Herausforderung für den Datenschutz

Smart Metering im Lichte der Informationssicherheit

Smart Metering wird als ein wichtiger Meilenstein gesehen, um bei den Verbrauchern Anreize zur Energieeinsparung oder Steuerung des Energieverbrauchs zu schaffen. Die dabei anfallende Massendatenhaltung und -übertragung stellt neue Anforderungen an die Informationssicherheit.
Die TTS trusted technologies and solutions GmbH entwickelt hierfür gemeinsam mit Kunden neue, passgenaue Sicherheitsarchitekturen.

Die Zähldatenermittlung und Zählerfernauslesung bedingt zum einen intelligente Messsysteme, zum anderen einen flächendeckenden Aufbau von Kommunikationsnetzen zwischen Verbrauchern und Erzeugern. Dadurch wird über die vollständige Lieferkette aller Prozessbeteiligten die technische Voraussetzung geschaffen, um eine bedarfsgerechte Optimierung der Energieerzeugung und -nutzung zu ermöglichen. Smart Metering ist der Wegbereiter, um die nachhaltigen ökologischen und wirtschaftlichen Aspekte des Smart Grid verwirklichen zu können. Die Einführung des Smart Metering wird noch von einigen Startschwierigkeiten begleitet. So erschweren u. a. die fehlende Infrastruktur zur Übertragung und Speicherung von Massendaten, Probleme beim Datenschutz und fehlende Standards zur Zeit die praktische Umsetzung.

Massendatenhaltung führt zu neuen Bedrohungen

Die Energieverbrauchsabrechnung beruht für Privatkunden bisher auf Jahresverbrauchsinformationen. Durch Artikel 13 der Richtlinie 2006/32/EG des Europäischen Parlaments und des Rates vom 5.4.2006 über Endenergieeffizienz und Energiedienstleistungen wird durch das Smart Metering eine Massendatenhaltung von Zähldaten eingeführt. Die Massendatenhaltung entsteht durch eine periodische Erhebung und Übertragung von Zähldaten, die z. B. stündlich, viertelstündlich oder sogar im Sekundentakt stattfindet. Dadurch entsteht ein Bedarf an Massenspeichervorrichtungen, die der Messstellenbetreiber vorhalten muss. Darüber hinaus ist eine konsequente IT-Anwendungs- und -Systemkonstruktion notwendig, in der die Datenverarbeitung für die kaufmännischen und technischen Prozesse effektiv und im Einklang zu den bestehenden und absehbaren regulatorischen Vorgaben realisiert wird.

Gerade für den Datenschutz entsteht durch Smart Metering jedoch auch eine neue Bedrohungslage, da sich durch eine gezielte Auswertung der Verbrauchsdaten in kurzen Zeitintervallen Erkenntnisse über die Betriebszeiten der elektrischen Gerätschaften in einem Haushalt gewinnen lassen. Diese geben wiederum Auskunft über die persönlichen Lebensverhältnisse der jeweiligen Nutzer und stellen ein Nutzungsprofil dar, an dem Dritte durchaus Interesse haben könnten. Smart Metering ist daher eine Herausforderung für die Informationssicherheit und speziell für den Datenschutz, der den Schutz von personenbezogenen und personenbeziehbaren Daten fordert.

Mit ein wenig Phantasie lassen sich schnell einige Bedrohungsszenarien entwickeln. Aus den in *Tafel 1* dargestellten Bedrohungen lässt sich die Brisanz der Massendatenhaltung erkennen.

Bedrohungsszenarien

- **Prüfung von Lebensgewohnheiten/Alibis**

Aus den Lastgängen lässt sich teilweise erkennen, wann welche Gerätschaften genutzt werden. Darauf basierend können Profile entwickelt werden, die Rückschlüsse auf Lebensgewohnheiten ermöglichen oder dazu genutzt werden können, um z. B. Alibis zu prüfen.

- **Abwesenheitszeiten**

Bei längeren Abwesenheiten wird sich der Stromverbrauch auf ein Grundmuster absenken. Ein Haushalt kann auf diese Weise elektronisch observiert werden, um ihn dann in einem günstigen Augenblick leer zu räumen.

- **Nutzerspezifische Profile**

Die oben erwähnten Profile können auch genutzt werden, um zielgruppenspezifische Werbeaktionen durchzuführen. Mit hoher Zielsicherheit können z. B. die Benutzer von Mikrowellen erkannt und beworben werden.
Die GEZ könnte Informationen über Fernsehbesitzer mit den Listen der Gebührenzahler abgleichen.

Tafel 1: Bedrohungsszenarien aus der Massendatenhaltung des Smart Metering

Dr.-Ing. ***Jörg Cordsen*** (links), Geschäftsführer
Dr.-Ing. ***Michael Gehrke***, Geschäftsführer
TTS Trusted Technologies and Solutions GmbH
Essen und Berlin

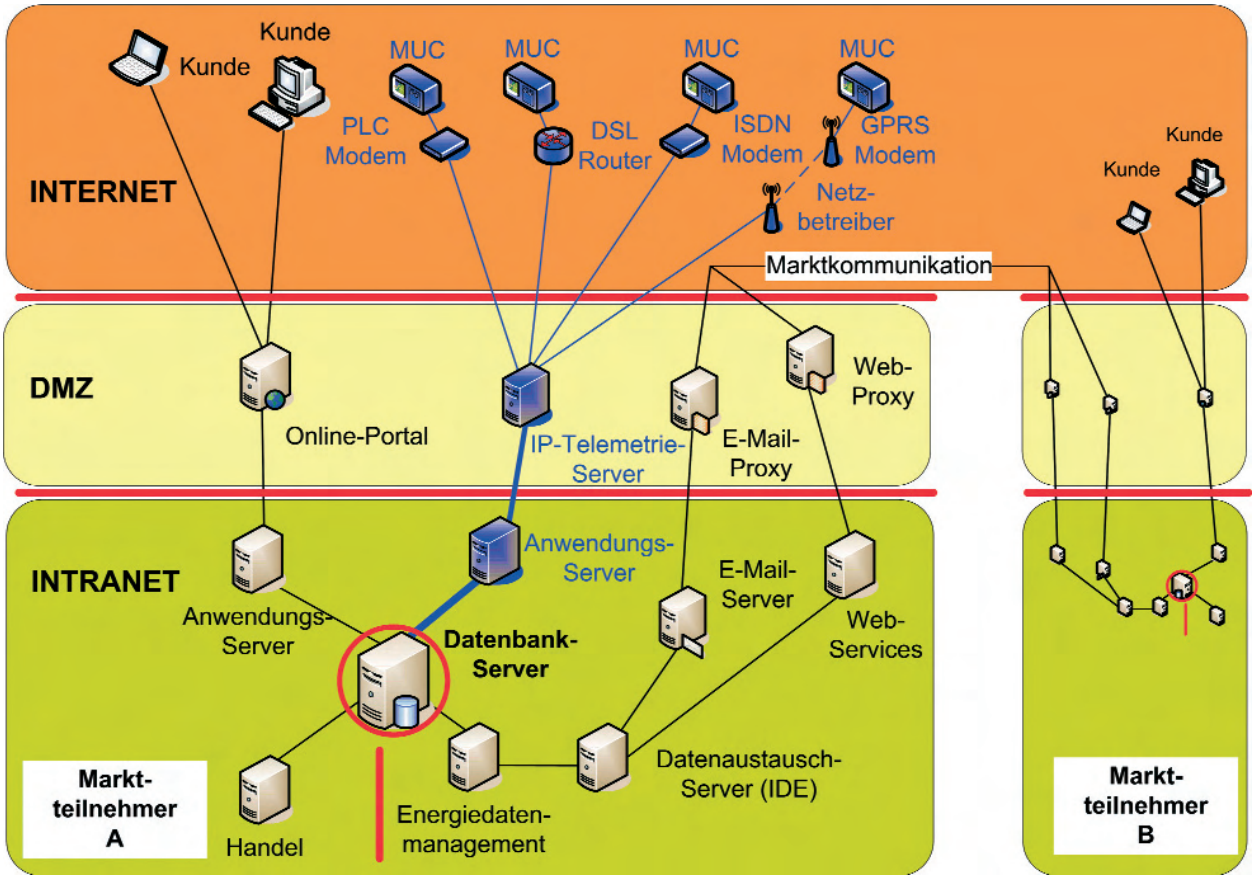

Bild 1: Kommunikationsvorgänge und Datenhaltung im Energiesektor

Legende:

MUC	Multi Utility Communication – Standard zur automatisierten Messdatenerfassung bei Privatkunden über offene Netze
PLC	Power Line Communication (auch PDSL) – Daten aus der Steckdose
DMZ	Demilitarized Zone – Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf angeschlossene Server
ISDN	Integrated Services Digital Network – digitales Telekommunikationsnetz
DSL	Digital Subscriber Line – digitaler Teilnehmeranschluss

Ver- und Entschlüsselung mit Haushaltszählern

Datenschützer fordern deshalb den Einsatz von Verschlüsselungs- und Signaturtechnik, um die personenbezogenen und personenbeziehbaren Informationen sowie abrechnungsrelevante Daten (z. B. Verbrauchswerte oder Einspeisungen) abzusichern. Diese Forderung mit den am Markt befindlichen Haushaltszählern (MUC – Multi Utility Communication) umzusetzen, wird ein schwieriges Unterfangen. Denn sie besitzen weder eine entsprechende Software noch ist die zur Verfügung stehende Prozessorleistung (z. T. 25 MHz) geeignet, um die komplexen kryptografischen Operationen, wie sie für die Ver- und Entschlüsselung von sicheren Kommunikationsvorgängen notwendig sind, in angemessenen Zeiträumen durchzuführen. Bei der Einführung intelligenter Messsysteme muss der Sicherheitsaspekt aber von Anfang an berücksichtigt werden.

Effiziente und effektive Sicherheitsarchitektur

In *Bild 1* ist die Zähldatenermittlung und Zählerfernauslesung des Smart Metering durch blau gekennzeichnete Systemkomponenten und Kommunikationsverbindungen dargestellt. Die ermittelten Daten fließen in den rot umrandeten Datenbank-Server, der durch die periodische Ermittlung über die Zeit Massendaten enthält.

Für die in *Tafel 1* beschriebenen Bedrohungsszenarien ist ein Zugriff auf die Datenbank des Messstellenbetreibers weitaus effektiver, als der Abgriff von Zähldaten eines einzelnen Haushalts. Entsprechend sollte der Fokus nicht allein darauf ausgerichtet sein, die Netzwerkverbindungen zwischen Verbraucher und Messstellenbetreiber abzusichern. Vielmehr ist es von Bedeutung, dass die Messstellenbetreiber eine effiziente und effektive Sicherheitsarchitektur aufweisen. Die Sicherheitsarchitektur sollte durch ein aktives Informationssicherheitsmanagementsystem (ISMS) betrieben werden und u. a. gewährleisten, dass

- die IT-Netze der einzelnen Kommunikationspartner voreinander geschützt sind,
- die zum Einsatz kommenden zentralen wie auch dezentralen Systeme abgesichert sind,

- stets der aktuelle Sicherheitsstandard berücksichtigt wird,
- rigide Zugangs- und Zugriffsberechtigungen eingerichtet sind,
- Kommunikationsvorgänge verschlüsselt werden,
- vor Kommunikationsvorgängen eine vorherige Authentisierung des jeweiligen Kommunikationspartners stattfindet,
- alle zum Einsatz kommenden Komponenten überwacht werden und
- Vorkehrungen für eine Data Leakage Prevention getroffen sind.

Bild 1 zeigt eine Vereinfachung der tatsächlich zum Einsatz kommenden Anwendungs- und Systemlandschaft. Trotzdem ist ersichtlich, dass eine Vielzahl weiterer Geschäftsprozesse Zugriff auf die zentrale Datenbank benötigen. Über Online-Angebote bieten z. B. Energiedienstleister Strom- und Gasprodukte an. Nach Vorgabe der Bundesnetzagentur sind bundesweit einheitliche elektronische Datenaustauschformate sowie einheitliche Prozesse vorgeschrieben, um z. B. die Abläufe des Lieferantenwechsels, Stammdatenänderungen oder Netznutzungsabrechnungen mit größtmöglicher Automatisierung vorzunehmen. Diese Dienste stehen der Öffentlichkeit über das Internet zur Verfügung und sind daher im besonderen Maße bei der Konzeption einer Sicherheitsarchitektur zu berücksichtigen.

Sicherheit auf der Anwendungsebene

Sicherheit lässt sich nicht mehr allein durch den Einsatz von Firewalls oder das Einspielen von Sicherheitspatches gewährleisten. Statt direktem Zugriff auf Server über programmiertechnische Fehler, sind heute zunehmend »logische« Angriffe zu verzeichnen. Diese nutzen die Kopplung von Webdiensten mit komplexen, im Hintergrund arbeitenden Applikations- und Datenbanksystemen aus. Die Komplexität dieser gekoppelten Systeme bietet häufig die Möglichkeit, Angriffe über die normalen Eingabemasken auszuführen. Angriffsmethoden wie SQL-Injection, Cross-Site-Scripting oder die automatisierte Manipulation von Parametern oder Sessions sind allgegenwärtig und verlangen eine Abkehr vom alleinigen Paradigma der Netzwerk- und Systemsicherheit. Stattdessen ist eine unternehmensspezifische Sicherheitsarchitektur notwendig, um alle Komponenten von den Webservern über die Applikationen bis hin zu den Datenbanken einzubeziehen und ein durchgängiges Sicherheitsniveau zu gewährleisten.

Entwicklung einer unternehmensspezifischen Sicherheitsarchitektur

Die TTS Trusted Technologies and Solutions GmbH betreut langjährig einige Kunden im Energiesektor. Dabei wird das Thema Smart Metering als weitere Anforderung an die Sicherheitsarchitektur betrachtet und alle Anwendungen, System- und Netzwerkkomponenten berücksichtigt, die in den involvierten Geschäftsprozessen des Smart Metering zum Einsatz kommen. Auf Basis einer Schutzbedarfsfeststellung und anschließender Risikoermittlung sowie -behandlung werden risikomindernde Sicherheitsmaßnahmen entwickelt und geeignet in die Sicherheitsarchitektur integriert. Flankierend werden Sicherheitsanalysen durchgeführt, um die Wirksamkeit der Sicherheitsarchitektur zu prüfen und ggf. Nachjustierungen vorzunehmen. So werden kontinuierliche Prozesse für eine hohe Informationssicherheit geschaffen, die den Unternehmen auch einen sicheren und geordneten Einstieg in das Thema Smart Metering eröffnen.

Zum Unternehmen

Seit 2002 berät die TTS Trusted Technologies and Solutions GmbH Kunden zur Informationssicherheit. Das Portfolio umfasst langjährig erprobte Projektkonzepte, die auf nationalen und internationalen Sicherheitsstandards basieren. Mit dem Information Compliance Management Tool (ICMT) hat die TTS ein datenbankgestütztes Werkzeug für das integrierte Management der Informationssicherheit und der Notfallplanung geschaffen, das die bewährte Methodik auf die individuellen Gegebenheiten ihrer Kunden anwendet. Die hohe Professionalität und Beratungsqualität drückt sich auch in mehreren erfolgreich abgeschlossenen Zertifizierungen nach ISO 27001 aus. Von den operativen Standorten Essen und Berlin aus gewährleistet TTS dauerhaft sichere Geschäftsprozesse bei zahlreichen Konzernen und großen mittelständischen Unternehmen. Zu den langjährigen Kunden der TTS GmbH zählen Unternehmen wie Bayern LB, T-Systems, Eon, EWE, Marienhospital Gelsenkirchen und die Pfalzwerke-Gruppe.

michael.gehrke@tts-security.com

joerg.cordsen@tts-security.com

www.tts-security.com