Bild: Elchinator/pixabay

Cyber Security in virtuellen Kraftwerken

Sicherheit dezentraler Anlagen | Der Energiesektor wird zunehmend zur Zielscheibe für Cyber-Kriminelle. Im Jahr 2019 wurden weltweit mehr Cyber-Angriffe auf den Energiesektor gezählt als auf die Finanz-, Software-, Automobil- oder Logistik-Branche.[1)] Sind heute noch die traditionellen Akteure betroffen, werden in Zukunft auch neue Technologien und Geschäftsmodelle unweigerlich zu Zielen.

STEFAN DÖRIG, TONI SULANKIVI

Die Zukunft des Energiesystems ist erneuerbar, digital und dezentral. Die grossen fossilen Kraftwerke werden zunehmend ersetzt durch dezentrale Produktionsanlagen wie Solar- oder Windkraftwerke. Hinzu kommt der Hochlauf von steuerbaren und vernetzten elektronischen Geräten wie Heimbatterien, Wärmepumpen oder Elektrofahrzeugen.

Virtuelle Kraftwerke bauen auf solchen dezentralen Stromerzeugern und -verbrauchern auf. Tausende Geräte in Haushalten und Unternehmen werden vernetzt und gesteuert, und können so beinahe wie ein herkömmliches Kraftwerk betrieben werden. Solche «virtuellen Kraftwerke» vermögen schnell auf Änderungen der Netzfrequenz zu reagieren und sind damit prädestiniert, um die Netze zu stabilisieren. Heutzutage geschieht dies hauptsächlich über Systemdienstleistungen im Hochspannungsnetz. Zukünftig werden Lastmanagement und virtuelle Kraftwerke aber auch im Verteilnetz eine wichtige Rolle einnehmen und den Hochlauf von erneuerbaren Energien und Elektrofahrzeugen unterstützen.

Die Komponenten eines virtuellen Kraftwerks sind real. Das «virtuelle» Element des Konzepts besteht darin, dass die dezentralen Anlagen aus der Ferne gesteuert werden, was eine Menge IT und intelligente Algorithmen erfordert. Damit werden auch virtuelle Kraftwerke zu möglichen Angriffszielen von Cyber-Kriminellen, Terroristen, oder böswilligen staatlichen Akteuren. Heute sind virtuelle Kraftwerke, welche am Strommarkt teilnehmen, noch vergleichsweise klein. Dies wird sich mit der zunehmenden Digitalisierung und der Elektrifizierung in den Wärme- und Mobilitätssektoren aber rasch ändern. Wenn Millionen von elektronischen Geräten vernetzt und koordiniert gesteuert werden können, werden diese Komponenten zu einem wesentlichen Teil des Stromsystems und sollten als kritische

Infrastruktur betrachtet werden. Angesichts der rasanten Entwicklung im Energiebereich ist es wichtig, bereits heute mit der Diskussion zu beginnen, wie diese Geschäftsmodelle vor digitalen Bedrohungen geschützt werden können.

Bereits bestehende Aggregationen als Risiko

Ist die Rede von virtuellen Kraftwerken, sind meist Infrastrukturen, welche am Strommarkt teilnehmen, gemeint. Beinahe unbemerkt von der breiten Öffentlichkeit haben sich aber in den letzten Jahren riesige Pools von aggregierten elektronischen Geräten gebildet, welche bereits heute eine potenzielle Gefahr für das Stromnetz darstellen. Die Rede ist von grossen Herstellern von Heimbatterien, Solar-Wechselrichtern, Wärmepumpen oder Elektrofahrzeugen, welche die Kontrolle über Millionen von Geräten haben, die sie theoretisch koordiniert an- und abschalten können. Fällt diese Kontrolle in falsche Hände, sind grossflächige koordinierte Angriffe auf das Stromnetz nicht auszuschliessen. Die Universität Princeton nennt solche potenziellen Angriffe «Manipulation of demand via IoT», oder kurz «Mad-IoT»-Attacken.[2]

Die derzeit bemerkenswerteste Vernetzung von elektronischen Geräten findet im Elektromobilitätsbereich statt. Allein in Europa wird die Zahl der reinen Elektroautos in diesem Jahr wahrscheinlich drei Millionen überschreiten. Die kombinierte Ladeleistung der Fahrzeuge, die gleichzeitig über Ladestationen an das Netz angeschlossen sind, liegt bereits weit über der Gigawatt-Grenze. Fällt die Kontrolle dieser Ladeleistung in die Hände eines böswilligen Akteurs, sind die Folgen nicht absehbar. Auch Softwarefehler oder menschliches Versagen können gravierende Auswirkungen haben. Es ist deshalb wichtig, die Risiken der bestehenden Aggregationen zu untersuchen und gegebenenfalls Massnahmen zu ergreifen. Dies könnte auch wertvolle Erkenntnisse darüber liefern, wie zukünftige virtuelle Kraftwerke besser vor Cyber-Angriffen geschützt werden können. Auf EU-Ebene wird das Thema zurzeit intensiv diskutiert.

Europäische Regulierung

In der EU wird derzeit an zwei Gesetzestexten gearbeitet, welche für die Cyber Security im Energiebereich von Bedeutung sind: Die überarbeitete NIS-Richtlinie (Directive on security of network and information systems) und der Network Code zu Cyber Security. Während die NIS-Richtlinie zahlreiche Sektoren (unter anderem Telekommunikation, Verkehr, Energie, Wasser, Gesundheit) umfasst, ist der Network Code auf die Risiken und Massnahmen im Energiebereich fokussiert. Die Herausforderung von neuen Geschäftsmodellen und existierenden Aggregationen wurde in beiden Gesetzesvorlagen erkannt. Im Network Code werden nun die Einzelheiten definiert. Im zweiten Quartal 2022 soll der finale Entwurf konsultiert werden.

Die Schweiz mit Nachholbedarf

In der Schweiz hat man bisher auf die Eigeninitiative der Unternehmen gesetzt, um die Cyber Security im Energiebereich sicherzustellen. Dies könnte sich jedoch ändern, denn einer aktuellen Studie des Bundesamtes für Energie BFE zufolge besteht dringender Handlungsbedarf.[3] Bereits laufen Arbeiten an einem Umsetzungskonzept für den Strombereich. Es ist zu hoffen, dass die neuen Geschäftsmodelle und die Risiken von bestehenden Aggregationen angemessen berücksichtigt werden.

Autoren

Toni Sulankivi ist Head of Cyber Security bei Tiko Energy Solutions AG.
→ Tiko Energy Solutions AG, 8004 Zürich
→ toni.sulankivi@tiko.energy

Stefan Dörig ist Head of Regulatory and Public Affairs bei Tiko Energy Solutions AG.
→ stefan.doerig@tiko.energy

[1] energymonitor.ai/technology/digitalisation/cybersecurity-threats-escalate-in-the-energy-sector.
[2] princeton.edu/~pmittal/publications/blackiot-usenix18.pdf.
[3] energeiaplus.com/2021/06/28/wie-ist-der-stand-der-cyber-security-in-der-schweizer-stromversorgung-und-wie-sieht-die-strategie-fuer-ihre-digitale-zukunft-aus.

RÉSUMÉ

La cybersécurité dans les centrales virtuelles

Sécurité des installations décentralisées

L'avenir du système énergétique est renouvelable, numérique et décentralisé. Les grandes centrales fossiles sont toujours plus remplacées par des installations de production décentralisées telles que des centrales solaires et éoliennes. Les centrales virtuelles sont fondées sur ce type de producteurs et de consommateurs d'électricité décentralisés. Dans les ménages et les entreprises, des milliers d'appareils sont interconnectés et commandés, et peuvent ainsi être exploités pratiquement comme les centrales traditionnelles. De telles « centrales virtuelles » sont en mesure de réagir rapidement aux changements de la fréquence du réseau et sont ainsi prédestinées pour stabiliser les réseaux. Mais, si des millions d'appareils électroniques peuvent être interconnectés et commandés de manière coordonnée, ces composants vont devenir une partie importante du système électrique et devraient être considérés comme une infrastructure critique. Au vu de l'évolution ultrarapide dans le secteur de l'énergie, il est important d'entamer dès aujourd'hui la discussion sur la façon dont ces modèles d'affaires peuvent être protégés contre les menaces numériques.

Jusqu'à présent, en Suisse, on a misé sur l'initiative individuelle des entreprises pour garantir la cybersécurité dans le secteur énergétique. Mais cela pourrait changer, car, d'après une étude récente de l'Office fédéral de l'énergie OFEN, il faut agir d'urgence. Des travaux sont déjà en cours pour élaborer un concept de mise en œuvre pour le secteur électrique. Reste à espérer que les nouveaux modèles d'affaires et les risques d'agrégations existantes soient pris en compte de façon appropriée. MR