Sicherheit im Smart Grid

TECHNOLOGIE **SMART GRID**

Sicherheit im Smart Grid

Manipulationen verhindern, Daten schützen

Mittelfristig werden sich Smart Grids auch in der Schweiz zu einem zentralen Element der Infrastruktur im Energieversorgungssystem entwickeln. Neben weiteren, technischen Herausforderungen stellen Smart Grids auch hohe Ansprüche an die Sicherheit. Energieversorger tun gut daran, sich frühzeitig mit dieser Thematik auseinanderzusetzen, um sich auf die kommenden Entwicklungen einzustellen.

Candid Wüest

Intelligente Energieversorgungssysteme, sogenannte Smart Grids, sind auf dem besten Weg, die weltweit wichtigste Entwicklung der letzten 100 Jahre im Bereich der Stromnetze einzuläuten. In zahlreichen Ländern werden bereits flächendeckende Rollouts von Smart Metern umgesetzt. Allein in Grossbritannien sieht die Regierung vor, bis 2020 in jedem Haushalt einen Smart Meter zu installieren. Auch in der Schweiz wird das Thema sowohl auf politischer wie auch auf wirtschaftlicher Ebene rege diskutiert. In seiner geplanten Energiestrategie 2050 spricht der Bundesrat unter anderem von einer Modernisierung der Stromnetze und möchte im Stromversorgungsgesetz die nötigen Rechtsgrundlagen zur Einführung von intelligenten Stromzählern (Smart Meters) schaffen. Insbesondere für Länder wie die Schweiz, die sich verstärkt erneuerbaren Energiequellen zuwenden, werden Smart Grids in Zukunft eine vitale Rolle spielen.

Über die nächsten 10 Jahre werden weltweit schätzungsweise über 100 Milliarden intelligente Messgeräte und Sensoren installiert. Damit wird eine neue Ära eingeläutet, die eine transparentere und gerechtere Preisgestaltung mit sich bringen und massgeblich zur Netzstabilität beitragen soll. Die Energieversorger erhalten damit eine Infrastruktur, dank derer sie tages- und jahreszeitabhängige Verbraucherpreise für ihre Kunden einführen können. Ausserdem können Smart Grids als virtuelle Kraftwerke fungieren, die zur Steuerung der Netzstabilität eingesetzt werden können.

Aufgrund der enormen Grösse und zentralen Funktion unserer Stromnetze muss der Sicherheit von Smart Grids höchste Bedeutung beigemessen werden: Wie können Smart Grids bestmöglich geschützt werden? Den Vorteilen intelligenter Versorgungssysteme sowohl für die Produzenten wie für die Konsumenten stehen auch potenzielle Gefahren gegenüber – diese sind systematisch abzuwägen.

Zahlreiche Sicherheitsstufen

Wie bei jeder vernetzten Infrastruktur müssen auch bei Stromnetzen von Beginn an verschiedene Sicherheitsstufen und -faktoren berücksichtigt werden. Dazu zählen geeignete Richtlinien, Prozesse, Partner und die Wahl der Sicherheitslösungen. Die berühmt-berüchtigten Computerwürmer Stuxnet und Duqu sind nur die Spitze des Eisbergs, doch durch sie haben Sicherheitsbedrohungen eine neue Dimension erreicht: Sie sind um ein Vielfaches komplexer und raffinierter und damit letztlich gefährlicher geworden.

Während früher Sicherheitssysteme vor Angreifern schützen mussten, die lediglich auf Ruhm oder Öffentlichkeit aus waren, muss der Schutz eines Systems heutzutage Angreifern mit deutlich geänderten und damit gefährlicheren Motivationen standhalten. Es muss hoch entwickelte, gezielt und minutiös geplante Angriffe abwehren, die beispielsweise politisch motiviert sind oder mit dem Ziel der Wirtschaftsspionage ausgeübt werden. Meist stehen hier, ähnlich der «analogen» organisierten Kriminalität, den Angreifern grosse Ressourcen für ihre Machenschaften zur Verfügung. Versagt der Schutz, können kritische Elemente der Infrastruktur wie Energieknotenpunkte oder -speicher für feindlich gesinnte Dritte sichtbar oder, schlimmer noch, kontrollierbar werden.

Des Weiteren müssen einzelne Komponenten innerhalb der Infrastruktur, wie etwa individuelle Smart Meter oder Kommunikationszentralen, gesichert werden, um sowohl die Daten als auch die Geräte des Systems zu schützen – damit beispielsweise nicht auf einmal des Nachbars Strom auf dem eigenen Zähler erscheint und in Rechnung gestellt wird. Professionelle Hacker könnten hier beispielsweise die Identifikationsnummer des Smart Meters manipulieren. Daher

Wenn vermehrt dezentral und stochastisch einspeisende Stromerzeuger wie Windanlagen am Netz angeschlossen werden, ist eine zuverlässige Stromversorgung ohne Smart Grid kaum möglich.

TECHNOLOGIE **SMART GRID**

Bilder: Fotolia

Ein flächendeckendes Smart Grid wird einen hohen Kommunikationsbedarf aufweisen – mit entsprechend vielen Möglichkeiten für Cyberattacken. Um die hohe Versorgungssicherheit nicht zu gefährden, sollten Sicherheitsmassnahmen eine hohe Priorität haben.

sollte sichergestellt werden, dass nur authentifizierte Komponenten in die Infrastruktur eingebaut werden können und die gesamte Kommunikation zwischen den Geräten und den Back-end-Systemen verschlüsselt erfolgt.

Datenschutzfragen

Aus Sicht des Datenschutzes generieren Smart Meter Unmengen an persönlichen und sensiblen Daten, die von den Energieversorgern verwaltet und gesichert werden müssen. Zusätzlich zu den Auflagen bezüglich Sicherheit, Authentifizierung und Geheimhaltung stehen die Dienstleister in der Pflicht, die von den Smart Metern und Back-end-Systemen erzeugten Daten zu archivieren.

Ein Smart Grid besteht aus Millionen Smart-Meter-Endgeräten und verarbeitet eine Datenmenge im Bereich von Petabytes. Diese Daten müssen unter Einhaltung der Audit- und Compliance-Vorschriften gespeichert und entsprechend gesichert werden. Erschwerend kommt hinzu, dass viele Energieversorger international tätig sind und an unterschiedliche Rechtsvorschriften und Compliance-Richtlinien in den verschiedenen Ländern gebunden sind. Stromnetze müssen daher in Einklang mit unterschiedlichen Gesetzgebungen betrieben werden.

Die grosse Menge der generierten Daten und die Notwendigkeit, die Integrität dieser über grosse Zeiträume erfassten Informationen sicherzustellen, erfordert die Entwicklung spezieller Datenträger, Speichergeräte und Backup-Strategien. Die heute angewendeten und erprobten Lösungen müssen erst auf ihre Tauglichkeit in einer Smart-Grid-Umgebung überprüft werden.

Skalierbarkeit als Kriterium

Beim Aufbau eines solchen Systems dürfen Offenheit und Skalierbarkeit nicht ausser Acht gelassen werden. Der Rat an alle Unternehmen: auch darauf schauen und davon lernen, was die anderen Organisationen tun. Die weltweite «Smart Grid Community» besteht aus Energieversorgern, Dienstleistern und Produzenten, die erfahrungsgemäss gern zum Wissensaustausch bereit sind und bei dem alle Beteiligten voneinander lernen können.

Zum Beispiel gibt es neue Ökosysteme in anderen Märkten, wie etwa der Unterhaltungs- und Haushaltselektronik, bei welchen der Kundschaft neue Dienstleistungen angeboten werden. Die Herausforderung liegt darin, diese Geräte abzusichern. Wegen der schieren Masse an Geräten eines solchen Ökosystems wurden hoch anpassungsfähige Sicherheitslösungen entwickelt und eingesetzt, die bereits Millionen von Geräten schützen. Es lohnt sich daher, diese Lösungen genauer zu betrachten, um sich einen tiefergehenden Einblick in grossflächige Umsetzungen zu verschaffen.

Geplante Sicherheit

Die sicherheitstechnischen Herausforderungen für Smart Grids sind zwar erheblich, aber nicht unüberwindbar. Die wichtigste Aufgabe besteht darin, schon bei der Planung von vornherein eine Sicherheitsstrategie zu erarbeiten, um die Risiken für das System auf ein Minimum zu reduzieren. Die Lösung muss den Einbau einer Sicherung in jede Komponente des gesamten «Ökosystems» beinhalten. Ist dieses Problem gelöst, lassen sich die Vorteile intelligenter Energiesysteme vollumfänglich nutzen – ohne die Integrität der Infrastruktur, die Kundenbeziehungen, das Markenimage oder den Umsatz zu gefährden.

Angaben zum Autor

Candid Wüest, Principal Threat Researcher.
Symantec AG, 8052 Glattbrugg, Email@symantec.com

Résumé **La sécurité des smart grids**

Empêcher les manipulations et protéger les données

À moyen terme, les smart grids deviendront également en Suisse un élément majeur de l'infrastructure du système d'approvisionnement en énergie. Au-delà d'autres défis techniques à relever, ces réseaux intelligents présentent des exigences élevées en matière de sécurité. Les défis relatifs à cette dernière sont certes considérables, mais ils ne sont pas insurmontables. La mission la plus importante consiste à élaborer d'emblée une stratégie de sécurité dès l'étape de planification afin de réduire les risques liés au système à un niveau minimal. La solution doit comporter l'intégration d'une sécurité dans chaque composant de « l'écosystème » global. Ce problème résolu, l'intégralité des avantages des systèmes énergétiques intelligents pourraient être exploités, et ce, sans compromettre l'intégrité de l'infrastructure, les relations avec la clientèle, l'image de marque ou bien le chiffre d'affaires.

No