

Smart Metering

Gefahren des Blackouts vermeiden

[28.03.2019] Bei der Entwicklung und Produktion von Smart Meter Gateways gelten hohe Sicherheitsanforderungen. Die Infrastruktur für den sicheren Betrieb intelligenter Messsysteme steht inzwischen. Noch wartet die Branche allerdings auf den Startschuss für den Roll-out.

„An einem kalten Februartag brechen in Europa alle Stromnetze zusammen. Der totale Blackout.“ So heißt es im Klappentext eines Buches, das nicht nur in der Energiewirtschaft vor einigen Jahren für Furore sorgte. In Marc Elsbergs Thriller Blackout – Morgen ist es zu spät kann man nachlesen, was ein Hacker-Angriff auf die technische Infrastruktur der Stromnetze auslöst. Das Buch zeigt drastisch auf, was passiert, wenn europaweit intelligente Stromzähler eingebaut werden, die nicht die notwendigen Sicherheitsstandards aufweisen. Der österreichische Autor hat das Thema so recherchiert, dass auch Fachleute sagen: Ja, genau so wäre es, das ist ein realistisches Szenario.

Damit die im Thriller Blackout beschriebene Katastrophe nicht eintritt, wurden in Deutschland Sicherheitsauflagen für die intelligenten Messsysteme erlassen. Zentrale Komponente der Systeme ist das Smart Meter Gateway (SMGW) als Kommunikationseinheit mit integriertem Sicherheitsmodul. Die Sicherheitsanforderungen an diese Komponente hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) entwickelt. Die Einhaltung der Vorgaben wird im Rahmen eines Zertifizierungsverfahrens vom BSI überprüft.

Zertifizierung mit Hindernissen

Der Einbau der intelligenten Messsysteme bei den Kunden kann erst starten, wenn die Behörde Smart Meter Gateways von drei verschiedenen Herstellern zertifiziert hat. Ursprünglich sollte der flächendeckende Roll-out bereits im Herbst 2017 starten, also ein Jahr nach Inkrafttreten des Messstellenbetriebsgesetzes (MsbG). Bei der Zertifizierung und Entwicklung von Smart Meter Gateways der ersten Generation ist es allerdings zu massiven Verzögerungen gekommen. Erst im Dezember 2018 wurde das erste Smart Meter Gateway zertifiziert. Bis heute warten die Messstellenbetreiber also vergeblich auf den Startschuss des BSI.

Die Energiewirtschaft zeigt dafür wenig Verständnis. Stefan Kapferer, Vorsitzender der Hauptgeschäftsführung des Bundesverbands der Energie- und Wasserwirtschaft (BDEW), kommentiert: „Der Zertifizierungsprozess hat sich bedauerlicherweise zu einem nicht enden wollenden Hindernislauf mit immer neuen Hürden entwickelt. Dies ist besonders ärgerlich, da die Branche ihre Hausaufgaben längst gemacht und bereits Ende 2017 mit Millionenaufwand alle notwendigen technischen Prozesse implementiert hat.“

Marktanalyse des BSI

Das bestätigt das BSI in der Ende Januar vorgelegten ersten Marktanalyse zum Stand der Umsetzung beim intelligenten Messstellenbetrieb: Die für den sicheren Betrieb intelligenter Messsysteme notwendige Infrastruktur steht vollständig zur Verfügung. Zehn Zertifizierungsdienstleister garantieren laut der Marktanalyse, dass die Messwerte verschlüsselt und integritätsgesichert übertragen werden. Zudem habe die Energiewirtschaft ihre Prozesse so angepasst, dass Daten aus den intelligenten Messsystemen

empfangen und verarbeitet werden können. Bislang seien 31 Unternehmen als Smart-Meter-Gateway-Administrator (SMGWA) beim BSI registriert, acht Hersteller von Geräten befänden sich aktuell im Zertifizierungsverfahren. Nun wird damit gerechnet, dass die für den Start des flächendeckenden Roll-outs weiteren Zertifizierungen im ersten Halbjahr 2019 erfolgen.

Im Zertifizierungsverfahren werden neben dem Nachweis der Einhaltung der Sicherheitsvorgaben im Smart Meter Gateway auch die Herstellungs- und Entwicklungsprozesse sowie die Auslieferungswege der Geräte betrachtet und vom BSI zertifiziert. Die Hersteller der Smart Meter Gateways müssen dafür einen enormen Aufwand betreiben. Darüber informierte das Unternehmen devolo Vertreter der Fachpresse bei einer Werksbesichtigung in Leipzig.

Manipulationen verhindern

devolo entwickelt die Smart Meter Gateways am Firmensitz in Aachen. Die Mitarbeiter in der hochgesicherten Entwicklungsabteilung werden speziell sensibilisiert und müssen alle ein polizeiliches Führungszeugnis vorlegen. Georg Offner, Leiter Produkt-Management Smart Grid bei devolo, erklärt: „Die Gefahren der Manipulation der Geräte müssen in allen Entwicklungs- und Produktionsphasen ausgeschlossen werden. Denn was nützen sichere Netze, wenn Schad-Software im Produktionsprozess eingeschleust wird.“

Produziert werden die devolo-SMGW bei der Firma Leesy in Leipzig, einem Spezialisten für Electronic Manufacturing Services. Jedes Gateway wird individuell für die Kunden, also einen bestimmten Messstellenbetreiber gefertigt. Nach der Herstellung und Prüfung der Hardware wird jedes Gerät auf die Kommunikation in der Smart Meter Public Key Infrastructure vorbereitet, welche die Übertragung der Messdaten absichert. Die Speicherung der kryptografischen Komponenten ist der kritische Teil bei der Produktion von Smart Meter Gateways. Dafür hat Leesy in der Produktionshalle eine Art Käfig aufgebaut, zu dem nur autorisierte Mitarbeiter Zutritt haben.

Nur 72 Stunden

Zudem wird die Auslieferung der Geräte speziell abgesichert. Je nach Liefermenge werden die SMGW in alarmgesicherten Lastwagen mit plombierter Ladefläche oder in einer verplombten Sicherheitsbox verschickt. Der Versand erfolgt Punkt-zu-Punkt, wobei eine Transportzeit von 72 Stunden nicht überschritten werden darf. Auch der Messstellenbetreiber muss vorsorgen. Die vom Hersteller gelieferten Geräte müssen in einer durch Video- und Einbruchüberwachung gesicherten Umgebung gelagert werden, die nur autorisiertes Personal betreten darf. Zum Einbau beim Endkunden dürfen nur so viele Geräte geschickt werden, wie an einem Arbeitstag installiert werden können. Schaffen die Monteure das nicht, müssen die Gateways wieder sicher eingelagert werden. Eine Schwachstelle scheint die Installation zu sein. Die SMGW sollen im „sicheren Bereich“ des Letztverbrauchers eingebaut werden.

Aufwand ist gerechtfertigt

Der Hersteller devolo rechnet damit, dass seine Smart Meter Gateways im ersten Halbjahr 2019 zertifiziert werden. Dann soll die Produktion hochgefahren werden. In diesem Jahr könnten 50.000 Geräte produziert werden, danach sollen die Stückzahlen auf 100.000 pro Jahr steigen. Richtig interessant wird das Geschäft nach Angaben von devolo aber erst mit der zweiten Generation der SMGW, da diese netzdienlich sind und neue Tarifmöglichkeiten bieten.

Der enorme sicherheitstechnische Aufwand, den auch die Hersteller betreiben müssen, ist aus Sicht von devolo gerechtfertigt. Produkt-Manager Georg Offner sagt: „Hundertprozentige Sicherheit gibt es im IT-Bereich nicht, aber mit dem Konzept des BSI wird ein Szenario wie im Thriller Blackout vermieden.“

()

Dieser Beitrag ist in der März/April-Ausgabe von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Smart Metering, devolo,