Cyber-Sicherheit beginnt im Haus

PV-Anlage, Batteriespeicher, Wärmepumpe und Wallbox kommunizieren über digitale Schnittstellen miteinander und mit der Außenwelt. Heim-Energiemanagementsysteme fungieren dabei als zentrale Schaltstelle. Doch mit der Vernetzung steigt auch die Angriffsfläche.

Cloudbasierte Energiemanagementsysteme geraten zunehmend in den Fokus der Cyber-Sicherheitsdebatte. Das Forum Netztechnik/Netzbetrieb im VDE (VDE FNN) forderte so bereits im vergangenen Jahr in einem Positionspapier die lokale Verarbeitung netzorientierter Steuerbefehle in der Kundenanlage. Die Firma beegy, Tochterunternehmen der MVV Energie AG, hat diesen Grundsatz von Anfang an in die Architektur ihres Heim-Energiemanagementsystems (HEMS) eingebettet und setzt damit Maßstäbe über die aktuellen regulatorischen Anforderungen hinaus.

Die Energiewende verändert nicht nur die Erzeugungslandschaft, sondern auch die IT-Architektur im Eigenheim. Wo früher ein Zähler und eine Sicherung genügten, kommunizieren heute PV-Anlage, Batteriespeicher, Wärmepumpe und Wallbox über digitale Schnittstellen miteinander und mit der Außenwelt. Heim-Energiemanagementsysteme orchestrieren diese Komponenten und werden zur zentralen Schaltstelle der dezentralen Betriebsführung. Doch mit der Vernetzung steigt auch die Angriffsfläche. Spätestens mit dem Roll-out der §14a-EnWG-Steuerung stellt sich die Frage: Wie sicher sind die Systeme, die künftig Millionen dezentraler Anlagen steuern sollen?

Genau diese Frage adressierte das VDE FNN in seinem Positionspapier zur Cyber-Sicherheit im Umgang mit cloudbasierten Energiemanagementsystemen. Die Kernaussage ist eindeutig: Energiewirtschaftlich relevante Daten – insbesondere Steuerbefehle des Verteilnetzbetreibers – dürfen nach der Übergabe durch die Steuerungseinrichtung des Messstellenbetreibers nicht über das öffentliche Internet an eine Cloud weitergeleitet werden. Eine solche Weiterleitung konterkariere das hohe Sicherheitsniveau der iMSys-Infrastruktur, denn was nützt die verschlüsselte Übertragung über das gesicherte Weitverkehrsnetz des Smart Meter Gateways, wenn der Befehl anschließend über eine potenziell ungesicherte Internetverbindung in die Cloud geschickt wird?

Systemrelevante Schwachstelle

Das Positionspapier benennt zudem weitere Risiken. Bei einem Ausfall der kundenseitigen Internetverbindung kann der Steuerbefehl nicht mehr zuverlässig weitergegeben werden. Auch die Quittierung der erfolgreichen Umsetzung wird durch die Cloud-Verarbeitung erschwert. Im schlimmsten Fall müssen Netzbetreiber also davon ausgehen, dass ein Steuerbefehl nicht umgesetzt wurde. Vor dem Hintergrund einer wachsenden Zahl steuerbarer Verbrauchseinrichtungen stellt diese Unsicherheit laut VDE FNN eine systemrelevante Schwachstelle dar.

Für beegy ist diese Position eine Bestätigung der eigenen Entwicklungsphilosophie. Das Unternehmen hat sich frühzeitig für ein physisches HEMS entschieden, das vor Ort installiert wird und das Energiemanagement lokal durchführt. „Der Grundsatz für unsere IT-Architektur war von Anfang an die Trennung der Datenströme. Es ist eindeutig definiert, welche Programme und welche Datenarten an das Back End übermittelt werden und welche nicht“, beschreibt beegy-Geschäftsführer Carsten Bruns den Ansatz.

Der eigenentwickelte beegy Energiemanager, Herzstück des sogenannten beegy ComKits, baut im Eigenheim ein eigenes HEMS-Subnetzwerk auf. In diesem separaten Netzwerk werden alle Energiekomponenten – vom Wechselrichter über Batteriespeicher und Wärmepumpe bis zur Wallbox – lokal angebunden, ausgelesen und gesteuert. Die Kommunikation erfolgt dabei über den Industriestandard Modbus TCP. Alle Optimierungsalgorithmen laufen lokal auf dem Energiemanager. Eine ständige Internetverbindung ist für die lokale Optimierung somit nicht erforderlich.

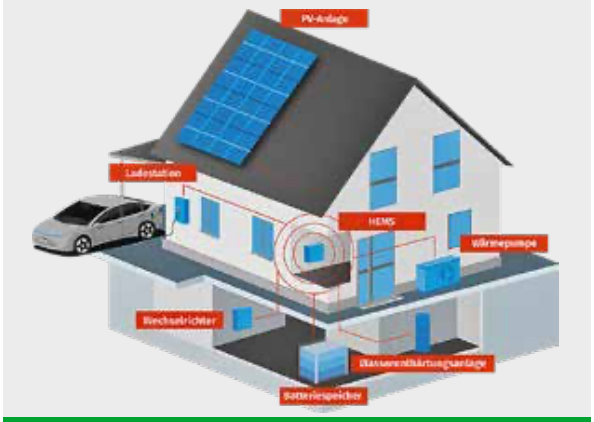
Das Sicherheitskonzept geht jedoch über die lokale Datenverarbeitung hinaus, das HEMS fungiert auch als zusätzliche Firewall. Alle im Subnetzwerk verbauten Komponenten sind so von außen nicht sichtbar. Die Kommunikation aus dem Internet zu den Geräten im Haushalt wird gesperrt. Die lokalen Komponenten können zwar ausgehende Verbindungen zu Herstellerportalen aufbauen, doch auch diese lassen sich über die Firewall des Energie-

managers gezielt einschränken oder komplett unterbinden. Um physisch auf die Komponenten zuzugreifen, müsste ein Angreifer also in das Subnetzwerk vor Ort eindringen.

Die Verbindung zwischen dem HEMS und dem Back End ist durch moderne Verschlüsselungs- und Authentifizierungsverfahren geschützt. Jedes System verfügt über eine eigene digitale Identität, wodurch Angriffe auf die Kommunikationsstrecke verhindert werden. Auf Back-End-Seite sorgen zusätzliche Sicherheitsmechanismen dafür, dass nur autorisierte Zugriffe möglich sind und alle Zugriffe nachvollziehbar bleiben. „Das HEMS sendet an unser Back End nur definierte Datenpunkte. Skripte oder andere Programme können nicht übertragen werden", erläutert Carsten Bruns.

Die regulatorischen Anforderungen werden weiter zunehmen. Der EU Cyber Resilience Act (CRA), im Dezember 2024 in Kraft getreten und nach 36 Monaten verpflichtend, stellt an Produkte mit digitalen Komponenten im Bereich Kritischer Infrastrukturen die höchsten Anforderungen hinsichtlich Security by Design. Das VDE FNN fordert darüber hinaus, dass im Rahmen einer Festlegung durch die Bundesnetzagentur (BNetzA) oder das Bundesamt für Sicherheit in der Informationstechnik (BSI) klargestellt wird, dass energiewirtschaftlich relevante Steuerbefehle nach der Übergabe durch die Steuerungseinrichtung ausschließlich lokal verarbeitet werden dürfen.

Das beegy HEMS ist darauf vorbereitet. Über eine EEBus-Schnittstelle werden die Steuerimpulse aus dem CLS-Management über die Steuerbox am Smart Meter Gateway direkt in das HEMS eingespeist. Die Verarbeitung erfolgt vollständig lokal – der Steuerbefehl des VNB verlässt zu keinem Zeitpunkt den geschützten Bereich der Kundenanlage. Dank der Umwandlung in Modbus-Signale ist die Steuerung zudem nicht auf die EEBus-Welt beschränkt, es können nahezu alle offenen Systeme eingebunden werden. Auch die Quittierung gegenüber dem Netzbetreiber kann so zuverlässig erfolgen.



beegy GmbH

Bild vergrößern

Als White-Label-Partner bietet beegy Lösungen rund um Photovoltaik-, Wärme- und Wasseranlagen sowie Elektromobilität.

Bereit für den Roll-out

Die Praxistauglichkeit des Systems belegen die Zahlen: Mehr als 3.500 Prosumer-Haushalte mit über 12.000 angeschlossenen Komponenten betreibt beegy im Feld. „Wir haben unser HEMS jetzt schon sehr häufig installiert und noch keinen Ausfall registriert", berichtet Carsten Bruns. Ein zentraler Baustein hierfür sind die Over-the-Air-Updates. Diese werden für das HEMS und die angebundenen Geräte bequem aus der Ferne eingespielt. Die Aktualisierungen erfolgen dabei über gesicherte Prozesse, sodass Verbesserungen und Sicherheitsanpassungen ohne einen Einsatz vor Ort möglich sind.

Mit seinem White-Label-Angebot richtet sich beegy an Stadtwerke, die das Geschäftsfeld Heim-Energiemanagement erschließen wollen, ohne die Entwicklungskompetenz selbst aufbauen zu müssen. Partner können somit das HEMS und die gesamte Software-Suite von der digitalen Vertriebsstrecke bis zum technischen Monitoring unter eigener Marke nutzen. „Wir bieten unseren Stadtwerke-Partnern die Möglichkeit, ohne großen Investitionsaufwand in ein zukunftsträchtiges Geschäftsfeld einzusteigen – mit einer Lösung, die im Feld bewährt ist und den wachsenden Cyber-Sicherheitsanforderungen standhält", fasst Carsten Bruns zusammen.

Christoph Buck ist Fachjournalist in Ulm.