IT-Sicherheit

# Energieversorgung sicher gestalten

**[05.12.2016] Mit zunehmender Digitalisierung und Vernetzung wächst die Angriffsfläche für potenzielle Manipulationen. Gerade im Bereich der Energie- und Wasserversorgung, die beide zu den kritischen Infrastrukturen zählen, können Sicherheitslücken fatale Folgen für die Bevölkerung haben.**

Die Herausforderungen der Energiewende sind dieser Tage präsenter denn je. Während der Ausbau der Übertragungsnetze noch immer stockt, nimmt die erzeugte Energiemenge durch die Erneuerbaren weiter zu – und hiermit auch die Belastung für die Netze. Um diese im Gleichgewicht zu halten, musste die Zahl der netzstabilisierenden Maßnahmen zuletzt rapide erhöht werden. Auch mehren sich Stimmen, die einen Netzausbau und eine Smartization im Mittel- und Niederspannungsbereich befürworten. Gleichzeitig wächst die Kritik an intelligenten Netzen – zu groß sind doch die Sicherheitsbedenken.

**Stabilität durch Intelligenz**

Der Umbau des heutigen Stromnetzes zum Smart Grid setzt voraus, dass Erzeuger, Speicher und Verbraucher kommunikativ miteinander vernetzt werden. Nur so ist es möglich, Energieangebot und -nachfrage in der Balance und damit das Stromnetz stabil zu halten. Experten gehen davon aus, dass von den rund 600.000 über Deutschland verteilten Ortsnetzstationen rund 20 Prozent mit Steuerungsintelligenz ausgestattet werden müssen. Gesetzliche Vorgaben fordern überdies die Integration mehrerer Millionen Smart-Meter-Gateways in das Stromnetz. Wo aber geregelt und gesteuert wird, da fließen Daten. Bedenkt man zudem, dass im Rahmen einer ökonomisch verträglichen Dekarbonisierung auch die Bedeutung der Gasnetze – etwa als Speicher für Wind- und Solarenergie – rapide zunehmen wird, ergibt sich ein komplexes und facettenreiches Geflecht, das einer intelligenten Steuerung bedarf. Denn eines ist längst klar: Ohne zusätzliche Sektorenkopplung keine Energiewende.
Vor diesem Hintergrund finden zunehmend internetbasierte Netzwerktechnologien oder mobile Datendienste Verwendung. Gemeinhin bieten diese Kommunikationswege viel Angriffsfläche für Manipulationen: Auf der Strecke zwischen Energieerzeuger und Leitstelle ebenso wie auf dem Weg zum Verbraucher. Der Abgriff persönlicher Daten oder die Manipulation von Einspeisedaten, wie sie beispielsweise zur Steuerung der Regelenergie erforderlich sind, sind verglichen mit den Auswirkungen, die es haben könnte, wenn Hacker in der Leitstelle eines Netzbetreibers eine Schad-Software platzieren würden, das kleinere Problem.

**Gesetzliche Vorgaben erfüllen**

Dass dem Datenschutz im Zusammenhang mit dem Ausbau eines intelligenten Stromnetzes eine wichtige Bedeutung zukommt, dokumentiert nicht zuletzt die Verabschiedung des IT-Sicherheitsgesetzes im Sommer 2015. In diesem regelt die Bundesregierung, dass Betreiber von Energieanlagen und Versorgungsnetzen ein Mindestniveau an IT-Sicherheit einhalten müssen. Es schreibt neben regelmäßigen Sicherheitsaudits auch die Meldung von IT-Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor. Darüber hinaus definieren die IT-Grundschutzkataloge mögliche Szenarien und Schutzmaßnahmen, basierend auf der ISO 27001. Auf diesen bauen wiederum die verschiedenen branchenspezifischen Richtlinien und Empfehlungen auf, die Unternehmen verpflichten, die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Daten zu gewährleisten. Leitlinien dazu,

wie diese Anforderungen in der Energiewirtschaft umgesetzt werden können, geben das Whitepaper des Bundesverbands der Energie- und Wasserwirtschaft (BDEW) und der IT-Sicherheitskatalog der Bundesnetzagentur (BNetzA) vor.

**Höchsten Anforderungen genügen**

Schon heute existieren technische Möglichkeiten, die vermeintlichen Sicherheitslücken im Smart Grid zu schließen. Die Controller PFC 100/200 von WAGO zeichnen sich beispielsweise durch ein plattformübergreifendes Realtime-Linux aus, das als Open-Source-Betriebssystem langzeitverfügbar, skalierbar und updatefähig ist und Tools wie Rsync, Fail2Ban sowie Viren-Scanner unterstützt. Es können außerdem verschiedene Schnittstellen und Feldbusse wie CANopen, PROFIBUS DP und Modbus-TCP/RTU herstellerunabhängig bedient werden. Zudem unterstützt die PFC 200 Plattform die Protokolle IEC 60870, 61850 und DNP3.0.
Natürlich gibt es je nach Einsatz und Risikoanalyse auch unterschiedlich hohe Anforderungen an das Niveau einer Sicherheitslösung. Die WAGO PFC100/200 Familie ist in jedem Fall für die Umsetzung der aktuell höchsten Sicherheitsanforderungen nach ISO 27001 aufgestellt. Sie bietet Onboard-VPN-Funktionalität basierend auf dem so genannten Strongswan Package, einer sicheren Kommunikationslösung für Linux-Betriebssysteme. Dadurch müssen Modems oder Router keinen zusätzlichen VPN-Tunnel aufbauen. Doch was noch entscheidender ist: Die Strecke zwischen Steuerung und Modem ist dadurch direkt mitverschlüsselt, denn die Daten können bereits im Controller mittels SSL/TLS 1.2-Verschlüsselung (Secure Sockets Layer/Transport Layer Security) codiert werden. Der Controller baut den VPN-Tunnel dann über OpenVPN oder IPsec direkt auf. Er wird von Verteilnetzbetreibern und Energieversorgern daher häufig dazu eingesetzt, alle relevanten Mess- und Steuerdaten bei der Stromerzeugung, -wandlung und -verteilung zu erfassen beziehungsweise zu übergeben. Es entstehen abhör- und manipulationssichere Kommunikationsverbindungen zwischen den Controllern und den Netz-Zugangspunkten.
Auch ein vorgeschalteter VPN-Router ist nicht mehr erforderlich. Bei der Kommunikation wird eine verschlüsselte LAN/WAN-Verbindung aufgebaut, deren Inhalt nur die beiden Endpunkte verstehen können. Verbindungen werden nur nach erfolgter Authentifizierung aufgebaut. Mit Pre-Shared-Key kommt ein Verschlüsselungsverfahren zum Einsatz, bei dem die Schlüssel vor der Kommunikation bei den Teilnehmern bekannt sein müssen. Dieses Verfahren hat den Vorteil, dass es einfach zu realisieren ist. Eine zertifikatsbasierte Authentifizierung findet ebenfalls Verwendung.
Der PFC200 von WAGO kann projektindividuell gemäß den hohen Anforderungen des BDEW-Whitepapers gehärtet werden. Dazu zählt etwa die Unterstützung des Patch Managements durch regelmäßiges Bereitstellen sicherheitsrelevanter Updates, die Rollback-Möglichkeit für die Kopfstation zur Umsetzung des Konfigurations- und Change Managements, aber auch die Verschlüsselung der Kommunikation mittels anerkannter kryptografischer Bibliotheken für den sicheren Fernzugriff.

()

Dieser Beitrag ist in der November/Dezember-Ausgabe von stadt+werk erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Informationstechnik, WAGO Kontakttechnik, IT-Sicherheit, Smart Grid