Leitfaden zum sicheren Betrieb von Smart Meter Gateways

Wer Smart Meter Gateways verwaltet, muss die IT-Sicherheit seiner dafür eingesetzten Infrastruktur nachweisen. Diesen Nachweis erbringt ein Gateway-Administrator durch die Vorlage eines BSI-Zertifikats nach ISO 27001 auf Basis von IT-Grundschutz.

Die Standard-Reihe „BSI-Standard 100-x“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist eine Sammlung von Standards für Managementsysteme zur IT-Sicherheit (Information Security Management Systems, ISMS).

Die Standards stellen eine praktische Methode zur Bewertung und Dokumentation aller Aspekte der IT-Sicherheit einer IT-Landschaft vor und geben detaillierte Handlungsanweisungen zur Aufrechterhaltung und Verbesserung der IT-Sicherheit. Die Vorgehensweise auf Basis von IT-Grundschutz eignet sich für „typische“ IT-Landschaften mit einem „normalen“ Schutzbedarf. Maßnahmen für höheren Schutzbedarf können, je nach Bedarf, ergänzt werden.

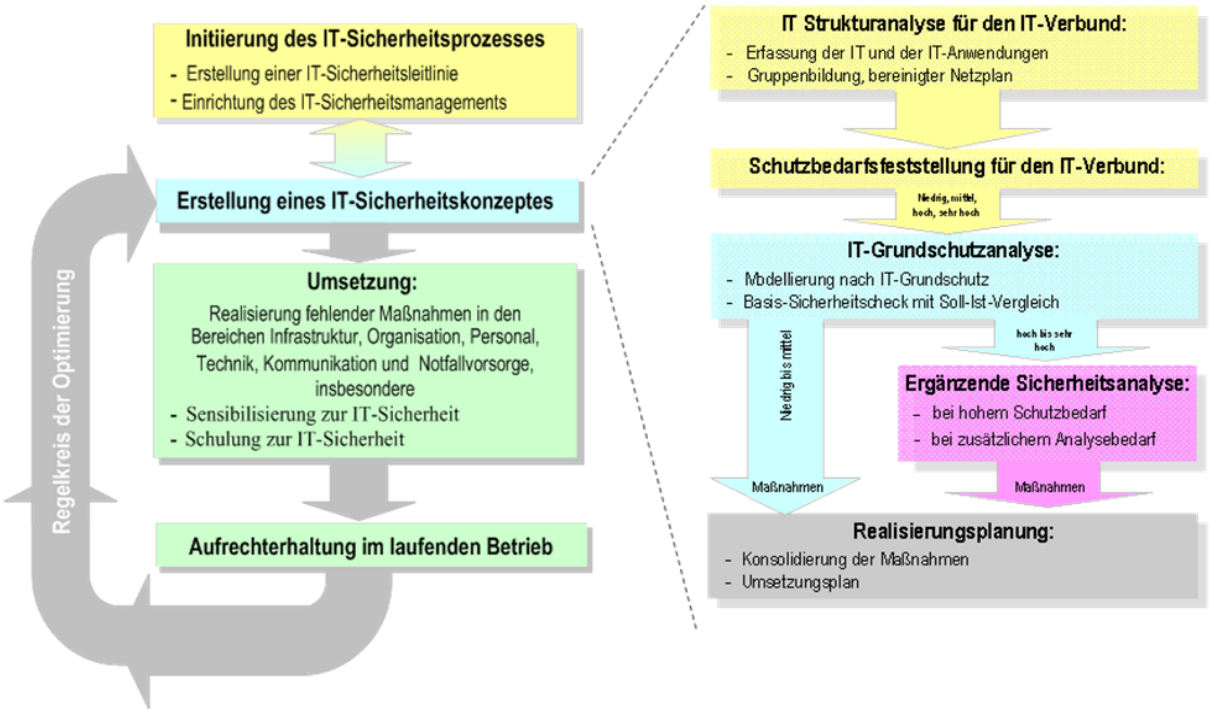
Nach einem erfolgreichen Audit mit anschließender Zertifizierung wird ein BSI-Zertifikat „ISO 27001 auf der Basis von IT-Grundschutz“ vergeben.

Mit diesem BSI-Zertifikat können z. B. Smart Meter Gateway Administratoren die Eignung ihrer IT-Infrastruktur für einen sicheren Betrieb nachweisen, dessen Anforderungen in der Technischen Richtlinie BSI-TR-03109 (Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems) formuliert sind, die das BSI spezifiziert hat.

Die Reihe „BSI-Standard 100-x“ besteht aus den folgenden Teilen:

- 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
- BSI-Standard 100-4: Notfallmanagement
- IT-Grundschutzkataloge: Baustein-Kataloge (B1 bis B5), Gefährdungskataloge (G0 bis G5), Maßnahmenkataloge (M1 bis M6)
- GSTOOL: IT-Grundschutz-Tool, Programm zur Unterstützung der Umsetzung von Maßnahmen

Für eine BSI-Zertifizierung sind zunächst die Anforderungen aus BSI-Standard 100-2 umzusetzen und nachzuweisen. BSI-Standard 100-2 verlangt die **Realisierung eines ISMS** (siehe folgende Abbildung):



Quelle: Darstellung nach Informationen aus BSI-Standard 100-2

Das geforderte **ISMS** wird in den folgenden Schritten 1) bis 5) realisiert:

1. Initial muss das verantwortliche Management eine **IT-Sicherheitsleitlinie** erstellen, in der festgelegt wird, „**WAS**“ zur IT-Sicherheit zu tun ist (Ziele). Es muss ein Sicherheitsgremium eingerichtet werden und mit Ressourcen (Personal, Zeit, Budget) ausgestattet werden.
2. Dann muss ein **IT-Sicherheitskonzept** erstellt werden, in dem festgelegt wird, „**WIE**“ die Ziele der IT-Sicherheit zu erreichen sind (Wege). Das IT-Sicherheitskonzept hat als Ergebnis einen Umsetzungsplan.
3. **Umsetzung** der Maßnahmen zur IT-Sicherheit nach Umsetzungsplan.
4. Änderungen im **laufenden Betrieb** müssen erkannt und dadurch notwendige Änderungen der IT-Sicherheit berücksichtigt werden. Das IT-Sicherheitskonzept muss eventuell aktualisiert werden.
5. Damit schließt sich der Sicherheitsregelkreis der permanenten Verbesserung des ISMS.

Das **IT-Sicherheitskonzept** als Kernkomponente erstellt man wie folgt:

1. Initial muss durch die **IT-Strukturanalyse** die vorhandene IT-Landschaft erfasst, geeignet aufbereitet und dokumentiert werden (IST-Analyse). Beginnend mit den Geschäftsprozessen, werden die IT-Anwendungen, IT-Netze, IT-Systeme und IT-Infrastruktur dokumentiert (Vorhandene Unterlagen, Reviews der Mitarbeiter) und als IT-Verbund dargestellt. In diesem IT-Verbund werden Daten verarbeitet, die Werte darstellen und geschützt werden sollen.

2. Für die **zu schützenden Daten** muss der angemessene **Schutzbedarf** in den Kategorien (normal=überschaubare Schäden, hoch=erhebliche Schäden, sehr hoch=bedrohliche Schäden) festgelegt werden. Aus dem Schutzbedarf der Daten ergeben sich Anforderungen an den IT-Verbund (Vererbungsprinzip). Werden Daten unterschiedlichen Schutzbedarfs an einer Stelle des IT-Verbunds verarbeitet, bestimmen die Daten mit dem höchsten Schutzbedarf die notwendigen Schutzmaßnahmen (Maximumsprinzip).
   Die Technische Richtlinie BSI-TR-03109 geht von einem **hohen** Schutzbedarf aus.

3. Der erfasste und dokumentierte IT-Verbund, der die zu schützenden Daten verarbeitet, wird nun **nach IT-Grundschutz modellier**t. Dazu werden die **IT-Grundschutzkataloge** benutzt.

   Für die verschiedenen **Bausteine Bi** (i=Übergreifende Aspekte, Infrastruktur, IT-Systeme, Netze, Anwendungen) aus den Bausteinkatalogen werden zu den möglichen **Gefährdungen Gi** (i=Elementare Gefährdungen, höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen, vorsätzliche Handlungen) aus den Gefährdungskatalogen die erforderlichen **Maßnahmen Mi** (i=Infrastruktur, Organisation, Personal, Hardware und Software, Kommunikation, Notfallvorsorge) aus den Maßnahmenkatalogen zugeordnet.

   Die Maßnahmen sind zum Einen gekennzeichnet, wo sie im Lebenszyklus des Geschäftsprozesses vorkommen: Planung und Konzeption (PK), Beschaffung (B), Umsetzung (U), Betrieb (B), Aussonderung (A), Notfallvorsorge (N).

   Die Maßnahmen sind zum Anderen gekennzeichnet, wie ihre Qualifizierungsstufe (Wichtigkeit) ist: Einstieg (A), Aufbau (B), Zertifikat (C), Zusätzlich (Z) und Wissen (W).

4. **Maßnahmen der Stufe A** sind essentiell und vorrangig umzusetzen zum Erhalt des Auditor-Testats IT-Grundschutz Einstiegsstufe.

   Maßnahmen der Stufe B sind ergänzend für das Auditor-Testat IT-Grundschutz Aufbaustufe umzusetzen.

   Maßnahmen der Stufe C (mit den Stufen A und B) sind für das ISO 27001-Zertifikat auf Basis von IT-Grundschutz umzusetzen.

   Zur Unterstützung der Erstellung der Zuordnungsmatrix (Gefährdungen vs. Maßnahmen) kann das GSTOOL eingesetzt werden. Als Ergebnis erhält man einen (in der Regel umfangreichen) **spezifischen Maßnahmenkatalog**.

   Durch einen **Basis-Sicherheitscheck** wird dieser spezifische Maßnahmenkatalog einem SOLL-IST-Vergleich unterzogen. Dabei wird für jede vorgesehene Maßnahme ermittelt, ob die Maßnahme bereits umgesetzt, teilweise umgesetzt, noch nicht umgesetzt oder begründet entbehrlich ist.

5. Ist der Schutzbedarf der Daten höher als normal (also hoch bis sehr hoch), muss zusätzlich eine **ergänzende, spezifische Sicherheitsanalyse** vorgenommen werden, da die Gefährdungen und Maßnahmen der IT-Grundschutzkataloge nur für „typische“ IT-Verbünde mit „normalem“ Schutzbedarf ausgelegt sind.

6. Der resultierende spezifische Maßnahmenkatalog wird für die Realisierungsplanung benutzt. Darin wird festgelegt, wie und wann die noch umzusetzenden Maßnahmen (oder Teile davon) realisiert werden können.

Zu Planung, Realisierung und Nachweis aller Anforderungen ist **zum Teil umfangreiche Dokumentation** anzufertigen und zu Audits und Zertifizierung vorzulegen.

Danach können Audits (mit Auditor-Testaten) durch anerkannte Auditoren und die Zertifizierung (mit BSI-Zertifikat) stattfinden.

Unser Beratungsangebot für Sie:

mtG kann Sie bei der Planung und Durchführung aller oben geschilderten Schritte, insbesondere der Erstellung des IT-Sicherheitskonzepts, zum Erreichen eines BSI-Zertifikats “ISO 27001 auf der Basis von IT-Grundschutz“ beratend unterstützen.

Wir freuen uns auf Ihren Kontakt!

Telefon: 06151/8193-0
E-Mail: contact@mtg.de

Mehr Informationen zu unserer Prüfstelle für IT Sicherheit finden auf unserer Webseite:

http://www.mtg.de/it-security/pruefstelle-it-sicherheit:

media transfer AG
Firmensitz: Dolivostr. 11, 64293 Darmstadt
Registergericht: Amtsgericht Darmstadt, HRB 8901
Vorstand: Jürgen Ruf (Vors.), Tamer Kemeröz
Aufsichtsratsvorsitzender: Dr. Thomas Milde
www.mtg.de