

30.05.2011

Positionspapier

IT-Sicherheit im Smart Grid

1 Smart Grid – Zukunft der Stromwirtschaft mit Sicherheit

Die Stromversorgung steht vor völlig neuen Herausforderungen: Der fortschreitende Klimawandel, die Liberalisierung der Energiemärkte und der politisch gewollte Ausstieg aus der Atomenergie machen einen tiefgreifenden Umbau der Elektrizitätsinfrastruktur innerhalb der nächsten Jahre erforderlich.

Als Konsequenz wird die Stromerzeugung aus regenerativen Energiequellen – Wind, Photovoltaik, Wasserkraft, Bioenergie und anderen erneuerbaren Energieträgern – massiv ausgebaut. Wurde Strom in Deutschland bislang zentral in rund 300 Kraftwerken produziert und in Richtung der Verbraucher verteilt, so wird er künftig verstärkt aus regenerativen Energieträgern an einer Vielzahl von Standorten – also dezentral – erzeugt. Dezentrale Erzeugung bedeutet aber auch eine komplexere Verteilung. Für diese Anforderungen sind die heutigen Stromnetze nicht ausgelegt. Auch der weitere Ausbau von großen On/Offshore Windparks mit hohen Leistungskapazitäten lässt die Infrastruktur zunehmend an ihre Leistungsgrenzen stoßen. Zu Spitzenzeiten sind die Netze bereits heute "verstopft", regenerativ erzeugter Strom kann deshalb häufig nicht sinnvoll genutzt werden.

2 Voraussetzung: Lastausgleich im Stromnetz

Die Erzeugungsleistungen erneuerbarer Energien sind nicht konstant. In der Regel sind sie von Wetter, Wind und Sonne abhängig. Eine Hauptaufgabe wird also sein, einen Lastausgleich im Stromnetz zu schaffen und die Versorgungssicherheit zu gewährleisten.

Zentrale und dezentrale Erzeugung müssen intelligent kombiniert werden. Die zahlreichen neuen Erzeuger müssen vollständig und effizient in das Stromnetz integriert werden. Dies kann nur gelingen, wenn Stromerzeuger, -verbraucher und -speicher sowie die für die Übertragung und Verteilung notwendige Infrastruktur unter Einhaltung einer hohen Versorgungssicherheit intelligent miteinander vernetzt werden. Ein Umbau der heutigen Netze ist nötig.

3 Die Netze müssen "intelligent" werden

Das sogenannte Smart Grid – auch als Internet der Energie bezeichnet – wird die Zukunft unserer Energieversorgung bestimmen. Es wird Erzeugung, Transport, Speicherung, Verteilung und Verbrauch von Strom steuern und kontrollieren. Möglich wird das durch den verstärkten Einsatz von IT, insbesondere Technologien, die seit Jahren in der Kommunikations- und Datentechnik vielfältig und preiswert zur Verfügung stehen, wie beispielsweise das TCP/IP-Protokoll.

Intelligente, kommunikative Stromzähler, sogenannte Smart Meter sind Kernstücke des Smart Grids und werden auch in Privathaushalten Einzug halten. Sie ermöglichen die digitale Erfassung der Verbrauchsdaten und deren Übermittlung zur Abrechnung und Steuerung. Gleichzeitig werden über die Kommunikationsschnittstellen auch Tarifinformationen oder auch weitere Daten zur Steuerung von Verbrauchsgeschäften, aus dem Energienetz geladen. Die Steuerung des Energieflusses erfolgt maßgeblich auf Basis der durch die Smart Meter viertelstündlich übermittelten aktuellen Verbrauchsdaten. Durch diese Informationen wird die Lastenregelung vereinfacht, der Stromfluss gesteuert und ggf. die Stromerzeugung und die –verteilung möglichst genau an den Bedarf angepasst.

4 IT-Sicherheit macht Smart Grid möglich

Dreh- und Angelpunkt für das Gelingen dieses Umbruchs in der Stromwirtschaft ist die Einhaltung von Sicherheitsanforderungen. Dazu zählen die Sicherheit vor Angriffen auf die IT-Infrastruktur ("Security"), die Betriebssicherheit ("Safety"), aber auch die Datenschutzaspekte ("Privacy"). Mit dem zunehmenden Einsatz von Informations- und Kommunikationstechnologie beim Smart Grid steigt auch die Verwundbarkeit. Künftig können über das IT-Netzwerk eine Vielzahl von Hackern bzw. Terroristen das Smart Grid auch aus der Ferne angreifen. Voraussetzung für Konzeption und sicheren Betrieb ist ein angemessen hohes IT-Sicherheitsniveau, um beispielsweise Schutz vor

- Stromausfall;
- Manipulation der Tarifinformationen oder Zählerstände;
- Zahlungsausfällen aufgrund von fehlerhaften bzw. manipulierten Identitätszuweisungen;
- unberechtigter Abstreitbarkeit bei Rechnungsstellungen;
- Fehlsteuerungen des Stromflusses oder
- Missbrauch von Kunden- und Verbrauchsdaten zu etablieren.

Die Stromversorgung gilt aufgrund ihrer Bedeutung und überlebensnotwendigen Funktion für Bevölkerung und Wirtschaft als kritische Infrastruktur. Die unverzichtbare Kernfunktionalität der Versorgungssysteme muss auch in Krisenlagen ("Graceful Degradation") aufrechterhalten und Mechanismen zur schnellstmöglichen Wiederherstellung nach Totalausfällen (Schwarzstartfähigkeit) vorhanden sein. Dazu ist es notwendig, die einzelnen Netz-Teilstrukturen sehr widerstandsfähig zu konzipieren und aufrechtzuerhalten.

TeleTrusT fordert:

- **Berücksichtigung von IT-Sicherheitsaspekten bereits in der Planungsphase**
- **Etablierung eines hohen bzw. teilweise sehr hohen Niveaus hinsichtlich der Sicherheitsziele im gesamten Smart Grid (Vertraulichkeit, Integrität, Authentizität, Nicht-Abstreitbarkeit, Verfügbarkeit, Verbindlichkeit, Zuverlässigkeit)**
- **Vorgaben von IT-Sicherheitsstandards durch Politik bzw. Gesetzgebung**
- **Überwachung der Umsetzung von Sicherheitsvorgaben**
- **Regelmäßige Prüfung und Anpassung der Sicherheitsvorgaben an geänderte Rahmenbedingungen**
- **Definition von Schutzprofilen und Zertifizierungsprozessen für kritische Komponenten**
- **Aufbau und Nutzung von vertrauenswürdigen Sicherheitsinfrastrukturen und -Dienstleistungen**
- **Angemessene Notfall-/Krisen- und Business Continuity-Konzepte und der Nachweis der Umsetzbarkeit dieser Konzepte**

5 Datenschutz vermeidet gläsernen Kunden

Mit der Einführung des Smart Grids in der Energiewirtschaft werden große Mengen unterschiedlicher Energiedaten auf verschiedenen Aggregationsstufen erzeugt und übertragen. Das Schadpotenzial bzgl. personenbezogener Daten in einem nicht ausreichend gesicherten Smart Grid ist außerordentlich hoch.

Datenschutz muss deswegen – und auch wegen der hohen Sensibilität und des Misstrauens der Verbraucher – ausdrücklich eine hohe Priorität in der Konzeption und Umsetzung des Smart Grids haben. Vertrauliche Kommunikation zwischen Endkunden und ihren Dienstleistern sowie rechtssichere elektronische Transaktionsmechanismen müssen von vorneherein konzeptioniert und umgesetzt werden. Einmal aufgetretene Fehler und die daraus entstehende Ablehnung machen eine nachträgliche Implementierung unter Umständen nicht mehr möglich oder aufwändig und teuer. Erst eine klare und transparente gesetzliche Regelung von Zugriffsrechten und -beschränkungen sowohl für Daten aus Mess- und Verbrauchseinheiten als auch für den steuernden Zugriff auf Erzeuger und Verbraucher kann die notwendige Akzeptanz für diese neuen Technologien schaffen. Wenn nötig, ist das Datenschutzgesetz in diesem neuen Umfeld entsprechend anzupassen. In diesem Sinne ist IT-Sicherheit eine Voraussetzung für den Aufbau und Betrieb eines von allen Beteiligten akzeptierten Smart Grids.

TeleTrusT fordert:

- **Klare und transparente Regelungen zu Zugriffsrechten auf Daten aus Mess- und Verbrauchseinheiten, ggf. Anpassung des Datenschutzgesetzes**
- **Praxisnahe Datenschutzvorgaben und datenschutzkonformes Design des Smart Grids**

6 Akzeptanz braucht Vertrauen und Sicherheit

Jedes neue Thema oder Großprojekt erfordert, dass alle Beteiligten frühzeitig "mitgenommen" bzw. über Änderungen und deren Auswirkungen sachlich und neutral informiert werden. Innerhalb der Gesellschaft muss ein breiter Konsens über die Notwendigkeit zur Realisierung des neuen Projektes geschaffen werden. Die Diskussion um den Kraftstoff E10 hat gezeigt, dass die Integration neuer Lösungen in existierenden Märkten durchaus mit Problemen einhergehen kann.

Die Akzeptanz in der Bevölkerung steht und fällt auch mit der Sicherheit der Netze und auch dem Schutz der anfallenden Verbrauchsdaten. Erforderlich ist eine offene Kommunikation mit allen Beteiligten – und das bereits während der Konzeption und Errichtung des Smart Grids. Neben den Chancen und Freiheiten, die Smart Grids bieten, dürfen die Risiken nicht außer Acht gelassen werden. Maßnahmen, die die Eintrittswahrscheinlichkeiten der Risiken reduzieren, müssen ergriffen werden und sich ergebende Restrisiken müssen plausibel, transparent und verständlich dargestellt werden.

TeleTrusT fordert:

- **Offene Kommunikation über Chancen und Risiken sowie akzeptierte Restrisiken**

TeleTrusT Deutschland e.V.

Der IT-Sicherheitsverband TeleTrusT Deutschland e.V. wurde 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. TeleTrusT entwickelte sich zu einem bekannten Kompetenznetzwerk für IT-Sicherheit. Heute umfasst TeleTrusT mehr als 110 Mitglieder aus Industrie, Wissenschaft, Forschung und öffentlichen Institutionen sowie Partnerorganisationen aus Deutschland und Europa. In Projektgruppen zu aktuellen Fragestellungen der IT-Sicherheit und des Sicherheitsmanagements tauschen die Mitglieder ihr Know-how aus. TeleTrusT äußert sich zu politischen und rechtlichen Fragen, organisiert Veranstaltungen und Veranstaltungsbeteiligungen und ist Trägerorganisation der "European Bridge CA" (Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation) sowie des Zertifikates "TeleTrusT Information Security Professional" (T.I.S.P.). Hauptsitz des Verbandes ist Berlin. TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI).

Verbandskontakt:	Pressekontakt:
Dr. Holger Mühlbauer	Sebastian Thümmel
TeleTrusT Deutschland e.V.	index Agentur für strategische
Geschäftsführer	Öffentlichkeitsarbeit und Werbung GmbH
Chausseestraße 17	Zinnowitzer Straße 1
10115 Berlin	10115 Berlin
Tel.: +49 30 / 40 05 43 10	Tel.: +49 30 / 390 88 190
holger.muehlbauer@teletrust.de	s.thuemmel@index.de
www.teletrust.de	www.index.de