EMT-Sicherheitskonzept ist mehr als ein Dokument

Messdatenempfang gehorcht künftig neuen Regeln

Mit der Digitalisierung der Energiewende ändert sich auch der Messdatenempfang für alle Marktteilnehmer. Dabei spielen die IT-Sicherheit und das Sicherheitskonzept eine zentrale Rolle, denn ohne Zertifikate gibt es künftig keinen Zugriff auf Messdaten und damit keinen Empfang von Messwerten.

Das Gesetz zur Digitalisierung der Energiewende verpflichtet nicht nur die Messstellenbetreiber zur schrittweisen Installation intelligenter Messsysteme und moderner Messeinrichtungen. Auch der Messdatenempfang ändert sich – und zwar für alle berechtigten Empfänger.

Ab dem Jahr 2020 sollen die Messwerte direkt vom Smart-Meter-Gateway kommen, das als neue zentrale Datendrehscheibe fungiert, und aus den Empfängern werden externe Marktteilnehmer (EMT). Diese stellen gedanklich das Ende der Informationskette dar. Weil der Grundsatz gilt, dass eine Kette nur so stark ist wie ihr schwächstes Glied, sollte auch der Datentransfer an dieser Stelle hohen Sicherheitsanforderungen genügen.

Neue Anforderungen durch geänderte Gesetze und Verordnungen

Falls sich die Akteure der Energiewirtschaft und die darin verwurzelten Unternehmen seit dem Jahr 1998 an etwas gewöhnt haben, dann sicherlich an die stetigen Veränderungen durch neue oder modifizierte Gesetze, Verordnungen und Richtlinien. Mit dem Messstellenbetriebsgesetz (MsbG), das im September 2016 in Kraft getreten ist, wurden die wesentlichen Regeln für den Rollout intelligenter Messsysteme in Deutschland festgelegt. Damit verbunden ist eine Vielzahl von Anforderungen, die sich in Änderungen assoziierter Gesetze und Verordnungen niederschlagen. Einige Gesetze wie das Energiewirtschaftsgesetz, das Erneuerbare-Energien-Gesetz und das Kraft-Wärme-Kopplungsgesetz sowie Verordnungen wie die Anreizregulierungsverordnung, die Mess- und Eichverordnung sowie die Stromnetzzugangsverordnung wurden aufgrund des neuen MsbG umgearbeitet oder gestrichen. Wesentlicher Kern sind aber die (Neu-)Regelungen im MsbG.

Außer den vielen übernommenen Inhalten aus der Messzugangsverordnung (MessZV) sind es vor allem die Neuerungen, die viele Marktakteure verunsichern und Fragen aufwerfen. Dabei gelten für die verschiedenen Marktrollen und Akteure auch unterschiedliche Anforderungen. Ein Beispiel dafür ist die sternförmige Marktkommunikation, die den Eintritt in die neue Welt markiert: Jeder Empfänger, ob Netzbetreiber, Messstellenbetreiber oder Lieferant, erhält die Messwerte ohne Umweg über den Verteilungsnetzbetreiber direkt aus dem Smart-Meter-Gateway. Diese Kommunikation muss verschlüsselt stattfinden (**Bild 1**). Damit erlangt das Thema Informationssicherheit zentrale Bedeutung, denn ohne Zertifikate gibt es künftig keinen Zugriff auf Messdaten und damit keinen Empfang von Messwerten.

Sicherheitskonzept für passive externe Marktteilnehmer

Um Zertifikate und Schlüssel beantragen zu können, ist die Teilnahme an der Smart Meter Public Key Infrastructure (SM-PKI) Pflicht. Dafür muss ein passiver externer Marktteilnehmer (pEMT) – zum Beispiel ein Lieferant – so etwas wie ein »digitales Führungszeugnis« oder einen »PKI-Führerschein« für den Umgang mit dem privaten Schlüssel besitzen – offiziell Sicherheitskonzept genannt. Dies gilt für jeden, denn ohne Sicherheitskonzept gibt es keine Schlüssel und Zertifikate, und ohne Schlüssel keine Messwerte.

Was ist aber der Inhalt des Sicherheitskonzepts? Es handelt sich um eine Aufstellung sicherheitsrelevanter Betriebseinrichtungen und Prozesse sowie von Zuständigkeiten und Maßnahmen für den sicheren Umgang mit dem privaten Schlüssel – zusammengefasst in einem Dokument. Darin sind

- Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Systeme formuliert
- Risiken in einer Risikoanalyse identifiziert und bewertet
- mögliche Sicherheitslücken und Bedrohungen analysiert
- Maßnahmen zur Behebung eventueller Sicherheitslücken dokumentiert.

Die sbc soptim business consult GmbH hat bereits in mehreren Projekten EMT-Sicherheitskonzepte erstellt. Leitplanken waren dabei verschiedene Vorgaben unter anderem aus dem Risiko- und Sicherheitsmanagement, den technischen Richtlinien sowie der Certificate Policy der SM-PKI. Dabei wurde ein Template erstellt, das im Kundenprojekt konkret für den externen Marktteilnehmer ausgeprägt wird. Inhalte sind unter anderem organisatorische Regelungen wie Objekt- und Zugriffsschutz, das Schlüsselmanagement und die sichere Aufbewahrung des Schlüsselmaterials. Auf Basis des Templates kann das Sicherheitskonzept in einem verkürzten Verfahren erstellt werden.

Für einige Marktteilnehmer ist die sofortige Erstellung eines Sicherheitskonzepts dringend erforderlich. Dies gilt vor allem für Messstellenbetreiber (MSB), die im Interimsmodell von Anfang an die zentralen Aufgaben des Empfangs und der Weiterverteilung der Messwerte übernehmen. Für MSB ist die PKI-Teilnahme mit dem Start des Smart-Meter-Rollouts Pflicht.

Für fast alle anderen externen Marktteilnehmer gelten die Regelungen des Interimsmodells (Ausnahme: EE-Einspeisung ins Übertragungsnetz). Das heißt, beim Messwertempfang bleibt vorerst alles beim Alten. Diese EMT haben bis zum 31. Dezember 2019 Zeit für die Vorbereitung. Die Jahre 2018 und 2019 sollten aber nicht als Schonfrist aufgefasst, sondern zur Vorbereitung genutzt werden: also für die Erstellung eines unternehmensspezifischen Sicherheitskonzepts für den Umgang mit dem privaten Schlüssel. Die Unternehmen sollten mit der Projektarbeit also nicht bis kurz vor dem Stichtag warten, sondern beizeiten starten.

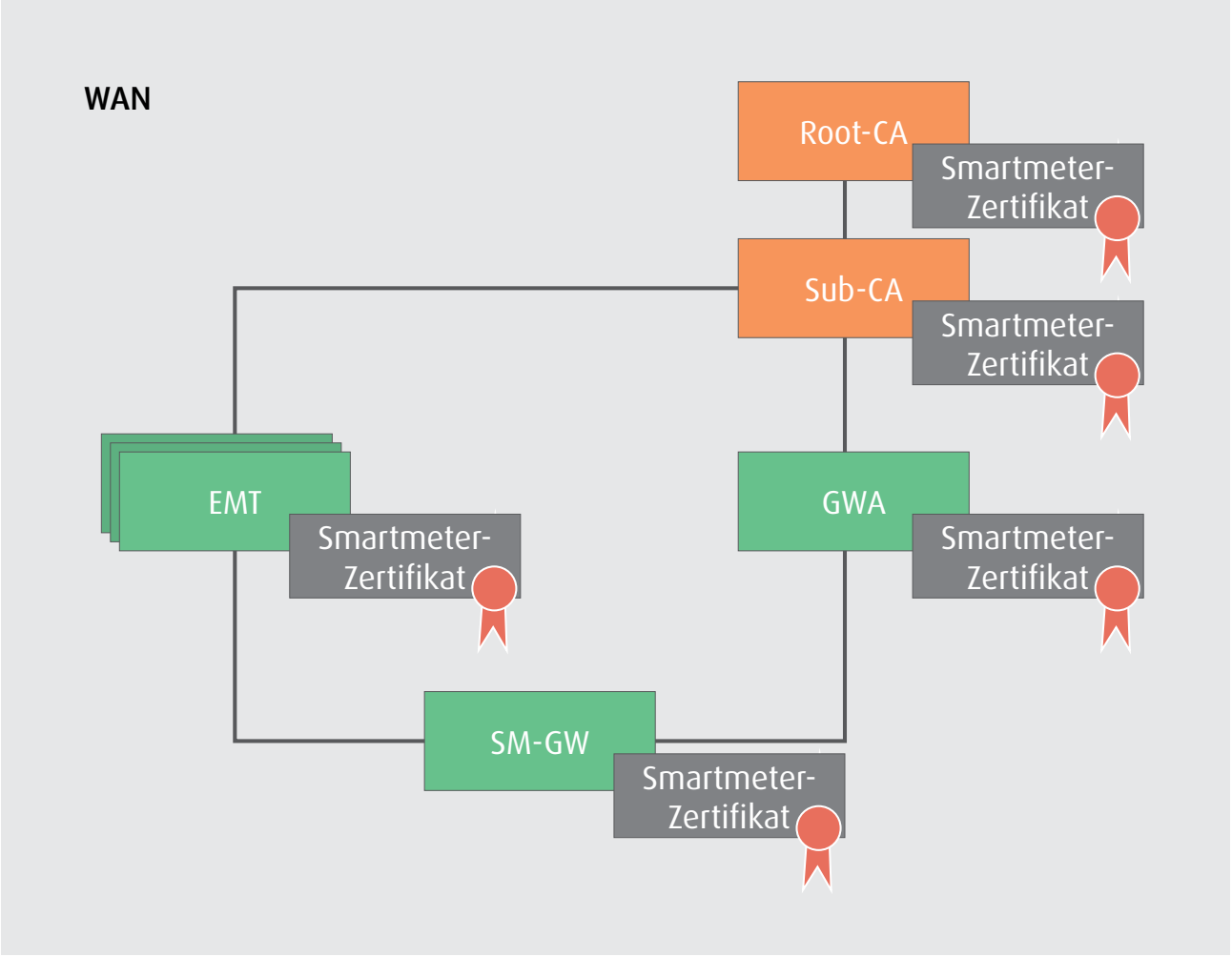

Bild 1. Anbindung und Integration der externen Marktteilnehmer (EMT) in die Smart-Meter-PKI. Die Themen Informationssicherheit und Sicherheitskonzept erlangen hierdurch zentrale Bedeutung – und zwar für alle Marktrollen.

Erfahrungen aus bisherigen Projekten

Eine wichtige Erkenntnis aus den bisherigen EMT-Projekten ist: Das Sicherheitskonzept ist mehr als ein Dokument. Zu den obligatorischen Aufgaben gehört ebenso, die Organisation und das Verhalten der Mitarbeiter in den Fokus zu rücken. Nur so können die notwendigen Veränderungen auch tatsächlich erreicht werden.

Laut neuester Gesetzeslage muss das Sicherheitskonzept bei der Beantragung eines Schlüssels zwar nicht vorgelegt werden, es ist aber wesentliche Voraussetzung, um einen Schlüssel zu bekommen. Daher sollte die Erstellung des Sicherheitskonzepts ernst genommen werden. Niemand möchte erst aus Schaden klug werden.

Darüber hinaus bietet das Sicherheitskonzept viele Chancen, sich dem Thema Sicherheit in der zunehmend digitalen Welt zu widmen. Mögliche Bedrohungen und die generelle Sicherheitslage im Unternehmen – und im Umfeld – werden dokumentiert, bewertet und Handlungsempfehlungen abgeleitet. Dies führt zu einer proaktiven Verbesserung der Sicherheitslage.

Auch bei verschiedenen rechtlichen Konstellationen ist eine gesonderte Betrachtung für die Erstellung des Sicherheitskonzepts erforderlich, beispielsweise wenn ein Dienstleister beauftragt wird oder eine Software-as-a-Service(SaaS)-Lösung genutzt werden soll. Die verschiedenen Konstellationen, die aus der Beauftragung eines Dienstleisters, der Nutzung einer SaaS-Lösung oder dem Hosting in einem Rechenzentrum resultieren, erfordern eine spezielle Lösung.

Fazit

Ein Sicherheitskonzept ist mehr als nur ein Dokument. Es erfüllt mehr als die bloße Abarbeitung der Anforderung aus der Certificate Policy der SM-PKI. Stadtwerke sollten den Mut haben und die Chance nutzen, das Thema IT-Sicherheit gewinnbringend zu bearbeiten. In einer Zeit wachsender Gefahr durch Cyber-Kriminalität ist es das Engagement auf jeden Fall wert.

Sascha Rülicke,
Senior Consultant,
sbc soptim business consult GmbH, Essen

Gunther Hahn,
Senior Consultant,
sbc soptim business consult GmbH, Aachen

>> sascha.ruelicke@soptimbc.de
gunther.hahn@soptim.de

>> www.soptimbc.de