www.pwc.de

Technische Vorgaben zur Gewährleistung von Datenschutz und Informationssicherheit durch den Einsatz von Smart Meter Gateways

8. Dezember 2015

pwc

Agenda

1. Einführung
2. Begriffsdefinitionen und Grundsätze zu Datenschutz & Informationssicherheit
3. Die energiewirtschaftliche Systemlandschaft
4. Regelungswerke mit Bezug zu Datenschutz und Informationssicherheit im Kontext Smart Metering und deren wesentliche Inhalte
5. Ausgewählte Risiken für EVUs aus dem neuen MsbG
6. Zusammenfassung und Fazit

Einführung

Cyberbedrohungen für EVUs sind real

„Der Quellcode von Stuxnet und seinen deutlich mehr als zehn Derivaten ist im Internet verfügbar und kann mit geringem Aufwand an andere Ziele wie Kraftwerke und Stromverteilung angepasst werden [..]. Er kann damit auch eine Gefahr für Leib und Leben von Bundesbürgern darstellen.“ - Gesellschaft für Informatik, 26.06.2013

SPIEGEL ONLINE

Hacker-Angriff:
USA warnen vor Cyber-Sabotage bei Energiekonzernen

Der US-Heimatschutz ist alarmiert. Die Behörde meldet neue Cyber-Angriffe gegen amerikanische Unternehmen. Den Angreifern geht es dabei nicht um Spionage. Stattdessen suchen sie offenbar Sicherheitslücken, um die Energieversorgung des Landes lahmzulegen.

Von Matthias Kremp — Montag, 13.05.2013 – 15:09 Uhr

U.S. DEPARTMENT OF DEFENSE

Clapper Places Cyber at Top of Transnational Threat List

By Jim Garamone
American Forces Press Service

WASHINGTON, March 12, 2013 – Ten years ago, the idea that cyber posed a leading threat against the United States would be laughed at. But no one is laughing any more.

James R. Clapper, the director of national intelligence, testified before the Senate Select Committee on Intelligence today, and cyber led off his presentation of transnational threats.

OSZE — 12.7.2013, 20:45

golem.de IT-NEWS FÜR PROFIS

Cyberangriffe gefährden Energieversorgung

Cyber-Angriffe auf kritische Infrastruktur sind heute schon Realität. Die OSZE hat ein Rahmenwerk von Maßnahmen vorgelegt, die die Energieversorgung vor Schadsoftware wie Stuxnet schützen soll.

Frankfurter Allgemeine

Trojaner „stuxnet“

Der digitale Erstschlag ist erfolgt

Fieberhaft arbeiten die besten Sicherheitsexperten der Welt an der Analyse eines völlig neuartigen Computervirus. Jetzt legen erste Indizien einen erstaunlichen Verdacht nahe: Offenbar hat die digitale Waffe das iranische Atomprogramm sabotiert.

22.09.2010, von FRANK RIEGER

WIRTSCHAFT STROMVERSORGER — DIE WELT

Russische Hacker attackieren Stromnetzbetreiber

50 Hertz betreibt und überwacht die Stromnetze in Berlin, Hamburg und großen Teilen Ostdeutschlands. Das Unternehmen sieht sich Angriffen aus Osteuropa und Russland ausgesetzt.

Cyberattack on Energy Sector would be 'Devastating'

By Daniel J. Graeber | Sun, 16 February 2014 00:00 — Oilprice.com

An annual index from IHS Jane's Terrorism and Insurgency Center said acts of violence committed by non-state actors since 2009 increased by more than 150 percent. But for Internet security company Kaspersky Lab, it may be a state actor that launches the next major attack against the energy sector and it may be from a computer.

Hintergrund | 27.09.2011 | — Spektrum

ENERGIEVERSORGUNG

Angriff auf das Stromnetz

Computerviren haben bereits gezielt industrielle Steuerungssysteme infiziert. Als Nächstes könnte das Stromnetz in das Fadenkreuz von Saboteuren geraten.

DAVID M. NICOL

REUTERS

Energy companies need insurance cover for cyber attack 'time bomb'

BY MICHAEL SZABO — LONDON | Tue Apr 8, 2014 11:44am EDT

(Reuters) - Energy companies have no insurance against major cyber attacks, reinsurance broker Willis said on Tuesday, likening the threat to a "time bomb" that could cost the industry billions of dollars.

01.07.2014 | 11:26

Westlicher Energiewirtschaft droht Hacker-Angriff

Berlin - Eine professionell agierende Hacker-Gruppe hat offenbar auf breiter Front die westliche Energiewirtschaft im Visier.

Begriffsdefinitionen und Grundsätze zu Datenschutz & Informationssicherheit

Informationssicherheit und Datenschutz

Informationssicherheit

- Mit Informationssicherheit wird der Schutz von Informationen hinsichtlich gegebener Anforderungen an deren Authentizität, Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet.

Datenschutz

- Datenschutz soll den Einzelnen davor schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
- Mit Datenschutz wird daher der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet

Maßnahmen zur Gewährleistung von Informationssicherheit basieren im Allg. auf vier Zielen

Ziel	Erläuterung
Authentizität	• Zweifelsfreie Identifikation der Geschäftspartner • Identität ist durch geeignete Signaturen sicherzustellen
Integrität	• Unversehrtheit der übermittelten Informationen / Daten • Vollständige, richtige und unveränderte Übermittlung der Daten
Vertraulichkeit	• Geheimhaltung der übermittelten Informationen • Angemessene Verschlüsselung und Zugriffsschutz
Verfügbarkeit	• Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netze sind für Anwender stets verfügbar

Die Ziele gelten sowohl für die Sicherheit des Messsystems (Zähler +Gateway) als auch für die Übertragung der Daten (Kommunikationssicherheit)

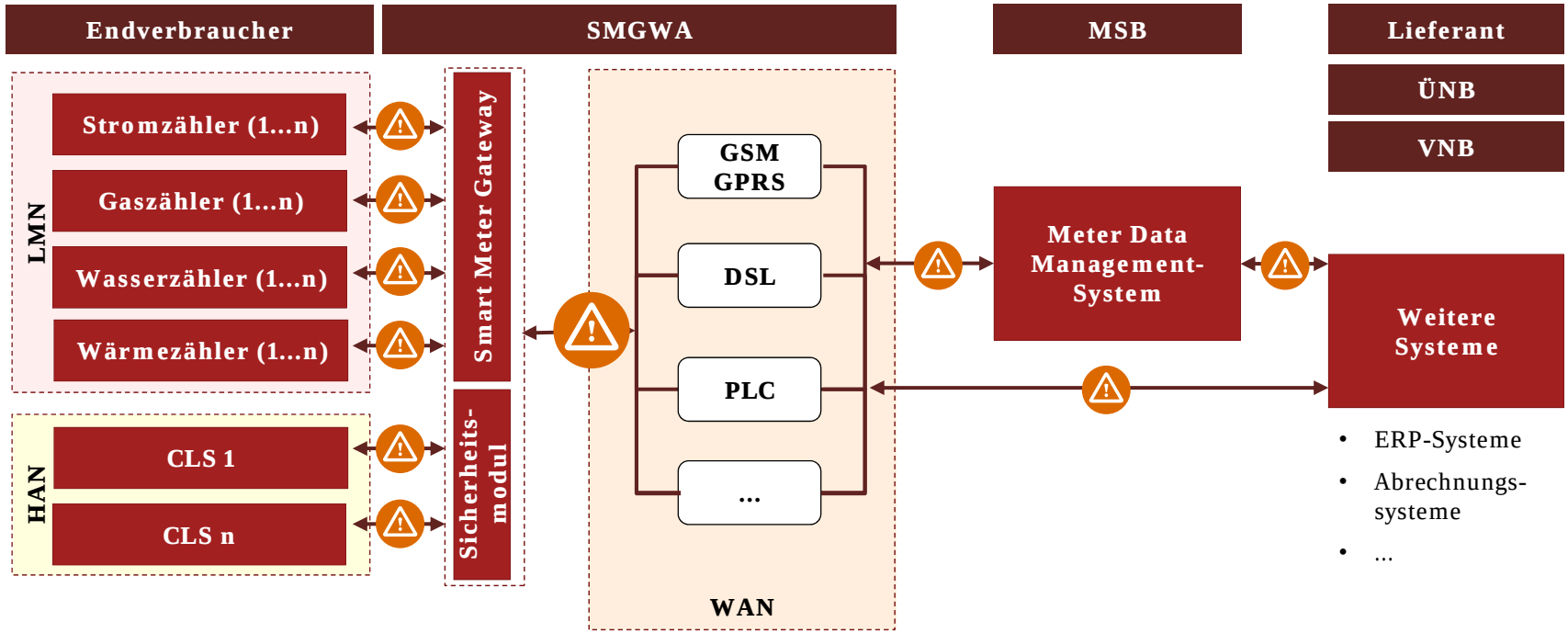
Aus dem Bundesdatenschutzgesetz lassen sich vier Grundsätze des Datenschutzes ableiten

Ziel	Erläuterung
Datenvermeidung & Datensparsamkeit	• Erhebung, Nutzung und Verarbeitung keiner oder so wenig personenbezogener Daten wie möglich
Zweckbindung	• Verwendung personenbezogener Daten nur für festgelegte eindeutige und rechtmäßige Zwecke • Weiterverarbeitung der personenbezogener Daten nur im Rahmen der Zweckbestimmung
Verbot mit Erlaubnisvorbehalt	• Verwendung personenbezogener Daten nur mit Einwilligung des Betroffenen oder im Falle gesetzlicher Erlaubnis bzw. Anordnung
Transparenz	• Einsicht des Einzelnen in die ihn betreffende Datenverarbeitung • Informationspflicht des Datenverarbeiters → Auskunftsrecht des Betroffenen

Die Erfüllung von Datenschutzstandards sollten bereits in frühen Projekt-Entwicklungsphasen berücksichtigt werden („privacy by design“)

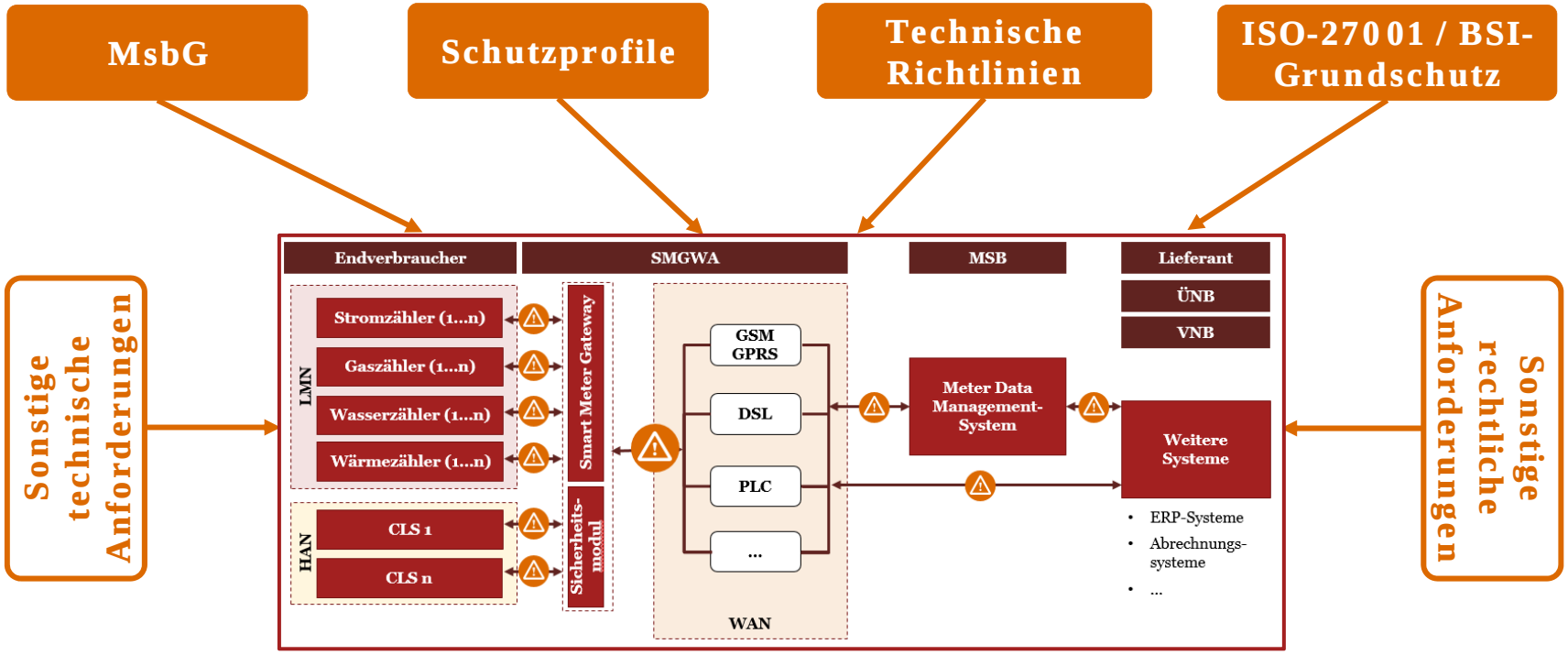
Die energiewirtschaftliche Systemlandschaft

Die energiewirtschaftliche Systemlandschaft weist eine Vielzahl an Schnittstellen auf



Datenschutz- und Informationssicherheitsanforderungen für Schnittstellen sind in verschiedenen rechtlichen & technischen Anforderungen verankert

Die energiewirtschaftliche Systemlandschaft weist eine Vielzahl an Schnittstellen auf

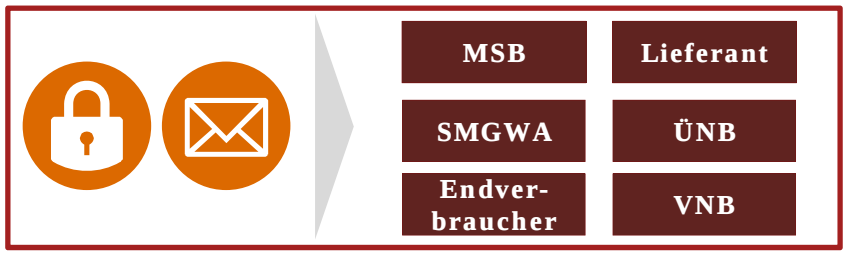


Datenschutz- und Informationssicherheitsanforderungen für Schnittstellen sind in verschiedenen rechtlichen & technischen Anforderungen verankert

Regelungswerke mit Bezug zu Datenschutz und Informationssicherheit im Kontext Smart Metering und deren wesentliche Inhalte

Datenschutz- und Informationssicherheitsaspekte bilden ein Kernziel des neuen MsbG

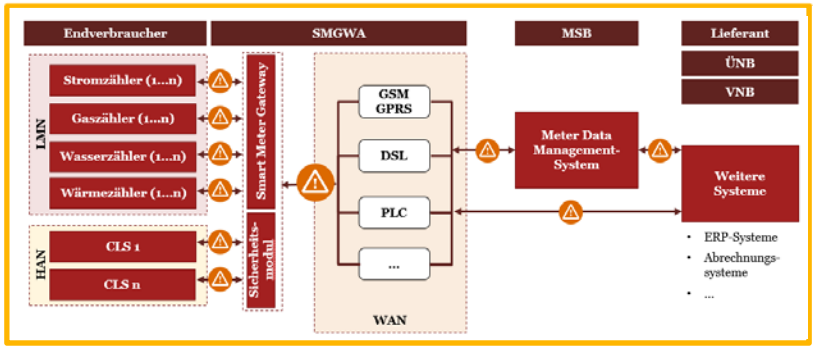
Geltungsbereich MsbG



Insb. Kapitel 3 des MsbG:

- Technische Vorgaben zur Gewährleistung von Datenschutz und Informationssicherheit beim Einsatz von Smart-Meter-Gateways

Implikationen auf die Systemlandschaft

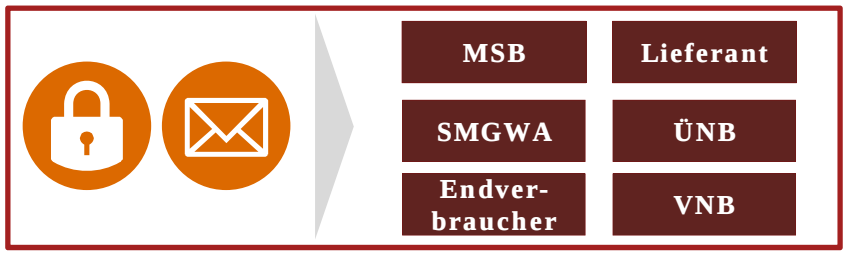


Kerninhalte MsbG zu Informationssicherheit

- Gesetzliche Verankerung der Mindestanforderungen an das Smart-Meter-Gateway durch Schutzprofile und Technische Richtlinien
- Smart-Meter-Gateways müssen nach Common Criteria durch das BSI zertifiziert werden
- SMGWA muss sein ISMS, seine IT-Sicherheitskonzeption und Maßnahmen zur Informationssicherheit und die Erfüllung der technischen und organisatorischen Maßnahmen regelmäßig auditieren lassen
- Keine technologische Festlegung des Fernkommunikationsverfahrens
- Das BSI ist Inhaber der Wurzelzertifikate für die Smart-Metering-Public-Key-Infrastruktur
- BSI und PTB entwickeln Schutzprofile und Technische Richtlinien kontinuierlich weiter

Kerninhalte Datenschutz: Das BSI hat aus dem MsbG 10 Datenschutzanforderungen abgeleitet (1)

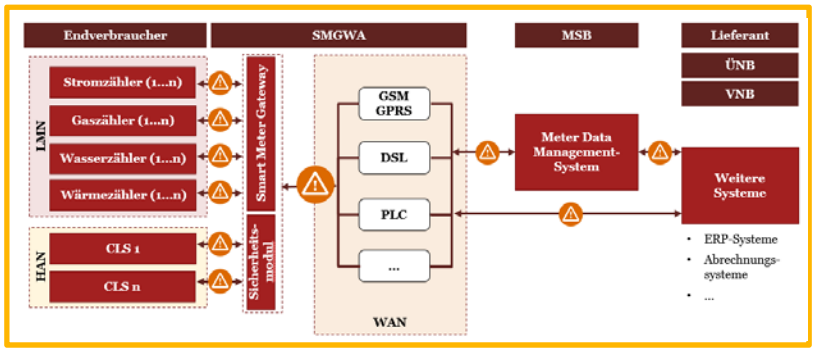
Geltungsbereich MsbG



Insb. Kapitel 3 des MsbG:

- Technische Vorgaben zur Gewährleistung von Datenschutz und Informationssicherheit beim Einsatz von Smart-Meter-Gateways

Implikationen auf die Systemlandschaft



Kerninhalte MsbG zu Datenschutz

Datenerhebung

- Datenerhebung und -nutzung ohne Zustimmung des Verbrauchers nur so weit erlaubt, wie es für energiewirtschaftliche Zwecke erforderlich ist

Ableseintervalle

- Datensparsame Vorgabe von Ableseintervallen, so dass keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können

Vertraulichkeit

- Datenübermittlung erfolgt anonymisiert, pseudonymisiert oder aggregiert

Datenverarbeitung

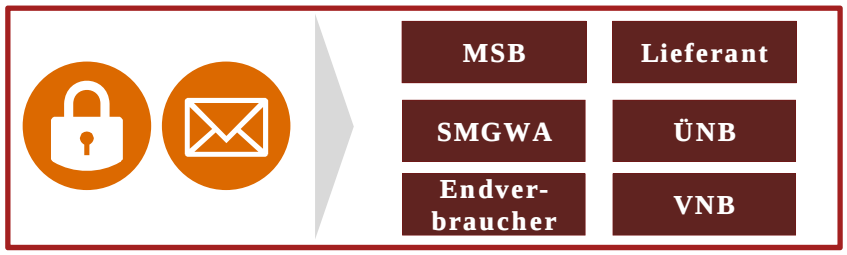
- Lokale Datenverarbeitung beim Verbraucher statt extern

Datenübermittlung

- Übermittlung der Energiedaten an möglichst wenige Stellen

Kerninhalte Datenschutz: Das BSI hat aus dem MsbG 10 Datenschutzanforderungen abgeleitet (2)

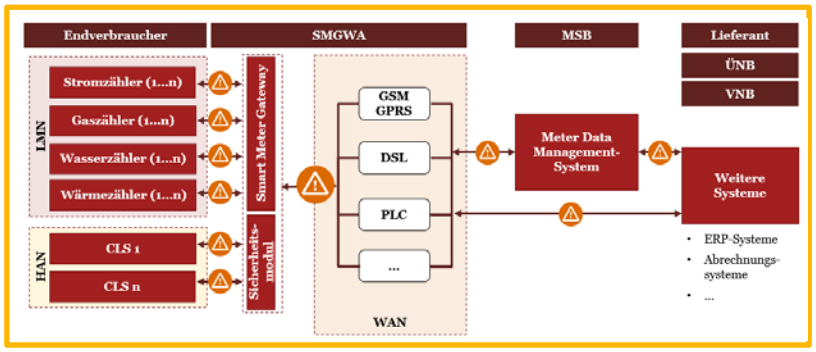
Geltungsbereich MsbG



Insb. Kapitel 3 des MsbG:

- Technische Vorgaben zur Gewährleistung von Datenschutz und Informationssicherheit beim Einsatz von Smart-Meter-Gateways

Implikationen auf die Systemlandschaft



Kerninhalte MsbG zu Datenschutz

Datenlöschung

- Löschung personenbezogener Messwerte, wenn eine Speicherung nicht mehr erforderlich ist

Transparenz

- Kommunikations- und Verarbeitungsschritte sind zu jeder Zeit für den Verbraucher sichtbar und nachweisbar

Datenmissbrauch

- Rechte auf Löschung, Berichtigung und Widerspruch sind durch Logging einfach durchsetzbar

Tarifwahl

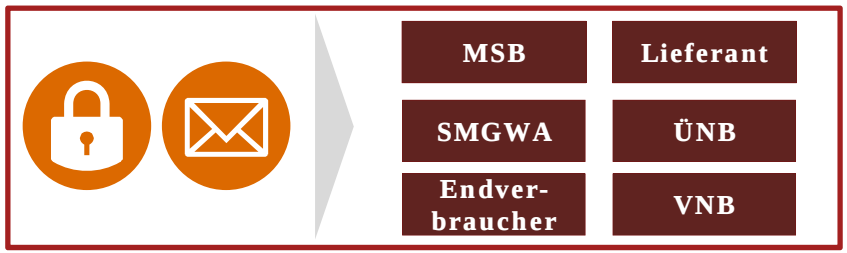
- Die freie Tarifwahl der Letztverbraucher wird nicht eingeschränkt

Zugang zum Smart Meter

- Es werden eindeutige Profile für den berechtigten Zugang definiert

Wer darf personenbezogene Daten zu welchem Zweck nutzen?

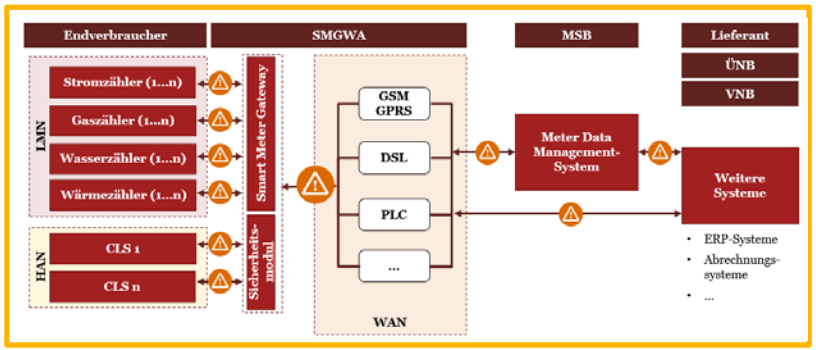
Geltungsbereich MsbG



Insb. Kapitel 3 des MsbG:

- Technische Vorgaben zur Gewährleistung von Datenschutz und Informationssicherheit beim Einsatz von Smart-Meter-Gateways

Implikationen auf die Systemlandschaft



Kerninhalte MsbG zu Datenschutz

Wer darf personenbezogene Daten erheben, verarbeiten, nutzen?

- Messstellenbetreiber
- Netzbetreiber
- Bilanzkoordinatoren
- Bilanzkreisverantwortliche
- Direktvermarktungsunternehmen nach EEG
- Energielieferanten
- Jede Stelle, der Einwilligung vorliegt

Dienstleister darf dies im Auftrag ausführen

Zu welchem Zweck dürfen personenbezogene Daten erhoben, verarbeitet oder genutzt werden?

- Erfüllung von Verträgen
- Vorvertragliche Maßnahmen
- Erfüllung rechtlicher Verpflichtungen
- Erfüllung von Aufgaben im öffentlichen Interesse
- Wahrnehmung einer Aufgabe des Netzbetreibers

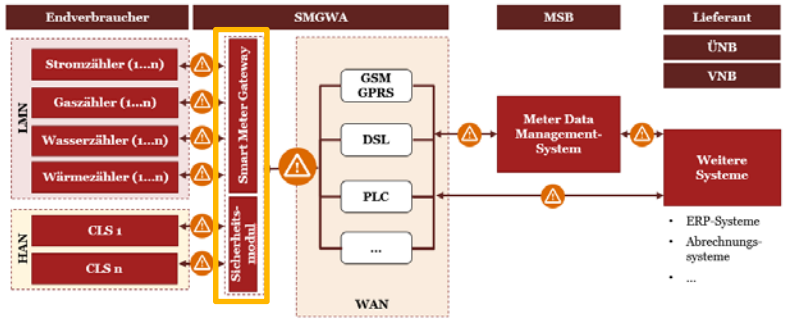
Eingrenzung durch Beispiele in § 50 Abs. 2 MsbG

In Schutzprofilen sind Anforderungen an SMGWs aus den Common Criteria durch das BSI abgeleitet

Geltungsbereich der Schutzprofile

- Schutzprofil BSI-CC-PP-0073: Anforderungen an das Smart-Meter-Gateway
- Schutzprofil BSI-CC-PP-0077: Anforderungen an das Sicherheitsmodul

Implikationen auf die Systemlandschaft



Kerninhalte der Schutzprofile

Definition von ***Risiken***, ***Sicherheitszielen*** und daraus abgeleiteten ***Anforderungen*** an Datenschutz und Informationssicherheit für die Schnittstellen des Smart-Meter-Gateways

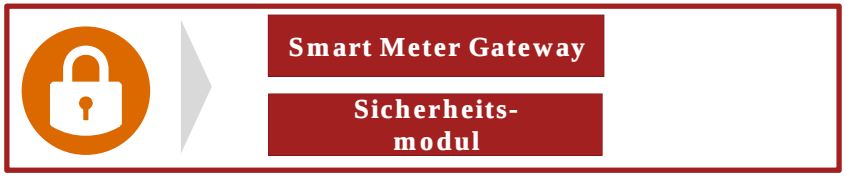
Wesentliche Anforderungen:

- Sicherheitsmodul
- Getrennte physische Schnittstellen
- Kryptographischer Schutz der Schnittstellen u.a. durch Zertifikate
- Beidseitige Authentifizierung (Sender und Empfänger)
- Zeitstempel und gesicherte Zeitsynchronisation
- Logging und Zugriffsschutz

Übergeordnete Ziele sind die Gewährleistung von Datenschutz, Informationssicherheit und Interoperabilität

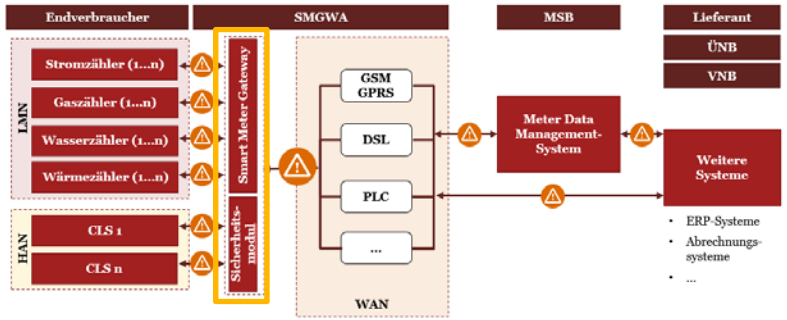
Technische Richtlinien beinhalten Vorgaben zur geeigneten Umsetzung der Schutzprofile

Geltungsbereich der Technischen Richtlinien



- BSI TR-0309-1: Smart Meter Gateway
- BSI TR-0309-2: Sicherheitsmodul für SMGW
- BSI TR-0309-3: Kryptographische Vorgaben
- BSI TR-0309-4: Public Key Infrastruktur
- BSI TR-0309-5: Kommunikationsadapter
- BSI TR-0309-6: Smart Meter Gateway Admin.

Implikationen auf die Systemlandschaft



Kerninhalte der Technischen Richtlinien

Definition von ***Maßnahmen***, ***Prozessen***, ***Schutzanforderungen***, ***Funktionen*** und ***Testspezifikationen***

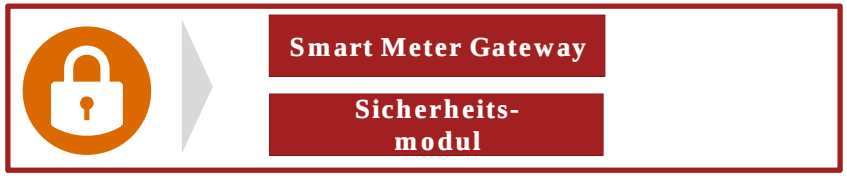
Wesentliche Inhalte:

- Sicherstellung von Interoperabilität
- Betriebsprozesse und organisatorische Mindestanforderungen des SMGWA
- Zertifizierungsverfahren
- Beschreibung der Public Key Infrastruktur
- Beschreibung der Schnittstellen
- Vorgaben zur Verschlüsselung
- Einrichtung, Betrieb und Dokumentation eines ISMS nach ISO 27001 (siehe Folgefolie)

Übergeordnetes Ziel ist die Vorgabe der Umsetzung der Schutzprofile auf technischer und organisatorischer Ebene

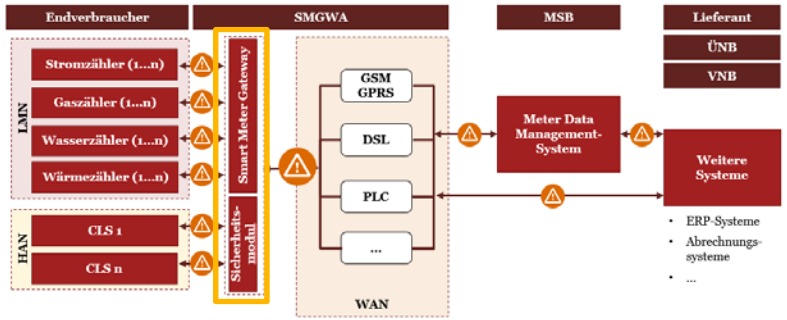
SMGWA haben bei der Zertifizierung ihres ISMS zwei Alternativen

Geltungsbereich ISO 27001 / BSI-Grundschutz



- BSI-Standard 100-1 bis 100-4
- ISO/IEC 27001 nativ

Implikationen auf die Systemlandschaft



Kerninhalte der Technischen Richtlinien

Zur Gewährleistung der IT-Sicherheit ist der SMGWA dazu verpflichtet ein ISMS einzurichten, zu betreiben und zu dokumentieren.

Zwei Standards zur Zertifizierung des ISMS für SMGWA:

a) ISO 27001 auf Basis von IT-Grundschutz (BSI)

- IT-Grundschutz-Vorgehensweise beschreibt Aufbau und Betrieb eines ISMS (siehe auch Folgefolie)
- Risikoorientierter Ansatz zur Ermittlung der zu implementierenden Maßnahmen (über Schutzbedarf)

b) ISO/IEC 27001 nativ

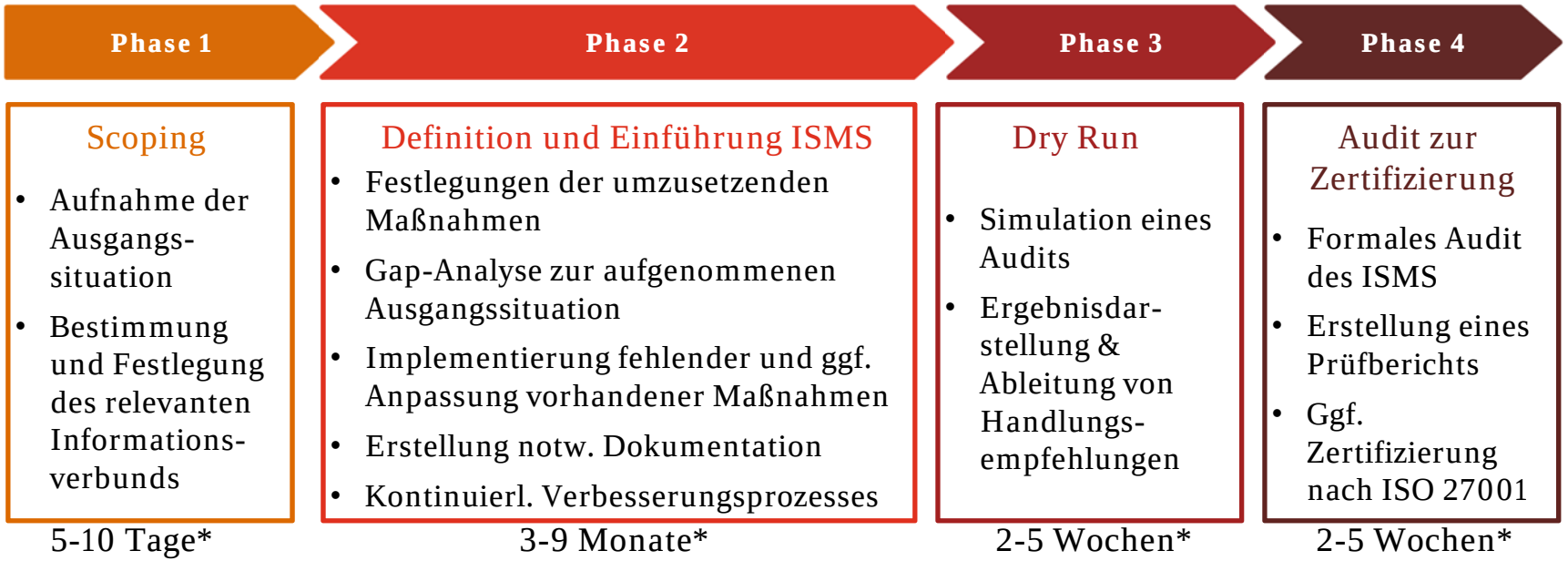
- Weniger detaillierte Definition von Anforderungen an ein ISMS in Form von Maßnahmen

Die Zertifizierung erfolgt durch das BSI oder einen akkreditierten Zertifizierer

Praxisbeispiel

Der Aufbau eines ISMS ist eine komplexe Herausforderung für den SMGWA!

Die Hauptaufgabe eines ISMS besteht darin, einen geregelten Prozess zu etablieren, der sich fortlaufend mit den bestehenden und neuen Sicherheitsbedrohungen für das Unternehmen auseinandersetzt und darauf reagiert.



**Die Aufwandsschätzung ist beispielhaft und hängt vom Geltungsbereich eines ISMS und den schon bestehenden Prozessen ab.*

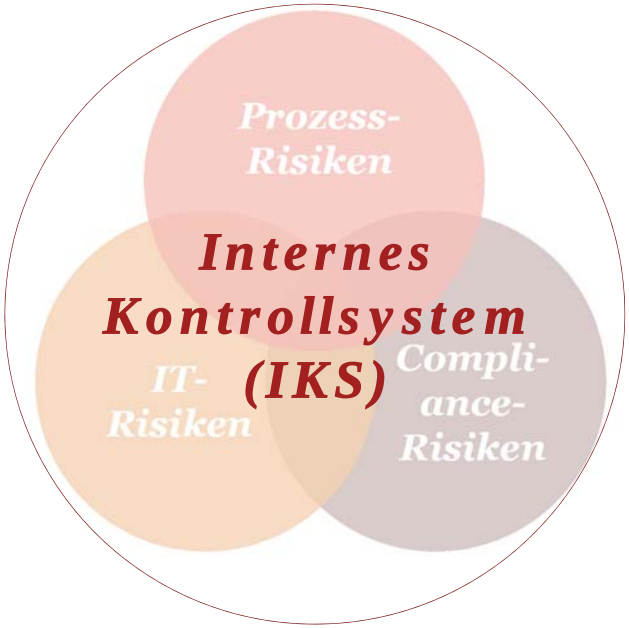
Ausgewählte Risiken für EVUs aus dem neuen MsbG

Die neuen Risiken lassen sich in IT- und Compliance-Risiken clustern

	IT-Risiken	Compliance-Risiken	Mögliche Kontrollen
MSB / SMGWA	• Betriebsstörungen • Angriffe von außen • Unvollständige oder falsche Messdatenübermittlung	• Anforderungen von Auditoren und Zertifizierern an ISMS nicht erfüllt • Keine fristgerechte Umsetzung der regulatorischen Anforderungen	• Wirksame Plausibilisierungs-mechanismen • Schnittstellenmonitoring • Integration der organisa-torischen Maßnamen zum ISMS in Internes Kontrollsystem
Lieferant	• Fehleinschätzung der Datenverarbeitungs-kapazitäten • Unzureichende Anpassung bestehender Systeme	• Prozesse nicht konform mit energiewirtschaftlichen Regelungswerken	• Wirksame Plausibili-sierungsmechanismen zur Abrechnung • Datenanalysen und kontinuierl. Datenqualitätsmanagement
VNB	• Unzureichende Ausgestaltung einer ggfs. nötigen Abbildung von zwei parallelen Systemlandschaften	• Prozesse nicht konform mit energiewirtschaftlichen Regelungswerken • Anforderungen an ISMS nicht erfüllt	• Wirksame Plausibili-sierungsmechanismen zur Abrechnung • Datenanalysen und kontinuierl. Datenqualitätsmanagement

Ein wirksames Internes Kontrollsystem adressiert Risiken ganzheitlich und berücksichtigt die Auswirkungen auf die gesamte Prozesskette

Die Risiken sollten mittels Risikoanalyse identifiziert und durch ein IKS adressiert werden



1. ***Identifikation von Risiken mittels Risikoanalyse***
2. ***Bewertung der identifizierten Risiken***
3. ***Adressierung der Risiken***
   - *Risiko-Reduktion durch Sicherheitsmaßnahmen und Kontrollen*
   - *Outsourcing an Dienstleister*
4. ***Kontinuierliches Monitoring der Risiken und Optimierung des IKS***

Prozess- und Systemanpassungen machen am Anfang einen erheblichen Kostenblock aus

Zusammenfassung und Fazit

Zusammenfassung und Fazit

- **Das zunehmende Risiko durch Cyberkriminalität und die Vielzahl an sensiblen personenbezogenen Daten machen Datenschutz- und Informationssicherheitsaspekte zu Kernthemen des neuen MsbG**
- **Es existiert eine Vielzahl an datenschutz- und informationssicherheitsrechtlich relevanten Schnittstellen**
- **Für alle relevanten Schnittstellen müssen durch EVUs Maßnahmen zur Einhaltung der Vorgaben getroffen werden**
- **Wesentliche Anforderungen an Datenschutz und Informationssicherheit im Bereich Smart Metering ergeben sich aus dem MsbG, Schutzprofilen, Technischen Richtlinien und ISO 27001**
- **Der Aufwand für das Interne Kontrollsystem darf beim Aufbau des ISMS nicht unterschätzt werden**

Gewährleistung von Informationssicherheit & Datenschutz nur durch aufeinander abgestimmte technische & organisatorische Maßnahmen möglich

Vielen Dank für Ihre Aufmerksamkeit.

PricewaterhouseCoopers AG
Wirtschaftsprüfungsgesellschaft
Bernhard-Wicki-Straße 8
80636 München
Telefon: +49 89 5790-5425
joerg.netzband@de.pwc.com
www.pwc.de

Jörg Netzband
Partner
Risk Assurance