Vorbildlicher *Kompromiss*

Prof. Dr.-Ing. Axel Sikora *ist unter anderem Wissenschaftlicher Leiter des Instituts für verlässliche Embedded Systems und Kommunikationselektronik (ivESK) der Hochschule Offenburg*

Die OMS-Group, eine Interessengemeinschaft von derzeit 54 Unternehmen, hat ihre Entwicklungsarbeit in die Vorgaben für intelligente Messsysteme des BSI eingebracht. Prof. Dr. Axel Sikora, einer der IT-Experten der OMS-Group, erläutert und bewertet die Sicherheitsarchitektur für Smart-Metering-Systeme.

Die neue, digitale Kommunikationstechnik für die Zählerfernauslesung (Smart Metering) und für die Energienetze (Smart Grid) hat das Potenzial, zu einer der ersten hochskalierten Machine-to-Machine-Anwendungen (M2M) zu werden. In den vergangenen Jahren konnten sehr positive Entwicklungen im Umfeld der drahtlosen Kommunikation für Smart-Grid-Anwendungen angestoßen werden, die nun das Potenzial haben, das Marktgeschehen weit über Deutschland hinaus und auch weit über die Versorgungstechnik hinaus zu beeinflussen.

Im September 2010 wurde das Bundesamt für Sicherheit in der Informationstechnik (BSI) durch das Bundesministerium für Wirtschaft und Technologie (BMWi) mit der Erarbeitung eines Schutzprofils (Protection Profile, PP) sowie einer Technischen Richtlinie (TR) für die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway) beauftragt. Diese Arbeiten sind mit der Veröffentlichung der ersten verabschiedeten Version 1.0 im März 2013 zu einem vorläufigen Abschluss gekommen. Nach § 21d des Energiewirtschaftsgesetzes (EnWG) ist diese Kombination aus Kommunikationsnetz und Messeinrichtung verpflichtend von bestimmten Kundengruppen einzubauen, wobei die Anforderungen des BSI an Datenschutz und Datensicherheit erfüllt werden müssen.

Modell für andere Branchen

Es ist davon auszugehen, dass diese BSI-Richtlinien aus zwei Gründen Modellcharakter auch für andere Branchen haben werden. Zum einen stellt das Ergebnis der Arbeiten mit dem Schutzprofil und den technischen Richtlinien einen (meist) sinnvollen Kompromiss zwischen dem technisch Möglichen und wirtschaftlich Machbaren dar. Das erreichte Sicherheitsniveau ist anspruchsvoll, es nimmt aber auch gleichermaßen auf viele praktische Aspekte Rücksicht. Es basiert auf bewährten Protokollen aus der „normalen" IT-Welt. Der Versuch, eine Parallelwelt zu entwickeln, wurde glücklicherweise nicht unternommen. Hierbei scheute man nicht davor zurück, auf Verfahren und Vorgaben von potenziellen (teilüberlappenden) Konkurrenten, wie den Common Criteria (CC), zurückzugreifen beziehungsweise auf diese zu verweisen. Zusätzlich wurden weitere Vorgaben in Bezug auf den korrekten Einsatz dieser Protokolle erarbeitet, die zur Sicherheit im praktischen Einsatz beitragen sollen.

Zum anderen kann auch der Prozess zur Erarbeitung der Schutzprofile und Richtlinien im Wesentlichen als erfolgreich bezeichnet werden, weil er innerhalb von etwa zwei Jahren zu tragfähigen und zukunftsfähigen Ergebnissen geführt hat. Dabei wurde gleichermaßen eine „führende Hand" des Staates und eine Rücksichtnahme auf die praktischen und wirtschaftlichen Belange der Industrie an den Tag gelegt.

Generell erscheint es immer weniger sinnvoll, die Sicherheitslösungen allzu anwendungsspezifisch zu definieren. Zum einen werden die Anforderungen – und auch die verwendeten Basisprotokolle, wie zum Beispiel das Internet Protocol (IP) – immer ähnlicher, so dass die technische Notwendigkeit in zunehmendem Maße entfällt. Zum anderen verbaut man sich durch allzu spezifische Lösungen die Möglichkeit von integrierten, gewerkeübergreifenden Lösungen.

BSI-Richtlinien

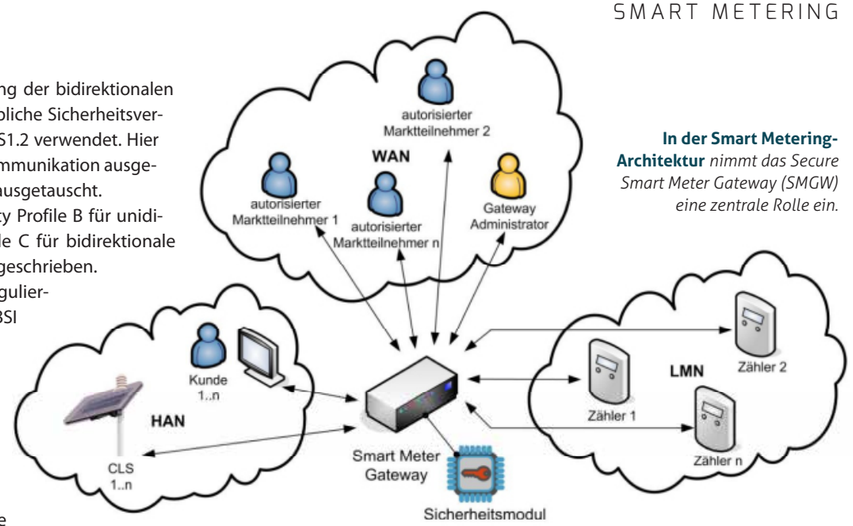
In Bezug auf die Absicherung der Kommunikationsstrecken besitzen die Gateways eine zentrale Stellung. Von den Gateways aus wird die Kommunikation abgesichert

- zwischen Sensor und Gateway (Local Metrological Network, LMN),
- mit externen Teilnehmern und damit unter Umständen auch einem Backend-System oder der (fälschlicherweise so benannten) Embedded Cloud im Weitverkehrsnetz (Wide Area Network, WAN),
- zwischen Gateway und weiteren Benutzern, sowie aktiv geschalteten Lasten (Home Area Network, HAN).

Hierbei sind drei unterschiedliche Profile beschrieben. Im Profil A werden die Daten lediglich verschlüsselt. In den Profilen B und C müssen sie auch noch authentifiziert werden. Der Datenerzeuger muss sozusagen die Informationen „unterschreiben". Damit stellt man sicher, dass die Daten auf dem Übertragungsweg nicht manipuliert werden können. In den Profilen A und B können die Schlüssel im Zähler zum Beispiel während des Produktionsprozesses oder bei der Installation hinterlegt werden, zumal dies bei unidirektionalen Geräten auch nicht anders möglich ist.

Im Profil C wird für die Absicherung der bidirektionalen Kommunikation das im Internet übliche Sicherheitsverfahren auf der Transportschicht TLS1.2 verwendet. Hier wird der Schlüssel während der Kommunikation ausgehandelt und von Zeit zu Zeit auch ausgetauscht.

In Deutschland sind das Security Profile B für unidirektionale und das Security Profile C für bidirektionale Geräte in der BSI TR 03109 vorgeschrieben. Dabei ist zu beachten, dass im regulierten Bereich (Strom und Gas) die BSI TR 03109 zwingend anzuwenden ist. Für den unregulierten Bereich sind diese Profile nicht vorgeschrieben, sollten aber ebenfalls angewendet werden. So kann man den Anwendern die Interoperabilität, Hersteller-, Medien- beziehungsweise Spartenunabhängigkeit bieten und dem Letztverbraucher einen hohen Datenschutz garantieren. Zusätzlich sind die Anforderungen an die Absicherung und die Architektur des Gateways an sich beschrieben.



In der Smart Metering-Architektur *nimmt das Secure Smart Meter Gateway (SMGW) eine zentrale Rolle ein.*

Da das Gateway eine zentrale Rolle in dem gesamten Sicherheitskonzept spielt, wird gefordert, dass in dem Gateway ein Sicherheitsmodul eingesetzt wird. Bei einem solchen Sicherheitsmodul handelt es sich entweder um einen getrennten Baustein oder um einen – mittlerweile in einigen leistungsfähigen Prozessoren – integrierten Funktionsblock, der in besonderer Weise auch gegen mechanische Angriffe geschützt ist. Vorgaben zu einem solchen Trusted Plattform Module (TPM) gibt es im Allgemeinen von der Trusted Computing Group (TCP). Die Vorgaben des BSI fordern ein nach Common Criteria zertifiziertes Modul mit speziellen Vorgaben.

Der intensiven Diskussion der OMS-Group mit Experten des BSI ist es zu verdanken, dass unidirektional kommunizierende Messgeräte (sie haben nur einen Sender und keinen Empfänger) in das BSI-Konzept aufgenommen wurden, ohne die Sicherheit der ganzen Architektur zu kompromittieren. Die in der OMS-Spezifikation enthaltenen Sicherheitsmodule wurden um die BSI-Forderungen erweitert. Jetzt verweist die Technische Richtlinie BSI TR 03109 für das drahtlose LMN auf die OMS-Spezifikation.

Fazit

Mit den Schutzprofilen und den technischen Richtlinien für die Anwendungen aus dem Smart Metering wurde für eine limitierte Anwendung, die auf Grund ihres öffentlichen Charakters ohnehin staatliche Vorgaben erfüllen muss, eine zeitgemäße und weitreichende Sicherheitsarchitektur entwickelt. Diese Architektur hält Gegenmaßnahmen für viele Risiken bereit, die auch in den sich stets weiterentwickelnden Netzwerken der Automatisierungstechnik auftreten, dort aber bislang selten so übergreifend und nachhaltig beantwortet wurden. Deswegen ist zu hoffen und zu erwarten, dass diese Sicherheitsarchitektur Vorbild für neuere Entwicklungen auch für industrielle Anwendungen sein wird.

Kontakt: OMS-Group, 50968 Köln, Tel. +49 231 39579802, info@oms-group.org
Prof. Dr.-Ing. Axel Sikora, Tel. +49 781 205-415, axel.sikora@hs-offenburg.de