise referenziert:

1. Definition Informationsverbund
2. Strukturanalyse
3. Schutzbedarfsfeststellung
4. Modellierung
5. Basissicherheitscheck
6. Ergänzende Sicherheitsanalyse
7. Risikoanalyse
8. Realisierungsplanung und IT-Sicherheitskonzept

Im Folgenden werden die Schritte zum Aufbau bzw. der Aufrechterhaltung eines ISMS detailliert erläutert.

Definition Informationsverbund

Der Informationsverbund stellt die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen, dar. [BSII08a]

Ein Informationsverbund kann aus der gesamten IT einer Institution bestehen oder auch einzelner Bereiche (z.B. Kernprozesse), die durch organisatorische Strukturen (z.B. Abteilungsnetz) oder gemeinsame IT-Anwendungen (z.B. Personalinformationssystem) gegliedert sind, umfassen. [BSII08a] Die folgenden Aspekte müssen für die Definition des Informationsverbundes berücksichtigt werden:

- die vorhandene Infrastruktur,
- die organisatorischen und personellen Rahmenbedingungen für den Informationsverbund,
- im Informationsverbund eingesetzte vernetzte und nicht-vernetzte IT-Systeme,
- die Kommunikationsverbindungen zwischen den IT-Systemen sowie nach außen und

- im Informationsverbund betriebene Anwendungen.

Strukturanalyse

Ziel der Strukturanalyse ist die genaue Kenntnis der im festgelegten Informationsverbund vorhandenen IT, ihrer organisatorischen und personellen Rahmenbedingungen sowie ihrer Anwendungen. Die Strukturanalyse dient der Erhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines Sicherheitskonzepts nach IT-Grundschutz benötigt werden. [BSII08a]

Folgende Schritte werden während der Strukturanalyse gemeinsam mit den jeweiligen verantwortlichen System- bzw. Anwendungsbetreuern durchgeführt:

- Erstellung und Auswertung des Netzplans,
- Identifizieren der Komponenten im Netzplan,
- Erhebung der IT-Systeme,
- Abgleich der IT-Systeme mit dem Netzplan,
- Erhebung der IT-Anwendungen und der zugehörigen Informationen,
- Erhebung der Abhängigkeiten zwischen den Anwendungen,
- Zuordnung der Anwendungen zu den IT-Systemen,
- Erfassung der IT-Räume und Gebäude,
- Erfassung aller relevanten IT-Räume und Gebäude,
- Komplexitätsreduktion durch Gruppenbildung und
- Erstellung eines bereinigten Netzplanes.

Schutzbedarfsfeststellung

Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse oder Verfahren, die dabei verarbeiteten Informationen und die eingesetzte IT ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. [BSII08a]

Modellierung

Bei der Modellierung werden der definierte Informationsverbund und seine einzelnen Komponenten mit Hilfe der Grundschutzbausteine nachgebaut. Das Ergebnis ist ein IT-Grundschutz-Modell, wobei sämtlichen innerhalb der Strukturanalyse erfassten Komponenten entsprechende IT-Grundschutzbausteine zugewiesen werden (z.B. Baustein B 3.212 Client unter Windows 7). Jeder Baustein besteht aus einer Menge an Gefährdungen und Maßnahmen, welche ab diesem Zeitpunkt für die jeweilige Komponente gelten. [BSII08a] Das resultierende IT-Grundschutz-Modell folgt dem folgenden Schichtmodell:

- Übergreifende Aspekte:
  Betreffen grundsätzliche organisatorische Aspekte der IT-Sicherheit und gelten in der Regel für den gesamten IT-Verbund.
- Infrastruktur:
  Behandeln baulich-technische Fragen und dienen insbesondere dem physischen Schutz etwa vor Feuer, Wasser oder Diebstahl.

- IT-Systeme:
  Beschreiben die Sicherheitsaspekte von IT-Systemen.
- Netze:
  Beschreiben die Sicherheitsaspekte von Netzen wie beispielweise WLAN oder VPN.
- IT-Anwendungen:
  Behandeln Aspekte zur Sicherheit ausgewählter Anwendungen.

Basissicherheitscheck

Der Basissicherheitscheck dient dazu, die bereits umgesetzten Maßnahmen mit den Empfehlungen der IT-Grundschutz-Kataloge zu vergleichen, um das erreichte IT-Sicherheitsniveau zu identifizieren, Verbesserungsmöglichkeiten aufzuzeigen und die Planung ihrer Umsetzung einzuleiten. [BSII08a] Die Erhebung des Basissicherheitschecks erfolgt in Form eines Interviews des jeweiligen Objekt-/Ressourcenverantwortlichen. Hierzu werden die Maßnahmen des jeweiligen Bausteins, für den die Interviewpartner zuständig sind, der Reihe nach durchgearbeitet und hinsichtlich des Umsetzungsstatus wie folgt bewertet:

- Umgesetzt
  Alle Empfehlungen in der Maßnahme sind vollständig und wirksam umgesetzt.
- Nicht umgesetzt
  Die Empfehlungen der Maßnahme sind größtenteils noch nicht umgesetzt.
- Teilweise umgesetzt
  Einige der Empfehlungen sind umgesetzt, andere noch nicht oder nur teilweise.
- Umsetzung entbehrlich
  Die Umsetzung der Maßnahmenempfehlungen ist in der vorgeschlagenen Art nicht notwendig, da den entsprechenden Gefährdungen mit anderen adäquaten Maßnahmen entgegengewirkt wird (z.B. durch Maßnahmen, die nicht im IT-Grundschutz aufgeführt sind, aber dieselbe Wirkung erzielen), oder die Maßnahmenempfehlungen nicht relevant sind (z.B. weil entsprechende Dienste nicht aktiviert wurden).

Ergänzende Sicherheitsanalyse / Risikoanalyse

In einer ergänzenden Sicherheitsanalyse wird geprüft, wie diejenigen Zielobjekte zu behandeln sind, die mindestens eines der folgenden Kriterien erfüllen:

- ein hoher Schutzbedarf existiert oder
- existierende Standardmaßnahmen sind unzureichend oder
- Einsatzszenarien möglich sind, die im Rahmen der Standardmaßnahmenpakete nicht berücksichtigt wurden.

Diese Überlegungen können zu dem Ergebnis führen, dass die Umsetzung der IT-Grundschutz-Maßnahmen genügt, sie können aber auch einen Bedarf an zusätzlichen oder höherwertigen Maßnahmen aufzeigen. [BSII08a]

Risikoanalyse

Im Rahmen der anschließenden Risikoanalyse muss bei allen an der Administration von SMGW beteiligten Daten, Anwendungen und Systemen des Informationsverbundes von einem hohen Schutzbedarf für die drei Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit ausgegangen werden. Die Risikoanalyse hat die Aufgabe, relevante Gefährdungen zu identifizieren und vorhandene Risiken für die Schutzobjekte abzuschätzen. Dabei muss der SMGW Betreiber,

bei der Anwendung des BSI Standard 100-3, mindestens die elementaren Gefährdungen berücksichtigen und die Abdeckung des hohen Schutzbedarfs explizit begründen. Ziel ist es, das im IT-Grundschutz vorgegebene Sicherheitsniveau zu erreichen und kontinuierlich zu verbessern. Daher müssen der Sicherheitsprozess und die Organisationsstrukturen für Informationssicherheit regelmäßig (mindestens jährlich) daraufhin überprüft werden, ob sie angemessen, wirksam und effizient sind. Ebenso muss sichergestellt werden, dass die Maßnahmen praxisnah sind und korrekt umgesetzt wurden. [BSIT13a]

Realisierungsplanung und IT-Sicherheitskonzept

Nach Abschluss des im Rahmen des Basissicherheitscheck durchgeführten Soll-Ist-Vergleichs werden die noch nicht oder nur teilweise umgesetzten Maßnahmen betrachtet und daraufhin analysiert, welche Maßnahmen technisch und welche organisatorisch (z.B. Richtlinien) umgesetzt werden sollten.

Möglicherweise ergeben sich aus der Risikoanalyse noch zusätzliche Maßnahmen, welche im Umsetzungsplan mit beachtet werden müssen. In einem priorisierten Maßnahmenkatalog sollte eine sinnvolle Umsetzungsreihenfolge definiert werden.

Das IT-Sicherheitskonzept besteht aus den wesentlichen Dokumenten der acht Schritte der IT-Grundschutzvorgehensweise und bildet die Grundlage für ein zertifizierungsfähiges ISMS im Smart Meter Umfeld.

4 Zusammenfassung

Der vorliegende Artikel fasst sowohl die Anforderungen für die Komponenten im Smart Meter Umfeld also auch für den Betrieb eines SMGW zusammen und integriert diese in ein zwingend nach IT-Grundschutz zertifizierungsfähiges ISMS. Die explizite Forderung nach dem Betrieb eines zertifizierten ISMS nach BSI IT-Grundschutz birgt jedoch einen Nachteil für Unternehmen, die über eine native ISO/IEC 27001 Zertifizierung, welche ebenfalls den Betrieb eines ISMS nachweist, verfügen. Die Technische Richtlinie BSI TR-03109 erkennt derzeit ein ISMS, welches ISO/IEC 27001 native zertifiziert wurde nicht als ausreichend an. Das BSI arbeitet derzeit an einer Lösung, um auch zukünftig Unternehmen mit einer nativen ISO/IEC 27001 Zertifizierung den Betrieb von Smart Meter Gateways zu ermöglichen.

Literatur

[BSIT13a] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie BSI TR-03109“ (2013)

[BSIT13b] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie BSI TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems“ (2013)

[BSIA13] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie BSI TR-03109-1, Anlage V: Anforderungen zum Betrieb beim Administrator“ (2013)

[BSIT13c] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie BSI TR-03109-2, Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls“ (2013)

[BSIT13d] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie BSI TR-03109-3, Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen“ (2013)

[BSIT13e] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie BSI TR-03109-4, Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways“ (2013)

[BSIT14] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie BSI TR-03116-3, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3 - Intelligente Messsysteme“ (2014)

[BSIP13a] Bundesamt für Sicherheit in der Informationstechnik, „BSI-CC-PP-0073, Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen“ (2013)

[BSIP13b] Bundesamt für Sicherheit in der Informationstechnik, „BSI-CC-PP-0077, Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen“ (2013)

[ISOI13a] ISO/IEC 27001:2013, „Information security management systems Requirements“ (2013)

[ISOI13b] ISO/IEC 27002:2013, „Code of practice for information security controls“ (2013)

[ISOT13] ISO/IEC TR 27019:2013(E), „Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry“ (2013)

[DINS12] DIN SPEC 27009:2012, „Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002“ (2012)

[BSII08a] Bundesamt für Sicherheit in der Informationstechnik, „BSI Standard 100-2, IT-Grundschutz-Vorgehensweise“, Version 2.0 (2008)

[BSII08b] Bundesamt für Sicherheit in der Informationstechnik, „BSI Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz“, Version 2.5 (2008)