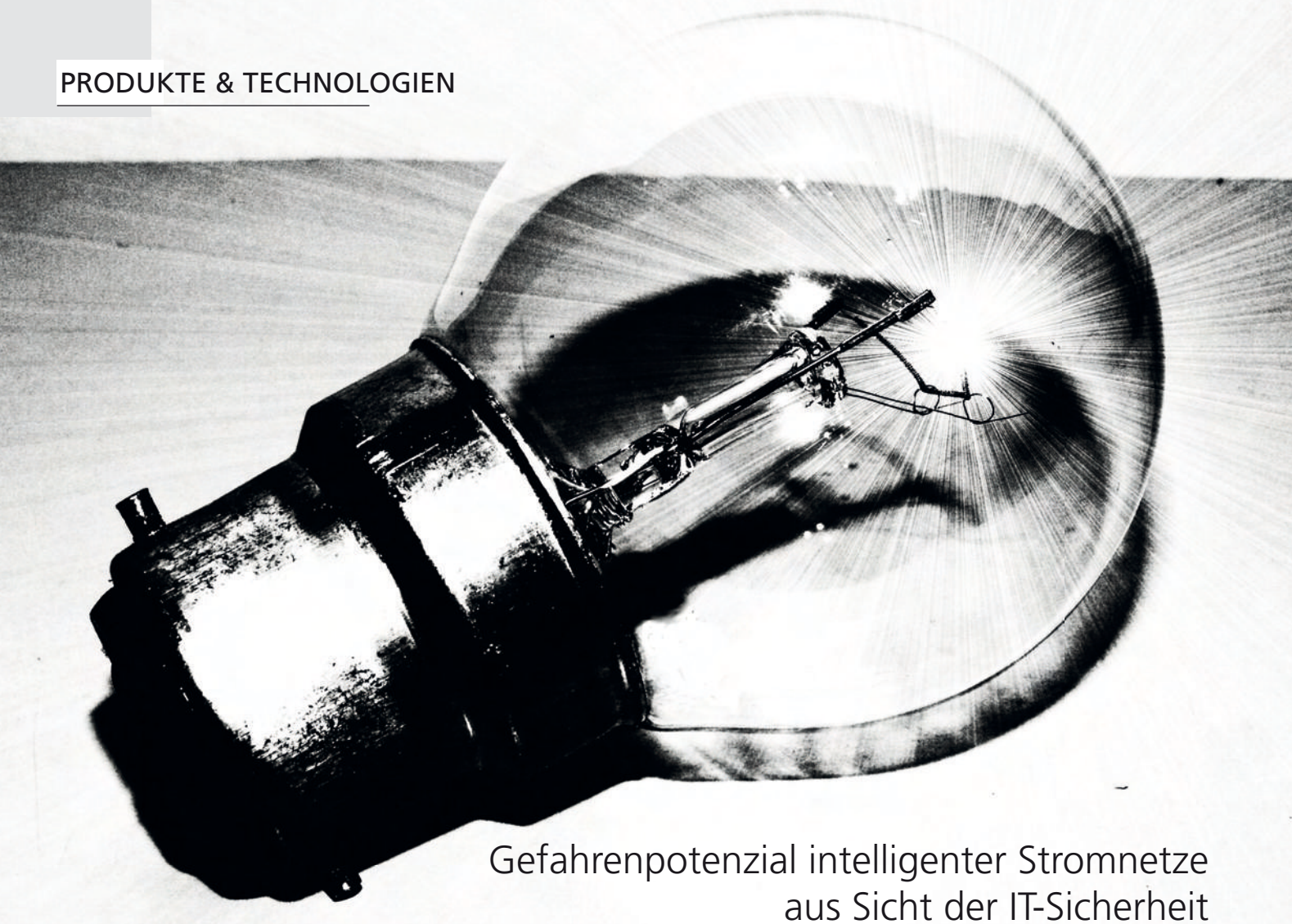

Gefahrenpotenzial intelligenter Stromnetze aus Sicht der IT-Sicherheit

Anforderungen an IT-Systeme in kritischen Infrastrukturen

Das Energienetz der Zukunft läuft zusammen mit IT-Komponenten, die eine intelligente Steuerung erlauben. Dadurch entstehen neue Angriffsflächen, die aber nun erstmals nicht auf ein bestimmtes IT-System wirken, sondern auf eine komplette Bevölkerung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat daher ein Schutzprofil für ein Smart-Metering-Gateway entwickelt, welches diese Problematik in intelligenten Stromnetzen adressieren soll.

Die Bundesregierung hat sich mit ihrem Energiekonzept eine ehrgeizige Aufgabe gesetzt: So soll bis zum Jahr 2020 der Anteil der erneuerbaren Energie im Stromsektor auf 38,6 Prozent[1] gesteigert und der Ausstoß von CO2 um 20 Prozent verringert werden. Dieses Ziel soll unter anderem durch die Einführung von immer mehr „grüner" Energie, also durch den Wechsel von beispielsweise fossilen Brennstoffen oder Atomenergie hin zu Solarenergie oder Windenergie, realisiert werden. Die Erzeugung des Stroms findet daher nicht mehr zentral in einigen wenigen großen Kraftwerken statt, sondern verteilt auf viele kleine Erzeuger. In der dezentralen Erzeugung der erneuerbaren Energie ist es von besonderer Wichtigkeit, dass die kleineren Erzeuger (Solaranlagen, Windparks …) mit den Verbrauchern (Haushalten, Fabriken, Elektroautos ...) kommunizieren, um eine genaue Bedarfsanalyse zu fertigen. Die Umsetzung des ambitionierten Energiekonzepts der Bundesregierung und die Lösung der Integrationsproblematik der erneuerbaren Energien führten zwangsläufig zum Aufbau eines intelligenten Stromnetzes (Smart Grid). Die Einführung einer passenden IKT, um zusätzlich zum Strom auch Informationen zu lokalen Netzzuständen zu übertragen, erfordert die Erweiterung des konventionellen Stromnetzes um informationstechnische Komponenten, welche auch die Haushalte und die bestehende Regelungstechnik erreichbar macht. Durch die Fähigkeit des Netzes, die aktuellen und zukünftig geforderten Systemlastzustände zu ermitteln und systemweit darauf zu reagieren, ist eine sehr gute Lastenverteilung möglich. Abbildung 1 stellt ein intelligentes Stromnetz mit den wichtigsten Komponenten exemplarisch dar.

Ein intelligentes Stromnetz ist als Evolution und nicht als Revolution des bestehenden Stromnetzes zu sehen. Problematisch gestaltet sich bei der Erzeugung des Stroms, dass erneuerbare Energien nicht zuverlässig Strom erzeugen. Ist es beispielsweise windstill, kann ein Windpark möglicherweise nicht die benötigte Menge Strom bereitstellen. Eine große Herausforderung innerhalb intelligenter Stromnetze ist die

effiziente Speicherung der elektrischen Energie. Besteht ein Überschuss an Energie, muss diese gespeichert werden, um diese bei Engpässen nutzen zu können. Beispiele für innovative Lösungen wären das Laden von Batterien ungenutzter Elektroautos oder das Herunterkühlen von Kühlhäusern, falls ein Stromüberschuss vorliegt.

Aus Nutzersicht ist die wohl größte Veränderung, dass die analogen Stromzähler in den Haushalten durch neue intelligente Stromzähler (Smart Meter) ausgetauscht werden. Diese intelligenten Zähler können zeitnah Informationen zum aktuellen Verbrauch beziehungsweise zur Erzeugung des Haushalts geben und ermöglichen so eine flexible Tarifierung. Der Einbau solcher Zähler ist in Deutschland bei Neubauten ab einem Jahresverbrauch von 6000 kWh und bei großen Sanierungen verpflichtend.

Gefahren und Schutzbedarfe

Die neuen technischen Anforderungen an das zum Teil veraltete, klassische Energieinformationsnetz und die zur Umsetzung benötigte IKT, mit den bekannten Angriffsvektoren aus dem Internet, schaffen ein hohes Gefahrenpotenzial. Der Transport von periodisch anfallenden Nutzdaten aus vielen privaten Haushalten, die Auswertung dieser Informationen zur weiteren Steuerung von Ressourcen und die generell vielfältigen Angriffsflächen auf ein IT-System machen es nötig, diese Gefahren eingehend zu behandeln. In intelligenten Stromnetzen spielen auch die sogenannten Schadenskategorien eine wichtige Rolle. Mit Schadenskategorien ist hier die Auswirkung auf bestimmte Benutzerkreise von IT-Systemen infolge eines Hacker-Angriffs gemeint. Grundsätzlich ist festzuhalten, dass der Benutzerkreis, also Fachanwender, Kunden, Entwickler etc., bei konventionellen Informationssystemen immer auf die jeweilige Fachanwendung beschränkt ist. Die Software einer Firma ist in der Regel beschränkt auf ihre eigenen Geschäftsabläufe und ihr eigenes Netzwerk. Ein soziales Netzwerk richtet sich zu einem Zeitpunkt an eine bestimmte Anzahl von angemeldeten Benutzern, und die Software einer Hochschule umfasst alle Abläufe, die unmittelbar zur Abwicklung eines reibungslosen Hochschulbetriebs notwendig sind. Natürlich gibt es bei all diesen Beispielen immer auch Schnittstellen zu externen Software-Systemen, aber primär wirken sich Angriffe immer nur auf den jeweiligen Benutzerkreis aus.

Betrachtet man nun die bereits vorgestellten Komponenten eines intelligenten Stromnetzes, dann bekommt das Stromnetz als Mittel zum Zweck einen herausragenden Stellenwert im Gesamtsystem. An dieses Stromnetz sind im Gegensatz zu den erwähnten konventionellen IT-Systemen nicht nur einige Benutzerkreise angeschlossen, sondern je Land mehr oder weniger fast alle Haushalte. Genau aus diesem Grund haben Angriffe auf ein intelligentes Stromnetz und die damit verbundenen Komponenten einen viel höheren Wirkungsradius als auf ein konventionelles Informationssystem. Es kann in diesem Zusammenhang zu weitreichenden Schäden, insbesondere zur Beeinträchtigung der persönlichen Unversehrtheit und ferner bis hin zum Tod von Menschen, kommen. Nicht umsonst gehört die Stromversorgung neben Trinkwasser, Abwasser, Nahrung, Verkehrsinfrastruktur etc. mit zu den kritischen Infrastrukturen eines Staates. Sie alle haben eine hohe Relevanz in Bezug auf die Ordnung innerhalb einer Gesellschaft. Kommt es zu einer Beeinträchtigung dieser Ressourcen, ist die Sicherheit und Gesundheit der Menschen gefährdet. Mögliche Auswirkungen bei einem Angriff auf diese Ressourcen sind Ausfälle in Krankenhäusern, Heizungen, Aufzügen, Fabriken oder Überlastgenerierungen durch falsche Last-Prognosen.

Viele neue „smarte" Technologien haben im letzten Jahrzehnt unseren Alltag geprägt. Mit Technologien wie dem Internet, Smartphones, Navigationsgeräten, Tablet-PCs und Kombinationen aus allem wurde auf der einen Seite ein schier unendlich großes Fundament für weitere Technologien gegossen und zum anderen die Denkweise der Technologieanbieter grundlegend verändert. Wer seine Wettbewerbsfähigkeit und somit seine Wirtschaftlichkeit sichern möchte, wird in Zukunft zwangsläufig seine Produkte auf die Vernetzung mit dem Internet ausrichten müssen. Kameras, die Bilder direkt im Internet und nicht mehr auf der Speicherkarte ablegen, oder Kühlschränke, die den Besitzer über das Internet auf fehlende Produkte hinweisen, sind nur die Spitze des Eisberges.

Jegliche Komponente, die bisher nur mit einer einfachen Steckdose ihren Betrieb verrichtet hat und in Zukunft zusätzlich Informationen über das Internet austauscht, stellt zwangsläufig eine neue potenzielle Angriffsfläche mit neuen Angriffsvektoren dar. Diese Überlegungen sind sehr eng mit der Idee eines intelligenten Stromnetzes verbunden. Für die Militärs auf der ganzen Welt ist somit also ein idealer Ansatzpunkt für die moderne Kriegsführung geschaffen. Mit einer Handvoll IT-Spezialisten kann theoretisch, ganz bequem aus dem heimischen Büro heraus, ein enormer Schaden hervorgerufen werden, ohne dass ein Soldat ein Schlachtfeld betreten muss. Solche Aussagen scheinen auf den ersten Blick immer weit hergeholt, aber sollte ein gezielter Militärschlag in Form eines Hacker-Angriffs aus dem Ausland unser Stromnetz

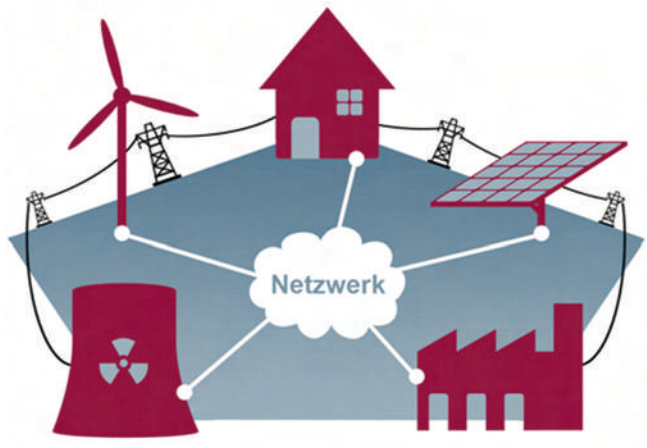

Abb. 1 Intelligentes Stromnetz

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

lahmlegen, könnte mit Blick auf das Münsterländer Schneechaos im Jahre 2005 ein echtes Problem entstehen. Aufgrund der ungewöhnlich hohen Schneemenge sind damals viele Strommasten eingeknickt. Mehrere tausend Haushalte mussten deshalb wochenlang ohne Strom auskommen.

Die Schwere eines militärisch motivierten Hacker-Angriffs wird durch ein Strategiepapier der Nato verdeutlicht. In diesem Strategiepapier wird der Angriff auf ein IT-System des Gegners als kriegerische Aktion, gleichzusetzen mit der Nutzung von Waffen, beschrieben. Selbst zivile Hacker können demnach unter bestimmten Voraussetzungen als anzugreifende Feinde eingestuft werden, wenn sie beispielsweise über Erpressung Geld verdienen wollen oder direkt Schaden anrichten. Mögliche Angriffsszenarien auf ein intelligentes Stromnetz könnten parallel zum Angriff mittels Malware à la „Stuxnet" auf Steuerungssysteme von Industrieanlagen ablaufen. Würde ein derartiger Wurm infolge der Vernetzung von Stromerzeugern und Verbrauchern ein intelligentes Stromnetz infizieren, so könnte die Stromversorgung ganzer Regionen manipuliert werden. Unabhängig von einem Militärschlag sind hier auch politische und wirtschaftliche Beweggründe denkbar, zum Beispiel in Form von Spionage. All diese Betrachtungen machen klar, warum an die Sicherheit eines intelligenten Stromnetzes höchste Anforderungen zu stellen sind.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Schutzprofil für ein Smart-Metering-Gateway entwickelt, welches diese Problematik in intelligenten Stromnetzen adressieren soll. In diesem Schutzprofil werden Vorgaben zur sicheren Umsetzung einer interoperablen Kommunikationseinheit für den Austausch von Messwerten innerhalb eines intelligenten Stromnetzes gemacht. Das Schutzprofil und die technische Richtlinie des BSI sind deshalb im Energiewirtschaftsgesetz verankert.

Auch wirtschaftlich motivierte Angriffe auf ein intelligentes Stromnetz sind sehr gut denkbar. Beispielsweise könnte die Stromversorgung aus dem Ausland im großen Stil manipuliert werden, um etwa Energieproduzenten aus dem eigenen Land Wettbewerbsvorteile auf dem globalen Markt zu verschaffen. Dieses Szenario lässt sich aber im kleinen Rahmen auch auf einfache Haushalte übertragen. Der einfachste Fall eines Angriffs durch die Manipulation von Daten richtet sich an die Abrechnung des Stromtarifs. Gelingt es einem Angreifer, die Messwerte der einzelnen digitalen Stromzähler zu manipulieren, können so anfallende Kosten für den Stromverbrauch verschleiert oder Stromeinspeisungen vorgetäuscht werden.

Die Manipulation von Messwerten hat neben den finanziellen Konsequenzen aber noch weitreichendere Folgen für das Gesamtsystem. Wie eingangs erwähnt, ermöglicht die Auswertung von Lastinformationen eine verbesserte Nutzung der vorhandenen Ressourcen. Sollten diese Informationen durch Schwarmangriffe im großen Maße manipuliert werden, kommt es zur Instabilität des Netzes. Hacker könnten dazu der zentralen Informationsverwaltung des intelligenten Stromnetzes falsche zukünftige Lastanforderungen vorgaukeln. Sowohl zu viel als auch zu wenig Energie im Netz wirkt sich nachteilig aus. Neben den allgemeinen Sicherheitsanforderungen gilt es also insbesondere, die Integrität und Verbindlichkeit der Messwerte zu gewährleisten. Hierzu werden im Schutzprofil des BSI Vorgaben für den sicheren Umgang mit Messwerten spezifiziert. Grundsätzlich müssen die Messwerte auf logische und technische Korrektheit hin geprüft werden. Beispielsweise dürfen Pakete mit einem veralteten Zeitstempel grundsätzlich nicht weiterverarbeitet werden. Des Weiteren kann anhand von Zählerprofilen festgehalten werden, ob ein Zählerstand saldierend ist, denn Zählerstände dürfen in der Regel nur monoton steigen.

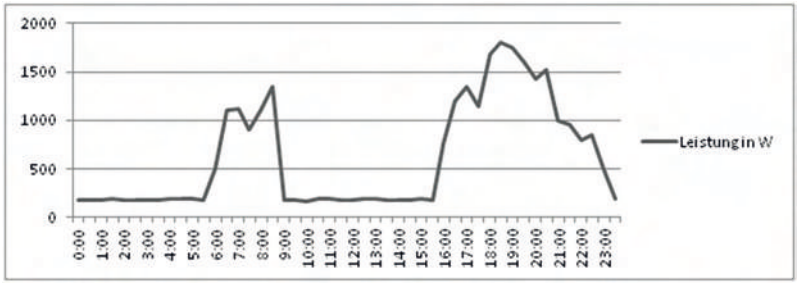

Abb. 2 Beispiel einer Energieverbrauchskurve

Datenschutz

Die Einführung von intelligenten Stromzählern erlaubt eine sehr flexible Tarifierung, welche dem Wunsch der Letztverbraucher nach niedrigeren Strompreisen Rechnung trägt. Der Kunde kann entscheiden, wann es ihm auf günstigen Strom (zum Beispiel Nutzung der Waschmaschine um 2 Uhr nachts) beziehungsweise auf die Verfügbarkeit des Stroms (der Herd muss jederzeit nutzbar sein) ankommt. Dies ist mit analogen Zählern nicht möglich, da diese nur jährlich ausgelesen werden und somit nicht die nötige Granularität an Messwerten liefern.

Wie auch in Abbildung 2 deutlich wird, speichern die intelligenten Stromzähler nicht nur den Verbrauch, sondern auch den Zeitpunkt der Erfassung des entsprechenden Messwertes. Somit ist mit den Messdaten die Möglichkeit gegeben, den Tagesablauf des Verbrauchers zu analysieren. In diesem Beispiel sind zwei deutliche Spitzen im Stromverbrauch erkennbar. Wahrscheinlich ist es, dass die Bewohner das Haus um ca. 9 Uhr verlassen und gegen 15:30 Uhr zurückkehren. Es könnte also auf Arbeits- beziehungsweise Urlaubszeiten oder andere Gewohnheiten im Tagesablauf des Verbrauchers geschlossen werden. Aus diesen Daten ließen sich weitere Informationen ableiten. So könnte beispielsweise der beste Zeitpunkt eines Einbruchs beziehungsweise Vertreterbesuches ermittelt werden. Durch eine weiterführende Analyse könnten auch Schlüsse auf Dinge wie Gehalt oder Wärmedämmung des Hauses gezogen werden. Bei einer Erfassung von Messwerten je ‚verbrauchendem' Gerät ließen sich sogar nicht nur haushaltsbezogene, sondern sogar personenbezogene Profile erstellen.

Es zeigt sich, dass diese sensiblen Daten eine große Herausforderung für den Datenschutz darstellen. Die direkte Identifizierbarkeit des Verbrauchers aufgrund der Energiedaten kann zur Beschneidung des Rechts auf informelle Selbstbestimmung führen, das auf verfassungsrechtlicher Ebene ein Grundrecht ist. Dieses regelt: „die aus dem

Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"[2]. Es muss also ein Kompromiss zwischen bestehendem Recht und dem unvermeidbarem Fortschritt in der Technologie gefunden werden. Zur Umsetzung der Datenschutzproblematik muss ein strikter und genau definierter standardisierter Umgang mit den Benutzerdaten geschaffen werden.

Das erwähnte Schutzprofil des BSI gewährleistet den sicheren Umgang mit den Daten der Verbraucher. Zwischen den intelligenten Zählern und verschiedenen Marktteilnehmern fungiert das Gateway als zentrale Kommunikationseinheit und verbindet das Weitverkehrsnetz (WAN) mit dem „Metrological Area Network" (MAN)[3].

Grundsätzlich werden von dem Gateway beim Schutz der Privatsphäre des Endverbrauchers zwei Aspekte verfolgt:

Der erste Aspekt umfasst die Datensparsamkeit, so werden nur die Daten eines Verbrauchers übertragen, die zwingend zur Erfüllung eines Anwendungsfalls nötig sind, so dass sichergestellt ist, dass keine unnötigen Daten einem externen Marktteilnehmer preisgegeben werden. Die Daten werden außerdem anonymisiert, sofern eine Zuordnung zu einem Verbraucher nicht zwingend nötigt ist. Dies ist vor allem bei abrechnungsrelevanten Daten nicht möglich. In diesem Fall werden die Daten pseudonymisiert. Die Verwendung mehrerer Pseudonyme pro Verbraucher erschwert eine konkrete Zuordnung. Der zweite Aspekt ist die vollständige Transparenz gegenüber dem Kunden. Der Kunde kann jederzeit einsehen, welche Daten an welchen Teilnehmer übermittelt wurden und aufgrund der aktuellen Gegebenheiten noch übertragen werden.

Die Übertragung von Messdaten findet über einen gesicherten Kanal statt. Die Inhaltsdaten, die auf diesem Kanal übertragen werden, müssen zusätzlich verschlüsselt und die Integrität muss sichergestellt werden. So lässt sich sicherstellen, dass nur autorisierte Marktteilnehmer die übermittelten Messdaten auswerten können, auch falls der direkte Kommunikationspartner des Gateways nicht der tatsächliche Empfänger der Daten ist.

Resümee und Ausblick

Für die kontrollierte und ressourcenschonende Integration von erneuerbaren Energien sind intelligente Stromnetze eine zwingende Notwendigkeit. Sie bieten als kritische Infrastruktur eine Vielzahl von Angriffsflächen mit neuen Herausforderungen. In Zukunft können durch weitere Anforderungen an ein intelligentes Stromnetz zusätzliche Gefahrenpotenziale entstehen. Im Zuge der Elektroautos und der dadurch benötigten Ladestationen ist es denkbar, dass ein intelligentes Stromnetz mit vielen anderen Domänen zusammenarbeitet. In diesem Fall könnte es für die Tarifierung nicht mehr wichtig sein, wo der Strom genutzt wird, sondern von wem. Ein mögliches Szenario wäre hier die Authentifizierung gegenüber eine Ladestation für Elektroautos und einer automatische Verbuchung des Betrags auf die Stromrechnung des Verbrauchers.

Das Schutzprofil des BSI nimmt sich der Herausforderungen in einem intelligenten Stromnetz an und bietet einen deutschlandweit verpflichtenden Standard für die Sicherheit der Kommunikation im Heimbereich. Es wurde so konzipiert, dass die Verarbeitung der Messwerte von der jeweiligen Ressource unabhängig, also auch auf Wasser, Gas oder Wärme übertragbar ist. Diese Skalierbarkeit des Systems hat Vorteile, ermöglicht aber auch neue Angriffsziele auf weitere kritische Infrastrukturen. Neben möglichen Angriffen aus dem Heimbereich heraus müssen politisch und kriegerisch motivierte Angriffe verhindert werden. Hier wird der Begriff des „Cyberwar" eine wichtige Rolle spielen, denn eine kontrollierte Nutzung von „grüner Energie" kann zwar im kleinen Format national funktionieren, wird sich aber mit vollständigem Potenzial nur in einem globalen Zusammenschluss von Erzeugern und Verbrauchern manifestieren. Es wird also zwangsläufig länderübergreifende Schnittstellen geben, die auch zu Friedenszeiten eine potenzielle Gefahr für die kritische Infrastruktur „Strom" darstellen. Im Institut für Internet-Sicherheit wird in diesem Bereich geforscht, um vertrauenswürdige und sichere Technologien für die Zukunft zu entwickeln. ■

Literatur

- *Protection Profile for the Gateway of a Smart Metering System, BSI, Bonn 2013*
- *Sicherheits- und Datenschutzanforderungen an SmartGrid-Technologien, S. Schriegel, J. Jasperneite, Springer Verlag 2012*
- *Nutzerdaten im Smart Grid – zur Notwendigkeit einer differenzierten grundrechtlichen Bewertung, G.Hornung und K. Fuchs, Springer Verlag 2012*
- *Datenschutz in Smart Grids, Raabe, Pallas, Weis, Lorenz, Boesche, 2011*
- *E-Energy Modellprojekte und -regionen, http://www.e-energy.de/de/modellregionen.php, abgerufen am 15.04.2013*
- *The Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press 2013*

RENÉ RIEDEL, studentischer Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen

TOBIAS URBAN, studentischer Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen

NORBERT POHLMANN, Informatikprofessor sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen

ANTONIO GONZÁLEZ ROBLES, wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen

1 *Nationaler Aktionsplan für erneuerbare Energie, BMU, August 2010*

2 *BVerfGE 65, 1 (42), s. zuletzt ausführlich Albers, Informationelle Selbstbestimmung, 2005.*

3 *Metrological Area Network = Lokales messtechnisches Netzwerk*