Klaus J. Müller

Verordnete Sicherheit – das Schutzprofil für das Smart Metering Gateway

Eine Bewertung des neuen Schutzprofils

Auch ohne konkrete Vorgabe durch das BSI sind Hersteller gehalten, ihre Produkte robust gegen Angriffe Dritter auszulegen. Für das Smart Metering Gateway wird allerdings mit der erneuten EnWG-Novelle eine Sicherheits-Zertifizierung nach dem neu erstellten Schutzprofil zur Pflicht.

Einleitung

Das Schutzprofil nach Common Criteria für das Smart Metering Gateway[1] ist eine von mehreren Komponenten, die eine Basis für sicheres „Smart Metering" bilden sollen. Die Schutzmaßnahmen für Smart Meter Infrastrukturen lassen sich in drei Bereiche einteilen:

- **Juristische Maßnahmen:** Hierunter fallen das novellierte EnWG sowie die zu erstellenden Rechtsverordnungen.
- **Technische Maßnahmen**: Neben dem Schutzprofil zählen hierzu auch die zu erstellenden Technischen Richtlinien zur konkreten Ausgestaltung der Geräte.
- **Organisatorische Maßnahmen**: Die Gerätehersteller, die Teilnehmer am Strommarkt (Energieversorger – EVN, Vereilnetzbetreiber – VNB, Messstellenbetreiber – MSB, …) und auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) müssen ihre Prozesse anpassen, um den neuen Gegebenheiten Rechnung zu tragen.

Klaus J. Müller

Security Consultant bei der Secorvo Security Consulting GmbH

E-Mail: klaus.j.mueller@secorvo.de

1 Siehe Laupichler/Vollmer/Bast/Intemann, in diesem Heft.

Das novellierte Energiewirtschaftsgesetz (EnWG) gibt die Rahmenbedingungen vor und regelt in § 21d Abs. 4, dass eine Zertifizierung nach dem Schutzprofil die Voraussetzung für den Einsatz eines Smart Meters darstellt. Für die genauere Ausgestaltung der Details wird in § 2 Abs. 1 EnWG auf die zu erstellende Technische Richtlinie verwiesen.

In diesem Beitrag sollen vorrangig die technischen Maßnahmen bewertet und Optimierungspotenzial aufgezeigt werden.

1 Smart Metering Gateway

Der „intelligente" Stromzähler (*Smart Meter*) war die erste sichtbare Komponente des *Smart Grids*, des „intelligenten" Stromnetzes. In § 21d Abs. 1 im novellierten EnWG wird der Smart Meter beschrieben als „eine in ein Kommunikationsnetz eingebundene Messeinrichtung zur Erfassung elektrischer Energie, [die] den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt". Die eigentliche Messung findet also in der Messeinrichtung (Smart Meter) statt, zusammen mit dem Gateway wird dieses zum Messsystem. Hierbei ist die Anforderung an die Einbindung in ein Kommunikationsnetz neu hinzu gekommen. Nach der Novelle von 2008 ergab sich diese Randbedingung nur indirekt bei Nutzung der Tarife nach § 40 EnWG.

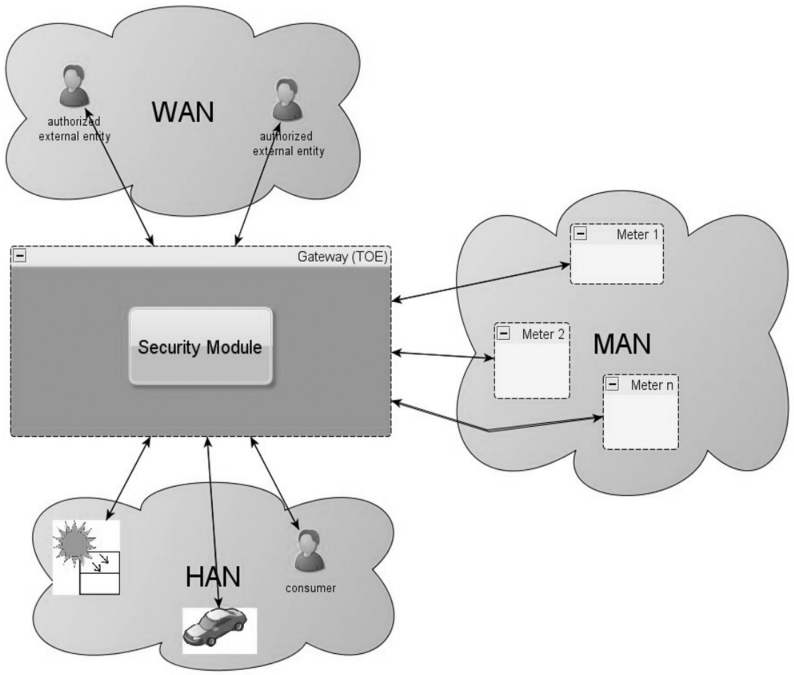
Das BSI erstellte daraufhin ein Schutzprofil für ein Smart Metering Gateway. Die darin vorgeschlagene Architektur (siehe Abb. 1) ähnelt dem Ansatz des *Multi Utility Communication* (MUC) des VDE FNN [MUC]. Darin ist vorgesehen, dass die eigentliche Messeinrichtung über eine zentrale Kommunikationseinheit mit den Teilnehmern im Strommarkt (VNB, MSB, …) kommuniziert. Dass ein Smart Meter dieses Gateway in seinem Gehäuse beheimatet, wird im Schutzprofil als Sonderfall („One Box Solution") behandelt. Die Funktion des Gateways wird dann isoliert von der Funktion der Messeinrichtung betrachtet.

Das Smart Metering Gateway stellt für die Messeinrichtungen die einzige Verbindung ins Weitverkehrsnetz (WAN) dar. Die Smart Meter selbst finden sich im *Metrological Area Network* (MAN).

Das Gateway bildet gleichzeitig die Basis für weitere Funktionen im Smart Grid. Hierfür sind zusätzliche Schnittstellen vorgesehen: im *Home Area Network* (HAN) befinden sich Geräte, über die Smart Grid-fähige Geräte mit Systemen im WAN kommunizieren können und auf diesem Weg Steuerinformationen erhalten.

Die wesentliche Funktion des Gateways ist dabei, die „erste Verteidigungslinie" für Angreifer aus dem WAN zu sein – daher wurde das Gateway als Sicherheitseinrichtung entworfen. Für einen Angriff auf Messeinrichtungen oder Geräte zur Heimautomatisierung müsste zuerst das Gateway erfolgreich angegriffen werden.

Abb. 1 | Architektur des Smart Metering Gateways (mit freundlicher Genehmigung des BSI)



2 Bedeutung des Schutzprofils

Während die populären Desktop-Betriebssysteme knapp 20 Jahre Zeit hatten, um sich auf die Bedrohungen durch die Vernetzung einzustellen, ist der flächendeckende Rollout der Smart Metering Gateways schon für die nächsten Jahre geplant. Hinzu kommt, dass die Netze heute deutlich mehr Angriffsmöglichkeiten bieten als dies vor 20 Jahren der Fall war. Das Schutzprofil nach Common Criteria bildet daher einen wichtigen Eckpfeiler beim Versuch, bereits zu Anfang möglichst viel richtig zu machen.

Die Aussagekraft einer Common-Criteria-Zertifizierung ohne Verwendung eines Schutzprofils hängt stark von den Details der Zertifizierung ab. Durch den Bezug auf ein Schutzprofil ist gewährleistet, dass das Produkt nicht nur die aufgestellten Anforderungen erfüllt, sondern auch dass diese Anforderungen im jeweiligen Anwendungskontext sinnvoll und geeignet sind.

Jenseits seiner formalen Bedeutung bewirkt das Schutzprofil, dass für diese Geräte an zentraler Stelle unter Beteiligung verschiedenster Mitspieler (Interessensverbände, Bundesbehörden, Hersteller, …) eine Analyse von Bedrohungen, Angreifermodellen und sicherheitstechnischen Anforderungen erstellt wurde. Natürlich ist ein Hersteller auch dann für die Sicherheit seiner Geräte verantwortlich, wenn es dafür kein formales Schutzprofil gibt – das alleine bedeutet jedoch noch nicht, dass sich jeder Hersteller dieser Verantwortung auch bewusst ist oder ihr gerecht wird.

Durch die Schaffung neuer Schnittstellen sind bestehende Paradigmen zu hinterfragen – sei es der fehlende Schutz beim Zugang zum Medium bei der Funkvernetzung (WLAN) oder die massenhafte Vernetzung von PCs. Während in „klassischen" IT-Produktkategorien die IT-Sicherheit inzwischen zu den Pflichtdisziplinen gehört, spielen insbesondere bei Produkten, die für den Betrieb in isolierten Umgebungen entworfen wurden, Anforderungen an die IT-Sicherheit in Entwurf und Implementierung häufig eine untergeordnete Rolle. Beim „intelligenten" Stromnetz handelt es sich jedoch um eine kritische Infrastruktur; daher kommt Fragen der Sicherheit eine besondere Bedeutung zu. Die spezifischen Gefährdungen, denen ein Smart Grid ausgesetzt ist, sind vor allem die folgenden drei:

- **Leistungserschleichung**: Aus Sicht der Verteilnetzbetreiber und Energieversorger hat dieser Aspekt höchste Priorität. Es ist davon auszugehen, dass das Eigeninteresse der Stromanbieter ausreicht, um dem Rechnung zu tragen.
- **Preisgabe von Lastprofilen**: Dieser Gefahr kann durch einen datensparsamen Entwurf der Smart Metering Lösungen begegnet werden [DuD]; sie wird nicht allein durch die technische Gestaltung der Smart Meter, sondern auch durch die Vorgaben des EnWG sowie die Gestaltung der Stromprodukte der Energieversorger bestimmt.
- **Unterbrechung der Stromzufuhr**: Eine massenhafte Unterbrechung der Stromzufuhr von Haushalten würde bereits nach kurzer Zeit katastrophale Folgen nach sich ziehen – nicht zuletzt, weil auch die Kommunikationstechnik heute in den meisten Haushalten von der Stromversorgung abhängt. Auch mobile Telefone würden durch den Ausfall der Basisstationen außer Betrieb gesetzt.

In populären Softwareprodukten funktioniert IT-Sicherheit inzwischen auch über den Rückkanal der Medien: Produkte mit Sicherheitsproblemen sind schädlich für die Reputation des Herstellers und somit für den weiteren Produktabsatz. Beim Smart Grid hingegen würden Probleme bezüglich der IT-Sicherheit zu große Konsequenzen mit sich bringen, als dass man die Aufgabe dem Markt überlassen könnte.

Auch einem möglichen Missverständnis über die Zuständigkeit zwischen dem Hersteller des Gateways und dem Messstellenbetreiber ist durch die verpflichtende Zertifizierung vorgebeugt: während der MSB davon ausgeht, ein sicheres Produkt zu kaufen, investiert ein Gerätehersteller bei der Entwicklung oft nur in die Bereiche, die explizit durch den Kunden beauftragt und somit bezahlt werden. Durch die Einladung des BSI an die Verbände der Gerätehersteller, der Energie-, Informations- und Kommunikationswirtschaft sowie des Verbraucherschutzes sich durch Kommentierungen an der Erstellung zu beteiligen, stehen die Chancen gut, dass ein zertifiziertes Smart Metering Gateway einen umfassenden Schutz gegen Bedrohungen bieten wird.

2.1 Status

Nach drei Expertenanhörungen (Tagungen Ende Januar, Ende März und Ende Mai) liegt das Schutzprofil zum Zeitpunkt der Drucklegung dieses Beitrags als Draft in Version 1.0.1 vor. Zu den Anhörungen

wurde jeweils eine Version des Schutzprofils vorgestellt und um Kommentierung gebeten. Die bis Anfang Juni eingereichten Kommentare werden derzeit eingearbeitet und anschließend eine finale Version veröffentlicht.

Im derzeitigen Draft finden sich noch Ungereimtheiten wie z. B. der logische Ablauf beim neu hinzugekommenen „Wake-Up-Service". Aus den Folien zur dritten Tagung geht die Intention hervor, so dass davon auszugehen ist, dass dies in der finalen Version des Schutzprofils korrigiert sein wird.

Nach vorsichtigen Schätzungen ist mit der Verfügbarkeit erster Gateways, die nach dem Schutzprofil zertifiziert sind, in der zweiten Jahreshälfte 2012 zu rechnen.

3 Stellungnahmen

Im aktuellen Entwurf des Schutzprofils wurde eine lokale, kryptografisch gesicherte Schnittstelle als verpflichtend eingeführt. In der Vorversion war diese noch optional. Die verpflichtende Schnittstelle ersetzt die Anforderung eines lokalen Displays. Sowohl der BfDI als auch der LDSB Schleswig Holstein beziehen sich in ihren Stellungnahmen insbesondere darauf.

3.1 Stellungnahme des BfDI

Der BfDI begrüßt in seiner Stellungnahme anlässlich der dritten Tagung zur Entwicklung des Schutzprofils diese Schnittstelle, da sie die Möglichkeit bietet, Verbrauchsdaten lokal zu visualisieren, so dass diese gar nicht erst den Haushalt verlassen müssen.

3.2 Stellungnahme ULD

Auch in der Stellungnahme des ULD zum Entwurf zur EnWG-Novelle [ULD] wird in Bezug auf das Schutzprofil insbesondere auf diese Schnittstelle verwiesen: „Verbraucher werden nicht darauf angewiesen sein, Daten Dritten zu überlassen, um eine Visualisierung des Energieverbrauchs zu erhalten. Verbraucher werden durch eigene Geräte ohne Beteiligung Dritter in der Lage sein, z. B. über ein externes Display den Energieverbrauch zu verfolgen. Ein Verlust der Datenkontrolle wäre damit nicht erforderlich."

Das Schutzprofil trifft keine Aussage über den Detaillierungsgrad, mit dem Verbrauchsdaten übermittelt werden. Es ist daher zu hoffen, dass die Appelle der Datenschutzbeauftragten in deutlicheren Formulierungen in den Rechtsverordnungen zum EnWG und den Technischen Richtlinien münden.

4 Bewertung

Das Schutzprofil für das Smart Metering Gateway muss verschiedenen Anforderungen gerecht werden. Dabei können minimale Änderungen weit reichende Konsequenzen nach sich ziehen.

So verschieden die Interessen der Beteiligten auch gewesen sind und so überschaubar der Einblick, den die Mitspieler in die Hintergründe der spezifischen technischen und organisatorischen Anforderungen der jeweils anderen hatten, so lässt sich doch sagen, dass das Ergebnis sowohl die funktionalen als auch die sicherheitstechnischen Anforderungen gleichermaßen berücksichtigt.

Als Beispiel für eine funktionale Anforderung, die deutliche Auswirkungen auf die Entwicklungs- und Produktionskosten gehabt hätte, sei das integrierte Display genannt. In der ersten Version (v0.7.3) war es nicht enthalten. In der 2. Version (v0.9.2) war es verbindlich vorgeschrieben. Für viele Hersteller hätte das bedeutet, dass nicht nur die Hard- und Software, sondern auch das Gehäuse ggf. bereits vorhandener Geräte komplett überarbeitet hätte werden müssen, obwohl in vielen Haushalten heute bessere Möglichkeiten zur Visualisierung vorhanden sind (TV-Gerät, PC). Durch den Verzicht auf die Vorgabe konnte an dieser wie an anderen Stellen ein guter Kompromiss erzielt werden.

Ein paar wenige Stellen verbleiben jedoch ungeklärt oder unnötigerweise ohne optimale Lösung. Diese werden im Folgenden näher erläutert.

4.1 Kommunikationsbeziehungen

Das Smart Metering Gateway nimmt keine Verbindungen aus dem WAN an. Einzige Ausnahme ist der im finalen Entwurf hinzu gekommene „Wake-Up-Service". Damit ist es einem legitimen Kommunikationspartner (z. B. VNB, MSB) möglich, eine Verbindung mit dem Gateway zu initiieren. Allerdings nur in einer indirekten Form, vergleichbar mit einer Rückruffunktion. Sobald das Gateway eine „Wake-Up"-Nachricht empfängt, überprüft es mit Hilfe eines Sicherheitsmoduls, ob diese vom MSB signiert und für das Gateway verschlüsselt wurde, und ob der Inhalt der Nachricht einen aktuellen Zeitstempel enthält. Schlägt eine dieser Prüfungen fehl, wird die Nachricht verworfen. Anderenfalls baut das Gateway eine Verbindung zu einem vorab konfigurierten Kommunikationspartner auf.

Während Verbindungen ins WAN grundsätzlich durch das Gateway initiiert werden und der MSB normalerweise den nächsten Verbindungsaufbau abwarten muss, kann er auf diese Weise auch einen Verbindungsaufbau anstoßen.

Für sämtliche Kommunikationsverbindungen des Gateways gilt, dass diese nur zu vordefinierten Adressen aufgebaut werden und immer kryptografisch gesichert (d. h. verschlüsselt und gegenseitig authentifiziert) sein müssen.

4.2 Sicherheitsmodul

Das Schutzprofil schreibt zwingend ein Sicherheitsmodul für das Smart Metering Gateway vor. Dieses wird verwendet, um Signaturen von Kommunikationspartnern zu prüfen, empfangene Nachrichten zu entschlüsseln und Inhalte zu signieren und zu verschlüsseln.

Im ersten Entwurf des Schutzprofils (v0.7.3) war auch für den Smart Meter selbst ein Sicherheitsmodul vorgesehen. Da sich das Schutzprofil jedoch ausdrücklich auf das Gateway und nicht auf den Meter bezieht, enthält das Schutzprofil nun keine Aussage mehr hierzu. Für den Smart Meter selbst soll ein separates Schutzprofil erstellt werden.

Gegen den zwingenden Einsatz eines Sicherheitsmoduls im Meter spricht grundsätzlich – insbesondere im Fall der Meter, die nicht zur Messung elektrischer Energie gedacht sind (Gas, Wasser, Fernwärme) – der erhöhte Energiebedarf. Während sich eine Messeinrichtung für elektrische Energie direkt aus dem zu messenden Medium bedienen kann und der Eigenverbrauch daher zweitrangig ist, werden andere Messgeräte in der Regel mit einer Batterie betrieben. Für maximale Standzeiten und minimalen Wartungsaufwand muss ein Smart Meter daher so wenig Strom wie möglich verbrauchen.

Aus Sicht der Sicherheit bedeutet ein Verzicht auf Sicherheitsmodule in Smart Metern jedoch, dass die lokalen Schnittstellen des Smart Metering Gateways auch Protokolle unterstützen müssen, die durch

schwächere Sicherheitsmechanismen geschützt sind.

Die im Schutzprofil verwendete Formulierung „Security Module (e. g. a smart card)“ sorgte im Laufe der Abstimmrunden zunächst für Verwirrung, da die Frage aufkam, ob sich hieraus eine Aussage über eine gewünschte Bauform ableiten lässt. Das ist natürlich nicht der Fall.

4.3 Unterbrechbare Verbrauchseinrichtungen

Über einen von außen steuerbaren Unterbrecher (engl. „circuit breaker“) beim Nutzer ist es möglich, die Stromzufuhr aus der Ferne zu unterbinden. Die möglichen Einsatzzwecke sind:

- **Laststeuerung zur Optimierung der Netzauslastung**: Der Netzbetreiber kann damit z. B. zu Spitzenzeiten die für die Zukunft erwarteten Elektromobile vom Netz trennen und stattdessen zu einem späteren Zeitpunkt wieder verbinden.
- **Trennung säumiger Kunden**: Ein Energieversorger kann auf diese Weise mit minimalem Aufwand verhindern, dass ein säumiger Kunde weiterhin Leistung bezieht.

Das Gateway selbst darf lt. Schutzprofil eine solche Funktionalität nicht beinhalten: “The TOE [Anm.: Smart Metering Gateway] has a fail-safe design that specifically ensures that any malfunction can not impact the delivery of a commodity“ – die Lieferung darf also selbst durch eine Fehlfunktion nicht beeinträchtigt werden, genauer noch: „this Protection Profile assumes that the Gateway and the Meters have no possibility at all to impact the delivery of a commodity. Even an intentional stop of the delivery of a certain commodity is not within the scope of this Protection Profile.“

Dies wurde im nun vorliegenden Entwurf des Schutzprofils durch folgende Ergänzung geändert: “such a functionality may be realised by a CLS”. Über ein externes Modul – Controllable Local System (CLS) – kann eine solche Funktion also implementiert werden. Da § 14a EnWG ausdrücklich „vollständig unterbrechbare Verbrauchseinrichtungen“ vorsieht, wurde an dieser Stelle ein Widerspruch zwischen Schutzprofil und EnWG aufgelöst.

Die konkrete Ausgestaltung sollte dabei so erfolgen, dass die möglichen Auswirkungen im Fehlerfall minimal sind (*Graceful Degradation*). Der Nutzer sollte daher die Möglichkeit haben, eine solche Unterbrechung zu überschreiben, das System sollte sozusagen *unter Nutzerkontrol*le bleiben.

Im Regelfall wird der Nutzer z. B. am Abend sein Elektromobil an die heimische Ladesäule anschließen. Der Verteilnetzbetreiber könnte dann – abhängig von der aktuellen Verfügbarkeit – den Ladevorgang starten und wieder unterbrechen, so dass der Nutzer sein E-Auto am Morgen wieder geladen vorfindet.

Am Abend vor der Urlaubsreise könnte der Nutzer jedoch wünschen, dass der Ladevorgang umgehend beginnt und bis zur Abreise um 1 Uhr nachts auch nicht unterbrochen wird. Da der Verteilnetzbetreiber das nicht voraussehen kann, sollte der Nutzer selbst die Möglichkeit haben, dies zu aktivieren. Für diesen Sonderfall muss es natürlich einen Preisaufschlag geben – sonst würde das durch den VNB nutzbare Laststeuerungspotenzial auf ein Minimum zusammen schrumpfen.

Sofern es sich bei den Geräten, die an diesen Anschlüssen betriebenen werden, tatsächlich nur um die im EnWG erwähnten Beispiele (Elektromobil, Wärmepumpen) handelt, ist der mögliche Schaden begrenzt – selbst eine im Winter auf diese Weise deaktivierte Wärmepumpe ließe sich so z. B. über einen Heizlüfter an einem weiteren Stromkreis betreiben. Dies setzt jedoch voraus, dass es einen solchen gibt: die Formulierung „die über einen separaten Zählpunkt verfügen“ dürfte auch Tarife zulassen, bei denen der gesamte Haushalt über einen solchen Unterbrecher angebunden ist. Eine alternative Möglichkeit zur Stromversorgung besteht dann nicht.

Im Fall einer Schwachstelle, die es einem Angreifer erlaubt, aus der Ferne in vielen Haushalten eine Unterbrechung herbei zu führen, ist die Option, den Unterbrecher zu „überschreiben“, noch wichtiger: dadurch wird erreicht, dass die betroffenen Nutzer sich selbst helfen und ihren Haushalt wieder mit Strom versorgen können. Für diesen Fall sollte außerdem vorgesehen werden, dass das Überschreiben für eine Weile, z. B. ein paar Stunden, Bestand hat.

In den „Guidelines for Smart Grid Cyber Security” [NIST7628] des US-amerikanischen NIST findet sich hierzu: “Cyber Security Objectives/Requirements: Integrity of control commands to the RCD switch is critical to avoid unwarranted disconnections […]. The impact of invalid switching could be very large if many meters are involved. Availability to turn meter back on when needed is important.“[2]

Auch hier ist ein Unterbrecher unter Nutzerkontrolle also nicht zwingend vorgeschrieben, aber doch immerhin als „wichtig“ bezeichnet. Eine Formulierung, die einer Unterbrechereinheit die Nutzung des Gateways untersagen würde, stünde im Widerspruch zu § 14a EnWG. Entscheidend ist, ob die Unterbrechereinheit oder der Verbraucher das letzte Wort hat:

- Wenn es darum geht, säumige Kunden effektiv vom Stromnetz zu trennen, darf dieser keine Möglichkeit haben, die Unterbrechung zu umgehen (*unter Netzkontrolle)*.
- Geht es aber um die Minimierung der Angriffsfläche, wird eine Vorrichtung benötigt, die es dem Kunden erlaubt, im Zweifelsfall die Zufuhr wieder herzustellen (*unter Nutzerkontrolle*).

Über eine deutliche Formulierung in den zu erstellenden Technischen Richtlinien ließe sich eine Implementierung der Unterbrecher *unter Nutzerkontrolle* erreichen – das Schutzprofil schließt derzeit eine Implementierung *unter Netzkontrolle* nicht aus.

4.4 Eskalationsprozess für kritische Sicherheits-Patches

Sicherheits-Patches bedürfen ebenso wie funktionale Patches einer angemessenen Qualitätssicherung. Anderenfalls könnte das Risiko durch das Ausbringen eines unzureichend getesteten Patches höher sein als das Risiko durch die zu behebende Schwachstelle selbst.

In kritischen Fällen, in denen betroffene Systeme jedoch z. B. aus dem Internet erreichbar sind und die Schwachstelle bereits ausgenutzt wird, gilt es abzuwägen: Soll die Aktualisierung erst nach erfolgreichem Durchlaufen des regulären Qualitätssicherungsprozesses eingespielt werden oder ist die Wahrscheinlichkeit einer Kompromittierung so hoch, dass das Gesamtrisiko durch das Ausbringen eines unvollständig getesteten Patches verringert wird?

Als „best practice“ hat sich in Unternehmen bewährt, ein Sicherheitsmanagement inkl. Eskalationsprozessen zu etablieren [NIST800, ISO, GS].

Eine Zertifizierung nach dem Schutzprofil verringert zwar die Wahrschein-

2 Vol. 3, 10.3.1, p. 95

lichkeit, dass eine solche Schwachstelle existiert – kann dies aber natürlich nicht ausschließen [nPA]. Im Falle einer Schwachstelle, die einen erheblichen Anteil der ausgerollten Smart Metering Gateways betrifft, stellt sich daher die gleiche Frage.

Wer aber kann eine solche Entscheidung treffen?

- **Hersteller**: Er hat weder technisch Zugriff auf die Geräte noch die Hoheit zu entscheiden, ob eine nicht-zertifizierte Softwareversion ausgebracht werden darf. Immerhin verbietet § 21d Abs. 4 EnWG das Ausbringen von Smart Metering Gateways, die keine Zertifizierung gemäß Schutzprofil haben. Der Hersteller kann also lediglich eine fehlerbereinigte – und im Rahmen seiner Möglichkeiten getestete – Version bereitstellen und eine Nachzertifizierung beantragen.
- **MSB**: Der MSB hat zwar technischen Zugriff auf die Geräte, aber auch ihm ist per EnWG untersagt, die fehlerbereinigte Version auszubringen, solange diese nicht zertifiziert ist. Zwar hat im Einzelfall die Landeseichbehörde die Entscheidungshoheit – jedoch ist nicht davon auszugehen, dass man das Ausbringen der neuen Version zulässt, solange hierfür keine Zertifizierung vorliegt.
- **BSI**: Das BSI hat zwar keinen Zugriff auf die Geräte, kann jedoch – in Zusammenarbeit mit dem Hersteller, den MSB und den Landeseichbehörden – das Risiko abwägen und ggf. eine „Ad-hoc"-Zertifizierung erteilen.

In einem Eskalationsprozess sollte definiert werden, wie die Zuständigkeiten in einem Notfall aussehen, wer welche Entscheidungsbefugnis hat und welche Randbedingungen für eine Ad-hoc-Zertifizierung erfüllt sein müssen.

Bei Bekanntwerden einer konkreten Schwachstelle könnte das BSI dann an Hand der vorgegebenen Prozesse und auf Basis der verfügbaren Informationen:

- Mögliche Auswirkungen
- Anzahl betroffener Systeme
- Verfügbarkeit von Schadsoftware
- Zur Ausnutzung der Schwachstelle erforderliche Authentifizierungsinformationen, …

entscheiden, welches Risiko geringer ist: Abwarten bis zur regulären Nachzertifizierung der Software – während weiterhin die ausgerollten Geräte die Schwachstelle enthalten oder Ausbringen der fehlerbereinigten, aber noch nicht in vollem Umfang zertifizierten Version.

Der MSB könnte dann ggf. die fehlerbereinigte Version zeitnah ausbringen. Über die Etablierung eines derartigen Eskalationsprozesses ist derzeit nichts bekannt.

5 Fazit

Das Smart Metering Gateway wird in den nächsten Jahren zum zentralen Element der Smart-Metering-/Smart-Grid-Infrastruktur in den Haushalten werden. Das Schutzprofil nach Common Criteria schafft eine gemeinsame Messlatte für die Sicherheit der Gateways.

Dadurch und durch die zusätzliche Sorgfalt, die der Zertifizierungsprozess mit sich bringt ist davon auszugehen, dass nicht nur eine hohe Resistenz gegen Schwachstellen erreicht wird, sondern dass auch die Auswirkungen beim Auftreten einer Schwachstelle gering sein werden (*Graceful Degradation*). Als Beispiel für die Qualität der gefundenen Lösungen sei der *Wake-Up-Service* angeführt, bei dem sowohl die Belange der Betreiber als auch hohe Anforderungen an die Sicherheit des Gateways berücksichtigt wurden. Der zwingende Einsatz eines Sicherheitsmoduls stellt sicher, dass sichere kryptografische Verfahren verwendet werden können.

In diesem Sinne wäre im Fall der Unterbrechereinrichtungen eine deutliche Formulierung einer Implementierung *unter Nutzerkontrolle* wünschenswert. Die möglichen Auswirkungen eines Angriffs auf diese Einrichtungen könnten damit auf ein Minimum reduziert werden.

Auch mit der Fertigstellung des Schutzprofils ist das Thema jedoch nicht abgehakt – die Gerätehersteller haben die Implementierung und die Zertifizierung noch vor sich. Viele Details mit potenziell großen Auswirkungen werden erst durch die zu erstellenden Technischen Richtlinien fixiert. Um beim Auftreten einer Schwachstelle in den Gateways eine notwendige Aktualisierung im Extremfall auch ohne ein Durchlaufen der regulären Zertifizierung vorzusehen, sollten die technischen Richtlinien auch eine Eskalationsstrategie für Sicherheitsvorfälle definieren.

Außerdem ist zu hoffen, dass die Umsetzung der von den Datenschutzbeauftragten angemahnten Abrechnung in den Messgeräten im Haushalt ausdrücklich gefordert wird. Dadurch würde eine datensparsame Auslegung der Stromprodukte ermöglicht. Personenbeziehbare, fein aufgelöste Energieverbrauchsprofile würden so außerhalb der Haushalte gar nicht erst anfallen.

Quellen

[DuD] Müller, Klaus J.: *Gewinnung von Verhaltensprofilen am intelligenten Stromzähler.* DuD 08/2011, S. 359-364. http://www.secorvo.de/publikationen/verhaltensprofile-smart-meter-mueller-2010.pdf

[MUC] *Lastenheft Multi Utility Communication (MUC)*, 2009. http://www.vde.com/de/fnn/arbeitsgebiete/messwesen/documents/fnn_lh-muc_1-0_2009-08-05.pdf

[NIST7628] *Guidelines for Smart Grid Cyber Security* (NISTIR 7628), 2010. http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

[NIST800] NIST SP 800-40: *Creating a Patch and Vulnerability Management Program*, 2005. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

[ISO] ISO27002, 13.2 *Umgang mit Informationssicherheitsvorfällen und Verbesserungen*, 2008.

[GS] BSI: *IT-Grundschutz-Kataloge*, 2009, B 1.8 Behandlung von Sicherheitsvorfällen, https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b01/b01008.html, B 1.14 Patch- und Änderungsmanagement, https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/baust/b01/b01014.html

[ULD] Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) vom 10.06.2011 zum Gesetzentwurf der Bundesregierung eines Gesetzes zur Neuregelung energiewirtschaftlicher Vorschriften, 2011 https://www.datenschutzzentrum.de/smartmeter/20110615-smartmeterregelung.htm

[nPA] Secorvo: *Unqualifiziert qualifiziert*, Secorvo Security News, Juni 2010, http://www.secorvo.de/security-news/secorvo-ssn1006.pdf