Stellenweise sicher

Kritische Betrachtung der IT-Security-Anforderungen fürs Smart Metering

Die beim Smart Metering verwendeten Geräte müssen Manipulationen und das Auslesen privater Daten verhindern. Verschiedene Institutionen wie das BSI haben dafür Sicherheitsanforderungen herausgegeben. Allerdings sind diese Vorgaben nicht immer sinnvoll und ausgewogen, etwa bezüglich der Verwendung von Hardware-Sicherheitsmodulen in Metering-Gateways: Diese Security-Module versprechen zwar eine aufwändige Absicherung, bringen real aber kaum Nutzen.

Autor: Dr. David von Oheimb

Smart Meter sind aus technischer Sicht eingebettete Systeme mit speziellen Mess- und Kommunikationsfunktionen. Sie befinden sich in Haushalten und anderen, quasi-öffentlichen Räumen – jedenfalls nicht unter der physischen Kontrolle des Energieversorgers oder Abrechnungs- und Messdienstleisters. Aus deren Sicht hängen die digitalen Messgeräten und ihre zugehörigen Metering-Gateways also in feindlichem Terrain und sind mit der zentralen Anlaufstelle (englisch: Head End System, HES) des Messdienstleisters verbunden. Bild 1 gibt einen Überblick über das Szenario.

Wie jedes andere IKT-System auch, müssen Smart Meter die nötige Funktionalität und Sicherheit aufweisen, Echtzeit-Anforderungen erfüllen sowie wirtschaftlich herzustellen und zu betreiben sein. Einen Überblick aus ökonomischer Perspektive bietet [1], während [3] die Sicherheitsanforderungen und Sicherheitsmaßnahmen technisch detailliert diskutiert. Die wesentlichen Sicherheitsbedrohungen sind das Verändern von Zählerdaten, um die Abrechnung zu manipulieren, sowie das Auslesen von privaten Informationen, die den Lebensstil und die finanzielle Situation der Verbraucher betreffen. Bild 2 zeigt Angriffsmöglichkeiten im lokalen messtechnischen Netzwerk (LMN), im Heimnetz (HAN: Home Area Network) und auf dem Gateway, das die Smart Meter mit dem Weitverkehrsnetz (WAN: Wide Area Network) verbindet.

Angriffspunkte

Mögliche Angriffspunkte kann man in lokale physische Zugriffe und entfernte Netzwerk-basierte Zugriffe einteilen. Gegenmaßnahmen müssen daher den gesamten Fluss von Daten und Befehlen zwischen den Beteiligten schützen. Ob diese Maßnahmen auch wirksam sind, könnte zum Beispiel eine Zertifizierung nach den

Bild: Tobias Hellsten

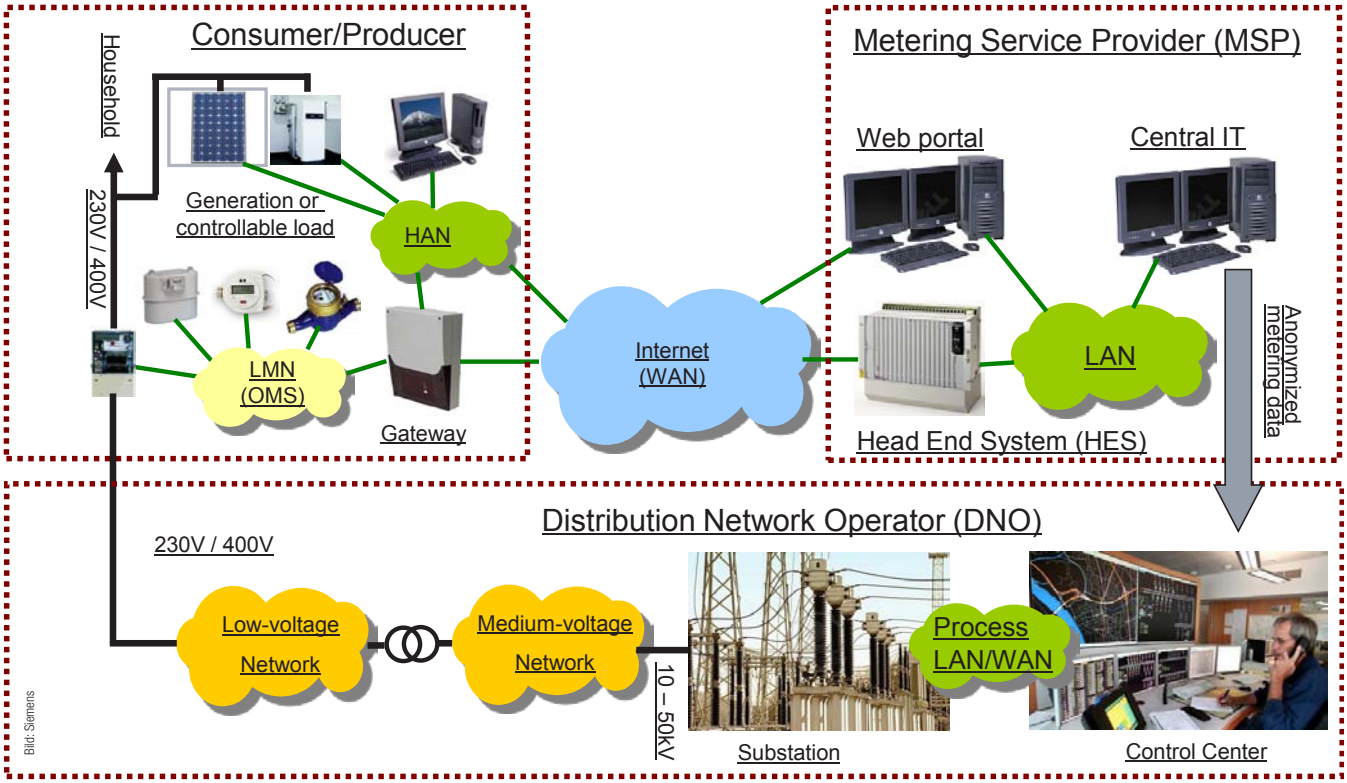

Bild 1: Übersicht über ein Smart-Metering-System. Die intelligenten Verbrauchszähler ermitteln die Daten beim Kunden und übermitteln sie an den Mess- und Abrechnungsdienstleister, der sie anonymisiert an den Verteilnetzbetreiber weitereicht.

Common Criteria [4] belegen. Besondere Herausforderungen ergeben sich durch den großen Umfang des Smart Grid und weil seine Komponenten weit im Feld verteilt sind. Da ein physischer Zugang durch die Berechtigten sehr teuer wäre, muss die komplette Verwaltung aus der Ferne möglich sein, außerdem müssen die Komponenten sehr stabil und langlebig arbeiten, wodurch die räumliche und zeitliche Angriffsfläche weiter wächst.

Sicherheitsbestimmungen

In Deutschland ist der Energiemarkt stark dereguliert, was die Situation komplizierter macht als in den meisten anderen Ländern. Zentrale und regionale Bereitstellung von Verbrauchsgütern wird entbündelt und damit auf unabhängige Institutionen verteilt. Dies führt nicht nur zu hohem organisatorischen Aufwand, sondern auch zu weiteren Funktions- und Interoperabilitäts-Anforderungen und zu Komplikationen bei Verantwortung und Vertrauen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der TÜV Informationstechnik (TÜViT) versuchen – in teilweiser Zusammenarbeit mit DKE, ZVEI und anderen Industrieverbänden – dem zu begegnen, indem sie Anforderungen an die IT-Sicherheit und Interoperabilität fürs Smart Metering definieren.

Im Gegensatz dazu sind in Österreich im Jahr 2011 eher abstrakte und vage Sicherheitsanforderungen in Kraft getreten. Die wesentliche Passage aus der Intelligente Messgeräte-Anforderungs-Verordnung (IMA-VO) lautet: „Die Intelligenten Messgeräte sowie ihre Kommunikation [...] sind nach anerkanntem Standplatz der Technik abzusichern und zu verschlüsseln, um Unberechtigten den Zugriff nicht zu ermöglichen. Die Kommunikation [...] ist nach dem Stand der Technik mit einem individuellen kundenbezogenen Schlüssel zu authentisieren und zu verschlüsseln.“ Genauere Anforderungen sind derzeit in Entwicklung. Sie scheinen zu einem gewissen Grad von den deutschen BSI-Anforderungen inspiriert, aber deutlich pragmatischer und mit wesentlich weniger Einschränkungen behaftet, was ein wesentlich besseres Kosten-/Nutzen-Verhältnis ermöglicht, sowie eine breitere Anwendbarkeit auch für andere Länder.

Absicherung der Geräte im Feld

Die Sicherheitsvorschriften des BSI fordern in ihrem „Smart Meter Gateway-Protection Profile“ [2] wie auch in der damit verbundenen detaillierten Technischen Richtlinie die Verwendung eines Sicherheitsmoduls (SM) für die Speicherung und Nutzung von kritischem Schlüsselmaterial. Die Sicherheitschip-Industrie hat das natürlich befürwortet und mit folgenden Worten beworben: „Ebenso können zertifizierte Gateways auf einfache Weise so entwickelt werden, dass sie Smartcard-Controller beinhalten. Folglich wird die Umsetzung des BSI-Schutzprofils die Einführung eines sicheren Smart-Meter-Netzwerks nicht verzögern.“ Allerdings haben sich diese Versprechungen nicht erfüllt.

Der Einsatz eines zertifizierten Smartcard-Chips hat zwar Vorteile bei der Zertifizierung des Gateways und bringt Verbesserun-

Auf einen Blick

Unausgewogen

Der alte Spruch, dass eine Kette nur so stark ist wie ihr schwächstes Glied, hat bei Security-Themen eine besondere Würze. Bedeutet er doch, dass einzelne Sicherheitsmaßnahmen ihre Wirkung verfehlen, wenn man nicht das Gesamtsystem schützt. Bei den Richtlinien für Smart-Meter-Gateways scheint diese Erkenntnis nicht gefruchtet zu haben: Einerseits fordern sie den Einsatz von Hardware-Sicherheitsmodulen, ohne den Zugriff darauf adäquat zu schützen. Das Ergebnis ist viel Aufwand mit so gut wie keinem Nutzen.

infoDIREKT www.all-electronics.de 501ejl0313

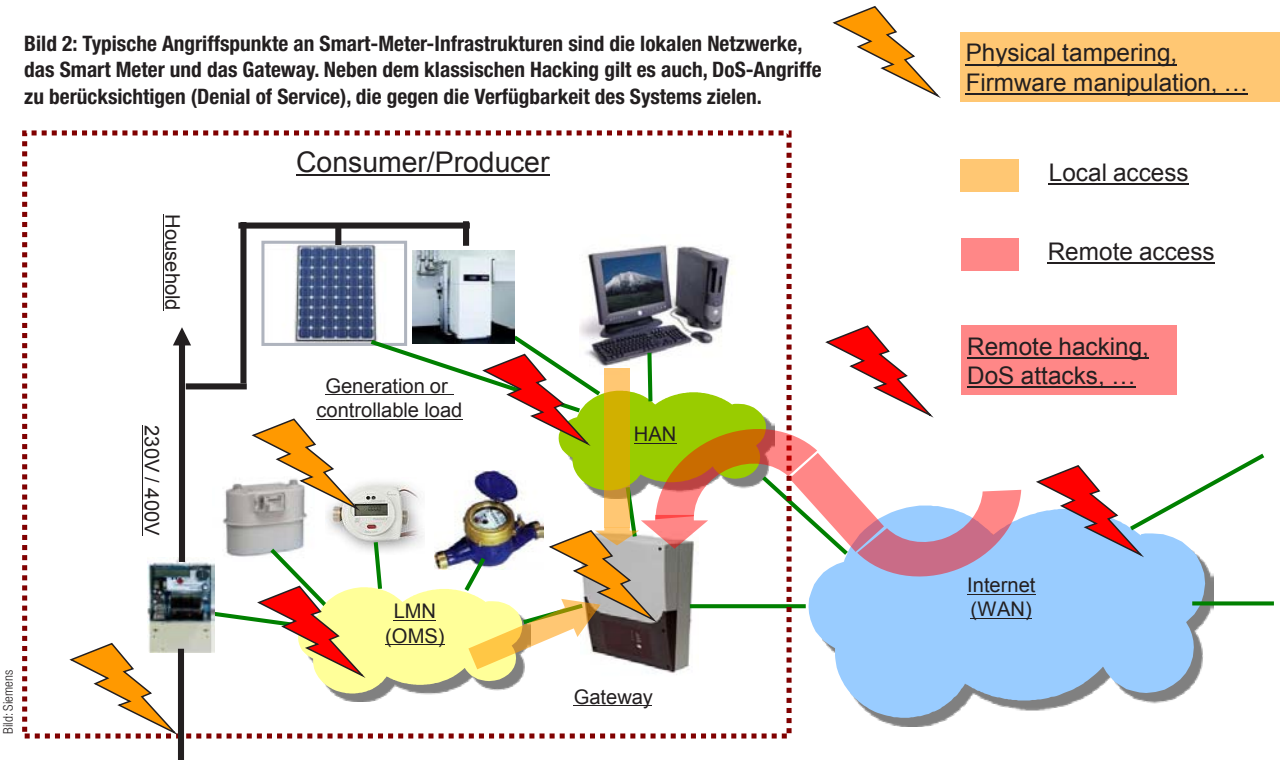

Bild 2: Typische Angriffspunkte an Smart-Meter-Infrastrukturen sind die lokalen Netzwerke, das Smart Meter und das Gateway. Neben dem klassischen Hacking gilt es auch, DoS-Angriffe zu berücksichtigen (Denial of Service), die gegen die Verfügbarkeit des Systems zielen.

gen bei der Personalisierung, aber nicht unbedingt in Bezug auf die tatsächliche Sicherheit. Tatsächlich erhöht die beabsichtigte Verwendung eines Hardware-Sicherheitsmoduls (SM) die Sicherheit des Gateways nur scheinbar. Für einen Sicherheitsarchitekten sind bezüglich des SM drei Arten von Angreifern zu betrachten:

- Entfernte Angreifer, die keinen Zugriff auf die Gateway-Hardware haben. Bei Zugriffen aus der Ferne sind ein Hardware-SM und jede alternative Software-Implementierung seiner Kryptografie- und Speicherfunktionen gleichwertig.
- Lokale Angreifer, die das Gateway nicht zu hacken versuchen oder denen es nicht gelingt. Diese Angreifer werden die Funktionalität des SM nicht einmal direkt erreichen.
- Lokale Angreifer, denen es gelingt, das Gateway selbst zu hacken, erhalten die Kontrolle über die Hardware- und Software-Anteile außerhalb des Sicherheitsmoduls. Auch wenn sie es nicht schaffen, das SM zu hacken, können sie seine Dienste missbrauchen und damit alle Verwendungszwecke des Gateways korrumpieren. Zum Beispiel können sie, auch ohne einen auf dem SM gespeicherten Schlüssel auszulesen, dem SM Befehle zum Signieren erteilen und somit effektiv beliebig (falsche) Daten im Namen des jeweiligen Gateways unterschrieben bekommen.

Damit folgt in jedem Fall, dass die Verwendung des Hardware-SM die Sicherheit effektiv nicht erhöht.

Authentifizierung

Den besonders problematischen dritten Punkt kann man dadurch zu beheben versuchen, dass man jede kritische Nutzung des SM authentifiziert. In diese Richtung wurde die aktuelle Version der BSI-Anforderungen nachgebessert. Während sich andere Parteien wie der Gateway-Administrator dem SM gegenüber tatsächlich authentisieren können, gibt es keine Chance für das übrige Gateway, mit dem SM auf sichere Weise zu interagieren. In einem Versuch, dieses Problem abzudecken, enthält das Schutzprofil für das SM eine Annahme mit der Bezeichnung „A.OperationalPhase“:

„Es wird angenommen, dass geeignete technische und/oder organisatorische Maßnahmen in der operativen Phase des integrierten Gateways die Vertraulichkeit, Integrität und Authentizität der zu schützenden Güter garantieren [...]. Insbesondere gilt dies für Schlüssel und PIN-Objekte, die in der operativen Phase des integrierten Gateways gespeichert, erzeugt und verarbeitet werden.“

Obwohl diese Annahme praktisch unerfüllbar ist, verlangen die Anforderungen an das SM, das PIN-basierte PACE (Password Authenticated Connection Establishment) zu verwenden – das müsste dazu auf dem SM und im Gateway implementiert sein. Jedoch wird dieser Mechanismus in den Anforderungen für das Gateway nicht einmal genannt. Insbesondere bleibt unklar, wie die für das PACE benötigte PIN sicher gespeichert werden soll. In der Tat ist das grundlegende Problem dieses Ansatzes nicht lösbar: Jeder Angreifer, der sich in das Gateway hackt, kann sich Zugriff auf die dort gespeicherte PIN verschaffen – und damit sein Hardware-SM missbrauchen. Um das zu verhindern, müsste das Gateway ebenso sicher sein wie das SM – und damit das SM ad absurdum führen.

In diesem Zusammenhang gibt es eine zweite Design-bedingte Lücke: Nachdem der Gateway-Administrator (GW-Admin) korrekt authentifiziert worden ist, sind Man-in-the-Middle-Angriffe möglich. Dies liegt daran, dass alle weiteren Befehle an das SM, die über das Gateway (auf dem „vertrauenswürdigen“ PACE-Kanal zwischen dem Gateway und seinem SM) ankommen, vom SM akzeptiert werden, während es keinen direkten sicheren Kanal zwischen dem GW-Admin und dem SM gibt – stattdessen endet der geschützte TLS-Kanal (Transport Layer Security) mit dem GW-Admin am Gateway. Mit anderen Worten: Sobald sich der GW-Admin erfolgreich gegenüber dem SM authentifiziert hat, kann ein Angreifer, der das Gateway durch Hacking unter seine Kontrolle gebracht hat, sich gegenüber dem SM als GW-Admin ausgeben, indem er weitere Befehle des GW-Admin abfängt und fälscht. Insbesondere kann er dann alle auf dem SM gespeicherten Schlüssel löschen oder (unter gewissen Einschränkungen) ersetzen.

Im Folgenden sind zwei alternative Ansätze beschrieben, um das Problem des lokalen SM-Missbrauchs zu lösen.

Trusted Platform Module

Der aus der IT bekannte TPM-Ansatz (Bild 3 zeigt ein Trusted Platform Module in einer Test-Einsatzumgebung) ermöglicht es, die Systemintegrität zu prüfen und zu beglaubigen. Zu diesem Zweck überprüft jedes Glied in der Kette der System-Inbetrieb-

nahme (also CPU, Betriebssystem-Bootloader, Anwendungs-Aufruf) die jeweils nachfolgende Komponente auf Echtheit und Integrität, bevor es sie startet. Auf diese Weise wird ein hierarchischer Prüfsummen-Wert berechnet und mit einem Referenzwert verglichen, der auf einem Chip fest mit der System-Hardware verbunden ist. Tatsächlich könnte ein Sicherheits-Chip wie das vom BSI vorgeschriebene SM diese Aufgabe übernehmen.

Dieser Ansatz wurde von mehreren Forschern für den Einsatz in der Smart-Metering-Domäne vorgeschlagen. Allerdings bringt er einige Probleme mit sich: Die CPU muss so ausgelegt sein, dass sie die Verwendung des TPM-Chips erzwingt. Auch muss man relativ aufwändig bei allen gewünschten Änderungen am System (etwa Software-Updates) die Soll-Prüfsumme neu setzen. Außerdem bleiben jegliche Manipulationen während des Systemablaufs (also nach dem Bootvorgang) unentdeckt. Letzteres ist eine fundamentale Begrenzung des TPM-Ansatzes: er kann temporäre Manipulationen nicht erkennen, geschweige denn verhindern.

Hardware-SM als Security Master

Eine saubere und hochsichere Architektur wäre, alle sicherheitskritischen Operationen des Gerätes in einem eingebetteten Hardware-Sicherheitschip anzusiedeln. Dies erfordert natürlich mehr Rechen- und Speicherkapazität als reine Krypto-Funktionalität. Doch mit der relativ hohen Leistung eines aktuellen Smartcard-Chips (wie etwa dem Infineon SLE88 oder SLE66, Bild 3) und einer geeignete Verteilung der Aufgaben zwischen dem Sicherheitschip und einem höher performanten Hauptprozessor ist dies durchaus möglich. Auch lassen sich größere Datenmengen mittels bekannter Techniken wie Merkle Trees außerhalb des Sicherheitschips sicher und effizient speichern. Dieser Ansatz wurde bereits erfolgreich eingesetzt, etwa im Bereich digitaler Tachographen.

Viele Köche

Der Sicherheitsaspekt von Smart-Metering-Systemen enthält also diverse Fallstricke und entpuppt sich als potenziell schädlich für die Wirtschaftlichkeit [1] und vielleicht sogar für die Sicherheit des Netzes. Dies ist auf mehrere Faktoren zurückzuführen.

Beim Smart Metering sind viele sehr unterschiedliche Akteure beteiligt, vom großen Energieerzeuger, Verteilnetzbetreiber und Verbraucher über Kleinproduzenten, Messdienstleister und IT-Komponenten-Entwickler/Anbieter bis hin zu mehreren Regulierungs- und Normungs-Institutionen. Die meisten dieser Parteien haben keinen starken Hintergrund in IT-Sicherheit. Dies mag erklären, warum die Smart-Metering-Infrastruktur, die bisher in diversen Ländern eingeführt wurde, offenkundig unsicher ist und warum viele bekannte Probleme nicht richtig angegangen wurden. So bleiben auch in der jüngsten Version der deutschen Vorschriften [2] die genannten Sicherheitsarchitektur-Probleme in Bezug auf die Integration von Hardware-Sicherheitsmodule ungelöst. Zudem hat ein Teil der Akteure widerstreitende wirtschaftliche Interessen, während sie für eine gemeinsame Lösung auf nicht-triviale Weise kooperieren müssten, und zwar sowohl bei der Definition als auch beim Einsatz von Sicherheitslösungen für das Smart Grid. Dies ist sicherlich einer der Hauptgründe dafür, dass heute noch keine einzige großflächige sichere Lösung im Einsatz ist.

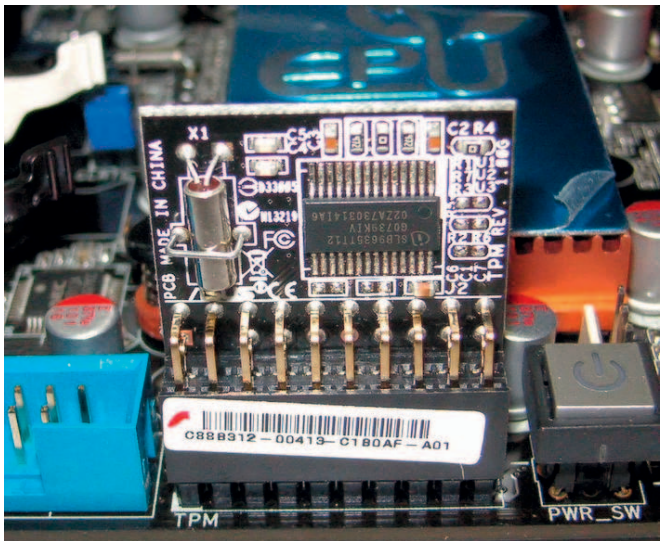

Bild: Public Domain

Bild 3: Ein Trusted Platform Module (TPM) wie dieser Infineon SLE66 kann zwar den Bootvorgang eines eingebetteten Systems schützen; Manipulationen im laufenden Betrieb erkennt es aber nicht.

Andererseits sind IKT-Security-Experten in der Regel nicht mit der Anwendungsdomäne der Energienetzwerke vertraut und neigen daher dazu, Randbedingungen zu übersehen, die durch ihre physikalischen, organisatorischen und wirtschaftlichen Charakteristiken gegeben sind. Wenn man diesen Randbedingungen Rechnung trägt, kann das den Einsatz bestimmter klassischer Security-Bausteine, beispielsweise TLS, ausschließen.

Herausforderung Smart Grid

Eine noch größere Herausforderung als das Smart Metering stellt der Netzautomatisierungs-Aspekt des Smart Grid dar. IT-Sicherheit wird in diesem Umfeld immer kritischer, weil Angriffe auf seine Kontrollmechanismen die Sicherheit und Verfügbarkeit des Netzes – und damit Kernziele der Smart-Grid-Steuerung – gefährden. Darüber hinaus entsteht eine weitere technische Komplikation dadurch, dass die IT-Sicherheit tendenziell widersprüchlich zur Verfügbarkeit ist: Bei vermuteten Angriffen einfach alles abzuschalten ist keine Option. Jede IT-Security-Lösung, die im Bereich Smart Grid angewendet werden soll, muss diese besonderen Umstände sorgfältig berücksichtigen und unterstützen.

Statt die Smart-Grid-Netzautomatisierung mit einzubeziehen, empfiehlt es sich, Smart Meter zunächst nur für Abrechnungszwecke zu verwenden, eventuell zur Steuerung von Geräten im Haushalt sowie für die schnelle Verbrauchs- und Preisinformation der Kunden. Auch bei diesen Anwendungen ist es schon schwer genug, für ausreichende Sicherheit und den gebotenen Datenschutz zu sorgen, und zwar mit vertretbarem Aufwand. *(lei)* ■

Infokasten

Literatur

[1] Ross Anderson, Shailendra Fuloria: „On the security economics of electricity metering". Workshop on the Economics of Information Security, WEIS, Juni 2010
[2] BSI: „Protection Profile for the Gateway of a Smart Metering System", Version 1.2, März 2013
[3] David von Oheimb: „IT Security architecture approaches for Smart Metering and Smart Grid". In: Jorge Cuéllar, Editor, SmartGridSec 2012, LNCS, Vol. 7823, S. 1-24. Springer, Heidelberg, 2013.
[4] „Common Criteria for Information Technology Security Evaluation", ISO/IEC 15408

Der Autor: Dr. David von Oheimb ist Wissenschaftler im Bereich Informatik und IT-Sicherheitsberater bei der Siemens Corporate Technology in München mit dem Schwerpunkt Sicherheitsarchitektur und -Zertifizierung.