Smart Metering – Chancen und Risiken

Strategische Infrastrukturen sind die Lebensadern einer modernen Gesellschaft. Die öffentliche Stromversorgung nimmt dabei eine ganz wesentliche Rolle ein, da alle wesentlichen Infrastrukturbereiche von einer funktionierenden Stromversorgung abhängig sind.

Quelle: Fotolia/Bartussek

Bei einem länger andauerndem Stromausfall muss innerhalb weniger Stunden mit schwerwiegendste Konsequenzen für das Allgemeinwesen gerechnet werden. Daher muss die Versorgungssicherheit mit Strom höchste Priorität haben. Dies betrifft einerseits die Erzeugung, Speicherung und den Transport zum Verbraucher, aber auch die Widerstandsfähigkeit des gesamten Systems gegenüber Störungen und Angriffen von außen.

Durch die zunehmende dezentrale Einspeisung von Energie aus erneuerbaren Energiequellen über z.B. Wind-, Photovoltaik oder Biomassekraftwerke, dem zu erwartenden Anstieg der Elektromobilität und der Forderung nach mehr Energieeffizienz, wird eine umfassende Einbindung von Informations- und Kommunikationstechnologien (IKT) zur Netzwerksteuerung unentbehrlich. Erst durch den Informationsaustausch zwischen den Erzeugungsanlagen, den Netzkomponenten, den Speichern und den Verbrauchern kann eine flexible Reaktion auf komplexe Veränderungen im Netz gewährleistet werden. Die Komplexität ergibt sich u.a. aufgrund der Eigenheiten von dezentralen, von beispielsweise Sonnen- oder Windenergie abhängigen, Erzeugungsanlagen, welche naturbedingt keine konstante Energieerzeugung gewährleisten können. Für diese informationstechnische Vernetzung und Steuerung wird der Begriff intelligentes Stromnetz oder Smart Grid verwendet.


Quelle: http://e-control.at

Grundvoraussetzung für intelligente Stromnetze ist das sogenannte Smart Metering („intelligentes Messwesen“). Beim Smart Metering wird der traditionell mechanische oder elektronische Drehstromzähler des Endkunden durch einen intelligenten Zähler (Smart Meter) in Form eines Computers ersetzt, der regelmäßig über elektronische Übertragungsmedien wichtige (Verbrauchs-)Daten an den Netzbetreiber übermittelt. Durch diesen Informationsaustausch wird eine optimierte Netzsteuerung ermöglicht. Zusätzlich soll für den Endkunden eine Verbrauchstransparenz geschaffen werden, die auch zu besseren Stromsparmaßnahmen führen soll. Der Smart Meter ist de facto ein Computer mit Mess- und Kommunikationsaufgaben.

Im Generellen wird dieses Thema bisher sehr euphorisch verfolgt. Die wesentlichen Sicherheitsbedenken wurden bisher im Bezug auf den Datenschutz geäußert, wo es auch entsprechende Diskussionen und ebenso Lösungsansätze gibt. Fallweise wird sogar behauptet, dass damit alle Sicherheitsbedenken gelöst seien. Das dem nicht unbedingt so sein muss, beleuchtet eine aktuelle Analyse zum Thema „Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit“.

Die Analyse verschiedener öffentlicher Quellen führt zum Schluss, dass aus derzeitiger Sicht mit der beabsichtigten Einführung von intelligenten Stromzählern und Messsystemen wahrscheinlich ein erhebliches Risiko für die Strategischen Infrastrukturen und damit auch für die nationale Sicherheit eingegangen wird.

Auffallend ist vor allem, dass in der bisherigen Diskussion und in den rechtlichen Grundlagen kaum Hinweise auf durchzuführende Risikoanalysen zu finden sind. Wenn das Thema Sicherheit angesprochen wird, dann im Sinne von Datenschutz und Betriebssicherheit (safety), aber so gut wie nie in Form von Angriffssicherheit (security). Aber gerade die letzten Monate haben eindrucksvoll vor Augen geführt, welche Sicherheitsprobleme in der IKT-Welt

existieren und das diese auch für großangelegte Angriffe ausgenützt werden.

Durch die bisherige Trennung des Stromnetzes von sonstigen öffentlichen Netzen ist ein relativ hohes Sicherheitsniveau gegeben. Durch die nunmehrige Absicht, IKT-Netze mehr oder weniger direkt mit dem Stromnetz zu verbinden, zumindest aber bisher in der IKT-Welt als unsicher geltende Systeme im Bereich der Stromnetze einzusetzen, ergibt sich eine völlig neue Situation. Diese wird mit dem Wissen, dass es auch in den jetzigen Stromnetzen ausreichend Schwachstellen gibt, welche jedoch so gut wie nicht ausnützbar sind, noch erheblich erschwert. Durch die stark steigende Komplexität steigt auch die Fehlerwahrscheinlichkeit. Komplexe Systeme zeichnen sich dadurch aus, dass ihr Ganzes immer mehr als die Summe ihrer Einzelteile ist. Darüber hinaus ergeben sich durch die beabsichtigte Vernetzung und dem Einsatz von Smart Metern beim Endkunden zahlreiche Ansätze für kriminelle Handlungen, bis hin zur Sabotage und Störung ganzer Stromnetze.

In diesem Zusammenhang muss auch das „Verletzlichkeitsparadoxon“ angesprochen werden, welches den Widerspruch zwischen Risikowahrnehmung und Realität beschreibt. Unsere technisch hoch entwickelte Energieinfrastruktur weist eine relativ zuverlässige, über lange Zeiträume funktionierende Stromversorgung auf. Darüber hinaus bauen nahezu alle technischen Systeme und sozialen Handlungen auf dieser relativen Verlässlichkeit auf. Nicht oder nur unzureichend wird die damit einhergehende massive Verletzbarkeit berücksichtigt. Darüber hinaus führt dies dazu, dass Versorgungsleistungen zunehmend weniger störanfällig organisiert werden.

Dieses Phänomen ist auch im Bereich von Smart Metering zu beobachten. Es gibt einen enormen wirtschaftlichen und politischen Druck für eine rasche Umsetzung, welcher scheinbar gleichzeitig alle möglichen Bedenken ausblendet, bzw. die Betrachtung nur auf Einzelteile beschränkt. Smart Meter sind Computer, welche in einer weitgehend ungesicherten Umgebung beim Endkunden zum Einsatz kommen. Darüber hinaus sollen diese mehrere Kommunikationsschnittstellen für eine flexiblen Einsatz aufweisen, die wiederum als Eintrittspunkt für einen Angriff genutzt werden können. Von diesem Eintrittspunkt kann es möglich sein, je nach vorhandenem Fachwissen und Ressourceneinsatz, bis tief in die Netzwerksteuerung vorzudringen, oder zum Beispiel Schadsoftware einzubringen. Im geringsten Fall beschränkt sich ein möglicher Angriff nur auf den lokalen Smart Meter, um etwa Abrechnungsbetrug zu begehen. Dieses Wissen könnte sich aber, wie auch in der IKT-Welt, sehr rasch verbreiten und zu unzähligen Nachahmern führen. Energieversorgungsunternehmen müssen in einem solchen Fall mit beachtlichen wirtschaftlichen Schäden rechnen.

Der enorme Kostendruck bei den Herstellern lässt nur einen eingeschränkten Spielraum für entsprechende Absicherungsmaßnahmen zu, insbesondere so lange es keine entsprechend kritische Diskussion zu diesem Thema, bzw. auch öffentlichen Druck dazu gibt.

Mit der Einführung von Smart Metering entsteht eine Vielzahl von Angriffsmöglichkeiten auf unsere hochkritische Strominfrastruktur. Derzeit stehen viele Staaten und auch Österreich noch am Beginn der Implementierung. Damit können noch kostengünstiger Änderungen und Verbesserungen vorgenommen werden. Je weiter Systeme ausgerollt werden, desto schwieriger und kostenintensiver wird die Implementierung von möglichen, nachträglich erforderlichen Sicherheitsmaßnahmen.

Nicht vergessen werden darf, dass die Verwundbarkeit mit dem Umfang der Ausrollungen steigt. Einerseits, weil damit die Komplexität des Gesamtsystems steigt und auf der anderen Seite, weil sich damit für mögliche Angreifer lohnendere Ziele ergeben.

Hersteller und Betreiber sind aufgefordert, Sicherheit als Qualitätsmerkmal zu sehen. Diese muss auch Sicherheitsvorkehrungen betreffen und nicht nur am Gerät selbst, sondern im Gesamtsystem. Kein Hersteller wird sich nachsagen lassen wollen, dass sein Produkt eine schlechte Qualität aufweist. Netzbetreiber und Kunden müssen akzeptieren, dass sich dieses Qualitätsmerkmal wahrscheinlich auch auf den Preis, zumindest geringfügig, niederschlägt. Einsparungen zum falschen Zeitpunkt können im Nachhinein ein Vielfaches an Kosten verursachen, die letztendlich wieder die Kunden, direkt oder indirekt, bezahlen werden müssen.

Eine entsprechend kritische Diskussion vor einer umfangreichen Einführung ist daher unabdingbar. Die Risiken, die mit unserem modernen Lebensstil verbunden sind, müssen wieder stärker in unser Blickfeld gerückt werden, ohne jedoch Panik zu erzeugen. Eine offene Kommunikation über Chancen und Risiken, sowie über akzeptierte Restrisiken wären ein wichtiger Beitrag zur Krisenprävention und Bewusstseinsschaffung. Unsere Stromnetze haben eine zu hohe gesellschaftliche Relevanz, als damit leichtfertig umgegangen werden kann.

Alle beteiligten tragen eine hohe soziale Verantwortung für unser aller Zukunft.