Sicherheit im Smart Grid

Klaus J. Müller
Secorvo Security Consulting GmbH
Ettlinger Strasse 12-14
76137 Karlsruhe
klaus.j.mueller@secorvo.de

1 Inhalt

„Nachtstrom 2.0“ oder „Die Rückkehr der Rundsteuerempfänger“ könnte man die Technologie Smart Grid auch nennen. Bereits vor Jahrzehnten hatten die Energieversorgungsunternehmen (EVU) technische Einrichtungen, um zu Schwachlastzeiten – also nachts – bundesweit tausende von Verbrauchern aus der Ferne einzuschalten: elektrisch betriebene Nachtspeicheröfen. Das Problem von damals – die effiziente Speicherung elektrischer Energie – ist auch heute noch ungelöst.
Durch den steigenden Anteil regenerativer Energien an der Stromerzeugung – insbesondere aus Sonne und Windkraft, die nicht konstant zur Verfügung stehen – wird die Planung der erzeugten Energiemenge schwieriger, da ins Stromnetz eingespeiste und verbrauchte Energie übereinstimmen müssen; anderenfalls droht im schlimmsten Fall ein Zusammenbruch des Energienetzes. Insbesondere bei der Windenergie kann es kurzfristig zu erheblichen Spitzen kommen.

Um den Stromverbrauch und die z. T. erheblich schwankende Energieerzeugung besser aufeinander abzustimmen, soll neben einer Meldung des aktuellen Verbrauchs durch „Smart Meter“[1] auch die Möglichkeit geschaffen werden, elektrische Verbraucher in Abhängigkeit von der aktuell verfügbaren Leistung ein- und auszuschalten.
„Ganz normale Haushaltsgeräte“ sollen mit Kommunikationstechnik ausgestattet werden und damit über das Internet kommunizieren. Die sich dadurch ergebenden neuen Angriffsszenarien werden in diesem Beitrag beleuchtet.
Infrastrukturelemente des Smart Grid finden sich in den Haushalten, im Verteilnetz und bei den Versorgern. Im Fokus dieses Artikels stehen die Aspekte, die sich auf die Haushalte beziehen. Auch im Bereich der Steuertechnik gibt es einige Angriffspunkte (Stichworte: „Digitale Leittechnik trifft öffentliche Netze“ und „Stuxnet“) – diese sind jedoch nicht Gegenstand der Betrachtung.[2]

2 Was ist das „Smart Grid“?

Unter „Smart Grid“ versteht man das „intelligente Stromnetz“, bei dem das bereits vorhandene Leitungsnetz zur Energieübertragung durch ein zweites Leitungsnetz zur Übertragung von Informationen (Datennetz) zwischen Messstellenbetreibern,

[1] „Smart Meter“, die „intelligenten Stromzähler“ [1]
[2] Beispiele hierfür finden sich z. B. in [2]

Energieversorgern uns „Smart Metern“ überlagert wird. Über dieses Datennetz sollen zukünftig die Messdaten, die aktuellen Preise, Steuersignale etc. zwischen den Beteiligten ausgetauscht werden.

2.1 Warum brauchen wir das „Smart Grid“?

Die Gewinnung elektrischer Energie aus regenerativen Quellen wie Sonne und Wind ist im Gegensatz zu herkömmlichen Energielieferanten sehr viel schlechter planbar. Da für elektrische Energie heute nur geringe Speicherkapazitäten zur Verfügung stehen[3], muss diese im gleichen Moment verbraucht werden, in dem sie auch erzeugt wird. Stimmt Gewinnung und Abnahme nicht überein, wirkt sich dies auf die Netzfrequenz aus [3] , wodurch die Stabilität des Netzes gefährdet sein kann. Um diese Einbußen bei der Planbarkeit auf der Seite der Gewinnung auszugleichen gibt es zwei Ansätze:

- Ausrichtung der Stromerzeugung nicht mehr am Standardlastprofil (s. Abbildung 1) sondern am realen Verbrauch durch zeitnahe Messung an den Verbrauchsstellen via Smart Meter

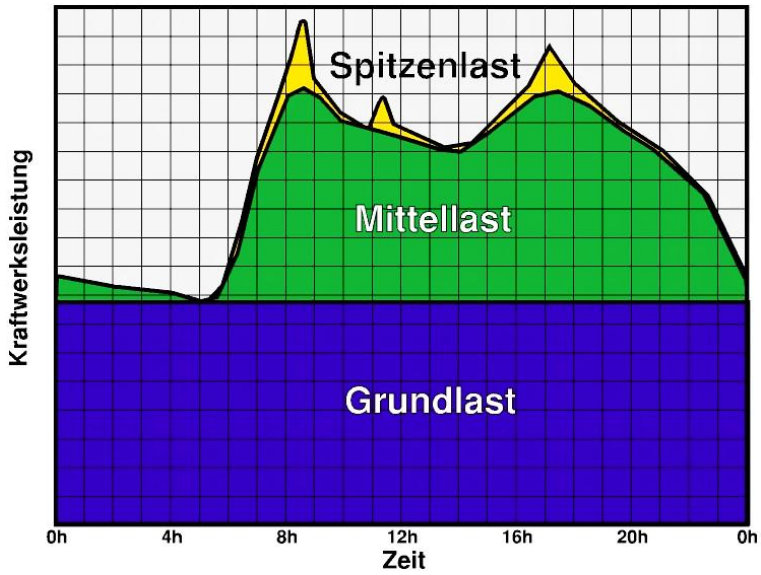

Abbildung 1: Standardlastprofil für einen Haushaltskunden (Quelle: [4])

- Steuerung des Verbrauchs durch gezieltes Ein- und Ausschalten von Lasten (Wärmepumpen, Kühlgeräte, Klimaanlagen – also bevorzugt thermische Großverbraucher, die selbst eine gewisse Pufferfunktion mit sich bringen)

Das alte Paradigma wird also auf den Kopf gestellt: Während sich derzeit die Erzeugung nach dem (Plan-)Bedarf richtet, soll sich künftig der Verbrauch an der Verfügbarkeit orientieren. Bei starkem Wind in der Nacht werden Wärmepumpen im Land eingeschaltet, die die nun verfügbare elektrische Energie in Wärme wandeln und zur späteren Nutzung speichern. Das Smart Grid soll hier also ein Türöffner sein, der die Integration regenerativer Energien in den Stromhaushalt erleichtert.

Hinzu kommt ein zweiter Paradigmenwechsel: die Energiegewinnung, die bislang an einigen wenigen zentralen Kraftwerken geschieht, wird dezentral verteilt. Viele kleinere Windparks,

[3] Große Hoffnungen werden in Bezug auf die verfügbare Speicherkapazität auf die Elektromobilität gesetzt. In einigen Jahren könnte durch eine ausreichende Anzahl akkubewehrter Elektromobile im Land ausreichend Kapazität zur Speicherung elektrischer Energie zur Verfügung stehen.

Photovoltaikanlagen und Blockheizkraftwerke erzeugen dezentral Strom und speisen diesen in das Netz ein. Zur Koordination der Stromerzeugung – wenn ein Windrad Strom einspeist kann dafür an anderer Stelle beispielsweise der Gashahn zugedreht werden – wird ebenfalls ein Datenaustausch benötigt. Strom wird also künftig bidirektional fließen.

Sobald die Technik zur Steuerung in Haushaltsgeräte integriert ist, ist der Schritt zum „Smart Home“ auch nicht mehr groß: Der Wäschetrockner, der eine E-Mail verschickt, sobald das Flusensieb verstopft ist, ist da sicher nur der Anfang.

In den USA steht darüber hinaus eine Verbesserung der Netzstabilität auf der Wunschliste – in Europa ist das nur ein Randaspekt.

2.2 Welche „Smart Grid“-Geräte gibt es im Haushalt?

2.2.1 Smart Meter

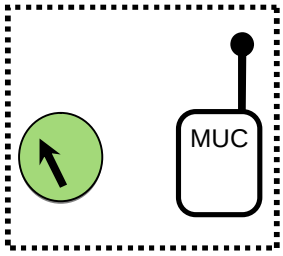

Abbildung 2: Stilisierter Smart Meter incl. Kommunikationsmodul

Der Grundbaustein des Smart Grid ist der Smart Meter, der digitale oder „intelligente“ Stromzähler. Vorgeschrieben durch das Energiewirtschaftsgesetz (EnWG[4]) findet bereits seit Anfang 2010 eine bundesweite Einführung statt. Smart Meter ermöglichen es, Stromverbrauchsmessungen in kurzen Zeitintervallen durchzuführen und die Ergebnisse in digitaler Form vor Ort im Zähler zu verarbeiten oder zu übertragen.

Mit Smart Metern an der Verbrauchsstelle lässt sich eine sehr genaue Lastbestimmung weitestgehend verzögerungsfrei durchführen[5]. Die Datenschutzprobleme, die sich durch die bei Smart Metern anfallenden haushaltsbezogenen Lastprofile ergeben, wurden an anderer Stelle ausführlich beleuchtet [5] [6]. Die spezifischen Fragestellungen in Bezug auf Datenschutz im Smart Grid werden im Beitrag von Ronald Petrlic (in diesem Tagungsband) behandelt [7].

Optional sind die heute verfügbaren Smart Meter mit einem Unterbrecher ausgestattet, der es dem Energieversorger erlaubt, den Haushalt aus der Ferne von der Stromzufuhr zu trennen. In der Argumentation der Zählerhersteller finden sich mehrere mögliche Einsatzszenarien für eine solche Funktion:

- Begrenzung der maximalen Leistungsaufnahme: Während sich das im Prospekt angenehm liest und nahe legt, dass mit dieser Funktion dem Stromkunden beim Stromsparen geholfen werden kann, lässt sich in der Praxis die Strommenge nur auf zwei Arten begrenzen: Da die Verringerung der Netzspannung keine vernünftige Option ist, bleibt nur die Unterbrechung der Stromzufuhr.
- Abklemmen säumiger Kunden: Der fernschaltbare Unterbrecher erspart nicht nur Kosten für Anfahrt und Arbeit, sondern vermeidet u. U. auch Gefahr für Leib und Leben des Monteurs, falls ein säumiger Kunde sich uneinsichtig zeigt.

Somit hält mit dem Smart Meter nicht nur ein Messgerät, sondern auch der erste Aktor Einzug in die Haushalte (siehe hierzu [8]).

[4] §21b (3a) EnWG

[5] Eine Messung im Straßenzug ist nicht zielführend: Durch die Marktliberalisierung sind heute an einem typischen Straßenzug Kunden verschiedener Versorger angebunden. Jeder Versorger soll jedoch die durch seine eigenen Kunden aufgenommene Energie bestimmen können.

2.2.2 „Intelligente Haushaltsgeräte“

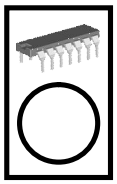

Abbildung 3: Stilisierte „intelligente Waschmaschine“

Auf der IFA 2010 wurden bereits erste Waschmaschinen und Wäschetrockner vorgestellt, die in der Lage sind, einen günstigen Stromtarif zu wählen und ihren Betrieb danach auszurichten [9]. In der ersten Generation lässt sich bei diesen Geräten lediglich der Startzeitpunkt von außen bestimmen. Für eine solche „Fernsteuerung“ eignen sich besonders solche Geräte, die einen hohen Stromverbrauch haben und bei denen sich der Zeitpunkt der Energieaufnahme vom Zeitpunkt der Benutzung entkoppeln lässt. Das sind also insbesondere thermische Systeme wie Kühl- und Gefriergeräte oder Wärmepumpen, aber auch Wasch- oder Spülmaschinen.
In einem weiteren Schritt wäre eine detailliertere Steuerung von Außen denkbar, z. B. des genauen Startzeitpunkts einer Heizphase innerhalb des Programmablaufs der Spülmaschine oder der Drehzahl des Trockners in Kombination mit der Laufzeit. Bei geringerer Drehzahl und Wärmezufuhr würde die Leistung reduziert – dafür würde die Laufzeit des Programms verlängert. Auf diese Weise könnte – in Abhängigkeit von der aktuell verfügbaren Leistung des Stromnetzes –der passende Ablauf gewählt werden. Hierbei würde ein Teil der Steuerung aus dem Gerät nach außen verlagert.
Daraus ergeben sich Haftungsfragen, die hier ebenfalls nur angerissen werden sollen: wer haftet, wenn ein Trockner ein Wäschestück beschädigt, weil die Trommel mit zu hoher Drehzahl gelaufen ist? An wen wendet sich der Besitzer wegen Ersatz seines aufgetauten Gefriertruheninhaltes? Es scheint, dass nicht nur der Ingenieurs- und IT-Branche die Arbeit vorerst nicht auszugehen droht…

2.2.3 „Intelligente Lüsterklemmen“

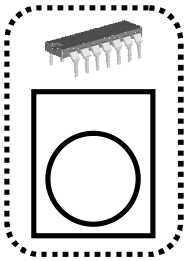

Abbildung 4: Stilisierte intelligente Waschmaschine, die durch eine externe Komponente „Smart Grid-fähig“ wird

Um auch mit „herkömmlichen“ Haushaltsgeräten in den Genuss der Möglichkeiten des Smart Grids zu kommen, soll es Schaltelemente geben, die sich vor die Geräte schalten lassen und ihre Steuersignale via Stromleitung (Power Line Communication – PLC) erhalten. Diese Schaltelemente werden eine Art „Brückentechnologie“ zu den intelligenten Haushaltsgeräten bilden – sie erlauben die Nutzung der neuen Technik auch mit herkömmlichen Geräten.

3 Was heißt „Sicherheit“ in diesem Kontext?

Die Tatsache, dass der Begriff „Sicherheit“ sowohl in der Informationstechnik als auch in der Elektrotechnik Verwendung findet, ist nur auf den ersten Blick beruhigend: Der Begriff wird in beiden Disziplinen unterschiedlich verwendet und erfordert daher eine genauere Betrachtung.

Sicherheit in der Informationssicherheit dient (nach dem Bundesamt für Sicherheit in der Informationstechnik, BSI) im Wesentlichen zur Gewährleistung von:

- Vertraulichkeit,
- Integrität,
- Authentizität und
- Verfügbarkeit.

In der Elektrotechnik hingegen richtet man sich danach, was der Verband der Elektrotechnik, Elektrotechnik, Elektronik und Informationstechnik e.V.[6] (VDE) darunter versteht:

- Vermeidung von Stromunfällen

In der englischen Sprache werden diese beiden Verständnisse in „safety“, den Schutz der Umgebung vor einem Objekt, und „security“, den Schutz eines Objektes vor seiner Umgebung unterschieden. Diese beiden Begriffe sind schnittmengenfrei.

[6] ehemals „Verband Deutscher Elektrotechniker“

Etwas weiter gefasst lassen sich aus Sicht der Elektrotechnik die Versorgungssicherheit und die damit einhergehende Netzstabilität noch unter „Sicherheit“ verbuchen. Diese decken sich am ehesten noch mit dem, was nach BSI unter der Verfügbarkeit verstanden wird.

Hier zeichnet sich also schon ein erstes Problem ab. Während für den Elektrotechniker „Sicherheit“ (safety) selbstverständlich höchste Priorität hat, sind ihm die Aspekte der Informationssicherheit (security) fremd.
Andererseits weisen die klassischen elektrotechnischen Geräte Standzeiten auf, die in der IT unerreicht sind. Die Herausforderung besteht nun unter anderem darin, Produkte zur Verfügung zu stellen, die allen diesen Anforderungen genügen.

Die Schutzziele, die in der Informationssicherheit primär verfolgt werden und im Smart Grid relevant sind Verfügbarkeit, Vertraulichkeit, Integrität sowie Authentizität. In den nachfolgenden Abschnitten werden diese Schutzziele kurz erklärt und an Beispielen die Auswirkungen von deren Verletzung beleuchtet.

3.1 Verfügbarkeit

Die Nicht-Verfügbarkeit der unterschiedlichen Smart Grid-Komponenten haben verschiedene Auswirkungen. Diese ist mit der Idee Versorgungssicherheit vergleichbar.

Die Nicht-Verfügbarkeit der Stromversorgung selbst bewirkt, dass der Nutzer seine elektrischen Geräte nicht benutzen kann.

Indirekt betroffen von einem Stromausfall ist die Kommunikation. Jegliche Internetkommunikation in einem normalen Privathaushalt benötigt das Stromnetz. Sofern das Telefon noch über analoge Technik oder ISDN angebunden ist, gibt es hier zumindest einen Notbetrieb: auch bei einem kompletten Stromausfall ist das Telefon noch nutzbar. Diese Betriebsart setzt allerdings voraus, dass die Stromversorgung durch die Telefonleitung zur Speisung des Telefons ausreicht. Dies ist bei vielen Geräten – insbesondere, wenn es sich um schnurlose Geräte handelt – heute nicht mehr der Fall.

Durch einen Ausfall der Smart Grid-Kommunikationsverbindung ist – auch bei vorhandener Stromversorgung – eine Steuerung der Smart Grid-Geräte nicht möglich.

3.2 Vertraulichkeit

Der Schutz vor unberechtigter Kenntnisnahme wird als Vertraulichkeit bezeichnet. Eine Entsprechung zur Welt der Elektrotechnik gibt es hier wie bei den Folgenden Zielen nicht.

Mit den intelligenten Zählern können Ablesungen in kurzen Zeitabständen vorgenommen werden. Hierdurch lassen sich Lastprofile bilden, die detaillierte Rückschlüsse auf den Tagesablauf des Nutzers erlauben [5] [6].

Nicht nur die Zähler erzeugen im Smart Grid Daten, sondern auch die Smart Grid-Geräte selbst: Wäschetrockner, Klimaanlage, Kühlschrank, Wärmepumpe, … Zu wissen, dass sich solche Geräte im Haushalt befinden und wann, wie oft und wie lange sie benutzt werden gibt ebenfalls Einblicke in die Lebensverhältnisse des Nutzers.

Die optimale Abstimmung der eigenen Geräte auf die Randbedingungen erfordert das Einstellen einiger Parameter. Die akzeptablen Nutzungszeitfenster sagt etwas über die Wohnverhältnisse aus: bei dem die Waschmaschine auch nachts laufen kann, wohnt wahrscheinlich nicht in einer kleinen Mietwohnung. Dass ich bevorzugte Zeitfenster für meine Klimaanlage einstelle sagt aus, dass ich eine solche habe und vermutlich nicht in den einfachsten Verhältnissen lebe. Ob der Nutzer atomstromfreien Strom bevorzugt erlaubt eine Aussage in Bezug auf seine umwelttechnische Orientierung. Und schließlich kann man aus den akzeptablen Preisgrenzen eine Abschätzung über sein verfügbares Haushaltsbudget ableiten. All diese Parameter sollten im Haushalt selbst eingestellt werden und diesen auch nicht verlassen. Da dies jedoch nahezu beliebig komplex werden kann, könnten Dienstleister anbieten, diese Einstellungen auf Basis entsprechender Vorgaben des Benutzers vorzunehmen. Eine solche „Energieoptimierungsagentur“ hätte Kenntnis über all diese Parameter und damit entsprechenden Einblick in die Lebensverhältnisse des Kunden.

Im Detail werden die Auswirkungen von Verletzungen dieses Schutzziels im Beitrag von Ronald Petrlic (in diesem Tagungsband) behandelt [7].

3.3 Integrität

Die Integrität der Zähler sowie der durch den Zähler verarbeiteten Daten (Preise, Zählerstände, aufsummierte Kosten) dürfte aus der Perspektive der Energieversorger das höchste zu schützende Gut darstellen, da diese Daten die Basis für die Rechnungslegung bilden.

3.4 Authentizität

Der Kunde möchte sich sicher sein, dass er tatsächlich mit seinem EVU kommuniziert, denn einem fremden EVU möchte er z. B. seinen Zählerstand nicht anvertrauen. Ein fremdes Unternehmen (auch eine Versicherung oder die GEZ) könnte sich aus ganz anderen Gründen für den Zählerstand interessieren.

Das EVU auf der anderen Seite möchte sicher sein, dass es tatsächlich mit dem richtigen Kunden spricht. Ein verärgerter Ex-Kunde könnte z. B. versuchen, dem EVU gefälschte Messwerte unterzuschieben, um so die Strombereitstellungsplanung zu stören.

4 Kommunikationsbeziehungen und Angriffsszenarien

Die im Folgenden dargestellten Angriffsszenarien ergeben sich im Wesentlichen aus der Tatsache, dass die Geräte, die bislang ausschließlich in einer „freundlich gesinnten“ oder geschlossenen Umgebung eingesetzt wurden, sich nun in einer potenziell unfreundlichen Umgebung wieder finden. Das gilt besonders für die Smart Meter aber auch für die Smart Grid-fähigen Geräte im Haushalt und deren Kommunikationspartner auf der Seite der Energieversorger.

4.1 Rund um den Smart Meter

Smart Meter sind die ersten Smart Grid-Geräte im Haushalt und als konkrete Produkte auch schon seit Monaten am Markt verfügbar. Die Kommunikationsbeziehungen der Smart Meter sind in diesem Abschnitt – nach einem Einschub zum Thema „Zähler-Kompromittierung“ – aufgeführt.

4.1.1 Zähler-Kompromittierung

Eine Fälschung der Zählerstände zu seinen Gunsten kann für den Kunden erhebliche finanzielle Vorteile haben, daher stellt sich die Frage „Werden Smart Meter kompromittiert werden?“ nicht. Die richtige Frage lautet:

> „Was können wir tun, um die Auswirkungen minimal zu halten?“

In den vergangenen Jahren gab es mehrere Anläufe, manipulationsgeschützte Plattformen in großen Stückzahlen auszurollen. Hierzu eine kurze Betrachtung der Risiken und Chancen des Nutzers bezüglich einer Kompromittierung der Geräte:

- Risiken: Musste der Nutzer zur Kompromittierung gegen geltendes Recht verstoßen?
- Chancen: Welchen Vorteil hatte ein Besitzer durch eine Kompromittierung?

Beispiel	Risiken	Chancen (Auswahl)	Methode	Ergebnis
Empfänger für Bezahlfernseh-Sender	**Besitz und Nutzung** der Software **illegal**	**kostenloser Zugang** zu eigentlich kostenpflichtigen **Leistungen** (Fernsehprogramm); zusätzliche Features (Streaming-Client, Bildbetrachter, …)	reverse engineering	geknackt
Spielkonsolen	**Besitz und Nutzung** der Software **illegal**	**kostenloser Zugang** zu eigentlich kostenpflichtigen **Leistungen** (raubkopierte Spiele); zusätzliche Features (Streaming-Client, …)	reverse engineering	geknackt
SIM-Unlock für Smartphones	Nutzung der Software stellt zumindest einen **Vertragsbruch** das [10]	Nutzung **günstigerer** Netzanbieter im Ausland[7]	reverse engineering	geknackt
Smartcards	**Nutzung** gebrochener Smartcards zum Erlangen von Zugang **illegal**	z. B. **unberechtigter Zugang** zu Räumlichkeiten	Mechanisches Abtragen der Logikschichten [11], reverse engineering	geknackt
Firmware für Digitalkameras	Nutzung legal; Hersteller verweist auf mögliche Schäden	**kostenlose Nutzung** zusätzlicher Features [12] (Zeitraffer, Bewegungsmelder, Skriptmöglichkeit, …)	Ausgabe der Firmware via AF-Leuchte [13], reverse engineering	
Kopierschutz in DVD- und Blu-Ray-Spielern	**Vertrieb** der Software in Deutschland **illegal**	**Kostenloser Zugang** zu eigentlich kostenpflichtigen **Leistungen** (Filme)		geknackt
Smart Meter	**Nutzung illegal**[8]	**kostenloser Zugang** zu eigentlich kostenpflichtigen **Leistungen** (lt. Statistischem Bundesamt machten 2009 allein die Kosten für elektrische Energie 2,5% [14] der Ausgaben der privaten Haushalte aus)	?	?

Fazit:

→ „hacking smart meters for fun and profit!“

Ein Angriff auf einen Smart Meter ist für den Nutzer grundsätzlich leicht, da sich der Zähler in seinem physischen Zugriff befindet. Zudem ist die Entdeckungswahrscheinlichkeit vergleichsweise gering, da die Manipulation möglicherweise für den Energieversorger nicht leicht erkennbar ist und die Kosten für den Tausch eines Zählers oder eine Komponente hoch sind.

Da von einer Manipulation sogar kurzfristig eine große Anzahl von Zählern betroffen sein kann, ist der potenzielle Schaden für den Energieversorger erheblich. Die Anforderungen an die Schutzmechanismen (Verschlüsselung, Redundanz, Manipulationsschutz etc.) sind dadurch hoch, während umgekehrt die Kosten pro Gerät und der erforderliche Stromverbrauch minimal sein sollten.

[7] Sollte nicht die Tatsache, dass die EU die Mobilfunkanbieter vor sich hertreibt bedenklich stimmen? Stichwort: Roaminggebühren im Ausland

[8] §248c StGB Entziehung elektrischer Energie und §303 StGB Sachbeschädigung

4.1.2 Kommunikation zwischen Smart Meter und MUC

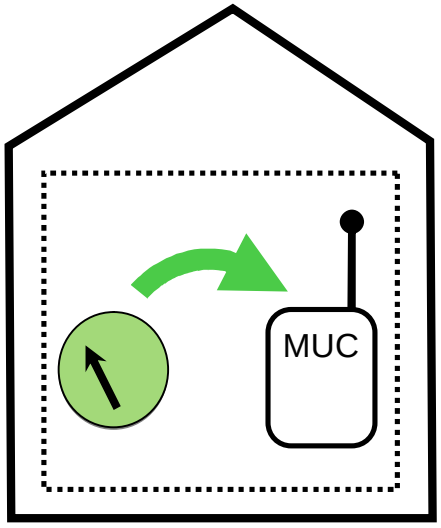

Abbildung 5: Smart Meter mit externem Kommunikationsmodul (MUC)

Als MUC[9]-Controller (Multi Utility Communication) bezeichnet man eine zentrale Kommunikationseinheit im Haushalt, die von verschiedenen Komponenten (Smart Meter für Strom, Gas, Wasser und ggf. weitere Smart Grid-Geräte) gemeinsam zur Kommunikation untereinander und mit dem Energieversorger genutzt werden. Vorteile sind neben den Kosten für die Hardware (das Kommunikationsmodul wird nur ein Mal benötigt) auch niedrigere Installations- und Betriebskosten.
Allerdings ergeben sich durch die zusätzlichen Schnittstellen zwischen Smart Meter und MUC auch neue Angriffsflächen – insbesondere wenn man sich vor Augen führt, dass der Hardwarekostenvorteil besonders dann zum Tragen kommt, wenn eine anspruchsvolle Verschlüsselungskomponente ebenfalls nur in der MUC ausgeführt ist. Damit stellt sich die Frage, wie die Sicherheit (Vertraulichkeit, Integrität, Authentizität) der Verbindung zwischen Smart Meter und MUC geschützt werden kann. Dabei ist sowohl der Nutzer zu betrachten, der die übermittelten Daten kompromittieren möchte als auch der Angreifer, der physikalisch (Nachbar, der Zugang zum Zählerkasten hat) oder via Luftschnittstelle Zugriff hat

Aus funktionaler Sicht ist eine Vielfalt an Schnittstellen wünschenswert: kabelgebundene (PLC, DSL, LON, M-BUS, …) und kabellose Protokolle (GSM, UMTS, Zigbee [15], WLAN, Bluetooth, Wireless M-Bus, …). Dadurch entsteht aus sicherheitstechnischer Sicht aber zugleich eine große Angriffsfläche, da alle Schnittstellen abgesichert werden müssen.

[9] Genau genommen heißt das Kommunikationsmodul natürlich nur dann „MUC“, wenn es nicht im Smart Meter integriert, sondern separat ausgeführt und in der Lage ist, die Kommunikation für mehrere Smart Meter zu übernehmen.

4.1.3 Service-Schnittstellen

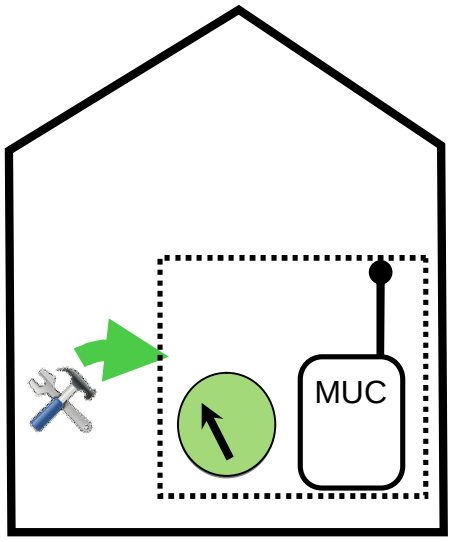

Abbildung 6: Serviceschnittstelle am Smart Meter

Über eine (lokale oder entfernte) Serviceschnittstelle wird ein Zugriff auf den Smart Meter möglich sein, z. B. um ein Upgrade der Firmware des Smart Meters vornehmen zu können. Hier lauern gleich mehrere Gefahren: Die Schnittstelle kann zur Manipulation des Zählers missbraucht werden, aber auch ein berechtigter Service-Mitarbeiter könnte eine manipulierte Firmware aufspielen (siehe Diebold-Wahlmaschinen [16] oder die AusweisApp [17]).

Sofern eine „Auto-Update“-Funktion integriert wird, kommen zu den oben genannten Kommunikationsprotokollen weitere Serviceschnittstellen (u. a. für Firmwareupgrades) hinzu.

4.1.4 Verbindung zwischen Smart Metern und Netzwerkinfrastruktur

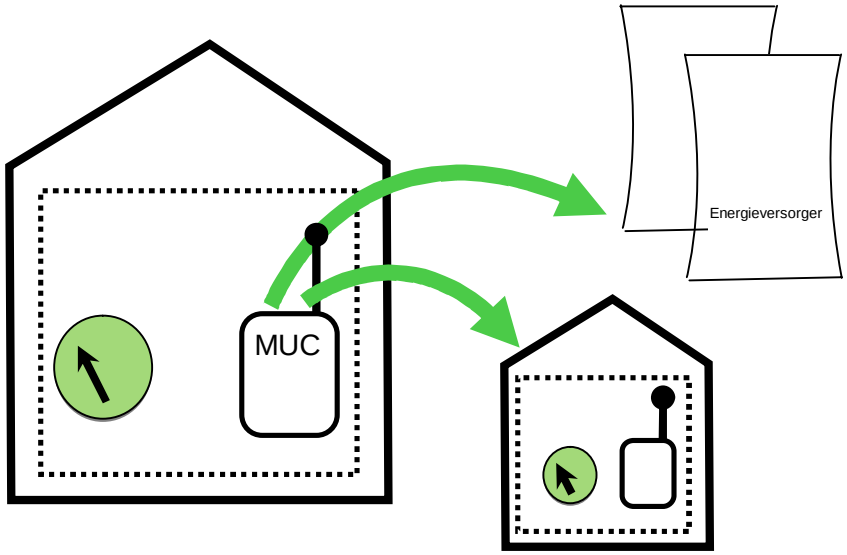

Abbildung 7: Aus Sicht der Netzwerkinfrastruktur sollten die Smart Meter als nicht vertrauenswürdig eingestuft werden. Direkte Verbindungen zwischen Smart Metern werden nicht benötigt und sollten daher durch die Infrastruktur unterbunden werden

Ein einzelner Smart Meter befindet sich – wenn auch mit „juristischen Sicherungen“ versehen – im physikalischen Zugriff des Nutzers. Eine lokale Kompromittierung muss daher als die wahrscheinlichste Möglichkeit angesehen werden – vergleichbar einem exponierten Server, der aus dem Internet erreichbar ist. Daher sollten Smart Meter nicht als vertrauenswürdig, sondern als potenziell kompromittiert eingestuft werden.

Läuft die Kommunikationsverbindung zwischen Smart Meter und EVU via PLC, liegt diese Verbindung – genau wie die Stromversorgung – außerhalb des direkten Zugriffs des Nutzers. Eine Unterdrückung der Kommunikation ist daher für einen Angreifer nicht einfach möglich – wohl aber eine Störung. Bei Standard-Kommunikationsprotokollen (DSL, ISDN, GSM) hat der Nutzer direkten Zugriff auf die Verbindung und kann die Kommunikation auch vollständig unterdrücken. Er könnte auf diese Weise die Abrechnung behindern oder verhindern, dass Messwerte übertragen werden. Als Abhilfe hierfür ist in den Smart Metern ein Speicher für Messwerte eines Zeitraums von 90 Tagen vorgesehen. Empfängt das EVU über diesen Zeitraum keine Messwerte vom Smart Meter, wird ein Techniker vor Ort geschickt. Er liest die gespeicherten Werte aus, klärt und behebt die Ursache der Störung.

4.1.5 Zugriff des EVU auf den Unterbrecher im Smart Meter

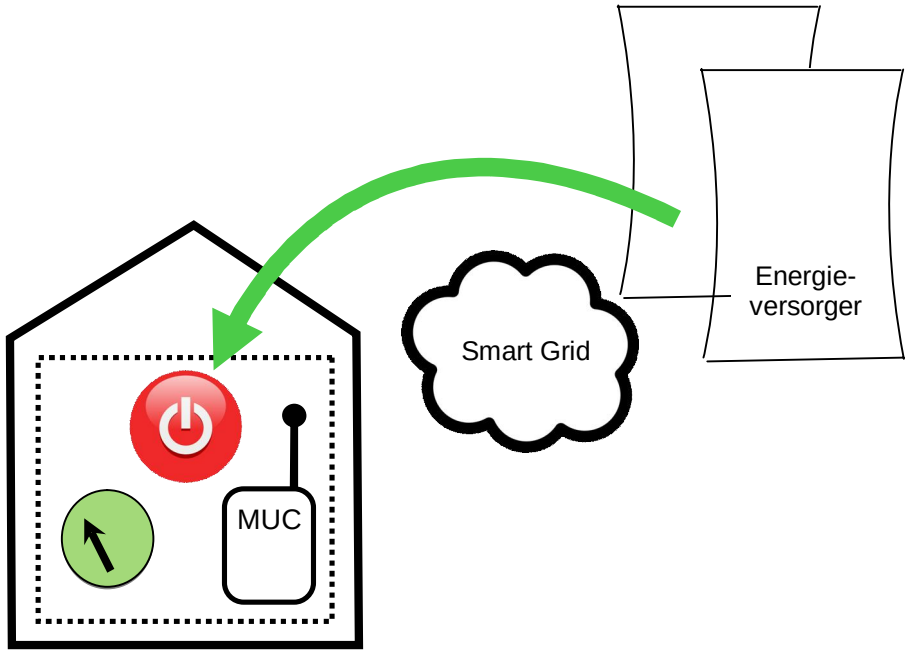

Abbildung 8: Zugriff des Energieversorgers auf den Unterbrecher im Smart Meter

Der Unterbrecher als Ausstattungsmerkmal im Smart Meter klingt im Moment nach einer interessanten Option. Neben den genannten Vorteilen, die sich aus Kundensicht konstruieren lassen zeigt sich als Argument aus Sicht des EVU die Sanktionierung säumiger Kunden.

Der Vergleich mit dem Telefonanschluss legt nahe, dass eine Sanktionierung aus der Ferne bislang an der Technik gescheitert ist. Beim Telefonanschluss konnte schon seit jeher prinzipbedingt – durch die separate Leitungsführung – auch mit geringem Aufwand an zentraler Stelle eine Trennung vorgenommen werden. Als verfeinerte Variante ist hier schon seit Jahrzehnten eine gezielte Teilsperrung möglich, bei der nur noch ankommende Rufe möglich sind und somit keine Gesprächskosten mehr anfallen können. Eine weitere Abstufung schließlich ist der reine Notrufbetrieb, bei dem dann auch ankommenden Rufe nicht mehr möglich sind, sondern ausschließlich Notrufe. In dieser Betriebsart kann ein Anschluss auch für längere Zeit verbleiben, ohne dass dem Anbieter hierdurch ein Geschäft verloren ginge oder Kosten entstünden.
Man könnte also meinen, das Nichtvorhandensein solcher Mittel sei rein der Technik geschuldet. Bei genauerer Betrachtung stellt sich dieser Ansatz jedoch als reichlich naiv heraus.
Im Gegensatz zum Telefon ist beim elektrischen Strom eine Leistungsbegrenzung immer mit einer Stromunterbrechung verbunden. Rein technisch wäre auch eine Begrenzung der abgegebenen elektrischen Leistung über eine Verringerung der Spannung möglich – allerdings verbietet sich dieser Kniff, da die Geräte hierfür nicht ausgelegt sind.[10] Als einzige Möglichkeit bleibt also die Überwachung eines Schwellwertes[11] und die Trennung der

[10] Genau genommen gilt das nicht für Schaltregler, wie sie sich in modernen Netzteilen finden. Diese können tatsächlich problemlos in einem sehr weiten Spannungsbereich arbeiten – dadurch wird jedoch das Ursprungsproblem – Begrenzung der Leistungsabgabe – nicht gelöst.
[11] z. B. 100 Watt für einen „Notbetrieb“, über den auch der maximale Rechnungsbetrag begrenzt würde

Stromzufuhr bei Überschreitung. Jede „Begrenzung“ ist in der Praxis also technisch immer eine „Trennung“.

Sehr viele Geräte in einem Haushalt funktionieren heute nicht mehr ohne elektrischen Strom. Das gilt in den meisten Fällen auch für das Telefon. Bei ISDN ist noch ein Notbetrieb gewährleistet, bei dem die Leitung auch ohne Strom in der Wohnung genutzt werden kann. Dies gilt allerdings dies nur für ISDN-Telefone, die selbst diese Betriebsart unterstützen – nicht aber für schnurlose Telefone, da der verfügbare Strom aus der ISDN-Leitung nicht zur Versorgung der Basisstation ausreicht. Dass bei VoIP kein Notbetrieb möglich ist, dürfte klar sein. Eine Stromunterbrechung könnte also bewirken, dass ggf. auch kein Notarzt gerufen werden kann. Besonders drastisch ist das Beispiel eines Dialyse-Patienten – was passiert, wenn der Strom während einer Behandlung unterbrochen wird?

Führt man sich also vor Augen, dass ein EVU die Auswirkungen einer solchen Trennung nicht bewerten kann, muss bezweifelt werden, dass ein EVU von dieser Möglichkeit überhaupt Gebrauch machen wird.

Die Ausstattung von Smart Metern mit Unterbrecherfunktion ergibt andererseits eine neue Angriffsfläche: Die Auswirkungen einer Schwachstelle, die einen Missbrauch der Unterbrecherfunktion ermöglicht, könnten erheblich sein. In [8] wird skizziert, welche Szenarien sich daraus ergeben. Allein die Frage nach dem „recovery plan“, dem „Wiederanlauf“, ist spannend. Die Reichweite der Konsequenzen geht hier deutlich über Haftungsfragen hinaus. Nicht zuletzt ist davon auszugehen, dass im *worst case* (die Haushalte werden über die Unterbrecher im Smart Meter durch einen Angreifer oder eine Schadsoftware großflächig vom Stromnetz getrennt) der Wiederanlauf so aussehen würde, dass Monteure die betroffenen Smart Meter überbrücken würden. Das Neubespielen mit fehlerbereinigter Software würde möglicherweise zu viel Zeit pro Einsatz in Anspruch nehmen, und ein Tausch würde angesichts mehrerer Mio. betroffener Geräte keine reale Option darstellen. Nach dem Wiederanlauf wären also bei entsprechenden Randbedingungen die Smart Meter – auch in ihrer schlichten Funktion als Energiemengenzähler – deaktiviert.

4.2 Kommunikation zwischen Smart Grid-Geräten im Haushalt

Im Falle der Nutzung eines „Max-Strom“-Tarifs darf der Kunde eine bestimmte Leistungsaufnahme zu keinem Zeitpunkt überschreiten. Anderenfalls wird die Versorgung entweder unterbrochen oder der Strompreis angehoben. Bei einem solchen Modell wäre eine Abstimmung der Verbraucher untereinander sinnvoll: Die Wärmepumpe, der Kühlschrank und die Gefriertruhe beziehen nur dann Strom, wenn die Gesamtabnahme unter dem Schwellwert liegt – im Idealfall funktioniert das sogar priorisiert. Zur Abstimmung müssen die Geräte direkt oder – bevorzugt – indirekt über eine zentrale Einheit kommunizieren.
Man könnte dieses Modell „kooperative Stromnutzung“ nennen. Ein Gerät, welches sich unkooperativ verhält, kann das Zusammenspiel allerdings lahmlegen:

- verbraucht es mehr, als es angegeben hat, wird der Schwellwert überschritten und der Unterbrecher ausgelöst
- meldet ein Gerät, dass es – demnächst – eine hohen Verbrauch haben wird, werden andere Geräte nicht aktiviert oder herunter gefahren, damit der Schwellwert nicht überschritten wird

Über ein fehlerhaftes oder durch Schadsoftware manipuliertes Smart Grid-Gerät ließe sich so die Verfügbarkeit der anderen Smart Grid-Geräte im Haushalt angreifen.

4.3 Steuerung intelligenter Haushaltsgeräte durch ein EVU

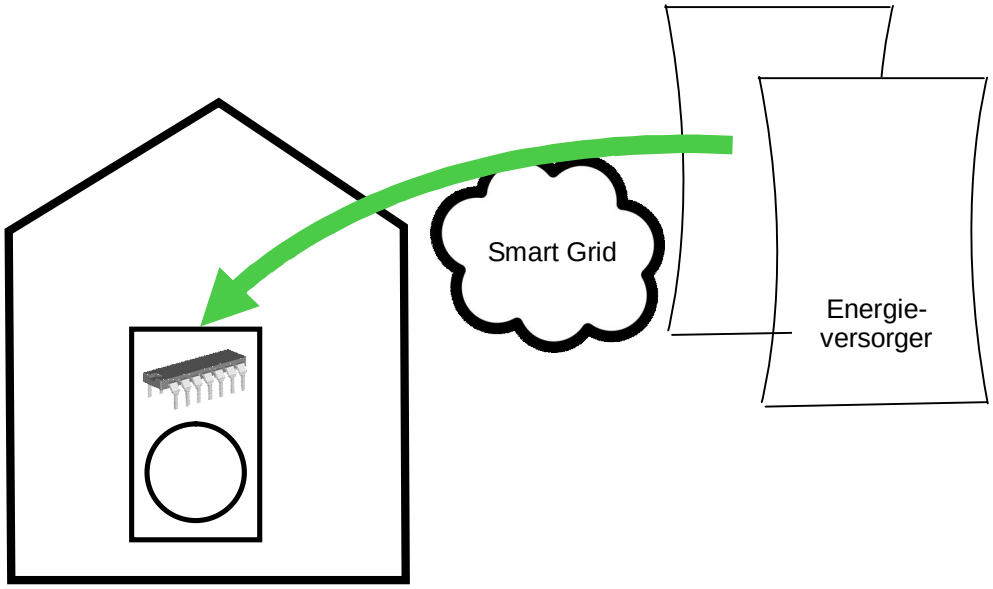

Abbildung 9: Zugriff des Energieversorgers auf ein intelligentes Haushaltsgerät

Als Reinkarnation der Rundsteuerempfängerfunktion erlaubt die Schnittstelle zwischen EVU und intelligentem Haushaltsgerät den Fernzugriff des EVU auf Verbraucher im Haushalt. Dies stellt eine der wesentlichen Funktionen des Smart Grid dar: Das EVU soll dadurch bei Stromüberschuss Lasten anschalten und bei Lastspitzen Lasten „abwerfen“ können, um so den tatsächlichen Verbrauch zu steuern.

Aus Sicht des Nutzers sind dabei die folgenden Angriffsszenarien zu betrachten:

- Deaktivierung der Geräte (Einschränkung der Verfügbarkeit)
- Änderung der Gerätekonfiguration, z. B. Setzen der Raumtemperatur der Klimaanlage auf +30° C oder der Solltemperatur der Kühltruhe auf +5° C (Manipulation der Lebensbedingungen)
- Das konstante Ein- und Ausschalten der Beleuchtung würde den dauerhaften Aufenthalt in der Wohnung nahezu unmöglich machen[12] („blinkenlights@home“ [18])
- Modifikation der Preisinformation bei der Übertragung (finanzieller Schaden für den Nutzer)
- Unerwünschte Aktivierung von Geräten (Verursachung von Verbrauchskosten, ggf. unangenehme Nebeneffekte wie Überlastung des Hausnetzes)

Die Rahmenbedingungen für Implementierungen bei „intelligenten Lüsterklemmen“ sind noch strikter als bei Haushaltsgeräten: Insbesondere der Ressourcenbedarf muss gering bleiben, um den Anforderungen an Baugröße und Preis zu genügen.

[12] Immerhin bliebe hier noch die Deaktivierung der Beleuchtung durch das Herausnehmen der Sicherung oder des Leuchtmittels selbst. Dann ginge es nur noch um einen DoS-Angriff.

4.4 Energieoptimierungsagentur

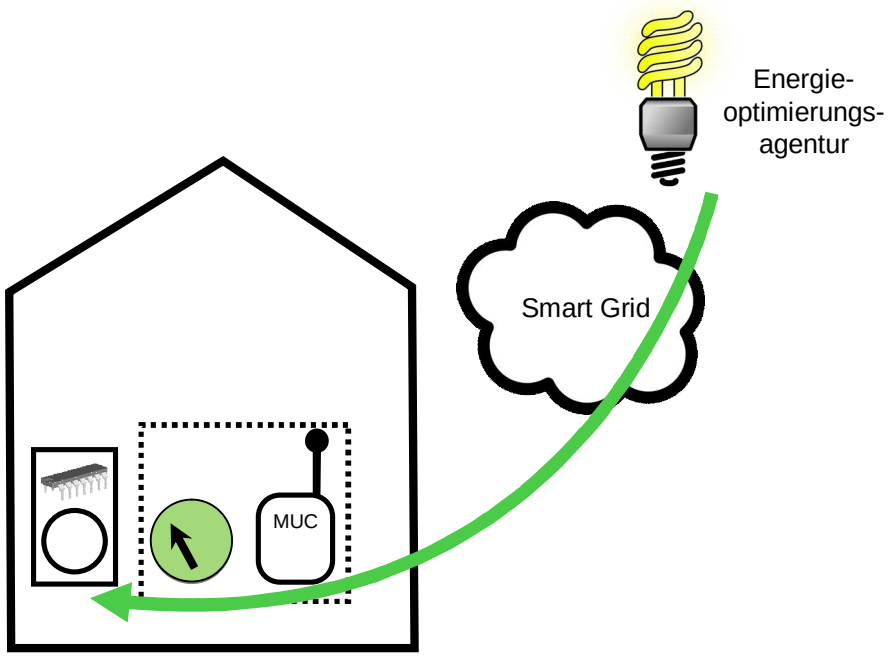

Abbildung 10: Zugriff der Energieoptimierungsagentur auf die Smart Grid-Geräte

Zusätzlich zu den im vorigen Abschnitt aufgeführten Möglichkeiten des EVU kommen bei der Nutzung einer Energieoptimierungsagentur folgende Aspekte hinzu:

- Im Gegensatz zum EVU ist für manche Energieoptimierungsagentur eine gute Reputation verzichtbar (siehe Call-by-Call-Anbieter im Telefonmarkt). Die Versuchung, diese Zugriffsmöglichkeiten zu missbrauchen, dürfte also wesentlich größer sein als für ein EVU.
- Die Energieoptimierungsagentur bekommt u. U. Zugriff auf Parameter und Schnittstellen, die eigentlich dem Nutzer vorbehalten sind – die Agentur handelt schließlich in Vertretung des Nutzers.
- Die detaillierten Informationen, die der Energieoptimierungsagentur über den Nutzer vorliegen, stellen an sich einen Wert dar und könnten z. B. für Marketingzwecke genutzt oder auch missbraucht werden:
  Als Basis für die Steuerung von Geräten gibt der Benutzer über die Nutzungsdaten (Nutzungs- und damit Verhaltensprofil) hinaus zu erkennen, wann ein Gerät im aktivierbaren Zustand ist (Spül-/Waschmaschine ist beladen bzw. wird – während des Urlaubs – über mehrere Tage nicht in diesen Zustand versetzt).

4.5 Gerätesteuerung durch Preismanipulation

Starke Lastschwankungen werden auch künftig problematisch sein.[13] Neben der direkten Möglichkeit, Verbraucher zu aktivieren, ergibt sich durch Tarifmanipulationen auch ein indirekter Vektor. Dabei ist es zweitrangig, ob der tatsächliche Strompreis an der Börse manipuliert wird [19] oder der Wert, der von den Geräten als Basis herangezogen wird – sei es durch Manipulation der Webseite, von der der Preis abgerufen wird, oder durch einen man-in-the-middle-Angriff [20] auf die Übertragung (siehe 4.3). Im Ergebnis würde ein Tarifsprung dazu führen, dass sehr viele Verbraucher gleichzeitig eingeschaltet würden.

5 Gegenmaßnahmen

Die zu erwartenden Herausforderungen liegen an den gleichen Stellen wie bei sonstigen IT-Systemen. Durch die beschriebenen besonderen Randbedingungen im Smart Grid sollten die folgenden Prinzipien besondere Beachtung finden: entweder weil das Problem unterschätzt werden könnte oder weil die Auswirkungen im Smart Grid besonders weit reichend wären. Die Gegenmaßnahmen lassen sich in 3 Bereiche einteilen:

- Designprinzipien
- IT-Sicherheits-Handwerk
- Maßnahmen gegen konkrete Angriffe

5.1 Designprinzipien

5.1.1 Folgeschäden begrenzen („fail securely“)

Der Ausfall einer Sicherheitseinrichtung sollte grundsätzlich so gut wie möglich vermieden werden, indem jede Sicherheitseinrichtung mit der maximal möglichen Robustheit versehen wird. Der Ausfall einer Einrichtung muss als Option jedoch mit berücksichtigt werden – und Designentscheidungen sollten so getroffen werden, dass die Auswirkungen eines Ausfalls möglichst gering sind [21].

Als Beispiel soll der Ausfall der Zähleinrichtung im Smart Meter betrachtet werden. Was soll passieren, wenn die Zähleinrichtung ausfällt?

- Sollte die Stromzufuhr unterbrochen werden oder nicht?
- Soll ein Alarm ausgelöst werden? Wer ist ggf. zu alarmieren?

Natürlich sollte nach Möglichkeit verhindert werden, dass eine Zähleinrichtung überhaupt ausfällt; wenn der Fall dann aber doch eintritt, sollte dieses Ereignis (sofern möglich) gemeldet werden.

5.1.2 Entkopplung kritischer Infrastrukturen von anderen

Die kritischen Systeme und Netze im Smart Grid sollten möglichst von den nicht-kritischen entkoppelt werden. Wenn man bedenkt, dass das durch den Virus „Blaster“ im Sommer 2003

[13] Eine sehr anschauliche Darstellung der Auswirkung von Lastsprüngen findet sich im Video [1]. Wie wirkt sich das gleichzeitige Einschalten von 1,5 Mio. Wasserkocher auf die Netzfrequenz aus?

verstopfte Kommunikationsnetz den Abgleich über die aktuelle Auslastung der Kraftwerke und Netze verhindert und in der Folge den plötzlichen Zusammenbruch weiter Teile der Energienetze in den USA geführt hat [22], wird klar, dass eine tatsächliche Entkopplung schwieriger ist, als es auf den ersten Blick erscheint.[14] Das Beispiel zeigt, dass ein erster wichtiger Schritt hierzu in der Identifikation der tatsächlichen kritischen Systeme und Netze besteht.

5.1.3 Angriffsfläche minimieren

Die Smart Meter sollten keine Unterbrecherfunktion beinhalten. Falls sie eine solche Einheit haben, sollte diese nicht aus der Ferne auslösbar sein, sondern einzig in der Art einer Sicherung arbeiten und bei der Überschreitung eines Schwellwertes auslösen. Das mit einem von Ferne aktivierbaren Unterbrecher einher gehende Risiko überwiegt den Nutzen bei Weitem.

Das US-amerikanische Verteidigungsministerium untersucht, ob über die Etablierung von Mikro-Grids, also kleinen, autarken Energieversorgungszellen bestehend aus Generatoren (Wind, Sonne) und Verbrauchern die Resistenz des Gesamtnetzes gegen großflächige Angriffe erhöhen können [23].

5.1.4 Nicht auf „juristische Sicherungen“ vertrauen

Wo möglich sollten technische Schutzlösungen zur Verhinderung der dargestellten Angriffsszenarien gewählt werden. „Juristische Sicherungen“ (wie § 248c StGB – Entziehung elektrischer Energie und § 303 – Sachbeschädigung) haben nur eine begrenzte Wirkung. Eine schwer zu entdeckende und vielleicht einfach umzusetzende Manipulation am Smart Meter sollte nicht einzig durch eine Plombe am Gerät und eine Strafandrohung in den AGB abgesichert sein. Essenziell ist hierbei die Erkennung von Manipulationsversuchen auf verschiedenen Ebenen.

Das Lastenheft des EDL sieht vor, dass äußere magnetische Einflüsse sowie optional das Öffnen oder Manipulieren des Gehäuses lokal angezeigt und im Logbuch dauerhaft festgehalten wird. Falls der Zähler durch starke Magnetfelder gestört werden kann, ist auch hierfür ein Sensor vorzusehen. Darüber hinaus würde ein optischer Sensor das Unerkannte Öffnen des Zählers erschweren [24]. Nach Möglichkeit sollten weitere technische Maßnahmen z. B. zum Schutz vor Software-Manipulationen ergänzt werden.

Um das Ergebnis der Chancen-/Risiken-Abwägung aus Sicht des Angreifers unattraktiver zu machen, sollten weitere Maßnahmen vorgesehen werden, insbesondere zur Integritätssicherung der Firmware. Darüber hinaus sollten – sofern eine Kommunikationsschnittstelle verfügbar ist – Manipulationsversuche mit den übermittelten Zählerständen/Energiekosten gemeldet werden.

[14] Ob „Blaster“ tatsächlich die Ursache für den Stromausfall war, ist umstritten. Bei der Diskussion wurde jedoch deutlich, dass auch bei „entkoppelten“ Systemen eine Störung im einen System den Ausfall des anderen

5.2 IT-Sicherheits-Handwerk

Die folgenden Maßnahmen zählen zum normalen „Handwerkszeug“ der IT-Sicherheitsbranche. Eine gesonderte Auflistung erscheint daher nicht erforderlich. Die Erfahrung zeigt jedoch, dass sich beim Schritt aus einer geschlossenen Umgebung in eine offene nicht nur die Anzahl der potenziellen Kommunikationspartner insgesamt, sondern insbesondere die Anzahl der potenziell unfreundlichen Kommunikationspartner drastisch steigt. Schwachstellen werden daher in kürzerer Zeit aufgedeckt und auch ausgenutzt.

5.2.1 Authentifizierung richtig machen

Der Schutz der Smart Grid-Geräte vor Angreifern baut auf einer robusten Authentifizierung. Standardpasswörter [25] sollten in aktuellen Produkten nicht mehr zu finden sein. Eine zertifikatsbasierte Authentifizierung würde gleich eine ganze Klasse von Schwachstellen vermeiden helfen.

5.2.2 Over-the-air-update vorsehen

Über ein Over-the-air-update (OTA) ist es möglich, die Software auf einem Gerät aus der Ferne zu aktualisieren. Gegen die Implementierung einer solchen Funktion spricht, dass auf diese Weise zusätzliche Angriffsfläche geschaffen wird, die ein lohnendes Ziel für einen Angreifer darstellt: Die Möglichkeit, die komplette Software auf einem Gerät auszutauschen entspricht einem maximalen Freiheitsgrad.

Auf der anderen Seite ist – realistisch betrachtet – davon auszugehen, dass Schwachstellen in den Geräten bekannt werden, die eine Kompromittierung erlauben werden. Über ein OTA-update lässt sich die fehlerhafte Software aus der Ferne durch eine bereinigte Version ersetzen.

Insbesondere im Hinblick auf die angestrebte Standzeit in Verbindung mit den Anforderungen an die Sicherheit (Schlüssellängen, Verschlüsselungsverfahren, Schlüsselmaterial, Zertifikate, …) erscheint eine Update-Funktion unverzichtbar. Es ist nicht davon auszugehen, dass die Software über die gesamte Laufzeit des Systems unverändert bleiben kann; ein Gerätetausch zu diesem Zweck verursacht allerdings zu hohe Kosten.

Die Verantwortung für den ordnungsgemäßen Zustand der Smart Meter liegt beim EVU bzw. dem MSB. Das Einspielen des Updates kann für die Smart Meter daher durch diesen erzwungen werden.

Für Smart Grid-fähige Geräte liegt die Verantwortung für die Durchführung von Updates hingegen beim Nutzer. Updates können nur durch diesen oder mit dessen Einverständnis angestoßen werden. Das Einspielen von Updates sollte deshalb möglichst einfach und attraktiv gemacht werden. Hier könnte sich als eine Situation ergeben, die dem schlechten durchschnittlichen Patchstand verbreiteter Heim-PCs ähnelt. Schlecht gepatchte Smart Grid-fähige Geräte werden ebenfalls als Brutstätte von Malware dienen.

5.3 Maßnahmen gegen konkrete Angriffe

5.3.1 Tarifsprünge

Durch Preisänderungen soll eine Steuerung der Last ermöglicht werden. Finden diese Änderungen – z. B. beim Wechsel von Tarifzeiten oder im Falle von lastabhängigen Tarifen durch starke Laständerungen – in Form von Sprüngen statt, werden diese wiederum starke Laständerungen zur Folge haben. Was eigentlich als Grundidee gedacht war, kann zu erheblichen Netzbelastungen führen. Zur Abmilderung der Auswirkungen von Tarifsprüngen sollten Verfahren etabliert werden, die ein zeitgleiches oder zeitnahes Schalten großer Mengen von Verbrauchern entzerren, z. B. indem das Gerät zwischen dem festgestellten Tarifwechsel und der Aktivierung eine zufällige Zeitspanne zwischen 0 und einem Maximalwert verstreichen lässt. Auf diese Weise kann die Belastung des Netzes über diese Zeitspanne entzerrt werden (vgl. CSMA/CD bei Ethernet).

5.3.2 Auslesen von Verbrauchsprofilen (Seitenkanalangriff)

Natürlich lässt sich vermeiden, dass über das Verbrauchsprofil Informationen über Vorgänge im Haushalt preisgegeben werden. Als radikale Methode könnte man den Ansatz aus dem militärischen Umfeld kopieren, bei dem z. B. bereits die Entstehung eines Profils dadurch verhindert wird, dass eine Leitung nicht nur dann benutzt wird, wenn tatsächlich Daten zu übertragen sind, sondern ständig gefüllt wird.
Theoretisch wäre diese Lösung auch beim Strom denkbar: ein Gerät, welches die Gesamtleistungsaufnahme auf z. B. 4.000 Watt auffüllt – allerdings ist dies weder aus Kostensicht sinnvoll noch in Anbetracht der Tatsache, dass es beim Smart Metering primär um das Stromsparen geht.

Ein Zwischenweg wäre allerdings in Form von „Anwesenheitssimulatoren“ denkbar: Zeitschaltuhren, die die Licht- und Rollladensteuerung zufällig übernehmen und auch per LED-Beleuchtung ein Flimmerlicht an die Wand werfen, existieren bereits [26][24]. Wenn nun als neuer „Blickwinkel“ auf die Vorgänge im Haushalt der Stromverbrauch dazu kommt, bräuchte man eben ein Gerät, welches Strom beziehen (und ggf. in Wärme umsetzen) kann, um auch auf diesem Kanal ein realistisches Bild abzugeben. Aus Umweltsicht wäre auch das Unsinn – das bedeutet aber leider noch nicht, dass es hierfür keinen Markt gäbe…

5.3.3 Smart Meter als vertrauensunwürdig einstufen

Die Manipulation der Smart Meter ist mit hohen Strafen bewehrt und die Geräte sind mit entsprechenden Erkennungsmechanismus ausgestattet. Trotzdem sollte die Infrastruktur so gestaltet sein, dass auch im Falle einer Kompromittierung eines Smart Meters weder die Infrastruktur in Richtung Netzbetreiber noch benachbarte Smart Meter gefährdet sind.
Konkret bedeutet das, dass eine direkte Kommunikation zwischen Smart Metern unterbunden werden sollte. Anderenfalls wäre über einen lokal kompromittierten Meter eine Ausbreitung auf weitere Geräte möglich. Das gleiche gilt für die Beziehung zwischen Smart Meter und zentraler Netzwerkinfrastruktur beim EVU. Auch hier sollte die Prämisse des potenziell kompromittierten Smart Meters gelten.

6 Fazit

Die Umrüstung von einigen Millionen Haushalten auf Smart Meter und deren Integration in Smart Grids steht bevor. Die Anforderungen an eine sichere Kommunikation und den Schutz vor Zugriffen aus einem nicht vertrauenswürdigen Netz stellen die Anbieter vor neue Herausforderungen.
Zusammenfassend kann festgestellt werden:

- Smart Meter werden kompromittiert werden – wird sollten uns darauf vorbereiten, um die Auswirkungen minimal zu halten.
- OTA-Updates sollten für Smart Meter und Smart Grid-Geräte vorgesehen werden. Die Updates sollten erzwungen (Smart Meter) oder attraktiv gemacht werden (Smart Grid-Geräte) – und vor allem besonders vor Angriffen geschützt werden.
- Smart Meter sollten keine Unterbrechermodule beinhalten – der potenzielle Schaden durch die vergrößerte Angriffsfläche überwiegt den potenziellen Nutzen erheblich

Beim Smart Grid wird sich für manche Geräteklassen – insbesondere Smart Meter – eine monokulturähnliche Struktur bilden. Es wird nur wenige Lieferanten geben, deren Geräte in sehr großer Zahl – unter unterschiedlichen Markennamen – installiert sein werden. Da es sich hierbei im Gegensatz zur Situation bei Heim-PCs um eine kritische Infrastruktur handelt, sind die potenziellen Auswirkungen von Schwachstellen ungleich größer.

Im Bereich der Netztechnik (SCADA-Systeme) gibt es noch viel zu erforschen. Dass auch dort Technik zum Einsatz kommt, die nicht auf den Einsatz in einer „unfreundlich gesinnten Umgebung“ vorbereitet ist, wurde durch den Trojaner-Virus „Stuxnet“ deutlich.

7 Abkürzungen

BSI – Bundesamt für Sicherheit in der Informationstechnik
CSMA/CD – Carrier Sense Multiple Access/Collision Detection
DSL – Digital Subscriber Line
EDL – Energiedienstleistung
EnWG – Energiewirtschaftsgesetz
EVU – Energieversorgungsunternehmen
GEZ – Gebühreneinzugszentrale
GSM – Global System for Mobile Communications
IFA – Internationale Funkausstellung
ISDN – Integrated Services Digital Network
LED – Leuchtdiode
LON – Local Operating Network, ein Feldbus
M-BUS – Meter-Bus, ein Feldbus für die Verbrauchsdatenerfassung
MDL – Messdienstleister
MSB – Messstellenbetreiber
MUC – Multi Utility Communication (Controller)
OTA – Over-the-air, Luftschnittstelle
PLC – power line communication, Kommunikation über die Stromleitung
SCADA – Supervisory Control and Data Acquisition
UMTS – Universal Mobile Telecommunications System
VDE – Verband der Elektrotechnik, Elektrotechnik, Elektronik und Informationstechnik e. V.
WLAN – Wireless Local Area Network

8 Literaturverzeichnis

[1] Wikipedia: Intelligenter Zähler, http://de.wikipedia.org/wiki/Intelligenter_Z%C3%A4hler
[2] Prof. Dr. Claudia Eckert, Peter Schoo, „Eckpunktepapier zum Thema Sicherheit im Smart Grid“
[3] BBC UK, „Britain from above: Tea-time Britain“ http://www.bbc.co.uk/britainfromabove/stories/people/teatimebritain.shtml
[4] Wikipedia: Stromnetz Lastkurve, http://de.wikipedia.org/w/index.php?title=Datei:Stromnetz_Lastkurve.png
[5] Dr. Moritz Karg, „Datenschutzrechtliche Rahmen-bedin-gungen beim Einsatz intelligenter Zähler“, Datenschutz und Datensicherheit (DuD), 6/2010, S. 365-372
[6] Klaus J. Müller, „Gewinnung von Verhaltensprofilen am Intelligenten Stromzähler“, Datenschutz und Datensicherheit (DuD), 6/2010, S. 359-364, http://www.secorvo.de/publikationen/verhaltensprofile-smart-meter-mueller-2010.pdf
[7] Ronald Petrlic, „Datenschutz im intelligenten Stromnetz“, 18. DFN-Workshop „Sicherheit in vernetzten Systemen“, Februar 2011
[8] Ross Anderson, Shailendra Fuloria, „Who controls the off switch?“, http://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf, Juli 2010
[9] Pressemitteilung Miele, „Smart starten – Stromrechnung drücken“, http://www.miele-presse.de/de/presse/artikel/artikel_095_2010.aspx, September 2010

[10] Heise Newsticker, „Copyright Office legt weitere Ausnahmen vom DRM-Umgehungsverbot fest“, http://www.heise.de/newsticker/meldung/Copyright-Office-legt-weitere-Ausnahmen-vom-DRM-Umgehungsverbot-fest-1045744.html, Juli 2010
[11] Karsten Nohl, Henryk Plötz „Mifare – Little Security, Despite Obscurity“, 24th Chaos Communication Congress, Dezember 2007, http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html
[12] New York Times, „Tweaking a Camera to Suit a Hobby“, http://www.nytimes.com/2010/05/27/technology/personaltech/27basics.html?_r=1&8dpc
[13] CHDK Wiki, „Porting the CHDK - Hardware-software solution“, http://chdk.wikia.com/wiki/Porting_the_CHDK#Hardware-software_solution
[14] Statistisches Bundesamt, Preis-Kaleidoskop, http://www.destatis.de/Voronoi/PreisKaleidoskop.svg
[15] root labs rdist, „Smart meter crypto flaw worse than thought“, http://rdist.root.org/2010/01/11/smart-meter-crypto-flaw-worse-than-thought/, Jan 2010
[16] Richard Sietmann, „Schach dem E-Voting, Hackerteam demonstriert die Manipulierbarkeit von Wahlcomputern“, c't 22/06; S. 52
[17] Heise Newsticker, „Deine wichtigste Karte? Vom Umgang mit dem neuen Personalausweis“, http://www.heise.de/newsticker/meldung/Deine-wichtigste-Karte-Vom-Umgang-mit-dem-neuen-Personalausweis-1133588.html, November 2010
[18] Project Blinkenlights, http://blinkenlights.de/
[19] Le Xie, Yilin Mo and Bruno Sinopoli, „False Data Injection Attacks in Electricity Markets“, http://www.ece.tamu.edu/~lx/papers/Xie_Mo_Sinopoli_2010.pdf, Oktober 2010
[20] Wikipedia: Man-in-the-middle-Angriff, http://de.wikipedia.org/wiki/Man-In-The-Middle-Angriff
[21] Bruce Schneier, „Secrets and Lies: Digital Security in a Networked World“, Wiley & Sons, September 2000
[22] Bruce Schneier, „Blaster and the August 14th Blackout“, http://www.schneier.com/crypto-gram-0312.html#1
[23] Fierce Government IT, „DoD preparing smart microgrid technology demonstration“, http://www.fiercegovernmentit.com/story/dod-preparing-smart-microgird-technology-demonstration/2010-08-22
[24] Nate Lawson, „Reverse-engineering a smart meter“, http://rdist.root.org/2010/02/15/reverse-engineering-a-smart-meter/, Februar 2010
[25] Multiple Vulnerabilities in Cisco Unified Videoconferencing Products, http://www.cisco.com/warp/public/707/cisco-sr-20101117-cuvc.shtml
[26] Wikipedia: Anwesenheitssimulation, http://de.wikipedia.org/wiki/Anwesenheitssimulation