



Quelle: arahan - Fotolia.com

Schadsoftware, unbefugter Zugang oder gezielte Angriffe sind im Netzbetrieb von Elektrizitäts- oder Gasversorgern real existierende Gefahren. Auch für GIS-Anwendungen gelten hohe Anforderungen, die ein sicherer Netzbetrieb und damit eine sichere Energieversorgung verlangen.

GANZHEITLICHE IT-LÖSUNGEN IM GIS-GESTÜTZTEN NETZBETRIEB

Der moderne Betrieb von Versorgungsnetzen für Elektrizität und Gas erfordert zukünftig, dass die vielfältigen IT-Systeme für die Netzplanung und -dokumentation, die Netzführung, das Instandhaltungs- und Störungsmanagement, das Zählerwesen und die kaufmännischen Aspekte mehr und mehr miteinander vernetzt werden müssen. Sicherheit ist dabei ein essenzieller Aspekt.

Ziel ist es beim modernen Betrieb von Versorgungsnetzen für Elektrizität und Gas, durch den Datenaustausch zwischen den IT-Systemen und zwischen den einzelnen Marktrollen die Arbeitsprozesse so effizient wie möglich zu gestalten, wobei es sich dabei um hochsensible Daten der Versorgungsbetriebe und der Verbraucher handelt.

Energiewirtschaftsgesetz, Atomausstieg und erneuerbare Energien führen zu völlig neuen Anforderungen an die Netze, wie dezentrale Einspeisung in den unteren Netzebenen, Lastflussumkehr und größere Transportwege von der Erzeugung zum Verbraucher, die nur durch intelligente Netze gelöst werden können, denn der Netzausbau kann dem nicht Schritt halten. Und Smart Grid und Smart Metering hängen untrennbar zusammen, wenn nicht nur die Prozesse der einzelnen Marktrollen, sondern auch die Netzauslastung optimiert werden sollen.

Mit dem Übergang auf die standardisierte IP-Technologie für die Kommunikation und Einbindung von Web-Lösungen in alle Ebenen der Netze – von der Energiequelle über das Transport- und Verteilnetz bis hin zum Haushalt – entstehen neue Gefährdungen etwa durch Schadsoftware, unbefugten Zugang oder durch gezielte Angriffe, wobei die umfangreichen und präzisen Netzinformationen der Informationssysteme zu unfreiwilligen Helfern werden könnten.

MEHR IT-SICHERHEIT

Seit einigen Jahren gibt es vielfältige Bestrebungen seitens der Netzbetreiber und des Bundesamts für Sicherheit in der Informationstechnik (BSI), die IT-Systeme in der Versorgungswirtschaft sicherer zu machen. Dabei stehen im Vordergrund:

- ▷ Verfügbarkeit der IT-Systeme und Daten

- ▷ Integrität (Korrektheit) der Daten
- ▷ Vertraulichkeit der Daten

Einer der Vorreiter ist das sogenannte bdeW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“, welches – seit 2008 getrieben durch die einflussreichen Transportnetzbetreiber und stark korrelierend mit den Normen der Reihe DIN ISO 27000 – für die Konzeption, den Aufbau und den Betrieb der Systeme für die Netzautomation und Smart Grids (Stationsleittechnik, Fernwirktechnik, Netzleittechnik) zunehmend Beachtung findet. Der bdeW oder Bundesverband der Energie- und Wasserwirtschaft hat damit dieses Thema in den Fokus gerückt. Der sichere Netzbetrieb und damit eine sichere Energieversorgung stehen dabei im Vordergrund.

Andererseits wurde seitens des BSI das „Schutzprofil für die Kommunikationseinheit eines intelligenten Messsys-

tems für Stoff- und Energiemengen“ für die Übertragung von Zählerdaten definiert, eine wichtige Voraussetzung für den geplanten Roll-out der Smart-Metering-Systeme. Darin steht der Manipulations- und Datenschutz im Vordergrund. Treibende Kraft ist dabei, dass eine Vielzahl von Marktteilnehmern Zugriff auf Teile dieser äußerst sensiblen und zum Teil persönlichen Daten haben müssen, um etwa Erzeugung und Verbrauch in Einklang zu bringen oder Netzüberlastungen zu verhindern.

Leider haben alle beide Dokumente grundsätzliche Nachteile: Zum einen wird jeweils nur ein Aspekt der Energiewirtschaft, Smart Grid oder Smart Metering, betrachtet und der ganzheitliche Ansatz fehlt. Zum anderen kommen beide über den nationalen Rahmen nicht hinaus, was im Bezug auf die zunehmende Internationalisierung der Energiewirtschaft Probleme aufwerfen wird. Ein ganzheitlicher und internationaler Ansatz (auf z.B. der DIN-Norm ISO 27000) mit entsprechenden technischer Untersetzung wäre wünschenswert, wie beispielsweise mit SAGA (Standards und Architekturen für E-Government-Anwendungen) Version 5 für die Bundesbehörden gelungen ist.

GIS UND IT-SICHERHEIT

GIS hat in der Versorgungswirtschaft eine entscheidende Bedeutung erlangt, die noch enorm an Gewicht gewinnen wird. Das „Wo“ steht hier im Vordergrund der Betrachtung. Wurde bisher ein GIS vornehmlich zur Dokumentation des Netzes und seiner Assets sowie zur Planung des Netzausbaus verwendet, stehen neue Anwendungen vor der Einführung und das im Online-Betrieb: Die auf Geodaten basierende Netzführung, Einsatzplanung für Entstörung und Instandhaltung oder Analyse von witterungsabhängigen Erzeugungs- und Verbrauchsdaten für die Optimierung der Energieflüsse.

Das GIS wird also direkt mit den Smart-Metering- beziehungsweise Smart-Grid-Intelligenz gebenden IT-Systemen, wie den klassischen Netzleit-

und den Zählerfernauslesesystemen, informationstechnisch vernetzt und erhält damit den Durchgriff auf die Steuerung einer Schaltanlage beziehungsweise auf das Verhalten der Verbraucher. In dieser Form integrierte GIS-Anwendungen müssen damit den gleichen Anforderungen an IT-Sicherheit in der Versorgungswirtschaft unterworfen werden.

SICHERE GIS

Während im Zusammenhang mit GIS die Diskussion über den freien Zugang von Informationen geführt werden – Stichwort: Karten für alle –, stellt sich die Situation für geographisch basierte Informationssysteme bei Ver- und Entsorgungsunternehmen naturgemäß anders dar. Diese Systeme decken Angriffspotenziale auf, sie beinhalten personenbezogene und wirtschaftliche Daten. Daher darf die Auseinandersetzung um IT-Sicherheit vor den GIS kein Halt machen. Die Entwicklung der GIS in den letzten Jahren war im Besonderen geprägt und beeinflusst durch den Hauptbedarfsträger, die öffentlichen Verwaltungen. Gerade hier steht die große Herausforderung, die Balance zwischen dem berechtigten öffentlichen Interesse und den personenbezogenen Informationen zu halten. SAGA 5.0 scheint hier eine entsprechende Antwort zu geben. Auf Basis des IT-Staatsvertrages kann das, was bisher nur eine Empfehlung war, zur bindenden Voraussetzung gemacht werden.

Wenn auch die Diskussion zu SAGA 5.0 gerade erst begonnen hat, auf jeden Fall scheinen die Architekten den Bestand bisheriger Architekturen berücksichtigt zu haben. Dadurch kann die stets – zu Recht – geführte Diskussion über die Kosten und Investitionen neuer Architekturen eingedämmt werden. SAGA 5.0 berücksichtigt in jedem Fall die bisherigen Investitionen. Deswegen könnte hier zum ersten Mal ein aus der öffentlichen Verwaltung stammender Architekturvorschlag auch für die Industrie bedeutend werden.

Ein sicheres GIS erreicht man nur, wenn sich die Hersteller von GIS und

GIS-basierter Anwendungen den Mainstream-IT-Strategien für die IT-Sicherheit unterwerfen. Denn hier treten die Bedarfe und Anforderungen am deutlichsten auf.

Im Ziel wird dieses Vorgehen auch wirtschaftlicher sein, denn die darauf aufbauenden Dienstleistungen (Implementierung, RZ-Betrieb, Integrationen) müssen keine besonderen Funktionalitäten mehr berücksichtigen – spezielle Sicherung für Daten, spezielle Firewalls für Geodaten. Diese Regeln zu befolgen, ist eine wesentliche Voraussetzung für die Verwendbarkeit von GIS in sensiblen Aufgabenbereichen.

INTELLIGENT GESTALTEN

Mit dem Zusammenwachsen von Netzführung, GIS, Smart Grid und Smart Metering entsteht praktisch ein mächtiges und durchgängig vernetztes IT-System. Für jede, bisher selbstständig agierende Organisation existieren jedoch unterschiedliche Herangehensweisen bezüglich IT-Sicherheit. Hier hat der Gesetzgeber noch ein gewaltiges Aufgabenfeld zu bearbeiten, um sicherzustellen, dass einheitliche Regelungen für die IT-Sicherheit und die zur Umsetzung notwendigen Normen geschaffen werden. Denn die technischen Anlagendaten, die Online-Prozessinformationen aus dem Energienetz, die Energiezählwerte von Erzeugern, Haushalten und Großverbrauchern und die dazugehörigen Geodaten werden benötigt, um die Energieversorgungsnetze intelligent zu gestalten und den gesellschaftlichen Willen nach einem Atomausstieg und erneuerbaren Energien umzusetzen. ◀

AUTOREN UND KONTAKT:

Dr.-Ing. Ralf Thomas, IDS GmbH, Ettlingen
Ulrich Neunfinger, CAIGOS GmbH, Kirkel
Nobelstraße 18
D-76275 Ettlingen
E: ralf.thomas@ids.de
I: www.ids.de