GAI NetConsult GmbH— Am Borsigturm 58 — 13507 Berlin — www.gai-netconsult.de — Tel: 030/417898-0

Sicherheit im Smart Metering: Das Schutzprofil für künftige intelligente Zähler

Holm Diening (GAI NetConsult GmbH)

Juni 2011 Sonderdruck aus Security *Journal* #55

Sicherheitsanforderungen im Smart Grid sind derzeit ein heiß diskutiertes Thema. Aktuelle Vorfälle wie „Stuxnet" heizen die Debatte noch zusätzlich an und erhöhen den Druck auf die Regulierer, hier verbindliche Sicherheitsstandards zu setzen. Für ein Teilgebiet des Smart Grid, dem Einsatz intelligenter Haushaltszähler, will Deutschland hier im europäischen Umfeld den Ton angeben: durch die Veröffentlichung eines Schutzprofils für Smart Meter nach den Common Criteria.

Das bisherige Konzept der zentralistischen Stromerzeugung aus quer über die Landkarte verteilten Kraftwerken scheint ausgedient zu haben. Der Trend, abermals beschleunigt durch die Katastrophe im Kernkraftwerk Fukushima, geht eindeutig hin zu den erneuerbaren Energien. Die Einspeisung aus erneuerbaren Energien erfolgt dabei aber entsprechend der Verfügbarkeit von Wind und Sonne, was sowohl zeitlich als auch örtlich nicht unbedingt dem Bedarf des Verbrauchers entsprechen muss. Dementsprechend ist neben einer intelligenten Netzsteuerung („Smart Grid") auch eine Flexibilisierung des Verbrauchsverhaltens beim Energieabnehmer und die bedarfsgerechte Steuerung privater Kleinsterzeugungsanlagen notwendig. Smart Meter, also intelligente Zähler, sind hierbei eine entscheidende Komponente des Smart Grid, welche einen Teil der Netzintelligenz in die Haushalte verlagern sollen.

Da die Stromnetze zu den sogenannten „Kritischen Infrastrukturen" [1] gehören, deren Sicherheitsanforderungen zunehmend auch in den Fokus staatlicher Regulierung gelangen, ist es nur konsequent, dass auch die Sicherheit der Haushaltskomponenten im Smart Grid nicht allein den Herstellern überlassen werden darf. Bekannte Schwachstellen bei Smart Meter Installationen in den USA und Europa sowie Sicherheitsvorfälle im Bereich von Prozesssteuerungsanlagen (Stichwort: Stuxnet), bilden hierfür zusätzliche Motivatoren. Aus diesen Gründen entwickelt das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Auftrag des Bundeswirtschaftsministeriums derzeit ein Schutzprofil nach den „Common Criteria" für Smart Meter [2]. Dabei stehen sowohl Anforderungen zur Sicherung der Netzintegrität, aber in wesentlichen Teilen auch der Datenschutz der betroffenen Endkunden im Vordergrund. Mittelfristiges Ziel ist es, dass zukünftig alle Smart Meter und deren Kommunikationsgateways nach diesem Schutzprofil zertifiziert werden müssen, bevor sie von der Bundesnetzagentur zum Einbau in die Haushalte zugelassen werden. Dieser Schritt ist notwendig, da nach derzeitiger Planung der Einbau von fernauslesbaren Smart Metern verpflichtend wird und der Bürger hier in seiner Wahlfreiheit eingeschränkt ist.

Schutzprofil nach Common Criteria

Die Common Criteria sind die „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" [3]. Sie sind ein Gemeinschaftsprodukt von Australien/Neu-seeland, Deutschland, Frankreich, Großbritannien, Japan, Kanada, Spanien und den USA. Zielsetzung der Common Criteria sind die Formulierung von Sicherheitsanforderungen an technische Produkte in einer einheitlichen formalisierten Sprache und ein gemeinsames Verständnis der teilnehmenden Länder für das Vorgehen bei der Evaluierung dieser Produkte. Zur Abgrenzung sei erwähnt, dass Aspekte der Informationssicherheit, die in das Umfeld des sicheren Betriebes fallen (wie Beispielsweise bei der ISO 27001) nicht Gegenstand der Common Criteria sind. Ein wesentliches Anwendungsgebiet der Common Criteria ist die Definition von Schutzprofilen (auch „Protection Profile" [PP]) für eine Produktgruppe. Hierbei wird ein abstraktes „Target of Evaluation" (TOE) angenommen, welches eine Produktgruppe repräsentiert, und sich bestimmten Sicherheitsanforderungen unterwerfen muss. Prominente Beispiele für Produktgruppen mit zugeordneten Schutzprofilen sind:

- elektronischer Personalausweis und elektronischer Pass
- elektronische Gesundheitskarte und deren Lesegeräte
- verschlüsselnde USB-Sticks
- u.v.m.

Ein Schutzprofil folgt immer einem festgelegten Aufbau, der an dieser Stelle nur in seinen wichtigsten Bestandteilen erläutert werden soll:

Zunächst definiert das Schutzprofil immer ein abstraktes „Target of Evaluation" und umschreibt dabei die Produktgruppe. An dieser Stelle sollten nur unbedingt notwendige Einschränkungen für das eigentliche Produktdesign festgelegt werden, um einem potentiellen Hersteller möglichst vielfältige Gestaltungsmöglichkeiten offen zu lassen, ohne die spätere Konformität zum Schutzprofil zu gefährden. Konkret formuliert werden hingegen die Bedrohungsszenarien, von denen der Autor des Schutzprofils ausgeht und die sich daraus ergebenden Sicherheitsziele. Ebenso wichtig (und ebenso gern übersehen) sind die Annahmen des Autors über die Umgebung in der das ggf. zertifizierte Produkt

betrieben wird. Den Hauptteil des Schutzprofils bildet die Beschreibung der Sicherheitsfunktionen, die der spätere Hersteller zur Gewährleistung der Sicherheitsziele umzusetzen hat. Ein Schutzprofil schließt mit der Angabe der „Assurance Requirements" mit denen der Entwickler zur Einhaltung bestimmter Mindestanforderungen im Entwicklungsprozess, in der Dokumentation, bei der Unterstützung des Produktlebenszyklus, bei den Tests sowie der Schwachstellenanalyse gezwungen wird. Ebenso definieren die „Assurance Requirements" wie der Evaluator diese Anforderungen zu prüfen hat [4].

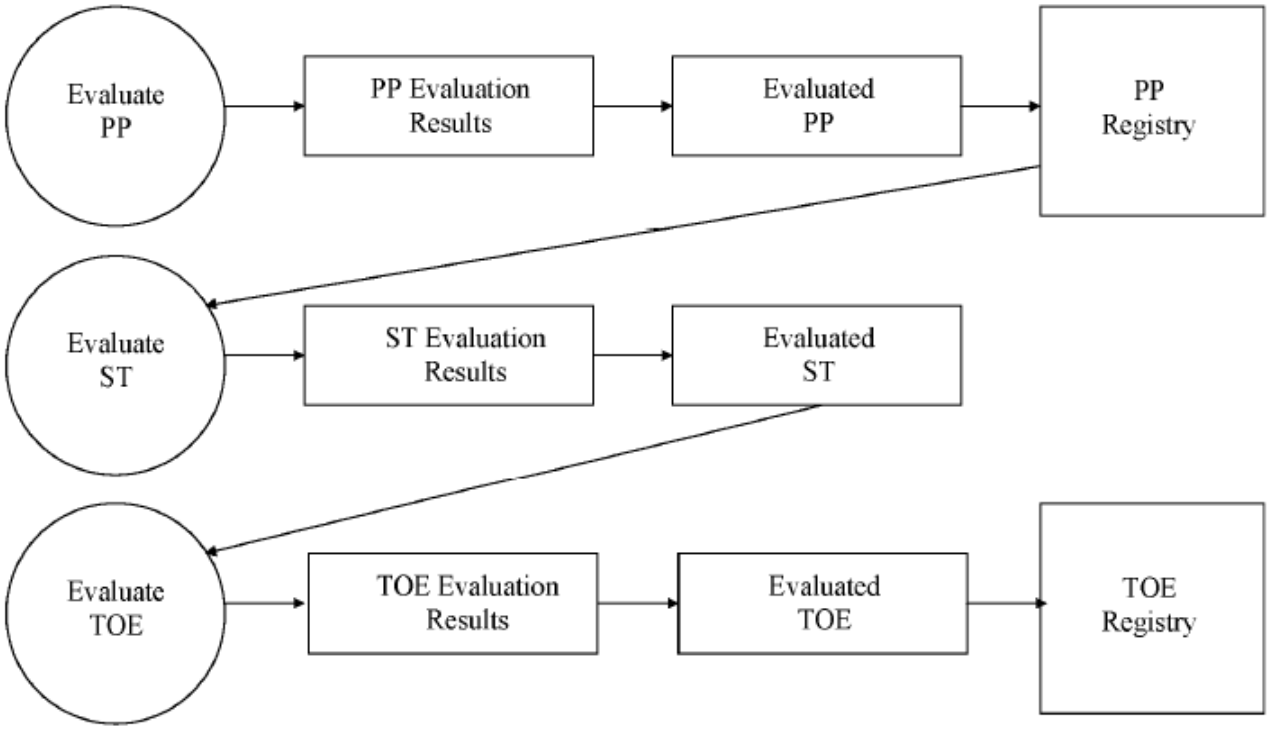

Abbildung-1: Zertifizierungsprozess (aus Common Criteria V3.1 Part 1)

Vom Entwurf eines Schutzprofils zum zertifizierten Produkt

Damit ein Hersteller ein Produkt nach einem Schutzprofil zertifizieren lassen kann, muss zunächst das Schutzprofil selbst evaluiert und registriert werden. Hierzu evaluiert ein anerkanntes Prüflabor, ob das Schutzprofil formal die Anforderungen der Common Criteria erfüllt und ob die Ableitung der Sicherheitsanforderungen aus den Sicherheitszielen und diese wiederum aus den Bedrohungen und Annahmen sachlich richtig und vollständig sind. Anschließend kann dieses Schutzprofil öffentlich registriert werden und somit als sicherheitsrelevante Norm für die adressierte Produktgruppe verwendet werden. In der Bundesrepublik wird diese Registrierung durch das BSI vorgenommen und veröffentlicht [5].

Hersteller, die ein zu diesem Schutzprofil konformes Produkt zertifizieren lassen wollen, müssen zunächst ein „Security Target" entwickeln und zertifizieren lassen. Dieses „Security Target" (ST) ist, analog zum Schutzprofil, ein Dokument, welches konkret die Implementierung der im Schutzprofil noch recht allgemein gehaltenen Anforderungen beschreibt. Die Struktur des ST ist dabei beinahe identisch zu der des Schutzprofils. Nach der Entwicklung des Security Target kommt wiederum das Prüflabor ins Spiel, welches das ST hinsichtlich seiner Konformität mit dem Schutzprofil sowie der formalen und sachlichen Richtigkeit der jeweiligen Detaillierungen evaluiert. Erst danach kann die Evaluierung des eigentlichen Produktes beginnen, welche formal einen Abgleich zwischen den Forderungen des ST und dem tatsächlich realisierten Produkt darstellt. Ein erfolgreich zertifiziertes Produkt kann wiederum öffentlich registriert werden.

Schwächen

Allerdings ist dieser gesamte Prozess nicht nur relativ aufwändig (und teuer), sondern auch keineswegs ein Garant für ein absolut sicheres Produkt. Bei der Evaluierung des Schutzprofils analysiert das Prüflabor beispielsweise nicht, ob die Liste der Bedrohungen auch vollständig ist oder ob ggf. wichtige Bedrohungen vergessen wurden. Im Fokus steht, wie bereits ausgeführt, im Wesentlichen die formale Richtigkeit des Dokumentes. Bereits an dieser Stelle wird klar, dass der Anwender eines zertifizierten Produktes höchstens die Gewissheit erhält, dass das fragliche Gerät oder die Software den Anforderungen der Zertifizierungsgrundlage entspricht (z.B. einem Schutzprofil), nicht jedoch, ob diese Zertifizie-

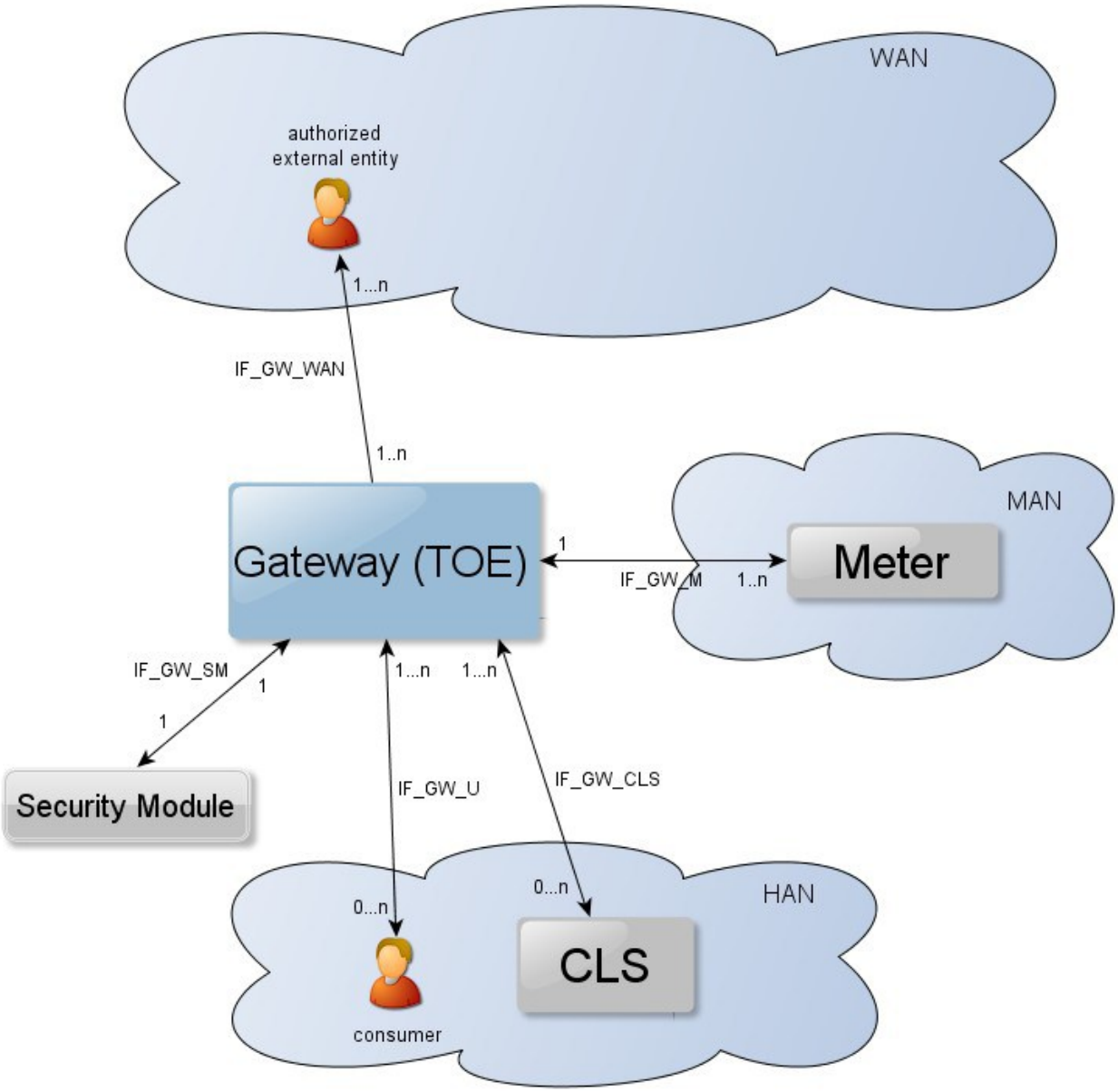

Abbildung-2: Darstellung der Schnittstellen des TOE (aus dem aktuellen Smart Meter Protection Profile)

rungsgrundlage auch mit den eigenen Vorstellungen von Sicherheit übereinstimmt. Und auch die Evaluierung des tatsächlichen Produktes nach den Common Criteria muss nicht zwangsläufig alle Schwachstellen aufdecken. Die erfolgreich ausgeführten Angriffe gegen das Ingenico i3300 Kreditkartenterminal zeigen dies eindrücklich [6].

Gegenseitige Anerkennung

Wird ein Produkt durch ein nationales Labor evaluiert und zertifiziert, so gilt diese Zertifizierung, mit Einschränkungen, auch international. So haben sich Australien, Neuseeland, Kanada, Finnland, Frankreich, Deutschland, Griechenland, Italien, die Niederlande, Norwegen, Spanien, Großbritannien und die USA im „Arrangement on the Recognition of Common Criteria Certificates" (CCRA) darauf geeinigt, Zertifizierungen bis zur EAL4 (später hierzu mehr) gegenseitig anzuerkennen. Innerhalb Europas gilt diese Vereinbarung sogar bis EAL7, sofern die Evaluierung in Deutschland, Frankreich, Großbritannien oder den Niederlanden durchgeführt wurde. Vielfältig wird diese Anerkennung jedoch begrenzt, wenn sicherheitspolitische Belange des jeweiligen Staates berührt werden. Dies gilt auch für die Anerkennung von ausländischen Zertifikaten durch das BSI.

Das Schutzprofil für ein Smart Meter

Die Entwicklung des Schutzprofils für Smart Meter nach Common Criteria durch das BSI kommt keineswegs aus heiterem Himmel, sondern hat eine gewisse

Historie. Tatsächlich ist der entsprechende Auftrag des Bundeswirtschaftsministeriums eng verknüpft mit den Arbeiten des E-Energy Forschungsprojektes [7]. Bereits im E-DeMa Projekt, einem der E-Energy Teilprojekte, wurde ein Schutzprofil nach Common Criteria für IKT Gateways entwickelt [8]. Während jedoch diese Entwürfe des Schutzprofils stark aus dem Forschungsumfeld des E-DeMa Projektes beeinflusst waren, beschreibt die Neuentwicklung durch den TÜV IT (im Auftrag des BSI) die Sicherheitsanforderungen an ein allgemeingültiges Smart Meter. Ziel ist dabei nicht nur einen verbindlichen Standard für den deutschen Markt zu etablieren, sondern auch auf europäischer und internationaler Ebene Pflöcke einzuschlagen und den sich anbahnenden Industriestandards für Smart Meter, die aus Sicht des Datenschutzes in keiner Weise mit dem Niveau des Schutzprofils vergleichbar sind, das Wasser abzugraben.

Dieses Schutzprofil entsteht unter Einbeziehung aller wesentlichen Verbände der Energieversorger und der Hersteller sowie des BfDI und der Physikalisch Technischen Bundesanstalt PTB. Diese hatten in der ersten Hälfte dieses Jahres in drei Kommentierungsrunden Gelegenheit, die Entwicklung des Dokumentes zu beeinflussen. Hierbei ging es weniger um technische Feinheiten, sondern vielmehr um grundsätzliche Fragen, wie z.B. die Relevanz nach dem Eichrecht, die obligatorische Verwendung eines Sicherheitsmoduls für kryptografische Operationen oder auch die grundsätzliche Vereinbarkeit des Vorhabens mit den standardisierten Wechselprozessen im Messwesen („WiM"). Nach der letzten Kommentierungsrunde zum aktuell veröffentlichten Schutzprofil (Version 1.0.1 vom 19.05.2011) [9], die am 09. Juni zu Ende ging, will das BSI im Juli eine stabile Version veröffentlichen und bis September zertifizieren lassen.

Im Folgenden sollen die wichtigsten Aussagen und Forderungen des aktuellen Entwurfs des Schutzprofils (V 1.0.1) näher beleuchtet werden:

Target of Evaluation (TOE)

Das Schutzprofil bezieht sich auf einen ganz bestimmten Teil der Smart Metering Infrastruktur im Haushalt des „Consumers", nämlich auf das Gateway, welches die Zähler (nicht nur Strom, sondern auch andere Medien wie Gas, Wasser, usw.) mit dem lokalen Netzwerk und den Interessensgruppen in der Außenwelt, wie z.B. dem Messstellenbetreiber, verbindet. In Abbildung-2 wird deutlich, welche Schnittstellen das Gateway hierzu anbietet:

- ⇒ IF_GW_WAN: die Schnittstelle zum WAN (zum Messstellenbetreiber und anderen Parteien)
- ⇒ IF_GW_M: die Schnittstelle zu den Zählern
- ⇒ IF_GW_CLS: die Schnittstelle zu den lokalen steuerbaren Systemen (CLS, Controllable Local Systems, z.B.: intelligente Haushaltsgeräte oder Mini-BHKW)
- ⇒ IF_GW_U: die Schnittstelle zum Anwender (Display oder Netzwerk)
- ⇒ IF_GW_SM: die Schnittstelle zum Sicherheitsmodul

Hierbei ist zu beachten, dass die hier aufgeführten Schnittstellen lediglich logische Interfaces darstellen und physikalisch sehr unterschiedlich ausgeprägt sein können. So ist es beispielsweise unerheblich, ob IF_GW_WAN über Powerline, GPRS oder eine DSL-Leitung realisiert wird. Das Schutzprofil macht hierzu keine Vorgaben. Andererseits hat der Entwickler für die Schnittstelle IF_GW_SM weniger Freiheitsgrade. Alle realistisch denkbaren Konstellationen (sowie die Beispiele im Protection Profile des Smart Meter) schließen das Sicherheitsmodul physikalisch in das TOE mit ein, damit die Verbindung zwischen Sicherheitsmodul und Gateway nicht angreifbar ist.

Besonders zu beachten ist die Schnittstelle zu den steuerbaren Systemen (IF_GW_CLS). Entsprechend des Schutzprofils soll das Gateway hier lediglich eine sichere Kommunikationsmöglichkeit zwischen den CLS und externen Parteien bereitstellen. Der Schutz der CLS an sich ist nicht Gegenstand des Schutzprofils. Dies ist insofern interessant, als das CLS auch durchaus Vorrichtungen zur Sperrung des Hausanschlusses sein können (noch nicht in Deutschland, aber in anderen europäischen Ländern). Der Schutz der CLS besteht vor allem darin, dass diese das TOE als sicheres Kommunikationsgateway und Firewall zum WAN verwenden können. Ein Schutz der CLS vor Angriffen aus dem lokalen Netz kann jedoch im Rahmen des Schutzprofils nicht zugesichert werden.

Als eine wesentliche Besonderheit des Gesamtkonzeptes ist hervorzuheben, dass das Gateway und damit auch die dahinter liegenden Zähler nicht mehr „fernabfragbar" sind. Vielmehr kommuniziert das Gateway von sich aus nach, in einem „Access Control Profile" festgelegten Schema, mit dem Messstellenbetreiber (oder anderen Parteien) und überträgt die erforderlichen Daten. Dadurch können vor allem datenschutzrechtliche Forderungen leichter erfüllt werden, weil das Kommunikationsintervall dem Abrechnungszeitraum entsprechen soll. Ein eingehender Verbindungsaufbau aus dem WAN ist aus Sicherheitsgründen nicht vorgesehen. Einzige Ausnahme bildet hier ein „wake up service". Hierbei wird das Gateway durch ein externes Datenpaket, welches eine passende elektronische Signatur tragen muss, veranlasst eine Verbindung außerhalb des vorgesehenen Zeitrasters zu einem vordefinierten Kommunikationspartner aufzubauen. Hierdurch können auch zeitkritischere Anwendungen umgesetzt werden, ohne dass das Gateway hierfür permanent Verbindungen zu Dritten offen halten muss.

Bedrohungen und Annahmen

Um die Sicherheitsanforderungen eines Schutzprofils beurteilen zu können, ist es zunächst wichtig in Erfahrung zu bringen, von welchen Bedrohungsszenarien und welchen Annahmen über die Umgebung der Autor ausgegan-

gen ist. Bedrohungen, die hier nicht auftauchen, werden auch nicht durch entsprechende Sicherheitsfunktionen abgedeckt sein. Ebenso muss der Anwender sicherstellen, dass die Betriebsumgebung des späteren Gateways auch alle Annahmen des Schutzprofils erfüllt, damit die Sicherheitsziele aufrecht erhalten werden können.

Im Schutzprofil des Smart Meter wird dabei von folgenden Bedrohungen ausgegangen (stark zusammengefasst):

- Ein lokaler bzw. externer Angreifer versucht Zählerdaten oder Konfigurationsdaten zu verändern. Dabei könnte versucht werden unberechtigten Zugriff auf das Gateway zu erlangen.
- Ein lokaler Angreifer versucht die Zeit des Gateways zu manipulieren (z.B. zur Rechnungsmanipulation).
- Angreifer könnten versuchen Zähler- oder Konfigurationsdaten zu lesen (z.B. bei der Übertragung).
- Ein externer Angreifer könnte versuchen die Kontrolle über das Gateway, die Zähler oder CLS zu erlangen und damit in die Lage versetzt werden, Schaden anzurichten.
- Ein lokaler Angreifer könnte auf temporäre Daten oder permanent gespeicherte Daten des Gateways zugreifen wollen.
- Eine externe Partei könnte versuchen, mehr oder häufiger Daten (z.B. Zählwerte) vom Gateway abzufragen, als es für die Erfüllung des Liefervertrages vereinbart wurde.

Auf den ersten Blick erscheint diese Bedrohungsliste relativ vollständig. Allerdings gibt es gerade im EVU Umfeld auch noch andere Bedrohungen, die nichts mit einem irgendwie gearteten Zugriffsversuch eines Angreifers auf Systeme oder Daten zu tun haben. Als Beispiel sei hier die Fehlfunktion des Gateways infolge von Software- oder Konfigurationsfehlern genannt. Hier wäre es wichtig, dass das Gateway diese selbständig erkennt und beispielsweise zur letztbekannten funktionierenden Firmwareversion oder den Werkseinstellungen zurückspringt. Man stelle sich vor, in Millionen von in Haushalten installierte Gateways könnten wegen eines Softwareproblems plötzlich nicht mehr kommunizieren und wären nicht mehr remote administrierbar. Mit dem Austausch der Geräte wären Heerscharen von Monteuren monatelang beschäftigt! Allerdings wurden diese Bedrohungen nicht etwa vergessen, sondern nach Aussage der Autoren bewusst nicht mit aufgenommen. Unabhängig davon ist es den Herstellern jedoch unbenommen, eine solche Funktionalität der eigenen Implementierung hinzuzufügen. Eine Verpflichtung hierzu gibt es aufgrund des Schutzprofils aber nicht.

Neben einem Verständnis der Bedrohungen ist für die Einschätzung des Sicherheitsniveaus des Schutzprofils auch die Kenntnis der Annahmen wichtig, deren Erfüllung als gegeben angesehen wird. Diese sind zusammengefasst:

- Externe Parteien, die berechtigterweise Abrechnungsdaten erhalten, arbeiten vertrauenswürdig hinsichtlich der Datenschutzanforderungen.
- Die Administratoren der Gateways sind vertrauenswürdig und gut geschult.
- Das Gateway und die Zähler befinden sich im nichtöffentlichen Raum auf dem Gelände des Anwenders, welches einen grundlegenden physikalischen Schutz bietet.
- Die „Access Control Profiles" sind korrekt und vertrauenswürdig.
- Softwareupdates wurden dem Zertifizierungsprozess unterzogen, bevor sie eingespielt werden.
- Das Gateway ist die einzige Kommunikationsverbindung der Zähler.
- Falls das lokale Netz eine weitere Verbindung mit dem WAN (z.B. Internet) unterhält, so ist diese ausreichend gesichert.

Ein Blick auf die letzte Annahme lässt dabei leicht erkennen, wo hier ein mögliches Bedrohungspotential für die lokalen Steuerungssysteme (CLS) liegen kann: Die Überbrückung des Gateways durch eine unsichere WAN-Anbindung seitens des Kunden und damit die Preisgabe der Steuerungssysteme an einen externen Angreifer. Ebenso werden auf diese Weise Szenarien, bei denen das User Interface (IF_GW_U) auf unsichere Weise mit dem WAN verbunden werden, nicht betrachtet.

Darüber hinaus wird die Annahme hinsichtlich der zertifizierten Softwareupdates bei sogenannten Hotfixes nicht haltbar sein. Nach gemeinsamer Abstimmung zwischen Zertifizierungsstelle und Hersteller ist es auch durchaus Usus kurzfristige Sicherheitsupdates ohne eine neue Evaluierung einzuspielen, sofern diese später im Rahmen der regulären Updates nachgeholt wird. Voraussetzung hierfür ist, dass das Risiko, den fraglichen Hotfix nicht einzuspielen, das Risiko einer nachgelagerten Evaluierung überwiegt.

Positiv ist zu erwähnen, dass das Schutzprofil der klassischen Plombe scheinbar keine Sicherheitsrelevanz mehr zubilligt, da die Annahme eines verplombten Zählerkastens fehlt. Die Sicherheitsfunktionen sind so ausgelegt, dass durch eine Plombe kein zusätzlicher Gewinn an Zugriffsschutz zu erreichen ist.

Sicherheitsziele

Den Bedrohungen und Annahmen werden nun die Sicherheitsziele gegenübergestellt, mit denen die Bedrohungen vollständig adressiert werden sollen. Diese lassen sich für das Smart Meter Schutzprofil wie folgt zusammenfassen:

- Bereitstellung einer Firewallfunktion zwischen allen angeschlossenen Netzwerkschnittstellen
- Selbsttest auf inkorrekte Verbindungen zwischen den Interfaces
- Verschleierung der Kommunikation nach außen

- verschlüsselte und authentisierte Kommunikation des Gateways mit allen Parteien (einschließlich der Zähler, sofern diese nicht im selben Gehäuse sind)
- Sicherstellen der Integrität und Authentizität der Zählerdaten
- Befolgen eines Access Control Profiles für die Verarbeitung der Zählerdaten (einschließlich der zeitlichen Steuerung des Versands der Daten)
- Pseudonymisierung der Daten bei Bedarf (z.B. Lastdaten für Netzbetreiber)
- Benutzung eines Sicherheitsmoduls für bestimmte kryptografische Operationen
- Bereitstellung einer gesicherten Zeitbasis
- fehlertolerantes Design
- Erkennbarkeit physikalischer Manipulationen
- umfangreiche Protokollierung für den Anwender (Transparenz / Datenschutz) und den Administrator (Störungsbeseitigung)

Besonders auffallend ist hier die Forderung nach verschleierter Kommunikation. Neben grundsätzlichen Forderungen zum Zugriffsschutz wird hierbei sogar gefordert, dass die Analyse der Häufigkeit, des Volumens oder auch die Tatsache der Abwesenheit von Kommunikation, keine Rückschlüsse auf Informationen zulassen dürfen, die der Privatsphäre des Consumers zuzuordnen sind. Ebenfalls hervorzuheben ist die Pseudonymisierung von Daten für bestimmte Interessensgruppen. So kann der lokale Netzbetreiber durchaus ein Interesse an der aktuellen Lastsituation in einem Netzsegment haben, muss aber dafür die Identität des Kunden nicht kennen. Ganz allgemein sieht das Schutzprofil aufgrund der verschiedenen Interessenslagen der potentiellen Datenempfänger vor, die Messdaten entsprechend eines „Access Control Profiles" aufzubereiten, ggf. zu pseudonymisieren und in angemessenen Intervallen an die entsprechenden Empfänger zu versenden. Dabei kann es durchaus sein, dass eine zentrale Stelle, wie z.B. der Messstellen- oder der Verteilnetzbetreiber als zentrale Datendrehscheibe fungiert. Allerdings werden die Datenpakete entsprechend ihrer Empfänger getrennt aufbereitet und verschlüsselt, so dass bspw. der Netzbetreiber nie die Abrechnungsdaten lesen können wird, auch wenn er in der praktischen Umsetzung des Systems für die Weiterleitung der Daten vorgesehen ist.

Unabhängig von der Weiterleitung der Daten zu Abrechnungszwecken kann der Consumer dennoch über seine lokale Schnittstelle sekundengenaue Verbrauchs- und Lastdaten sowie ein Übertragungsprotokoll für die Abrechnungsdaten im Gateway einsehen. Insofern geht dem technisch interessierten Kunden auch bei dieser datenschutzfreundlichen Variante eines Smart Meters kein Detail verloren. Hierfür ist die zwangsweise Übertragung von Verbrauchsdaten im 15 Minuten Takt an eine externe Stelle jedoch nicht mehr notwendig. Natürlich gibt es auch genug Enthusiasten, die den Stromverbrauch ihrer Kühltruhe auch im Urlaub vom iPhone aus verfolgen wollen. Das Protection Profile steht dem nicht im Wege, weil ein solcher Dienst lediglich eine entsprechende Berücksichtigung im Access Control Profile des Gateways und die ausdrückliche Zustimmung des Kunden erfordert. Die „Zwangsbeglückung" der restlichen Kunden entfällt jedoch.

Umsetzung der Sicherheitsziele

Ein Großteil des Schutzprofils befasst sich mit der Umsetzung der Sicherheitsziele durch sogenannte „Security Functional Requirements" und „Security Assurance Requirements" in einer formalisierten Sprache. Hierbei werden bestimmte Elemente von abstrakten Sicherheitsfunktionen aus einem Katalog (dem Teil 2 der Common Criteria) ausgewählt und deren Einsatz zur Erreichung der Sicherheitsziele beschrieben. Eine Wiedergabe dieser Details verbietet sich an dieser Stelle aufgrund des Umfangs und der erforderlichen Kenntnisse der Common Criteria. Einige allgemeine Aussagen zu den „Security Assurance Requirements" (Teil 3 der Common Criteria) scheinen jedoch angebracht.

Während die „Security Functional Requirements" definieren womit die Sicherheitsziele erreicht werden sollen, bestimmen die „Security Assurance Requirements" wie der Hersteller die ordnungsgemäße Implementierung dieser Sicherheitsfunktionen sicherstellen soll und damit auch, auf welchem Niveau das Prüflabor seine Evaluierung des Produktes vornehmen muss.
Die Definition der „Security Assurance Requirements" erfolgt üblicherweise im Rahmen von „Evaluation Assurance Level" (EAL), die in 7 hierarchisch aufsteigenden Stufen, EAL1 – EAL7, definiert sind. Jede EAL umfasst ein Paket sinnvoll zusammengestellter „Assurance Components", mit denen die korrekte Umsetzung der Sicherheitsfunktionen gewährleistet werden soll.

Die Assurance Components gliedern sich dabei in die Klassen:

- Development
- Guidance Documents
- Life-cycle support
- Security Target evaluation
- Tests
- Vulnerability assessment

Hieraus wird schnell ersichtlich, dass es für die Erfüllung der Zertifizierungsanforderungen keineswegs ausreichend ist, ein fertiges Gerät dem Prüflabor zu präsentieren. Vielmehr geht es auch darum, bereits den Entwicklungsprozess sicher zu gestalten, die Dokumentationsanforderungen zu erfüllen und den Produktlebenszyklus angemessen zu unterstützen.

Das Schutzprofil sieht für das Gateway die EAL Stufe 4, erweitert um eine Schwachstellenanalyse mit hohem Angriffspotential und einen verbindlichen Prozess zur Schwachstellenbeseitigung während des Produktlebenszyklus, vor. Die Anforderungen an

die Entwicklung des Smart Meter Gateways spielen damit in einer Liga mit dem elektronischen Reisepass, Firewalls oder Bankautomaten. Bei einigen Details dieser Anforderungen dürfte es schwer fallen, bereits vorhandene Entwicklungen nachträglich in die Zertifizierung einzubringen, weil diese ggf. nicht mit den erforderlichen Qualitätsmaßstäben erstellt wurden und daher nicht zertifizierungsfähig sind.

Wie geht es weiter?

Mit der Veröffentlichung des Schutzprofils allein ist es natürlich nicht getan. Damit die Hersteller tatsächlich in die Lage versetzt werden, entsprechende Geräte in naher Zukunft zu entwickeln, sieht der Zeitplan vor, bis September 2011 ein zertifiziertes Schutzprofil für das obligatorische Sicherheitsmodul zu veröffentlichen und bis zum Ende des Jahres auch drei technische Richtlinien zu den Themen „Systemarchitektur / PKI", „Kryptografische Vorgaben & Berechtigungsprofile" sowie „Kommunikationsprotokolle" auf den Weg zu bringen. Mit diesem Rüstzeug soll es Herstellern dann möglich sein, bis zum Ende des Jahres 2012 zertifizierte Produkte auf den Markt zu bringen.

Ob dem allerdings auch so sein wird, hängt noch maßgeblich davon ab, ob die Hersteller für die Entwicklung eines zertifizierungsfähigen Produktes auch eine hinreichende Investitionssicherheit sehen. Ob es nämlich einen flächendeckenden (und umsatzträchtigen) Rollout dieser Smart Meter geben wird oder ob es bei einer schrittweisen Ablösung der alten Ferraris Zähler im Zuge von Neubauten oder Renovierungen bleibt, hängt vom Ergebnis einer Kosten-/Nutzen Analyse des BMWi ab, die erst im August 2012 vorliegen soll [10]. Bis dato sind die Hersteller jedenfalls alles andere als euphorisch, wenn es um Investitionen in die Entwicklung zertifizierungsfähiger Smart Meter gemäß des aktuellen Schutzprofils geht.

Darüber hinaus hängt die Sicherheit der Daten des Verbrauchers nicht nur vom Smart Meter ab. Im Gegenteil: Die Datenskandale bei Telekom, Sony und vielen anderen Unternehmen zeigen deutlich, dass gerade dort, wo letztendlich die zentrale Speicherung der Kundendaten erfolgt, auch das größte Angriffspotential liegt. Die gesetzlichen Mindestanforderungen für den sicheren Betrieb der Infrastrukturen im Smart Grid und der zentralen Verarbeitung von Kundendaten im Smart Metering sind derzeit jedoch noch in der Entwicklung. In den aktuellen Fassungen der entsprechenden Regulierungen bleiben diese Anforderungen jedoch weit hinter dem angestrebten Sicherheitsniveau des Schutzprofils zurück.

Fazit

Die Entwicklung des Schutzprofils für Smart Meter ist der richtige Weg, verbindliche Sicherheitsanforderungen für die Smart Grid Komponenten im Haushalt der Endkunden zu definieren. Dabei legt das Dokument die Hürden für ein zertifiziertes Produkt recht hoch. Was aus Sicherheitssicht definitiv zu begrüßen ist, könnte aus ökonomischer Sicht eventuell dazu führen, dass sich die Einführung der Smart Meter in Deutschland noch verzögert. Für die Erreichung der im Schutzprofil definierten Sicherheitsziele ist, neben zertifizierten Produkten, jedoch auch die Erfüllung aller getroffenen Annahmen erforderlich. Dies betrifft insbesondere die Vertrauenswürdigkeit der Datenverarbeitung außerhalb des Smart Meters. An dieser Stelle besteht noch ein umfassender Handlungsbedarf.

Quellen

[1]Definition „KRITIS"
[2]Smart Meter
[3]Zertifizierungsanmerkung
[4]Genauer erfolgt dies jedoch in der „Common Evaluation Methodology" (CEM)
[5]Schutzprofil
[6]Drimer, Murdoch, Anderson; „Thinking inside the box: system-level failures of tamper proofing"
[7]**vgl. Pressemitteilung „Staatssekretär Jochen Homann gibt den Startschuss zur Entwicklung eines Schutzprofils für Smart Meter"** und **Antwort der Bundesregierung auf eine große Anfrage der SPD Fraktion (Drucksache 17/5346)**: Zusammenfassende Antwort auf Fragen 35-39
[8]vgl. Fußnote 84
[9]Download
[10]vgl. Bernd Kowalski (BSI), Foliensatz zum Schutzprofil auf dem Teletrust Informationstag "IT-Sicherheit im Smart Grid"