IT-Sicherheit

# Schutz vor dem Blackout

## [06.05.2014] Intelligente Stromnetze sind anfällig für Angriffe aus dem Cyberspace. Der Aufbau einer IT-Sicherheitsarchitektur ist jedoch teuer und macht die Einführung digitaler Zähler beim Verbraucher unwirtschaftlich. Doch es gibt Alternativen.

Der Thriller „Blackout“ von Marc Elsberg* hat für Furore gesorgt. Und tatsächlich ist das dort beschriebene Szenario eines flächendeckenden Stromausfalls durch Manipulation intelligenter Stromzähler gar nicht so abwegig. Analysiert man das Bedrohungspotenzial, so können neben Naturkatastrophen wie dem Sturm Kyrill insbesondere die Folgen des dynamischen Ausbaus der erneuerbaren Energien und vor allem Fragen der IT-Sicherheit mögliche Auslöser sein. Gleichzeitig kann es aber keine Sicherheit um jeden Preis geben, denn Smart Metering muss wirtschaftlich bleiben, wenn es tatsächlich umgesetzt werden soll.

### Mindestniveau an IT-Sicherheit

Ob Hacker-Angriff, menschliches Versagen oder schlicht Fehlfunktionen in Hard- oder Software – die Folgen können in jedem Fall dramatisch sein. So war beispielsweise der großflächige Stromausfall in den USA im Jahr 2003 auf einen Fehler in der Prozessleittechnik zurückzuführen. Der Trojaner Stuxnet hat ab 2010 weltweit Prozesssteuerungssysteme (SCADA-Systeme) in verschiedenen Bereichen infiziert. Diese Systeme werden unter anderem auch in Großkraftwerken eingesetzt.
Der Schutz solcher Einrichtungen mit wichtiger Bedeutung für unsere Gesellschaft ist deshalb eine zentrale Aufgabe, die von staatlicher Seite und den Verwaltungen in Form einer vorsorgenden Sicherheitspolitik wahrgenommen werden muss. Dies kann nur gemeinsam mit den Betreibern der betroffenen Infrastruktureinrichtungen zielführend geleistet werden. Bereits seit dem Jahr 2009 gibt es in Deutschland deshalb auch eine nationale Strategie zum Schutz kritischer Infrastrukturen. Sie fasst die Zielvorstellungen und den politisch-strategischen Ansatz des Bundes auf diesem Politikfeld zusammen. Kernpunkte der Strategie sind der verstärkte Schutz vor IT-Angriffen, der Schutz der IT-Systeme in Deutschland, der Aufbau eines Nationalen Cyber-Abwehrzentrums sowie die Einrichtung eines Nationalen Cyber-Sicherheitsrats.
Das Bundesinnenministerium hat zusätzlich ein IT-Sicherheitsgesetz auf den Weg gebracht. Der Entwurf sieht für Betreiber kritischer Infrastrukturen einschließlich der Anbieter von Telekommunikationsdiensten die Pflicht zur Einhaltung eines Mindestniveaus an IT-Sicherheit vor. Für Betreiber kritischer Infrastrukturen ist außerdem die Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle vorgesehen. Analog zu diesen Verpflichtungen wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seiner Beratungs- und Unterstützungsrolle für die Verpflichteten gestärkt.

### Gezielte Angriffe

Die Bedrohungslage wird bei allem Bemühen dennoch immer ernster. Nicht nur kriminelle Aktivitäten, sondern auch gezielte Angriffe einzelner Staaten häufen sich. Die Vernetzung hat einen solchen Umfang erreicht, dass auch Zwischenfälle in anderen Ländern die Sicherheit in Deutschland nachhaltig beeinflussen können. Die europaweite Einführung intelligenter kommunikationsfähiger Messsysteme bis hin zu intelligenten Netzen werden weitere Einfallstore für kriminelle Handlungen öffnen. Informationen über das Nutzerverhalten, die Lebensgewohnheiten, böswillige Schaltbefehle und vieles mehr sind

Gefahrenquellen der neuen Energiewelt.
Die Bundesregierung hat erkannt, dass es in diesem Zusammenhang auch erforderlich ist, von Anfang an Datenschutz und Datensicherheit zu gewährleisten. Das spiegelt sich bereits im Energiewirtschaftsgesetz aus dem Jahr 2011 wider, in dem erste Anforderungen an die Sicherheitsarchitektur von intelligenten Messsystemen und Netzen skizziert werden. Die Umsetzung obliegt dem BSI, das im September 2010 zunächst mit der Erarbeitung eines Schutzprofils (Protection Profile, PP) beauftragt wurde. Im Anschluss daran soll eine Technische Richtlinie (TR) für die Kommunikationseinheit eines intelligenten Messsystems (Smart Meter Gateway) entwickelt werden, um einen einheitlichen technischen Sicherheitsstandard für alle Marktakteure zu gewährleisten. Das daraus resultierende Schutzprofil für Smart Meter Gateways wird auf dieser Basis geprüft und zertifiziert.

**Intelligenz in der Software**

Die hohen Anforderungen des Schutzprofils ziehen natürlich entsprechende Kosten nach sich. Ein flächendeckender Roll-out von digitalen Zählern wäre auf dieser Basis kaum möglich gewesen. Daher war die Kosten-Nutzen-Analyse der Unternehmensberatung #bild2 Ernst & Young aus dem vergangenen Jahr ein Schritt in die richtige Richtung. Mit der Kernaussage – intelligente Zähler für die Kleinen und intelligente Messsysteme für die Großen – besteht nun auch wieder der Freiraum für die Entwicklung neuer Mehrwertangebote auf Basis der Smart Meter. Denn die Ergebnisse der Analyse zeigen eine Alternative zum komplexen BSI-Messsystem für Haushaltskunden auf. Die Intelligenz muss nun nicht mehr in eine teure Hardware beim Kunden, sondern kann jederzeit auch in die Software gesteckt werden. Das fordert der EDNA Bundesverband Energiemarkt & Kommunikation schon seit Längerem. Gleichzeitig stimmt der Verband mit der Ansicht von Ernst & Young überein, dass auch in der heutigen Marktkonstellation mit mehr als 800 Netzbetreibern das Thema zu stemmen ist, und es keines regulatorischen Eingriffs bezüglich der Rolle des Gateway-Administrators bedarf. Über Kooperationen und das Entstehen von Dienstleistungsunternehmen werden hier auch ohne Regulierung Szenarien für eine wirtschaftliche Umsetzung entstehen.

**Qualität sicherstellen**

Die Fragen der Datensicherheit und des Datenschutzes lassen sich aber keineswegs nur auf Zähler und Gateways beschränken. Nachgelagert beginnen eine Vielzahl von Marktprozessen und die Kommunikation Tausender von Marktpartnern untereinander. Milliarden Daten werden in diesem Zusammenhang täglich kreuz und quer durch die Republik geschickt. Aus diesem Grund muss auch die Qualität von Prozessen und die Funktionsfähigkeit der zugehörigen Datenformate bei ihrer Einführung und bei den anschließend erforderlichen Änderungen sichergestellt werden. Der EDNA-Bundesverband spricht sich für ein Einführungs- und Änderungsmanagement in diesen Bereichen aus, das die Qualitätssicherung oben anstellt. Erreicht wird dies unter anderem durch verlängerte Einführungszyklen (einmal jährlich statt halbjährlich) sowie durch marktweite Tests vor dem Produktivbetrieb.

**Herr über die eigenen Daten**

Absolute Sicherheit wird es dennoch auch in Zukunft nicht geben können, denn das wäre schlicht nicht bezahlbar. Deswegen muss abgewogen werden, wo Investitionen den meisten Sinn machen, und wo es besser ist, Kompromisse einzugehen. Und vielleicht lohnt es sich auch, über Alternativen nachzudenken. Denn die Frage stellt sich, ob es überhaupt nötig ist, Milliarden von Viertelstundenwerten aus Millionen von privaten Haushalten auf zentrale Server zu übertragen, um sie dort weiterzuverarbeiten und wieder zurückzuspiegeln. Eine Alternative wäre es, sich auf die tatsächlich abrechnungsrelevanten Werte zu

beschränken und den Rest der Informationen vor Ort, beim Kunden, zu speichern, der damit wieder zum Herr über die eigenen Daten werden würde.

*Marc Elsberg, BLACKOUT – Morgen ist es zu spät., Blanvalet Verlag, 2012, ISBN 978-3-7645-0445-8

()

Dieser Beitrag ist in der April-Sonderausgabe von stadt+werk mit Schwerpunkt Informations- und Kommunikationstechnologie für die Energiewende erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: Politik, edna, Informationstechnik, Smart Metering