ew
Magazin für die Energiewirtschaft
5 | 2017
ISSN 1619-5795 – D 9785 D

Intelligente Messsysteme

Koordinierte Testphase, Informations-sicherheitskonzept, Mehrwertdienste

Geschäftsobjekte

Kommunikationsstandard für den Datenaustausch

Gaswirtschaft

Europa bleibt wichtiger Markt für russisches Gas

Personalwirtschaft

Funktions- und markt-gerechte Bezahlung

Offshore

Prüfsystem für die Kabelfehlerortung

IKT-Lösungen

Funktechnologien für die Energiewende

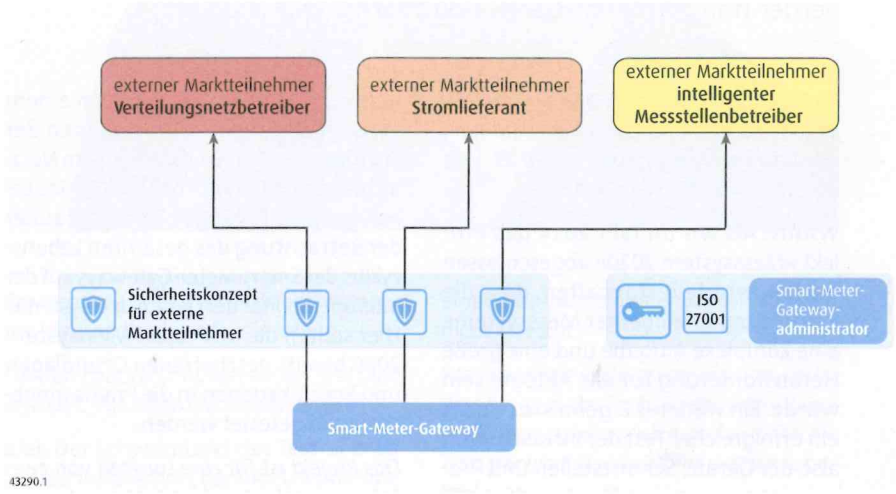
ULTRA-
HOCH-
FREQUENZ

Eine vielerorts unterschätzte Herausforderung

Informationssicherheitskonzept für externe Marktteilnehmer

Externe Marktteilnehmer können mit Daten aus intelligenten Messsystemen nur arbeiten, wenn sie an der Smart-Meter-Public-Key-Infrastruktur teilnehmen. Die Bedeutung des Faktors Informationssicherheit und der Aufwand, regelkonforme Systeme und Prozesse aufzubauen, werden vielerorts unterschätzt. Deshalb sollten EVU das Thema rechtzeitig aufgreifen.

Der bevorstehende Rollout intelligenter Messsysteme (iMSys) ist ein komplexer Transformationsprozess, der die Organisation und Arbeitsweisen vieler Unternehmensbereiche und Marktrollen tiefgreifend verändert. Betroffen sind vor allem die Bereiche Netzbetrieb, Messstellenbetrieb und Vertrieb, aber auch beliebige Lieferanten und Betreiber dezentraler Erzeugungsanlagen. All diese Akteure werden in der neuen Nomenklatur als externe Marktteilnehmer (EMT) bezeichnet. Als solche müssen sie grundlegende Neuerungen in Technik, IT und Prozessen umsetzen und gesetzliche Fristen einhalten. Da EMT mit dem Smart-Meter-Gateway (SMGW) als zentraler Datendrehscheine kommunizieren beziehungsweise über das SMGW Anlagen sogar aktiv steuern werden, ist auch bei ihnen das Thema Informationssicherheit von zentraler Bedeutung. Wie der Smart-Meter-Gatewayadministrator (SMGWA) müssen EMT an der Smart-Meter-Public-Key-Infrastruktur (SM-PKI) teilnehmen. Das heißt, sie können nur unter Verwendung ausgestellter Zertifikate mit den SMGW kommunizieren.



Auch externe Marktteilnehmer, die über das Smart-Meter-Gateway Daten beziehen, benötigen ein Sicherheitskonzept.

Aktive und passive EMT gleichermaßen betroffen

Grundsätzlich wird zwischen aktiven und passiven externen Marktteilnehmern unterschieden. Aktive EMT empfangen nicht nur Daten, sondern steuern über das SMGW auch nachgelagerte Geräte. Dies geschieht mit einem Controllable Local System (CLS) zum Beispiel zur Schaltung von EEG-Anlagen. Ein aktiver EMT muss eine Zertifizierung gemäß ISO/IEC 27001 oder IT-Grundschutz vorweisen, die alle SM-PKI-relevanten Prozesse und IT-Systeme umfasst.

Passive EMT können von Smart-Meter-Gateways nur Daten empfangen. Dies ist Voraussetzung, um ihre Geschäftsprozesse abwickeln zu können, zum Beispiel auf Basis empfangener Messwerte Abrechnungen zu erstellen und Netzzustände zu ermitteln. Zur Teilnahme an der SM-PKI hat ein passiver EMT ein Sicherheitskonzept zu erstellen. Dieses muss die Anforderungen der Certificate Policy der SM-PKI (SM-PKI-CP) des Bundesamts für Sicherheit in der Informationstechnik (BSI) berücksichtigen.

Fazit: Jeder passive EMT benötigt ein Informationssicherheitskonzept. Ausgenommen sind nur Unternehmen, die ihre SMGW-Datenkommunikation über einen beauftragten externen Dienstleister abwickeln, der wiederum die Sicherheitsanforderungen zu erfüllen hat. Das Informationssicherheitskonzept gilt es gemäß den gesetzlichen und regulatorischen Vorgaben rollenspezifisch auszuprägen. Darüber hinaus sind die Anforderungen des Datenschutzes zu erfüllen.

Vorgefertigtes Sicherheits-Template für EMT

Die Erfahrungen der Comet GmbH zeigen, dass die Einführung des Informationssicherheitskonzepts für EMT vielerorts noch unterschätzt wird. Das Thema ist umfangreicher als allgemein gedacht und erfordert einen entsprechend hohen Aufwand bei der Realisierung. Daraus kann als Handlungsempfehlung für künftige EMT abgeleitet werden, sich frühzeitig mit den Sicherheitsanforderungen zu befassen. Im Rahmen ihres Workshop- und Beratungsprogramms bietet Comet ein Sicherheitskonzept für passive EMT als Template an. Dieses lässt sich für EMT personalisieren und anpassen. Dadurch minimiert sich der Implementierungsaufwand erheblich.

>> **Uwe Sendlhofer,**
Sicherheitsbeauftragter,
Stadtwerke Saarbrücken AG, Saarbrücken,
Leiter Stabsstelle Beauftragtenwesen für Informationssicherheit,
Comet GmbH, Saarbrücken

>> kontakt@co-met.info

>> www.co-met.info

43290