Literaturverzeichnis

[1] Europäische Kommission, Proposal for a Regulation of the European Parliament and of the Council establishing a European Union Agency for the Cooperation of Energy Regulators (recast), Brüssel, 2016.

[2] J. Strüker, Blockchain in der Energiewirtschaft - Potenziale für Energieversorger, Berlin: Bundesverband der Energie- und Wasserwirtschaft e.V. , 2017.

[3] World Energy Council, PriceWaterhouseCoopers, The Developing Role of Blockchain, London: World Energy Council, 2017.

[4] M. Hinterstocker, C. Dufter, S. von Roon, A. Bogensperger und A. Zeiselmair, Potential Impact of Blockchain Solutions on Energy Markets, Łódź: 15th International Conference on the European Energy Market, 2018.

[5] A. Bogensperger, A. Zeiselmair, M. Hinterstocker und C. Dufter, Die Blockchain-Technologie - Chance zur Transformation der Energiewirtschaft?, München: FfE e.V., 2018.

[6] M. Hinterstocker, F. Haberkorn, A. Zeiselmair und S. von Roon, Faster switching of energy suppliers – a blockchain-based approach, Oldenburg: Energieinformatik 2018, 2018.

[7] Bundesnetzagentur, Monitoringbericht 2017 - Monitoringbericht gemäß § 63 Abs. 3 i. V. m. § 35 EnWG und § 48 Abs. 3 i. V. m. § 53 Abs. 3 GWB, Berlin, 2017.

[8] Bundesnetzagentur, Anlage zum Beschluss BK6-06-009 - Darstellung der Geschäftsprozesse zur Anbahnung und Abwicklung der Netznutzung bei der Belieferung von Kunden mit Elektrizität (Geschäftsprozesse zur Kundenbelieferung mit Elektrizität, GPKE), Berlin, 2011.

[9] D. Heckmann und A. Schmid, Blockchain und Smart Contracts, München: Vereinigung der Bayerischen Wirtschaft e.V., 2017.

[10] Regierung der Bundesrepublik Deutschland, „Antwort der Bundesregierung - auf die Kleine Anfrage der Abgeordneten Mario Brandenburg, Bettina Stark-Watzinger, Katja Suding, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/3313 – Distributed Ledger Technologie – Nutzung der Blockchain," Berlin, 2018.

F. Haberkorn, M. Hinterstocker, Serafin von Roon, Forschungsgesellschaft für Energiewirtschaft (FfE GmbH); A. Zeiselmair, Forschungsstelle für Energiewirtschaft (FfE e.V.), München

„Safety first": Smart Meter-Gateway-Produktion in sicherer Umgebung

Der Rollout im intelligenten Messwesen in Deutschland steht auf der Zielgeraden, das erste Smart Meter Gateway (SMGW) hatte noch im Dezember letzten Jahres die Common Criteria-Zertifizierung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erhalten. Die Marktanalyse wurde für den 31.01.2019 angekündigt. Damit geht ein langer Prozess der Geräteprüfung zu Ende, der aber nicht erst beim Produkt ansetzt, sondern schon viel früher.

Ein Blick in die nahe Zukunft: Neben einem Rückgrat aus Stromautobahnen, die für den großräumigen Austausch sorgen, bilden Millionen dezentrale Erzeuger, Speicher und Verbraucher ein fein abgestimmtes, vernetztes System. Diese dezentrale Struktur ist zwar ausfallsicherer als ein zentraleres mit wenigen großen Anlagen, anderseits birgt es generell die Gefahr der Manipulation. Was tun?

Werksbesuch bei Leesys in Leipzig, wo es Industrie 4.0 schon lange gibt. Neu ist eine aufwändig geschützte, BSI-konforme Produktionsumgebung für die Smart Meter Gateway-Produktion im Auftrag von devolo
Foto: devolo / Anne Schwerin

Voraussetzung: ein rundum sicheres Kommunikationsnetz

Wenn in der neuen Energiewelt das SMGW der Ankerpunkt ist, dann muss dieses so sicher und zuverlässig wie möglich sein. Dafür sorgen die Zertifizierung des BSI und die Prüfung der PTB. Was aber nützen die höchsten Sicherheitsvorschriften im Betrieb, wenn im Fertigungsprozess Schad-Software hineinkommt?

Laut dem SMGW-Hersteller devolo ist ein rundum sicheres Kommunikationsnetz die Grundvoraussetzung. Im Fokus der Sicherheitsüberlegungen steht das Wide Area Network – WAN, in dem die Kommunikation zwischen dem Gateway mit dem Gateway-Administrator und den externen Marktteilnehmern (Messdienstleister, Messstellenbetreiber, Verteilnetzbetreiber) stattfindet. Die SMGW-Kommunikation wird dort über Transport Layer Security – TLS abgesichert. Alle Teilnehmer des Netz-

werks benötigen Zertifikate. Die Sicherheitskette dafür ist lang und beginnt beim BSI, das eine PKI (Public Key Infrastructure) organisiert. devolo ist Teil dieser Smart Meter-PKI.

Sichere Produktionsumgebung

Zu den allgemeinen Aufgaben eines SMGW-Herstellers zählt, eine zertifizierte Produktionsumgebung bereitzustellen. Dabei müssen Manipulationen an den SMGW systematisch ausgeschlossen werden. Zudem muss die Vertraulichkeit von Sicherheits-kritischen Daten stets gewahrt werden - so Stephan Nöthen, Project Manager Manufacturing Services bei devolo. Nachdem das SMGW hergestellt und geprüft wurde, wird es vorpersonalisiert, d. h. jedes Gateway wird individuell auf die Kommunikation in der SMPKI vorbereitet. Die knifflige Aufgabe besteht darin, einen individuellen Schlüssel in jedes einzelne produzierte Gerät hineinzubringen. Nur das gibt höchste Sicherheit.

Devolo-Partner Leesys (403 Mitarbeiter erwirtschafteten 2017 einen Umsatz von 166 Mio. €) ist ein Systemdienstleister für Electronic Engineering and Manufacturing Services, der elektronische Baugruppen und Systeme entwickelt und herstellt. Dabei folgt man der Vision „Sichere Hardware für sichere Kommunikation" und verfügt über umfassende Zertifizierungen. Partner devolo entwickelt, testet und prüft jedoch selbst an seinem Standort Aachen. Man arbeitet schon seit 2012 zusammen.

Bei Leesys lebt man Automatisierung und Digitalisierung (Industrie 4.0) auf sehr hohem Niveau schon seit 1999. Es gibt in der Produktion acht SMT-Bestücklinien, in der Kunststoffverarbeitung 13 vollautomatisierte Spritzgießzellen und in der Lagerhaltung ein automatisches Kleinteilelager für 30.000 Behälter sowie ein Automatisches Hochregallager für 1.700 Paletten. Im Einsatz beobachten kann man fahrerlose Transportfahrzeuge.

Geht man durch die Hallen, fällt in einer ein „Käfig" auf. „Das ist das Herzstück der SMGW-Produktion", erklärt Stefan Salesch, Vertriebsleiter bei Leesys. Die Produktion von Geräten, die gemäß der Vorgaben des BSI gefertigt werden, findet komplett in diesem hoch gesicherten Bereich - dem „Käfig" - statt.

Sichere Lieferkette

Sicherheit fängt aber schon viel früher an. Ausgangspunkt der Lieferkette ist der elektronische Lieferschein - eLs (hier gibt es ein vom FNN definiertes Umlaufdokument). Dabei muss der Kunde mit der Bestellung initiale Konfigurationsdaten, v.a. das GWA-Zertifikat, an den Lieferanten schicken, die dann in die Produktion eingebracht werden. Nach der Herstellung müssen dann die individuellen Gütesiegelzertifikate der einzelnen SMGW an den Kunden übermittelt werden.

„Die BSI-Zertifizierung ist allumfassend und bezieht sich auf die gesamte Lieferkette. Hierzu muss der komplette Produktlebenszyklus beschrieben werden, die Produktkette endet erst beim Verbraucher", sagt der beim BSI gemeldete Projektleiter Georg Offner, Leiter Produktmanagement Smart Grid bei devolo. Zwar befindet sich die sichere Lieferkette für SMGW noch in der bilateralen Abstimmung zwischen Herstellern und BSI. Sie soll aber zukünftig prozessual und wirtschaftlich optimiert werden.

Der SMGW-Lieferant muss also nicht nur eine exklusive Produktionslinie für das SMGW bereitstellen, was den Aufbau eines zertifizierten Produktionsbereichs bedeutet, sondern auch für den sicheren Transport zum Messstellenbetreiber (MSB) sorgen. Das erfordert bei großer Auslieferung (über 1.000 Stück) alarmgesicherte LKW mit plombierter Ladefläche und Punkt-zu-Punkt-Lieferung, bei der eine Transportzeit von 72 Stunden nicht überschritten werden darf. Bei kleiner Lieferung, mit Stückzahlen unter dem genannten Wert, sind immerhin noch ein zertifizierter Lieferdienst und eine verplombte Sicherheitsbox erforderlich.

Die Sicherheitskette setzt sich dann lückenlos fort. Auch die Lagerung großer Mengen von SMGW beim MSB muss in einer gesicherten Umgebung erfolgen, für kleine Mengen genügt eine plombierte Sicherheitsbox; dies alles nur mit autorisiertem Personal.

Für Transport und Einbau der SMGW zum Endkunden gelten dann ähnlich strenge Vorschriften. So dürfen z.B. nicht mehr Produkte wie an einem Tag verbaut werden transportiert werden. Zudem darf der Einbau der Geräte im sicheren Bereich des Letztverbrauchers nur über vertrauenswürdige Monteure erfolgen und diese müssen vor jeder Montage eine Siegelprüfung und optische Prüfung an den Einzelprodukten durchführen.

Schließlich bleibt auch bei der späteren Entsorgung der SMGW nichts ungeregelt. Hierzu müssen zunächst die Geräte vom GWA vor der Deinstallation terminiert werden. Dann sind diese an einen zertifizierten Entsorgungsfachbetrieb zu übergeben, der dem Hersteller die ordnungsgemäße Zerstörung nachweisen muss.

Bestens vorbereitet

Man rechnet bei devolo bei der SMGW-Produktion mit einem seichten Ramp up am Anfang des Rollouts, danach könnte es steil nach oben gehen. Hierzu ist man, das haben Werksbesuch und Gespräche mit den Partnern Leesys und devolo deutlich herausgestellt, bestens vorbereitet.

„et"-Redaktion/FL