Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Energie BFE

Schlussbericht 07. September 2011

IT-Sicherheit bei Smart Metering

ewz
Die Energie

Auftraggeber:
Bundesamt für Energie BFE
Forschungsprogramme Netze / Elektrizitätstechnologien & -anwendungen
CH-3003 Bern
www.bfe.admin.ch

Kofinanzierung:
ewz Elektrizitätswerk der Stadt Zürich, CH-8050 Zürich

Auftragnehmer:
Compass Security AG
Werkstrasse 20
CH-8645 Jona
www.csnc.ch

Autor:
Martin Loher, Compass Security, martin.loher@csnc.ch

Beteiligte ewz:
Leiter Verteilnetz: Dr. Lukas Küng
Leiter Netzdesign: Hansruedi Luternauer
Leiter Messtechnik: Christoph Steinmann

BFE-Bereichsleiter: Dr. Michael Moser
BFE-Programmleiter: Dr. Michael Moser / Roland Brüniger
BFE-Vertragsnummer: SI/500573-01

Zusammenfassung

Das Thema Smartmetering ist in der Energiebranche momentan in aller Munde. Mit Hilfe dieser Geräte kann der Stromverbrauch der verschiedenen Haushalte über die Zeit gemessen und die Resultate direkt an den Energiedienstleister übertragen werden. Da momentan in der Schweiz Referenzimplementationen solcher Technologien fehlen, wurde die Sicherheit solcher Lösungen nur ungenügend beurteilt.

Im Rahmen eines Pilot Projektes haben die Elektrizitätswerke Zürich (ewz) einen Versuchsaufbau implementiert, welcher verschiedene Technologien beinhaltet. Compass Security wurde damit beauftragt, dieses Pilotprojekt auf dessen Sicherheit hin zu untersuchen. Dieses Dokument fasst vor allem die Empfehlungen welche aus dem Test hervorgegangen sind zusammen und stellt so auch einen Anforderungskatalog an Smartmetering Infrastrukturen dar.

Da die Infrastruktur auf verschiedenen Technologien aufbaut wurden die Resultate in vier Teilbereiche unterteilt:

- **Gateway basierte Smartmeters:** Dies sind Smartmeters welche ein Gateway Gerät im Haushalt besitzen und die Daten via IP basiertem Netzwerk an den Energiedienstleister senden.

- **Netzwerk / Firewalling:** In diesem Bereich wurden Anforderungen an das Netzwerk bezüglich der Firewall erarbeitet.

- **Server Hardening:** Da die verschiedenen Smartmeters jeweils mit einem Server auf Seiten des Energiedienstleisters kommunizieren, sollte dieser Server adäquat geschützt sein. Empfehlungen dazu wurden in diesem Kapitel erarbeitet.

- **PLC basierte Smartmeters:** Neben den Gateway basierten Smartmeters, kommen auch PLC basierte Smartmeters zum Einsatz, welche über das Stromnetz miteinander kommunizieren. Auch diese wurden im Rahmen dieser Überprüfung analysiert.

Diese Empfehlungen sollten beim Aufbau einer Smartmetering Infrastruktur beachtet werden, um ein angemessenes Sicherheitslevel zu erreichen.

Summary

The topic of Smartmetering is currently on everyone's lips in the energy sector. Using these devices the energy consumption of the various households can be measured over a period of time and the results can directly be transmitted to the energy management operator. Because reference implementations of such technologies are inexistent in Switzerland at present, the safety of such solutions has only been assessed insufficiently.

In the frame of a pilot scheme the "Elektrizitätswerke Zurich" (ewz) have implemented a test set-up, which contains different technologies. Compass Security has been assigned to test the safety of this pilot scheme. This documentation mainly summarises the recommendations resulting from this test and thus also illustrates a catalogue of requirements for Smartmetering Infrastructures.

As the infrastructure is built on different technologies, the results have been divided into for sub areas:

- **Gateway based Smartmeters:** These are Smartmeters which have a Gateway device in their households. The data are sent to the energy service provider via IP based network.

- **Network / Firewalling:** In this area requirements for the network regarding the firewall have been worked out.

- **Server Hardening:** As the various Smartmeters always communicate with a server from the energy service provider's side, this server should be adequately protected. This chapter is dealing with recommedations for this purpose.

- **PLC based Smartmeters:** Apart from Gateway based Smartmeters, PLC Smartmeters are also in use, which communicate with each other via the power network. These have also been analysed within this investigation.

These recommendations ought to be considered when establishing a Smartmetering Infrastructure, in order to achieve an adequate security level.

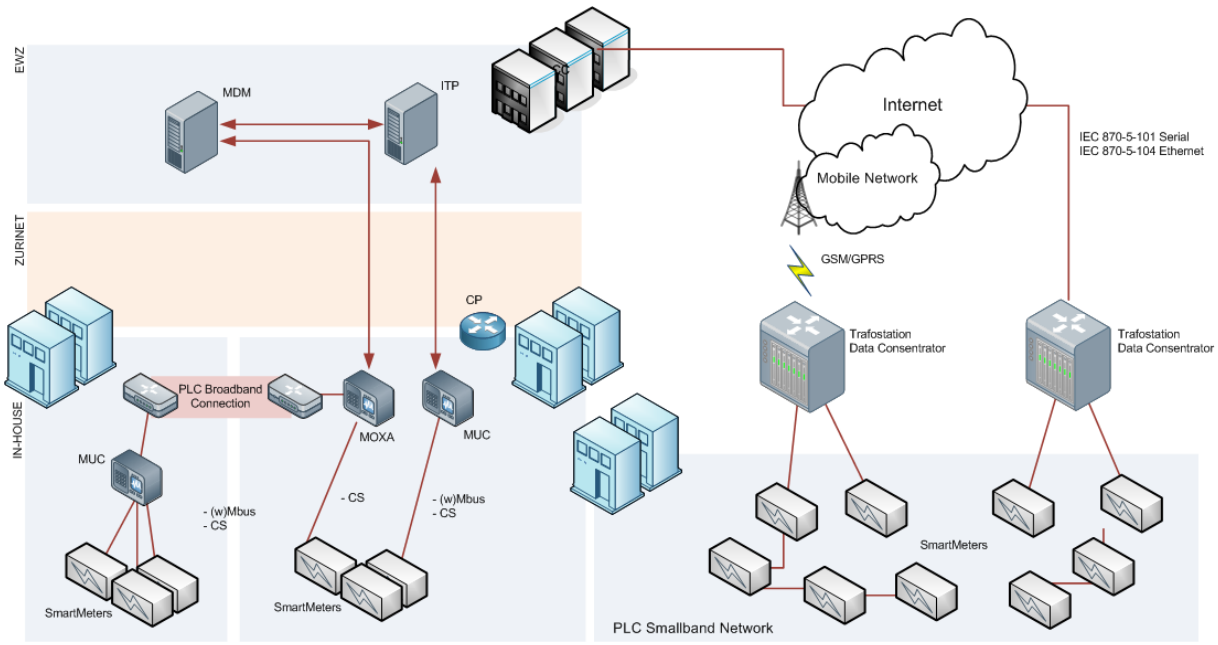
Ausgangslage

Der Begriff Smartmeter beschreibt einen intelligenten Stromzähler, welcher den Stromverbrauch in Abhängigkeit von der Zeit des Verbrauchs an einen Energiedienstleister übermitteln kann. Diese Smartmeters sind momentan ein grosses Thema.

Durch die automatisierte Rückspeisung der Zählerstände in die Systeme des Energiedienstleisters entfällt die manuelle Ablesung der verschiedenen Zähler. Die Daten werden an einer zentralen Stelle gesammelt und ausgewertet. Im Zusammenhang mit dieser Sammlung der Daten tauchen auch Fragen bezüglich Datenschutz auf. Ist die Übertragung dieser Daten sicher? Können Daten abgehört oder gar manipuliert werden?

Architektur

Um die Sicherheit einer Smartmetering Infrastruktur genauer beurteilen zu können wurde in Zusammenarbeit mit dem ewz ein Versuchsaufbau (siehe Fig. 1) analysiert. Dabei wurden die verschiedenen Technologien in einem Pilotbetrieb aufgebaut.



Figur 1: *Versuchsaufbau Smartmetering*

In diesem Versuchsaufbau kommen grundsätzlich zwei verschiedene Arten von Smartmeters zum Einsatz. Zum einen sind dies Gateway-basierte Lösungen, bei denen mehrere Zähler an einem Gateway angeschlossen sind, welcher mit den Servern beim ewz kommuniziert. Zum anderen sind dies Schmalband PLC basierte Meters, welche untereinander ein vermaschtes Netz aufbauen, welches mit einem Datenkonzentrator an einer zentralen Stelle kommuniziert. Dieser Datenkonzentrator übernimmt die Kommunikation zu den Servern, welche momentan über GSM läuft.

Auf physikalischer Ebene kommuniziert die Gateway basierte Lösung über das Zürinet, welches durch ein eigenes Glasfasernetz realisiert wird. Um die Reichweite dieses Netzes zu erweitern wird das Signal teilweise via Breitband PLC über das Stromnetz weitergeleitet. Die Verbindung zwischen Gateways und den Zählern selber funktioniert entweder kabelgebunden (MBUS, CS) oder kabellos (wMBUS).

Die PLC basierten Zähler kommunizieren über das Stromnetz miteinander. Dabei kann jeder Zähler auch die Rolle eines Repeaters übernehmen und die Daten anderer Zähler weiterleiten. Als Kommunikationsendpunkt dient hier der Datenkonzentrator, welcher die Daten an die ewz internen Server weiterleitet.

Ziel der Arbeit

Im Rahmen einer Sicherheitsüberprüfung sollte die implementiere Lösung des ewz bezüglich Sicherheit untersucht werden. Im Fokus dabei stand die Sicherheit der Daten, die von den einzelnen Haushalten zur Abrechnung an das ewz übertragen werden. Diese Daten sollten von niemandem eingesehen oder mitgelesen werden können.

Um dieses Ziel zu erreichen, wurde der Verkehr an mehreren Orten in der Infrastruktur abgehört und Systeme der Infrastruktur wurden direkt angegriffen um zu sehen wie resistent diese gegenüber Attacken aus den verschidenen Teilbereichen der Infrastruktur sind.

Ergebnisse

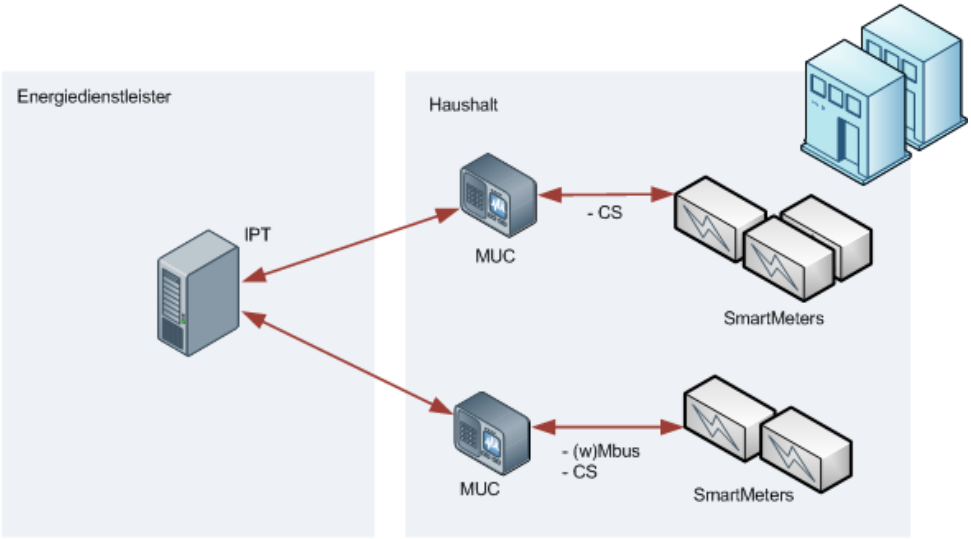
Da während den Tests mehrere verschiedene Lösungen untersucht wurden, sind die Resultate sehr unterschiedlich ausgefallen. Aus diesen Gründen soll dieser Bericht nicht dazu dienen die verschiedenen Produkte zu beurteilen. Vielmehr sollen hier Anforderungen an eine sichere Lösung definiert werden. Zur besseren Übersicht wurden diese Anforderungen in vier verschiedene Teilbereiche unterteilt.

- Gateway basierte Smartmeters
- Netzwerk / Firewalling
- Server Hardening
- PLC basierte Smartmeters

Die Ergebnisse und Empfehlungen zu den vier Teilbereichen können in den folgenden Kapiteln gefunden werden.

Gateway basierte Smartmeters

Gateway basierte Lösungen setzen auf herkömmlichen Zählern auf, welche über eine serielle Schnittstelle an einen MUC (Multi Utility Control) angeschlossen werden. Dieser MUC übernimmt die gesamte Kommunikation mit den Servern auf Seiten des Energiedienstleisters. Ein Beispielaufbau ist in folgendem Diagramm festgehalten (siehe Fig. 2).



Figur 2: *Aufbau Gateway basierte Smartmeters*

Da die MUCs und die Zähler selber direkt beim Kunden vor Ort eingesetzt werden, ist dies ein Punkt mit hohem Angriffspotential. Um bestmöglich geschützt zu sein sollten folgende Anforderungen eingehalten werden:

- **Physikalischer Schutz:** Um alle betroffenen Geräte vor direkter Manipulation zu schützen, sollten die Geräte (Zähler und MUC) in einem abgeschlossenen oder plombierten Kasten zum Einsatz kommen. Dadurch wird sichergestellt, dass der Kunde keine direkten Manipulationen an den Geräten durchführen kann.

- **Schutz des Gerätes:** Die verschiedenen Schnittstellen der MUC Geräte sollten nur mit einem gültigen Passwort erreicht werden, es darf kein anonymer Zugriff auf die Dienste des Gerätes möglich sein. Zudem muss organisatorisch sichergestellt werden, dass die werksmässig gesetzten Passwörter vor dem produktiven Einsatz geändert werden.

- **Kommunikation Zähler - MUC:** Es muss sichergestellt werden, dass zwischen Zähler und MUC keine Daten verändert werden können. Bei kabelgebundener Kommunikation sollte darauf geachtet werden, dass Zähler und MUC im selben Kasten abgeschlossen werden. Bei der kabellosen Verbindung (wMBUS) sollte unbedingt darauf geachtet werden, dass die Daten verschlüsselt und signiert werden. Der Schlüssel für die Verschlüsselung sollten dabei für jeden Zähler einzeln definiert werden können.

- **Kommunikation MUC – IPT:** Der IPT Server (IP Telemetrie) ist der direkte Kommunikationsserver auf Seite des Energiedienstleisters. Er dient als Proxy Server für die Meter Data Management Systeme, welche mit den MUCs kommunizieren. Für die Kommunikation zwischen MUC und IPT können Protokolle aus der IT Welt zum Einsatz kommen (SFTP/ FTPS / SSH) oder serielle Protokolle (SML über TCP/IP). Es sollte auch hier darauf geachtet werden, dass die Protokolle verschlüsselt und signiert sind. Ausserdem sollte der MUC vom IPT eindeutig identifizierbar sein (beispielsweise durch eine lange zufällige ID)

Netzwerk / Firewalling

Durch die neu eingesetzten Technologien werden die Daten zwischen dem Haushalt des Endverbrauchers und dem Energiedienstleister über ein IP basiertes Netzwerk übertragen. Um die Daten in diesem Netz nicht unnötig zu exponieren sollten auch hier einige Punkte beachtet werden:

- **Netzwerk Segregation:** Im Idealfall wird die Smartmetering Infrastruktur über ein eigenes Netz betrieben. Im getesteten Fall wird der Pilot über das Zürinet betrieben. Das Zürinet ist ein Glasfasernetz, welches vom ewz betrieben wird. Um die Reichweite des Netzes zu vergrössern, kommen allerdings Geräte zum Einsatz, welche das Signal auf das Stromnetz übertragen. In diesem Falle sollte die Verbindung verschlüsselt werden, um ein Abhören dieser Signale zu verhindern, da ein Angreifer seine Geräte ebenfalls ans Stromnetz anschliessen kann

- **VPN:** Ist es nicht möglich, ein eigenes Netz zu betreiben, sollte ein VPN (Virtual Private Network) zum Einsatz kommen. In diesem Fall wird eine verschlüsselte Verbindung vom Endverbraucher zum Energiedienstleister über bestehende Verbindungen aufgebaut. Diese Verbindung sollte mittels Zertifikaten authentisiert werden, um einen Einbruch in das VPN zu verhindern.

- **Firewalling:** Die Firewall zwischen den Zählern und den Servern des Energiedienstleisters sollte möglichst restriktiv konfiguriert werden. Grundsätzlich sollten alle Pakete verworfen werden. Nur ausgewählte Verbindungen sollten erlaubt werden. Dazu sollte beachtet werden, dass die erlaubten Verbindungen nur vom internen Netz nach aussen eine Verbindung aufbauen dürfen. Durch diese Massnahme wird ein Angreifer abgehalten die Infrastruktur des Energiedienstleisters direkt anzugreifen.

Server Hardening

Da gewisse Server direkte Verbindungen zu Hardware aufbauen, welche nicht vertrauenswürdig ist, sollten diese Server gehärtet werden, um einen Ausbruch auf andere Systeme zu verhindern, falls die Server kompromittiert werden. Die wichtigsten Massnahmen dazu sind in folgenden Punkten zusammengefasst:

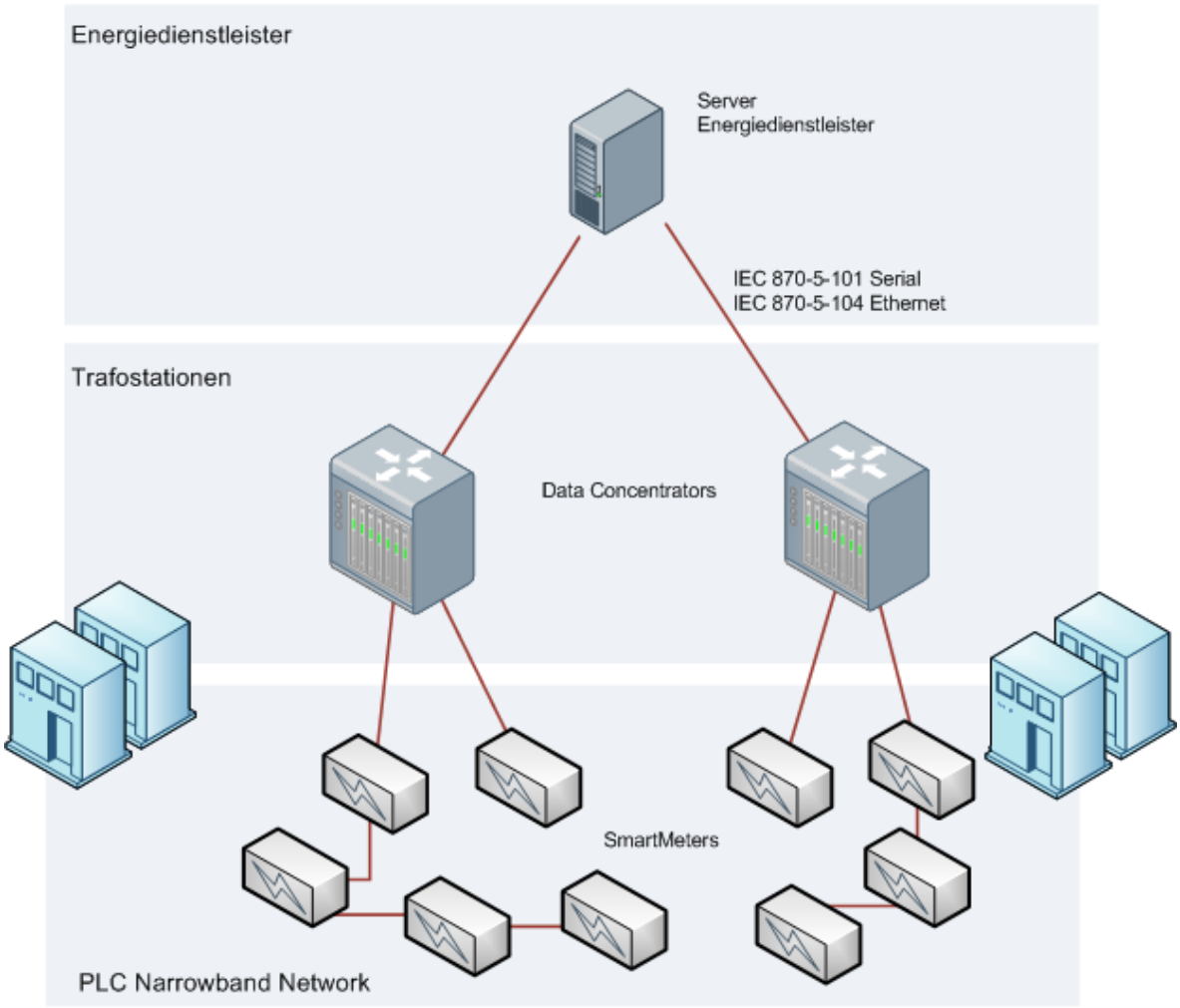
- **Starke Passwörter:** Für die Benutzer auf den Servern sollten starke Passwort Richtlinien eingesetzt werden. Insbesondere sollte darauf geachtet werden mindestens 8 Zeichen aus verschiedenen Zeichengruppen zu benutzen (Kleinbuchstaben, Grossbuchstaben, Ziffern, Sonderzeichen). Die Passwörter sollten auch in regelmässigen Abständen gewechselt werden (ca. alle 90 Tage) um ein Erraten der Passwörter zu verhindern.

- **Least Privilege Prinzip:** Dienste welche vom Netz aus erreichbar sind, sollten nie mit administrativen oder gar System-Privilegien betrieben werden. Falls es einem Angreifer nämlich gelingt, aus dem Dienst auszubrechen, hat er Vollzugriff auf den ganzen Server. Daher sollten für diese Dienste eigene Benutzer erstellt werden, welche möglichst wenig Rechte auf dem Server besitzen. So wird ein erfolgreicher Angreifer abgehalten, weitere Systeme anzugreifen.

- **Patch Management:** Es existiert keine Software ohne Fehler und Sicherheitslücken. Diese Lücken werden jeweils regelmässig mit Patches und Software Updates geschlossen. Daher sollten die Server (Betriebssysteme und eingesetzte Software) in regelmässigen Abständen auf den neuesten Stand gebracht werden.

PLC basierte Meters

Im Gegensatz zu den Gateway-basierten Smartmeter Lösungen, existieren auch Lösungen, welche über PLC miteinander kommunizieren (siehe Fig. 3).



Figur 3: *Aufbau PLC basierte Smartmeters*

Die Zähler bilden dabei ein vermaschtes Netz in welchen die Zähler auch Repeater für die Signale anderer Zähler sein können. Dabei erfolgt die Kommunikation über das Stromnetz bis zu den sogenannten Datenkonzentratoren. Diese wandeln das Signal und leiten es über ein IP-basiertes Netz weiter an den Energiedienstleister. Die Protokolle welche zum Einsatz kommen sind proprietär und können auch auf unterschiedlichen Transportmedien weitergeleitet werden. Trotz allem konnten auch hier einige Erkenntnisse erarbeitet werden.

– **Hardware:** Durch den Einsatz von Hardware, welche proprietäre Protokolle über PLC verwendet, war diese Lösung viel schwieriger zu analysieren. Dies erschwert es auch einem Angreifer, die Infrastruktur zu attackieren. Dafür muss nämlich erst das Protokoll durch Reverse Engineering ermittelt werden. Zudem ist bestimmte Hardware nötig um die Signale aus dem PLC Netzwerk zu extrahieren.

- **Verschlüsselung:** Um die Daten aber zusätzlich zu dieser Hardware basierten Hürde noch zu schützen, sollten diese verschlüsselt und signiert werden. Da die Zähler auch als Repeater für andere Zähler fungieren, ist es wichtig, dass jeder Zähler eigene Schlüssel besitzt und so nicht in der Lage ist, die Daten für einen anderen Zähler zu entschlüsseln, oder Daten eines anderen Zählers zu manipulieren.

- **Kommunikation Datenkonzentrator – Server:** Da die Kommunikation zwischen Datenkonzentrator und Server auch über ein IP basiertes Netz geschieht, sollte auch hier darauf geachtet werden, den Datenverkehr zu verschlüsseln und zu signieren um die Manipulation durch Dritte zu verhindern. Auch hier kommen proprietäre Protokolle zum Einsatz. Darum ist es auch hier nicht einfach möglich, den Verkehr zu analysieren.

Fazit

Grundsätzlich entsprechen die Sicherheitsanforderungen an ein Smartmetering System den Sicherheitsanforderungen an ein anderes ICT System. Die einzelnen Komponenten sollten eindeutig identifizierbar sein, um das vorgaukeln anderer Komponenten zu verhindern. Zudem sollten alle Verbindungen verschlüsselt und signiert werden um das Abhören sowie Veränderung der Daten zu verhindern.

Als zweite Sicherheitsmassnahme sollte darauf geachtet werden, dass die Kommunikation nur über sichere Netzwerke erfolgt, um die Angriffsoberfläche möglichst klein zu halten. Im Idealfall ist dies ein Netzwerk, welches vom Energiedienstleister selber betrieben wird. Alternativ kann aber auch ein VPN in Betracht gezogen werden.

Zusätzlich du diesen Anforderungen sollte auch in regelmässigen Abständen geprüft werden, ob alle Komponenten auf dem aktuellen Stand der Technik sind. Falls dies nicht der Fall ist, ist es möglich, dass gewisse Sicherheitslücken vorhanden sind, welche durch aktuelle Patches gefixt werden. Daher sollten alle Komponenten regelmässig updated werden.