



Swiss Made
Information Security

SIDLER

INFORMATION SECURITY



SUCCESS STORY

Landis+Gyr+

manage energy better



TREUHAND



AUSBILDUNG



VERWALTUNG



INDUSTRIE



FINANZ



LEGAL



GESUNDHEIT

Landis+Gyr sorgt für Sicherheit im Smart Metering

Schutzprofil für Smart-Meter-Gateway nach Common Criteria umgesetzt

Die Herstellung intelligenter Stromzähler, sogenannte Smart Meter, unterliegt rechtlichen Vorgaben und muss strenge Sicherheitsanforderungen erfüllen, deren Einhaltung geprüft und zertifiziert wird. Mit Unterstützung der Sidler Information Security GmbH hat der Smart-Meter-Pionier Landis+Gyr ein dafür erforderliches Informationssicherheitskonzept erstellt und so den Weg zu sicheren Smart-Meter-Lösungen geebnet. Das erste, nach neuestem Standard entwickelte Smart-Meter-Gateway konnte Landis+Gyr im Juli 2013 zur Zertifizierung Treuhand Gesundheit Finanz Industrie Verwaltung Legal Ausbildung anmelden.

Landis+Gyr mit Hauptsitz in Zug und Niederlassungen rund um den Globus, ist weltweiter Leader auf dem Gebiet des Smart Metering und führender Anbieter von integrierten Energiemanagementlösungen. Das Unternehmen ermöglicht es nicht nur Versorgungsunternehmen und Endkunden ihre Energieeffizienz zu verbessern, Energiekosten zu senken und zu einer nachhaltigen Nutzung der Ressourcen beizutragen. Nachhaltige Werte schaffen, zukunftsfähige Lösungen entwickeln und diese dabei mit den energiepolitischen Herausforderungen in Einklang bringen, gehört mit zum Tagesgeschäft des Branchenführers.

Rechtlich Anforderungen umsetzen

Der Einsatz intelligenter Stromzähler bzw. Smart Meter gilt als grundlegende Voraussetzung für die Umsetzung des "Aktionsplans für Energieeffizienz in Europa". Dieser sieht vor, dass mindestens 80 Prozent der Verbraucher aller EUMitgliedsstaaten bis zum Jahr 2020 mit intelligenten auszustatten sind. Im Rahmen der unter Berück-

sichtigung Deutschland eine Vorreiterrolle ein und hat durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein Schutzprofil (BSI-CC-0073) nach den "Common Criteria" für ein Smart Metering Gateway und die dazugehörigen Sicherheitsmodule herausgegeben. Für Hersteller wie Landis+Gyr stellen die umfangreichen Anforderungen des BSI-Schutzprofils und die damit verbundenen rechtlichen Vorgaben, die in den elektronischen Zählern und Smart-Meter-Gateways umgesetzt werden müssen, vor neuartige Herausforderungen. Denn nicht nur das Produkt an sich wird hinsichtlich Sicherheitsanforderungen dieser Zertifizierung unterzogen. Bestimmte Mindestanforderungen müssen auch im Entwicklungsprozess, in der Dokumentation, bei der Unterstützung des Produktlebenszyklus, bei Tests sowie der Schwachstellenanalyse erfüllt werden. Und nur wenn das Gesamtumfeld dieser Auditierung standhält, erhält das Produkt ein Zertifikat. Dazu Thomas Mosel, Head of Information Security EMEA, bei Landis+Gyr: «Das Schutzprofil nach den international anerkannten IT-Sicherheitsrichtlinien der Common Criteria beinhaltet eine grosse Anzahl von Sicherheitsanforderungen. Uns war schnell klar, dass wir für die Umsetzung dieses umfassenden Anforderungskatalogs, im speziellen für den IT-Sicherheitsbereich, jemanden mit entsprechendem Know-how beiziehen mussten. Auf der Suche nach einem Experten sind wir auf Wolfgang Sidler von der Sidler Information Security gestossen. Sein enormes Sicherheitswissen passte perfekt auf das bevorstehende Projekt. So sind wir ins Gespräch gekommen und haben ihn für die Umsetzung des Projektes verpflichtet.»

Bereichsübergreifende GAP-Analyse von A bis Z

Im April 2012 starteten Thomas Mosel und Wolfgang Sidler mit einer eingehenden Bestandsaufnahme mittels GAP-Analyse, in der die bestehende Informationssicherheit gegenüber dem vorliegenden Anforderungskatalog abgeglichen wurde.



Einen wichtigen Teil nehmen die "Assurance Requirements" der Common Criteria ein. Sie definieren, welche Mindestanforderungen im Entwicklungsprozess, in der Dokumentation, bei der Unterstützung des Produktlebenszyklus, bei den Tests sowie der Schwachstellenanalyse zwingend eingehalten werden müssen und, wie der Evaluator diese Anforderungen zu prüfen hat. Basierend auf diesem Katalog wurde anschliessend ermittelt, welche Anforderungen auf organisatorischer Ebene bereits vorhanden und welche zwingend zu erfüllen sind, welche Punkte in welcher Form ergänzt oder neu erarbeitet werden müssen und vor allem, wie der Massnahmenkatalog letztendlich aussehen muss. Das daraus abgeleitete Informationssicherheitskonzept, das Wolfgang Sidler nach der von ihm erarbeiteten Analyse erstellte, setzt bereichsübergreifend innerhalb der Landis+Gyr an und findet von der Soft- und Hardware-Entwicklung über das Konfigurationsmanagement bis hin zur Produktion und Qualitätssicherung seine Anwendung.

Das daraus abgeleitete Informationssicherheitskonzept, das Wolfgang Sidler nach der von ihm erarbeiteten Analyse Treuhand Gesundheit Finanz Industrie Verwaltung Legal Ausbildung erstellte, setzt bereichsübergreifend innerhalb der Landis+Gyr an und findet von der Soft- und Hardware-Entwicklung über das Konfigurationsmanagement bis hin zur Produktion und Qualitätssicherung seine Anwendung. Bis das Informationssicherheitskonzept dem Management vorgelegt und von diesem freigegeben wurde, vergingen rund zwölf Monate. Thomas Mosel erklärt: «Wir hatten das Privileg, nicht unter einem enormen Zeitdruck zu stehen. Sowohl für die Erstellung der GAP-Analyse, als auch für das anschliessende Sicherheitskonzept konnten wir uns genügend Zeit nehmen, alle einzelnen Punkte einer sehr detaillierten Prüfung unterziehen und uns intensiv und vor allem sehr genau auf die BSIZertifizierung vorbereiten.»

Mehr als nur ein Informationssicherheitskonzept

Mit dem heute vorliegenden Informationssicherheitskonzept hat Landis+Gyr den ersten entscheidenden Schritt auf dem Weg zu einem sicheren intelligenten Messsystem für Strom und Gas gemacht, das den neuen rechtlichen Vorgaben entspricht und konnte im Juli 2013 das erste Smart-Meter-Gateway zur Zertifizierung gemäss Common Criteria und Schutzprofil (BSICC-PP-0073) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anmelden. Die weitere Entwicklung wird jetzt mit den Anforderungen des Common-Criteria-Zertifizierungsprozesses abgestimmt.

«Eine Produktzertifizierung ist mit gewissen Einschränkungen international gültig. Aus diesem Grund haben wir das Sicherheitskonzept ebenfalls international ausgelegt, damit es landes- bzw. standortunabhängig anwendbar ist», erklärt Mosel und ergänzt:

«Die Erfahrungen im IT-Security-Bereich, die Wolfgang Sidler auf internationaler Ebene mitbrachte, waren uns auch hier sehr nützlich.» Konkret spricht Mosel das ISO 27001-Zertifizierungsprojekt von Landis+Gyr in England an, das zeitgleich mit dem Common Criteria Projekt durchgeführt wurde und alle mit dem Betrieb und der Implementierung sicherheitsrelevanter Funktionen eines Informationssicherheits-Management-Systems (ISMS) im Unternehmen definiert. «Im Rahmen der jeweiligen Analysen und Konzepterstellung haben beide Projekte sehr voneinander profitiert und Informationen sind vis versa eingeflossen. Dabei hat Wolfgang Sidler mit den internen Stellen in England zusammengearbeitet, das Sicherheitsaudit aktiv unterstützt und ist auch bei der erfolgreichen Zertifizierung Anfang Juli in England in beratender Funktion dabei gewesen.»

Security-Awareness für die Mitarbeitenden

Technische Sicherheitsmassnahmen bedürfen nicht nur organisatorischer, sondern vor allem auch personeller Massnahmen, um effektiv sein zu können. In Zusammenhang mit der Umsetzung der Sicherheitsrichtlinien und auf Basis des erstellten Informationssicherheits-Konzepts, wurde ergänzend ein Trainings-Konzept erstellt und auf Initiative von Wolfgang Sidler hin im Juni 2012 erstmals ein Awareness-Training für Mitarbeitende durchgeführt. 2013 folgte auf der Basis der erarbeiteten Projektergebnisse zum Common Criteria Projekt ein Security-Training für alle am Projekt beteiligten Mitarbeitenden. «Nicht nur die Resonanz der Mitarbeitenden war sehr positiv und hat konstruktive Diskussionen und gutes Feedback hervorgebracht», so Thomas Mosel. «Speziell das Review und die daraus resultierenden Verbesserungsvorschläge, die Wolfgang Sidler im Anschluss zu den Schulungs-unterlagen gemacht hat, waren überaus hilfreich. Das Awareness-Training entspricht heute aktuellen Standards und wir können

jederzeit und nach Bedarf weitere Trainings selber durchführen».

Fazit

Die Weichen für die Zukunft intelligenter Messsysteme sind bei Landis+Gyr gestellt, das Endresultat entspricht den Erwartungen und ist soweit auf Kurs, um Informationssicherheit, Datenschutz und Datensicherheit in Smart Grids zu gewährleisten. Was jetzt noch fehlt, ist die Zertifizierung. Sobald diese erteilt wird, können der Industrie bald auch zukunftsfähige Lösungen angeboten werden.

Projekt**details**

- *Smart Meter Gateway Common Criteria EAL4+ Product Certification*
- *Durchführen einer Informationssicherheits GAP-Analyse nach ISO 27001*
- *Erstellen von Security-Weisungen und Richtlinien für die Entwicklungs-, Projekt- und Produktions-Bereiche*
- *Durchführen von ISO 27001 Audits in den Smart-Meter Produktions-Werken in England und Frankreich*
- *ISMS Beratung basierend auf dem ISO 27001 und ISO 27002 Standard*

Projekt**kategorie**



TREUHAND



AUSBILDUNG



VERWALTUNG



INDUSTRIE



FINANZ



LEGAL



GESUNDHEIT

SIDLER
INFORMATION **SECURITY**

www.sidler-security.ch – info@sidler-security.ch
Holzhäusernstrasse 5a – CH-6331 Hünenberg / Zug