CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch

WISSENS-UPDATE

IoT Security – für eine smarte Energiezukunft

Der Energiesektor soll smart werden. So lautet das Ziel, das der Bund im Rahmen der Energiestrategie 2050 anstrebt. Dabei setzt man auf den flächendeckenden Einsatz von IoT Devices: Intelligente Messsysteme – sogenannte Smart Meters – sollen den Weg frei machen in eine effiziente und ressourcenschonende Energiezukunft.

Bis Ende 2027 werden Smart Meters in der ganzen Schweiz zur Pflicht. So wollen es die 2018 vom Stimmvolk abgesegneten Regelungen zur Förderung erneuerbarer Energien und zur Senkung des Energieverbrauchs. Aber was kann ein Smart Meter eigentlich? Und was macht ihn intelligent?

Smart Meter – Schlüssel zur Energiezukunft

Genauso wie herkömmliche Geräte zählt auch der Smart Meter die Energie, die aus dem Netz bezogen wird. Doch wie jedes andere IoT Device ist auch der Smart Meter ein Klein-Computer. So etwa verfügt der Zähler über ein Kommunikations-Tool (Smart-Meter-Gateway), das die Messdaten selbständig versenden kann. Damit erhalten Anwender die Möglichkeit, ihren Stromverbrauch über eine Smartphone-App zu beobachten und bei Bedarf darauf zu reagieren. Dies soll dazu beitragen, bewusst mit der Ressource Strom umzugehen.

Smart Meters senden aber nicht nur, sie können auch Daten empfangen. So kennt der intelligente Zähler beispielsweise den aktuellen Stromtarif, den er automatisch an Elektrogeräte weitergibt, welche das Label «Smart Grid Ready» tragen. Diese Geräte schalten sich ein, wenn der Strombezug besonders günstig ist – genauer gesagt, wenn dieser aus stochastischen Quellen wie Wind und Sonne im Überfluss zur Verfügung steht. So ermöglicht ein Smart Meter nicht nur, den eigenen Energieverbrauch im Blick zu behalten, sondern wird gleichzeitig zu einem wichtigen Steuerungsmittel für das Energiesystem der Zukunft – die Smart Energy.

Smart Energy – das intelligente Zusammenspiel

Mit dem Begriff Smart Energy sind alle intelligenten Technologien in der Wertschöpfungskette von der Energieerzeugung bis zum Energieverbrauch gemeint. Das Ziel von Smart Energy besteht darin, die 2018 vom Schweizer Stimmvolk beschlossene Energiestrategie 2050 umzusetzen – und damit die Energiewende zu schaffen.

Mit der Strategie soll der Energieverbrauch gesenkt, die Energieeffizienz erhöht und die Produktion aus erneuerbaren Quellen verstärkt werden. Dies setzt das intelligente Zusammenspiel folgender vier Teilbereiche voraus:

- **Smarte Produktion** Zentrales und dezentrales Erzeugen und Beschaffen von Energie
- **Smarte Verteilung** Automatisiertes Management des Energienetzes «Smart Grid»
- **Smarte Speicherung** Unterstützung durch dezentrale Speichereinheiten
- **Smarter Verbrauch** Effizienz- und Komfortsteigerung bei der Energienutzung

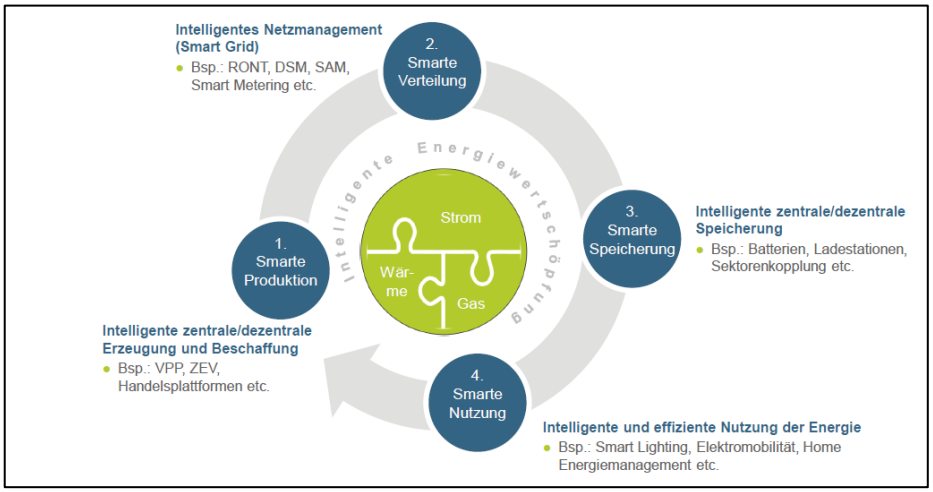

Abbildung 1: Smart Energy – das intelligente Zusammenspiel der Energiewertschöpfung
Quelle: Fachtagung Energiedaten und Informationssicherheit, AWK Group

IoT-Geräte spielen eine zentrale Rolle in der Smart Energy

Alle Bereiche des Energiesystems vernetzen und weitestgehend automatisieren – so lautet die Vision von Smart Energy. Der Einsatz von IoT-Komponenten, die Daten- und Energieflüsse steuern, ist dabei essentiell. Wie gezeigt übernehmen beispielsweise intelligente Messsysteme (Smart Meters) zentrale Funktionen im Stromnetz. Dabei liegt der Fokus längst nicht mehr allein nur auf der Automatisierung von Prozessen, sondern auch auf einem Informationsaustausch mit dem Energieproduzenten für die Individualisierung von Energieprodukten sowie auf automatisiertem Datenaustausch mit dem Stromnetz (Smart Grid) z.B. über den dynamischen Bezug oder die Einspeisung von Energie.

Cyber-Risiken werden durch die IoT-Vernetzung verschärft

IoT birgt aber auch ein oft vernachlässigtes Risiko: Bei zunehmender Konnektivität steigt die Gefahr der Manipulation. Datenmissbrauch, Sabotage und Erpressung sind mögliche Konsequenzen. Dazu kommt: Als Kritische Infrastruktur stellt die Energieversorgung eine zentrale Lebensader der Wirtschaft und Gesellschaft dar. Eine gezielte Cyber-Attacke kann die Versorgungssicherheit (Strom, Wasser und Wärme) gefährden. Der vielgenannte «Black-out» wird Realität, sollten Cyber-Kriminelle, z.B. mit einem Smart Meter Botnet, falsche Daten an den Netzbetreiber übermitteln oder erfolgreich entsprechende Handelsplattformen manipulieren können. Als Folge könnten die resultierenden Strom-Überkapazitäten zu einer Netz-Kaskade und zu einer Abschaltung führen. Dies führt in einer Kettenreaktion zum Ausfall der Kommunikationsnetze sowie zur grossflächigen Beeinträchtigung von Zahlungsprozessen. Hackerangriffe wie Mirai oder Botnet haben uns die Vulnerabilität von IoT-basierten Systemen bereits eindrücklich vor Augen geführt. Von daher liegt es nahe, die IoT-Prozesse im Energieversorgungssystem unter verschärfte Sicherheitsaufsicht zu stellen.

Handlungsbedarf für Hersteller und Betreiber

Werden mögliche Schwachstellen und Resilienz-Aspekte beim Einsatz von IoT nicht berücksichtigt, können Geräte weitreichende Schäden verursachen. Aber in welcher Entwicklungsphase sollen Sicherheitsfragen beantwortet werden? Je später Sicherheitslücken oder Fehlfunktionen in einem zukünftigen Produkt erkannt werden, desto höher sind die Behebungskosten. Müssen bei IoT-Geräten Sicherheitsversäumnisse erst im operativen Betrieb nachgebessert werden, kommen umständliche Härtungen des Umsystems oder des Kommunikationsnetzwerks sowie zusätzliche Hardware- und Softwarekomponenten ins Spiel, welche die Kosten explodieren lassen.

Die Maxime heisst deshalb «Security by Design». Hier liegt die Verantwortung einerseits bei den Herstellern. Sie müssen ihre IoT-Devices bereits mit den nötigen Sicherheits-Architekturen und den Möglichkeiten einer sicheren Vernetzung und der Update-Fähigkeit «from scratch» ausstatten. Umfassende Sicherheitsbetrachtungen müssen beim Hardware- und Softwaredesign von Anfang an berücksichtigt werden.

Andererseits stehen aber auch die Energieversorger in der Pflicht. Für sie geht es darum, im Rahmen eines umfassenden Supply Chain-Risikomanagements die Risiken auf Lieferantenseite zu minimieren und entsprechend bei der Evaluation der Komponenten auf die Sicherheitsstandards der IoT-Produkte zu achten. Dies mit Blick auf die gesamte Einsatzdauer des IoT-Produkts, denn klassischerweise wird heute ein Stromzähler zertifiziert, kalibriert und nach der Installation verbleibt er über Jahre beim Kunden. Ein Smart Meter verfügt über eine Online-Kommunikation und entsprechende Schnittstellen zu Hersteller, Betreiber und Benutzer. Diese Schnittstellen sind den sich dauernd weiterentwickelnden Cyber-Gefahren ausgesetzt. Darum muss zwingend eine Möglichkeit bestehen, die Software des Zählers den sich verändernden Cyber-Gefahren anpassen zu können. Eine sichere Möglichkeit für den Betreiber, zentral signierte Updates einspielen zu können, wird zur kritischen Funktionalität. Bei der Evaluation eines geeigneten Produkts sollen für den Energieversorger solche Aspekte zu zentralen Auswahlkriterien werden.

CyOne Security ist der kompetente Partner für die IoT Security in der Smart Energy

IoT-Devices wie Smart Meters sind bei der Umsetzung von Smart Energy essentiell. Mangelndes Sicherheitsbewusstsein erhöht das Risiko schädlicher Cyber-Angriffe. Um die vernetzten Produkte und Systeme zu schützen, müssen bisherige Sicherheitsansätze grundlegend überdacht werden. Denn Datensicherheit, eine Zonierung und Härtung der unterschiedlichen Schnittstellen im Gerät wie auch sichere zertifizierte Updatemechanismen sind zwingende Voraussetzungen, damit Smart Energy nicht zur Achillesferse wird.

Um die vernetzten Geräte und Systeme vor den Bedrohungen aus dem Cyberspace zu schützen, bringt die CyOne Security jahrzehntelange Erfahrung und vertieftes Expertenwissen auf dem Gebiet der Cyber Security und IoT Security in die Sicherheitskonzepte und -lösungen ein.

Energieversorger und Zulieferer der Energiebranche profitieren von einer ganzheitlichen Betrachtungsweise und einer fundierten Analyse für Schnittstellen und Übergänge aus Datensicht. Die CyOne Security unterstützt Hersteller und Betreiber bei der Umsetzung ihrer Schutzziele und setzt dabei auf die 360°-Sicherheitskompetenz von Product Security, System Security und Operational Security.

Beginnen Sie heute und schützen Sie Ihre Smart Energy-Produkte vor Cyber-Risiken – für eine sichere Schweiz.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren IoT Security-Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer Smart Energy, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.