

Datensicherheit in AMR-Systemen:

Sicherheit geht vor!

Am 15. Februar hat der englische Telegraph einen Artikel mit Titel „Smart meters in homes could be hacked“ veröffentlicht. Das heißt im deutschen Klartext: Intelligente Zähler in Haushalten könnten manipuliert werden. Zu diesem Schluss ist zumindest ein Berater der britischen Regierung gekommen.

In vielen Ländern wird die Datensicherheit in Systemen im Zuge der Einführung von Smart Metering inzwischen zur Frage der nationalen Sicherheit erklärt. In diesem Artikel sollen Zusammenhänge und Lösungsansätze zur Datensicherheit in diesen Systemen diskutiert werden.

Eine mögliche Smart Metering-Infrastruktur zeigt die Abbildung 1. In diesem System gilt es, die Eigenschaften Vertraulichkeit, Integrität und Verfügbarkeit zu schützen, um Sicherheit zu erlangen. Nachfolgend werden die Eigenschaften erläutert, durch die sich ein sicheres System auszeichnet. Ebenso sind Maßnahmen notwendig, um diese Eigenschaften zu erhalten.

Vertraulichkeit

Vertraulichkeit ist die erste Eigenschaft von Sicherheit. Vertraulichkeit bedeutet, dass Informationen niemals an nicht autorisierte Dritte gelangen. So erwartet ja auch jeder, dass seine E-Mails nicht von Unbefugten gelesen werden.

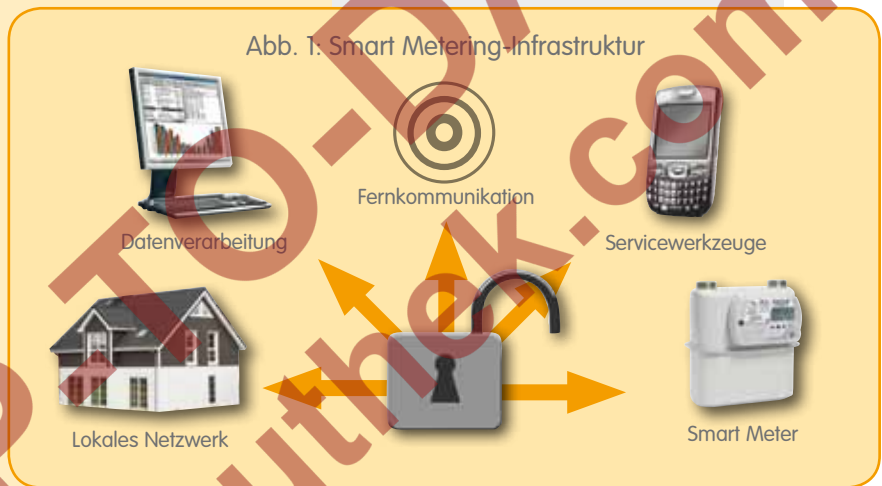
Integrität

Integrität ist die zweite Eigenschaft von Sicherheit. Integrität bedeutet, dass Informationen niemals in unautorisierter Weise verändert werden. So muss ein Zähler mit Abschaltvorrichtung sicher stellen können, dass nur dann abgeschaltet wird, wenn ein Abschaltbefehl von einer autorisierten Stelle erfolgt.

Verfügbarkeit

Verfügbarkeit ist die dritte Eigenschaft von Sicherheit. Verfügbarkeit meint, dass ein Smart Metering-System immer auf Anfragen und Kommandos von autorisierten Stellen antwortet. Ein typisches Angriffsszenario ist das sogenannte „Denial of Service“. Dabei würde ein System mit so vielen Anfragen blockiert, dass es nicht mehr in der geforderten Zeit antworten kann und so notwendige Informationen, z.B. zur Netzsteuerung, nicht mehr verfügbar sind.

Abb. 1: Smart Metering-Infrastruktur



Diesen drei Eigenschaften wird in einem Smart Metering-System mit den Maßnahmen Verschlüsselung, Authentifizierung und Autorisierung Rechnung getragen.

Verschlüsselung

Die Verschlüsselung transformiert die zu schützende Information anhand eines Algorithmus in eine für Dritte unleserliche Form. Ein aktuell häufig anzutreffender Algorithmus ist AES-128. Der AES-Algorithmus ist z.B. in den USA für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen.

Authentifizierung

Die Authentifizierung stellt sicher, dass Akteure, die Zugriff auf das Smart Metering-System nehmen wollen, tatsächlich die sind, die sie vorgeben zu sein.

Autorisierung

Die Autorisierung definiert, was ein Akteur tun darf, nachdem er authentifiziert ist. In Analogie zu Smart Metering-Systemen kann man Mobilfunksysteme oder Onlinebanking-Systeme betrachten. Hier ist es Standard, jeweils eine sogenannte „End to End Security“ aufzubauen. Das bedeutet, dass nur die beiden beteiligten Akteure Kenntnis über verwendete Schlüssel haben und der Kommunikationslink

dazwischen nur für den Datentransport benutzt wird. Hierbei bieten sich sogenannte asymmetrische Verfahren an, bei denen es jeweils einen privaten und einen öffentlichen Schlüssel gibt. Das hat den Vorteil, dass man den privaten Schlüssel, der auf jeden Fall geheim bleiben soll, nur an einer Stelle speichern muss.

Für die Autorisierung müssen geeignete Rollen definiert werden, denen dann bestimmte Rechte eingeräumt werden. Zum Beispiel muss sich ein Servicetechniker beim Batteriewechsel vor Ort in seiner Rolle am Zähler mit geeigneten Schlüsseln autorisieren. Das Gleiche gilt für ein Firmwareupdate auf dem installierten Kommunikationsmodul. Somit wird verhindert, dass sich z.B. ein Saboteur Zugang verschafft und Zählerstände manipuliert.

Es wird deutlich: Nur mit dem Kauf eines intelligenten Zählers ist es nicht getan! Mit der Einführung von Smart Metering muss immer auch eine Systembetrachtung durchgeführt werden, die Sicherheitsaspekte berücksichtigt. Insbesondere die Zählerindustrie und Versorgungsindustrie müssen zusammenarbeiten, um ein hohes Maß an Sicherheit zu erreichen, das den nationalen Ansprüchen gerecht wird.