Alcatel-Lucent Stiftung für Kommunikationsforschung

Schutz kritischer Infrastrukturen

**Claudia Eckert, Franz-Reinhard Habbel,
Reinhold Harnisch, Bernd Kowalski,
Andreas Memmert, Cornelia Rogall-Grothe**

DStGB
Deutscher Städte- und Gemeindebund
www.dstgb.de

Schutz kritischer Infrastrukturen

Dokumentation der 12. Fachkonferenz „Bürgernahe Sicherheitskommunikation für Städte und Gemeinden“

13. Juni 2012, Berlin

Impressum

Stiftungsreihe 101

Redaktion
Dr. Erich Zielinski
Petra Bonnet M.A.
Martina Schütz M.A.

Druck der Broschüre
DCC Kästl GmbH & Co. KG

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine nichtrechtsfähige Stiftung in der treuhänderischen Verwaltung des Stifterverbandes für die Deutsche Wissenschaft.

Angaben nach § 5 TMD/
§ 55 RfStv

Stifterverband für die Deutsche Wissenschaft e.V.
Barkhovenallee 1
45239 Essen
Telefon: (02 01) 8401-0
Telefax: (02 01) 8401-301
E-Mail: mail@stifterverband.de

Geschäftsführer:
Prof. Dr. Andreas Schlüter
(Generalsekretär)

ISSN 0932-156x

Inhalt

Cybersicherheit und Schutz kritischer Infrastrukturen

Franz-Reinhard Habbel

Das Thema Sicherheit hat für den Deutschen Städte- und Gemeindebund einen hohen Stellenwert. Sind es doch die Kommunen, die einen Großteil der Infrastrukturen verantworten. Wirtschaft, Gesellschaft und Staat sind immer mehr von funktionierenden Infrastrukturen abhängig. Die Gefährdungen, insbesondere in der Informationstechnologie, aber auch in der Energieversorgung sind – was die Sicherheit betrifft – in den letzten Jahren größer geworden.

Ich möchte ausdrücklich dem Bund dafür danken, gerade das Thema Cybersicherheit hier in besonderer Form aufzugreifen. Die Risiken sind groß und oft werden sie verdrängt. Das gilt auch für die Kommunen. Alles, was an Infrastruktur nicht sichtbar oder nur schwer fassbar ist, ist schwer einzuschätzen.

Die Bürger wollen Sicherheit. Sie wollen sich sicher sein, dass der Strom aus der Steckdose kommt, das Wasser aus dem Hahn und das Internet aus der Buchse. Sie wollen sich sicher sein, dass der Verkehr rollt, die Regale in den Läden voll, und die Mülltonnen einmal in der Woche leer sind. Bürger wollen nicht nur Internet und Kommunikation gewährleistet haben, sondern auch die Sicherheit und Anonymität dieses Netzwerkes. Wie schützen wir diese überlebenswichtigen Infrastrukturen? Eine aktive und sich ständig weiterentwickelte Sicherheitsstrategie für jede einzelne Infrastruktur ist notwendig!

Ein ägyptisches Sprichwort lautet: „Vertraue auf Allah, aber binde dein Kamel an!“ Das Kamel also anbinden. Das ist leichter gesagt als getan! In Zeiten der vernetzten Stadt ist so ziemlich jede Infrastruktur und öffentliche Dienstleistung vom Internet und verschiedenen Netzwerken abhängig. Diese Vernetzung macht vieles einfacher, kostengünstiger, schneller und effizienter. Aber sie ist potenziell auch anfällig für Eingriffe von außen.

Beispiel Flame: Der vor wenigen Wochen enttarnte Internet-Virus sorgte in der Fachwelt für ein ehrfürchtiges Erzittern: Nach Expertenmeinung übersteigt er alle bisher bekannten Cyber-Bedrohungen. Flame spionierte nach jetzigem Wissen über drei Jahre Firmen und Netzwerke im Iran, Nahen Osten und Nordafrika aus. Was wäre, wenn ein solcher Virus auch Deutschland befallen hätte? Wären auch sicherheitskritische Netzwerke und Infrastrukturen betroffen gewesen? Wir können es uns nicht leisten, dass unsere Lebensadern, die Leitungen, Verbindungen und Knotenpunkte im Cyber-Raum, gestört werden!

Wirtschaft, Bevölkerung, Staat und kritische Infrastrukturen sind durch zunehmende Vernetzung und Nutzung der weltweiten Informationskanäle auf ein verlässliches Funktionieren der Kommunikations- und Informationskanäle sowie des Internets angewiesen. Das gilt auch für die Energieversorgung. Welche Folgen hätte zum Beispiel ein Stromausfall, ein Blackout, für Deutschland?

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, welches von Professor Arnim Grunewald geleitet wird – welcher uns auch gleich durch das Programm begleiten wird –, liefert eine anschauliche Erläuterung, was ein Black-Out in Deutschland anrichten könnte:

- Hunderte Züge und U-Bahnen würden prompt liegen bleiben. Zehntausende Menschen wären eingeschlossen.
- Aufgrund eines Ausfalls der Straßenbeleuchtung und Verkehrssignalen würde die Zahl der Verkehrsunfälle mit Verletzten und Toten dramatisch steigen.
- Die Wasserversorgung und viele der 10.000 Kläranlagen würden kollabieren.
- Die Versorgung mit Lebensmitteln würde nicht mehr funktionieren. Hilfslieferungen und Essensrationen würden bei der Verteilung zu Gewaltausbrüchen führen, heißt es im Bericht des Büros für Technikfolgen-Abschätzung.
- Die 2.000 Krankenhäuser könnten sich nur kurze Zeit mithilfe von Stromgeneratoren mit Strom versorgen, bereits nach 24 Stunden ist mit erheblichen Einschränkungen zu rechnen.

Was müssen wir tun? Wir müssen bereits heute zukünftige Bedrohungslagen antizipieren! Was wäre alles möglich und wie könnte man reagieren, oder noch besser: Präventionsarbeit leisten, dass „es“ nicht passiert! Es hilft natürlich nichts, Panik zu verbreiten. Dies führt – etwas überspitzt gesagt – dazu, dass man sagt: „Wir haben unsere Sicherheit nicht mehr selbst in der Hand, es bringt alles nichts, wir sind verloren.“ Dennoch muss man sich auch über Worst-Case-Szenarien Gedanken machen.

Wir müssen also unser Kamel unter allen Umständen anbinden, und es mithilfe aller uns zur Verfügung stehenden Mittel – selbstredend in einem verfassungsrechtlichen Maße – bewachen! Ansonsten könnte das Kamel entführt und missbraucht werden, und wir ständen allein in der Wüste!

Franz-Reinhard Habbel *ist Sprecher des Deutschen Städte- und Gemeindebundes in Berlin*.

Cyber-Sicherheit für Deutschland

Cornelia Rogall-Grothe

Informationstechnik, insbesondere das Internet sind integrale Bestandteile unseres Lebens geworden. Dies gilt für unsere geschäftlichen als auch für unsere privaten Aktivitäten. Note- und Netbooks, Smartphones und Navigationsgeräte sind aus unserem Alltag nicht mehr wegzudenken. Eine Studie des Instituts der deutschen Wirtschaft in Köln vom November letzten Jahres ist zu dem Ergebnis gekommen, dass die Hälfte aller Unternehmen in Deutschland inzwischen vom Internet abhängig ist. Was das bedeutet, führt uns eine Schätzung aus der Schweiz vor Augen, wonach bei einem Totalausfall der Informatik 25 Prozent der Unternehmen Insolvenz anmelden müssten, wenn der Schaden nicht innerhalb kürzester Zeit behoben werden könnte. Nach dieser Schätzung wäre das beispielsweise bei einer Bank schon nach zwei, bei einem Handelsunternehmen nach drei Tagen der Fall.

Auch in der Verwaltung nutzen wir moderne Informationstechnologie. Für viele Städte und Gemeinden gehört eGovernment heute zum Tagesgeschäft.

Bedrohungslage

Um die Chancen weiter ausbauen zu können, müssen wir uns auch mit den Schattenseiten der Internetnutzung beschäftigen. Computersysteme haben systemimmanent Anfälligkeiten, ihre digitale Vernetzung potenziert die Gefahren. Hinzu kommt, dass auch die Internetkriminalität rapide zunimmt. Täglich werden durchschnittlich 13 neue Schwachstellen in Standard-Programmen entdeckt. Durchschnittlich alle zwei Sekunden wird ein neues Schadprogramm beziehungsweise eine Variante eines Schadprogramms erstellt. Täglich werden ca. 21.000 Webseiten weltweit mit Schadprogrammen infiziert. Die Zahl der Cybercrime-Fälle ist im Jahr 2010 um 19 Prozent gestiegen. Bei fast der Hälfte dieser Fälle handelt es sich um Computerbetrügereien wie z.B. Phishing von Onlinebanking-Daten oder den missbräuchlichen Einsatz von Kreditkartendaten. Der Schaden aller Cybercrime-Delikte beziffert sich im Jahre 2010 auf 61,5 Millionen Euro.

Auch die Bundesverwaltung war 2011 Ziel eines Angriffs auf den Zoll. Dabei waren sensible Daten der Bundespolizei betroffen. Auch Kommunen melden sich immer öfter beim BSI mit IT-Problemen und erfragen Unterstützung bei deren Lösung. Das Schadprogramm Stuxnet hat gezeigt, dass nicht nur das Internet, sondern auch industrielle Infrastrukturen, die als vom offenen Internet abgetrennt galten, von gezielten IT-Angriffen nicht mehr ausgenommen sind. Stuxnet hat uns vor Augen geführt, dass die Sammlung von Informationen zur Abschätzung der Bedrohung eine erhebliche Zeit in Anspruch genommen hat. Informationen, die notwendig sind, um Schäden zu verhindern beziehungsweise Schäden zu minimieren. Dies hat die Bundeskanzlerin im Oktober 2010 zum Anlass genommen und das BMI beauftragt, eine Cyber-Sicherheitsstrategie zu entwickeln. Kritische Infrastrukturen wie zum Beispiel der Energie-, der Telekommunikations- oder der Finanzsektor sind vor IT-Angriffen besonders zu schützen, weil Beeinträchtigungen ihrer IT-gestützten Prozesse die Lebensgrundlagen und den wirtschaftlichen Wohlstand in

Deutschland erheblich gefährden könnten. Zu den Kritischen Infrastrukturen gehören aber auch die öffentlichen Verwaltungen von Bund, Ländern und Kommunen.

Zur Verbesserung der IT-Sicherheit für die Bundesverwaltung existiert bereits seit 2007 der Umsetzungsplan Bund. Mit der Erarbeitung gemeinsamer Standards – auch Sicherheitsstandards für eGovernment Anwendungen – beschäftigt sich der IT-Planungsrat, in dem ich in diesem Jahr den Vorsitz habe. Ich komme noch einmal darauf zurück, welche weiteren Maßnahmen erforderlich sind. Cybersicherheit ist gemäß der Bedeutung der IT auf einem hohen Niveau zu gewährleisten, ohne dabei die Chancen, die das Internet bietet, zu beeinträchtigen.

Cyber-Sicherheitsstrategie für Deutschland

Aus diesem Grunde hat die Bundesregierung im Februar 2011 die Cyber-Sicherheitsstrategie für Deutschland beschlossen. Kernpunkte dieser Strategie sind

- der verstärkte Schutz Kritischer Infrastrukturen vor IT-Angriffen
- der Schutz der IT-Systeme in Deutschland einschließlich einer Sensibilisierung der Bürgerinnen und Bürger
- der Aufbau eines Nationalen Cyber-Abwehrzentrums sowie die Einrichtung eines
- Nationalen Cyber-Sicherheitsrates.

Nationales Cyber-Abwehrzentrum

Die Einrichtung eines Nationalen Cyber-Abwehrzentrums war dringend geboten, um die Handlungsfähigkeit bei IT-Vorfällen zu verbessern. Cyber-Kriminelle orientieren sich nicht an Behördenstrukturen oder Zuständigkeiten.

Das wichtigste Mittel zur Schadensverhinderung beziehungsweise Schadensminimierung sind Informationen. Dazu gehören Informationen zu technischen Fragen, zu möglichen Schäden von potenziell Betroffenen und zu Tätern sowie das Erfahrungswissen von allen Bundesbehörden, die mit IT-Angriffe befasst sind. Mit dem Cyber-Abwehrzentrum, in dem das Bundesamt für Sicherheit in der Informationstechnik gemeinsam mit anderen relevanten Behörden eine Informationsplattform bildet, ermöglicht es uns, schnell und abgestimmt alle wesentlichen Informationen zu einer Schadsoftware oder einem IT-Angriff aber auch zu den möglichen Schäden und Folgen vorliegen zu haben. Diese können wir analysieren und Empfehlungen zum Schutz der IT-Systeme wie auch weiteren Schadensminimierungsmaßnahmen zur Verfügung zu stellen. Die Aufsichtsführenden Bundesbehörden über die Betreiber der Kritischen Infrastrukturen werden wir im Laufe des Jahres in die Arbeit des Cyber-Abwehrzentrums integrieren, die ersten Behörden bereits in den nächsten Wochen. In einem zweiten Schritt soll dann ebenfalls die Anbindung von Aufsichtsbehörden auf Länderebene erfolgen – das Know-how und die Analysen zu Cybersicherheit sollen auf diesem Weg mit allen involvierten und verantwortlichen Behörden ausgetauscht werden.

Schon jetzt möchte ich Ihnen im Vorgriff ans Herz legen, dass ein solches Konzept nur funktioniert, wenn alle Beteiligten sich in die Zusammenarbeit aktiv einbringen. Gerade beim Schutz Kritischer Infrastrukturen ist ein hoher Grad an Expertise bei Ländern und auch Kommunen verortet – gemeinsam mit der Cybersicherheitskompetenz im Bundesamt für Sicherheit in der Informationstechnik

(BSI) wird uns dies zu enormer Schlagkraft beim Cyberschutz in Deutschland verhelfen.

Die im Cyber-Abwehrzentrum vertretenen Behörden haben unterschiedliche Aufgaben, aber eins gemeinsam: Sie bündeln ihre Erkenntnisse und Erfahrungen hinsichtlich neuer technischer Bedrohungen, die sie im Rahmen ihrer Aufgaben erlangen. Mit dem Nationalen Cyber-Abwehrzentrum setzen wir unsere präventive Sicherheitspolitik fort. Es geht hier um Schadensvermeidung oder -minimierung durch schnellstmögliche Information. Mit der Einrichtung des Nationalen Cyber-Abwehrzentrum kam die Bundesregierung ihrer gesamtstaatlichen Verantwortung zur Verbesserung der IT-Sicherheit nach.

Cyber-Sicherheitsrat

Cyber-Sicherheit ist eine gemeinsame – Staat und Wirtschaft gleichermaßen fordernde – Herausforderung. Nur in einem vernetzten Ansatz lassen sich präventive Instrumente und übergreifende Politikansätze koordinieren. Aus diesem Grund hat die Bundesregierung einen Cyber-Sicherheitsrat unter meiner Verantwortung ins Leben gerufen: Drei Sitzungen auf Staatssekretärs-Ebene – auch von zwei Ländervertretern und unter Beteiligung assoziierter Wirtschaftsvertreter – haben bereits stattgefunden und es wurden Themenschwerpunkte festgelegt.

Aufgrund der geschilderten Bedrohungslage und der Abhängigkeit von verfügbarer Informations- und Kommunikationstechnik in den Unternehmen der kritischen Infrastrukturen hat der Cyber-Sicherheitsrat aktuell seinen Fokus auf die Koordinierung des Vorgehens bei der Absicherung der kritischen Infrastrukturen gegen IT-Beeinträchtigungen gerichtet.

Weitere Themen sind neue Technologien und damit zusammenhängende Sicherheits-Herausforderungen und die Position Deutschlands in internationalen Gremien zu Cyber-Fragen. Diese internationale Dimension der Cyber-Sicherheit nimmt enorm an Bedeutung zu. Alle Staaten hängen am Internet, der zeit sind zwei Milliarden Menschen online, insbesondere in den Schwellenländern Südamerikas, Afrikas und Asiens warten Millionen Menschen auf weiteren Zugang. Daher müssen wir auch mit den Regierungen anderer Staaten über die Verbesserung der Sicherheit im Internet diskutieren und Vereinbarungen treffen. Ich komme später noch einmal auf das Thema zurück.

Ein weiteres Thema war in der letzten Sitzung am 31. Mai der größere Schutz der IT der Landes- und Kommunalverwaltungen. Derzeit erarbeitet eine Unterarbeitsgruppe des IT-Planungsrates Vorschläge für den Aufbau von CERT-Strukturen in den Ländern und deren Vernetzung mit dem BSI. Der Cyber-Sicherheitsrat hat die dort vertretenen Landesvertreter aufgefordert, über Fortschritte regelmäßig zu berichten.

Schutz Kritischer Infrastrukturen

Der wesentliche Kernpunkt der Cyber-Sicherheitsstrategie betrifft den Schutz der Kritischen Infrastrukturen. Zum ihrem Schutz wurde seit 2005 der Umsetzungsplan KRITIS erarbeitet und 2007 beschlossen. Dieser sieht vor, dass privatwirtschaftliche Betreiber Kritischer Infrastrukturen und der Staat eng beim IT-Schutz dieser Infrastrukturen zusammenarbeiten. Dieser kooperative Gedanke hat sich bewährt und wird mit der Cyber-Sicherheitsstrategie explizit fortgeführt.

Der IT-Schutz Kritischer Infrastrukturen hat im Bundesministerium des Innern höchste Priorität. So hat Bundesminister Dr. Friedrich Vorstandsvorsitzende und Wirtschaftsverbände zu Gesprächen eingeladen. Es ist wichtig, dass sich alle Branchen explizit und umfassend um die Sicherheit ihrer von IT-abhängigen kritischen Geschäftsprozesse bemühen. Wir brauchen bundesweit einheitliche Mindeststandards und zuverlässige Meldewege, um bei IT-Vorfällen eine schnelle Information und Reaktion aller Betroffenen sicherzustellen. Außerdem müssen wir auch die Branchen und Unternehmen der Kritischen Infrastrukturen, die noch nicht Teilnehmer des Umsetzungsplans Kritis sind, in die Strukturen integrieren.

Die zunehmende Durchdringung der IT hat dazu geführt, dass auch andere Bereiche der Wirtschaft, die bisher noch nicht in den Informationsaustausch mit dem BSI einbezogen waren, Hilfe angeboten werden soll. Das BSI ergänzt in einer auf der CeBit angekündigten Kooperation mit dem BITKOM unter dem Titel „Allianz für Cyber-Sicherheit“ den kooperativen Ansatz für nichtkritische Infrastrukturen. Auch die Aufsichtsbehörden über Betreiber Kritischer Infrastrukturen spielen eine wesentliche Rolle. Neben ihrer Einbindung in die Zusammenarbeit im Nationalen Cyber-Abwehrzentrum werden wir gemeinsam mit ihnen prüfen, welche Schutzmaßnahmen den Betreibern ggf. vorgegeben werden müssen und an welchen Stellen wir zusätzliche Befugnisse in Form von Anordnungsmöglichkeiten brauchen. Ob und an welchen Stellen solche Regelungen auch im Falle eine IT-Krise notwendig werden könnten, werden wir auch mit den Betreibern Kritischer Infrastrukturen diskutieren.

Internationales

Ein weiteres Ziel der Strategie ist das „Effektive Zusammenwirken für Cyber-Sicherheit in Europa und weltweit“. So erarbeitet derzeit die EU-Kommission eine Europäische Strategie für Internetsicherheit. In die Diskussion von harmonisierten Mindeststandards in Europa oder auch der Notwendigkeit einer umfassenden europäischen CERT-Infrastruktur bringen wir deutsche Erfahrungen nicht zuletzt auch aus der nationalen Strategie aktiv ein. So wird von Deutschland beispielsweise auch eine Arbeitsgruppe geleitet, die Mechanismen für eine Koordination in IT-Lagen zwischen EU-Staaten erarbeitet.

Ebenso setzen wir uns für eine Stärkung des Mandats der Europäischen Agentur für Netz- und Informationssicherheit, „ENISA“ ein. Schwerpunkte der Mandatserweiterung sollten die Beratung und Überprüfung von IKT-Vorhaben von Kommission und Rat, Unterstützung bei europäischen Regulierungsvorhaben mit IT-Sicherheitsbezug und die Unterstützung bei Aufbau und Betrieb eines zentralen Cert für die EU-Institutionen sein. Ein weiteres wesentliches Ziel unserer internationalen Aktivitäten ist die Verhandlung von Verhaltensregeln für Staaten im Cyber-Raum, die sogenannten „Norms of State Behavior in Cyberspace“.

Die Etablierung eines von möglichst vielen Staaten zu unterzeichnenden Kodex für staatliches Verhalten im Cyber-Raum, der auch vertrauens- und Sicherheitsbildende Maßnahmen umfasst, ist Teil der Cyber-Außenpolitik. Denn nur durch ein zwischen den Staaten abgestimmtes Vorgehen kann den Bedrohungen für den Cyberraum effektiv begegnet werden. Wir sprechen uns dafür aus, die Verhaltensregeln im Cyber-Raum

zunächst im Rahmen eines politisch verbindlichen VN-Verhaltenskodex zu vereinbaren.

Unser Ziel ist es, trotz und jenseits ideologischer Verwerfungen in einer differenzierten Welt eine rasche Verständigung im gesamtgesellschaftlichen Interesse aller Staaten zu erzielen. IT-Ausfälle jedenfalls dürften als reale Gefahr und globale Bedrohung eingeschätzt werden. Denn auch Länder, die nicht unsere Freiheitsmaßstäbe teilen, sind Teil des globalen Internets und damit sind auch deren Computersysteme und IT-gestützten Infrastrukturen grundsätzlich sehr verwundbar.

Wirtschaftsstandort Deutschland – Know-how-Schutz

Cyber-Sicherheit können wir heute nicht nur von der nationalen oder internationalen Warte betrachten, sondern müssen dies insbesondere als ein komplexes Geflecht unterschiedlicher Rahmenbedingungen ansehen – die zum Beispiel durch Datenschutzbestimmungen, Vernetzungen oder Virtualisierung konkurrieren. Durch die Konkurrenz in einer globalisierten Welt stehen auch deutsche Unternehmen unter stetigem Druck des internationalen Wettbewerbs. Problematisch wird es, wenn die für die Gewährleistung nationaler Cyber-Sicherheit wichtigen Nischenprodukte sich im internationalen Wettbewerb nicht behaupten können und somit auf dem nationalen Markt nicht mehr zur Verfügung stehen. Als Gründe werden oftmals eine fehlende Finanzierbarkeit bzw. die fehlende Wirtschaftlichkeit von Sonderlösungen genannt. Es gibt auch Fälle, bei denen aus Kostengründen IT-Sicherheitsaspekte in den Hintergrund gerückt werden mussten. Sensible Daten, sei es in Unternehmen oder in der Verwaltung, bedürfen eines besonderen Schutzes, der sich oftmals auch in den verwendeten IT-Produkten widerspiegelt. Der Staat wird daher prüfen müssen, inwiefern technologische Souveränität in Deutschland notwendig ist und wie wir diese erhalten bzw. fördern können.

Ausblick

Mit der Verabschiedung der Cyber-Sicherheitsstrategie für Deutschland hat die Bundesregierung ihren Handlungsrahmen zur Verbesserung der IT-Sicherheit in Deutschland abgesteckt. Die Umsetzung der Ziele wird seit Verabschiedung aktiv vorangetrieben. Durch gezielte Maßnahmen versuchen wir, IT-Sicherheits-Know-how in Deutschland zu erhalten. Aber: Der Staat allein kann Cyber-Sicherheit nicht gewährleisten. Zwar müssen die öffentlichen Verwaltungen von Bund, Ländern und Kommunen ihre Aufgaben wahrnehmen und ihre selbstbetriebenen Systeme adäquat schützen. Cyber-Sicherheit kann jedoch nur in einem umfassenden, kooperativen Ansatz verfolgt werden, der alle Akteure einbezieht. Wir brauchen ein Zusammenspiel aller gesellschaftlichen Gruppen und eine gemeinsame Übernahme von Verantwortung. Damit meine ich die nationale Verantwortung für die Gewährleistung von IT-Sicherheit auch durch Unternehmen. Es muss uns ein gemeinsames Anliegen sein, die technologische Souveränität und wissenschaftliche Kapazität Deutschlands auf dem Gebiet der Informations- und Kommunikationstechnik zu stärken, weiterzuentwickeln und vertrauenswürdige Produkte am Standort Deutschland zu produzieren.

Cornelia Rogall-Grothe *ist Staatssekretärin im Bundesministerium des Innern und Beauftragte der Bundesregierung für Informationstechnik.*

Datenschutz und Datensicherheit in der Energieversorgung

Bernd Kowalski

Die Ursachen für Cyber-Risiken sind vielfältig. Zu ihnen gehören neben der steigenden Komplexität und Verbreitung der IT die Verbindung von Unternehmensnetzen mit dem Internet sowie neue Anwendungen und komplexe Patchprozesse. Täglich tauchen im Netz 43.000 neue Schadprogrammvarianten auf, die es abzuwehren gilt. Außerdem existiert ein Schwarzmarkt für Verwundbarkeiten. Diese Faktoren betreffen auch die IT im Energiesektor.

Die strategische Zielsetzung zur Erlangung von mehr Cybersicherheit in Deutschland verdeutlicht ein Kabinettsbeschluss vom Februar 2011. Demnach soll „Cybersicherheit auf einem der Bedeutung und Schutzwürdigkeit angemessenen Niveau gewährleistet werden, ohne den Nutzen des Cyber-Raums zu gefährden“. Die von der Bundesregierung entwickelte Sicherheitsstrategie lässt sich im Folgenden kurz umreißen:

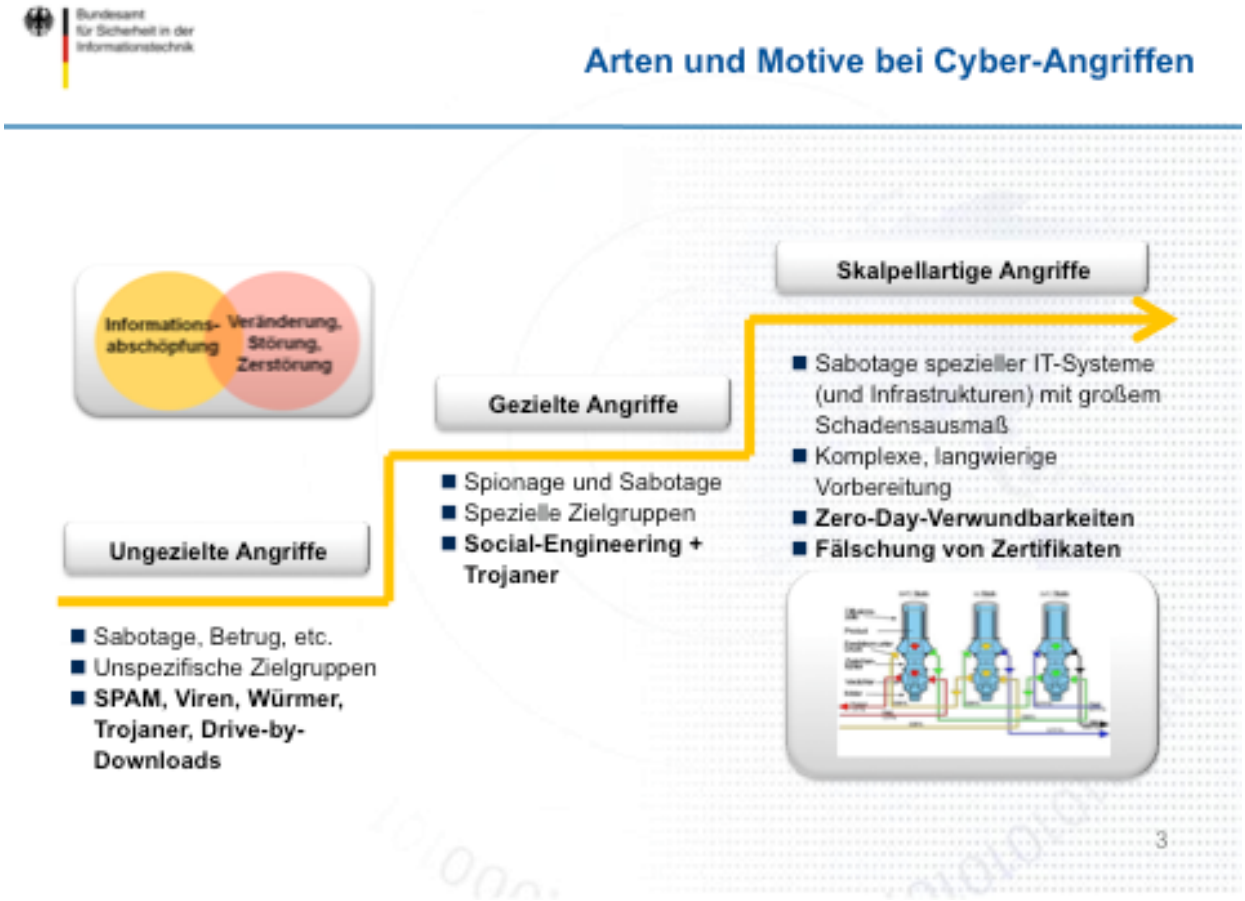

Abbildung: Arten und Motive bei Cyberangriffen

1. Schutz kritischer Informationsstrukturen

2. Sichere IT-Systeme in Deutschland

3. Stärkung der IT-Sicherheit in der öffentlichen Verwaltung

4. Nationales Cyber-Abwehrzentrum

5. Nationaler Cyber-Sicherheitsrat

6. Wirksame Kriminalitätsbekämpfung im Cyber-Raum

7. Effektives Zusammenwirken für Cyber-Sicherheit in Europa und weltweit

8. Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie

9. Personalentwicklung der Bundesbehörden

10. Instrumentarium zur Abwehr von Cyberangriffen

Erwartungen an das Intelligente Energienetz

Daraus folgern u. a. präventive Maßnahmen, die gesetzliche Verbindlichkeit von technischen Sicherheitsstandards für kritische Infrastrukturen wie beispielsweise das Intelligente Energienetz. Dazu bedarf es des Aufbaus einer sicheren IT-Infrastruktur zur Steuerung der Netze und ihrer Endeinrichtungen sowie der Gewährleistung von Datenschutz und -sicherheit.

Die Versorgungssicherheit, die zu den zentralen energiepolitischen Zielen der Bundesregierung gehört, stellt hohe Anforderungen an Verfügbarkeit, Qualität, Widerstandsfähigkeit in Bezug auf Störungen und Krisenlagen und Wiederherstellbarkeit nach sogenannten Großstörungen.

Bezüglich der Datensicherheit und des Datenschutzes benötigen Netzbetreiber und Lieferanten zum einen unverfälschte Daten über Verbrauch und Einspeisung, um so den Energiebedarf und sein Angebot zu steuern. Zum anderen sehen viele Kunden ihre Privatsphäre durch spezifische Verbrauchsprofile bedroht. Somit gehört zu dem wesentlichen Erfolgsfaktoren bei der Einführung von Smart Metering die Umsetzung von Daten- und Verbraucherschutzmaßnahmen. Des Wieteren muss eine Ausfallsicherheit des Energieversorgungsnetzes gewährleistet sein.

Der Einsatz von Smart Meter ist aus Sicht des Bundesamtes für Sicherheit in der Informationstechnik notwenig, um ein bedarfs- und angebotsgerechtes Lastenmanagement und eine Energieverteilung im Verteilnetz zu gewährleisten. Wegen der Verarbeitung von sensiblen Daten müssen Smart Meter jedoch besonders hohen Sicherheitsanforderungen genügen.

Rolle der Messsysteme

Die Einführung der modernen Messsysteme, die auf der EU-Richtlinie 2009/72 (Strom), 2009/73 (Gas) und in der nationalen Umsetzung auf dem Energiewirtschaftsgesetz von 2011 basieren, wird u.a. durch die Verpflichtung zum Einbau in Neubauten und bei größeren Renovierungen, bei Verbräuchen von über 6000 kWh sowie bei EEG und KWKG-Neukunden, die mehr als sieben Kilowatt verbrauchen, vorgeschrieben.

In der Zwischenzeit wurde mit der Erarbeitung eines Schutzprofils für die intelligenten Messsysteme begonnen, deren breite Einführung die Europäische Union von den Mitgliedstaaten verlangt. Das Schutzprofil ist in dem von der Bundesregierung im Juni 20122 verabschiedeten Energiepaket verankert. Es stellt strukturiert Bedrohungen für den siche-

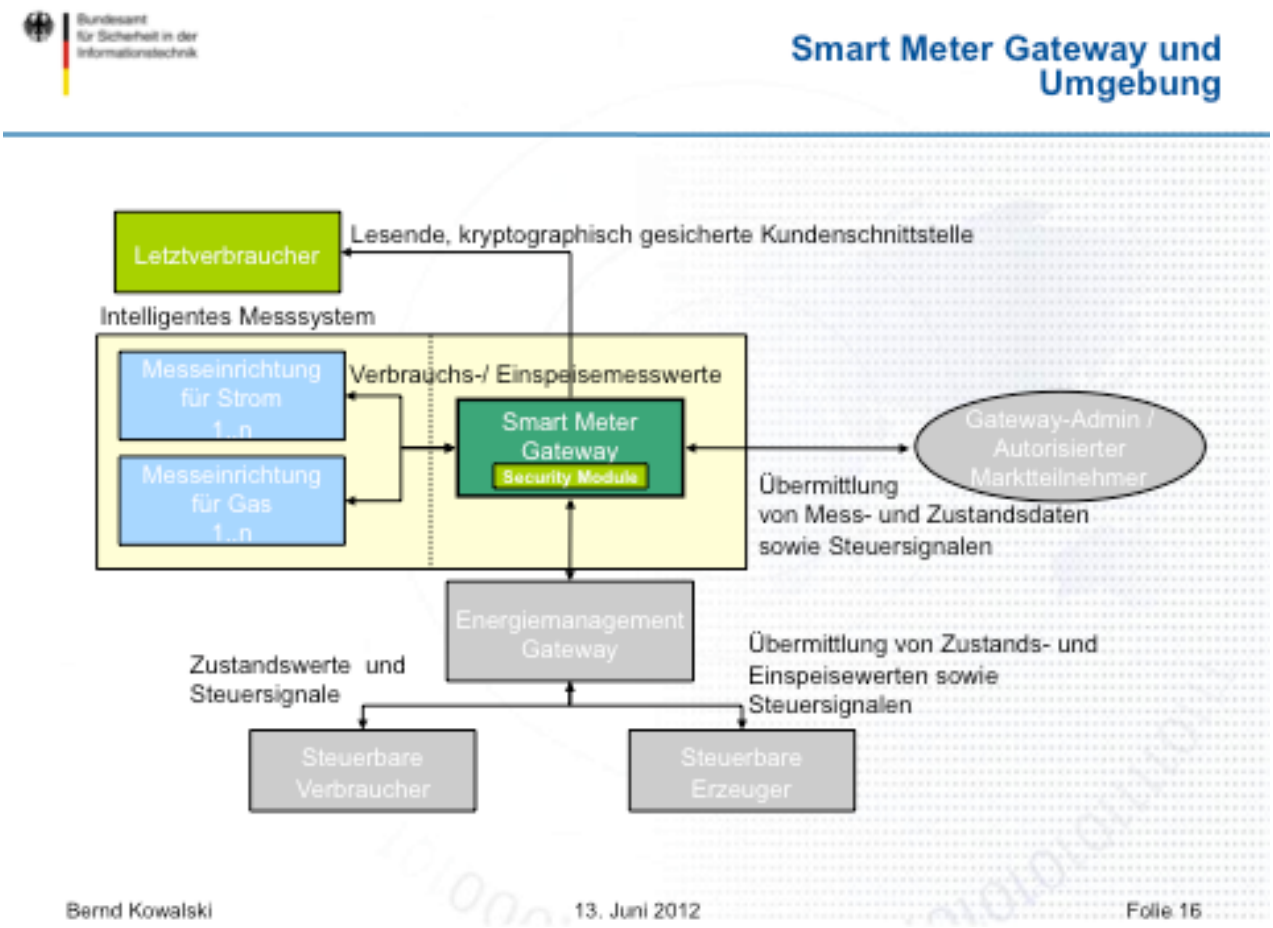

Abbildung: Smart Meter Gateway und Umgebung

ren und datenschutzfreundlichen Betrieb dar und legt Mindestanforderungen für entsprechende Sicherheitsmaßnahmen fest. So können Produkte geprüft werden, ein Zertifikat erhalten und somit das Schutzziel erfüllt werden. Das Profil ermöglicht dem Hersteller einen entsprechenden Spielraum bei der technischen Ausgestaltung, was auch bei unterschiedlicher Ausführung einen einheitlich hohen Sicherheitsstandard eine kontinuierliche Innovation der Produkte ermöglicht.

Gateway als zentrale Einheit

In einem Smart-Metering-System bietet das Gateway die zentrale Einheit, die Messdaten von Zählern empfängt, speichert und sie für Marktteilnehmer aufbereitet. Das Gateway kommuniziert dabei zur Verbraucherdatenüberragung wie auch zu seiner Administration mit verschiedenen Komponenten und beteiligten Parteien im Smart-Metering-Netz als Teil eines Smart Grids. Im Hinblick auf die besonderen Sicherheitsanforderungen werden insbesondere die Kommunikationsflüsse zwischen dem Gateway und den übrigen Komponenten und beteiligten Parteien des Smart-Metering-Systems auf kryptographischem Weg im Hinblick auf Integrität, Authentizität und Vertraulichkeit abgesichert.

Künftig wird es dezentrale – Gateway – wie auch zentrale – nachgelagerte Systeme –

Tarife geben. Das Konzept ist flexible in Bezug auf die Granularität der zu erhebenden Daten gestaltet. Es können zudem zeit-, last- und verbrauchsorientierte Tarife modelliert werden.

Zusammenfassend lässt sich sagen, dass die Zertifizierung nach dem CC-Standard für die Hersteller die Möglichkeit eröffnet, internationale Anerkennung und Vermarktung zu erlangen. Der vorgegebene Rechtsrahmen und die technischen Standards ermöglichen eine Planungs- und Investitionssicherheit, wobei sich die Energienetzbetreiber mit neuen Marktrollen auseinandersetzen müssen.

Bernd Kowalski *ist Leiter der Abteilung Sichere elektronische Identitäten, Zertifizierung und Standards beim Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn.*

Wie sicher sind die Rechenzentren?

Reinhold Harnisch

In zunehmendem Maße fragt sich die besorgte Öffentlichkeit, aber auch insbesondere die öffentliche Verwaltung, wie es mit der Sicherheit im Cloud-Zeitalter aussieht. Immer neue Szenarien der Bedrohung werden bekannt. Die jüngsten Sicherheitslücken auch in namhaften Produkten geben zu großer Sorge Anlass. Ganz besonders intensiv beschäftigen sich mit der IT-Sicherheitsfrage natürlich die entsprechenden Stellen auf Bundes-, Landes- und Kommunalebene und deren IT-Serviceprovider.

Das Kommunale Rechenzentrum Minden-Ravensberg/Lippe (krz) als einer der größten Selbsthilfeeinrichtung für Städte, Kreise und Gemeinden in NRW befasst sich seit längerem intensiv mit der Bedrohung der IT-Sicherheit und hat sich bereits vor sieben Jahren dazu entschlossen, die BSI-Zertifizierung nach ISO-27001 auf Basis von IT-Grundschutz durchzuführen.

Davon profitieren drei Kreise, 34 Städte und Gemeinden mit ca. 900.000 Einwohnern im Zweckverband sowie diverse Eigenbetriebe, Werke, gemeinnützige Vereine und Gesellschaften ebenso wie die Kooperationen in Ostwestfalen-Lippe und den Datenzentralen in Siegen und dem Rhein-Erft-Rur-Gebiet. Darüber hinaus beziehen ca. 600 Kommunale An-wender in dreizehn Bundesländern die Leistungen des Lemgoer Serviceproviders. Direkt oder indirekt werden damit über 9 Millionen Einwohner in NRW mit Services des krz betreut. Das krz ist eine Körperschaft des Öffentlichen Rechts in der Form eines kommunalen Zweckverbandes. Der Sitz ist in Lemgo.

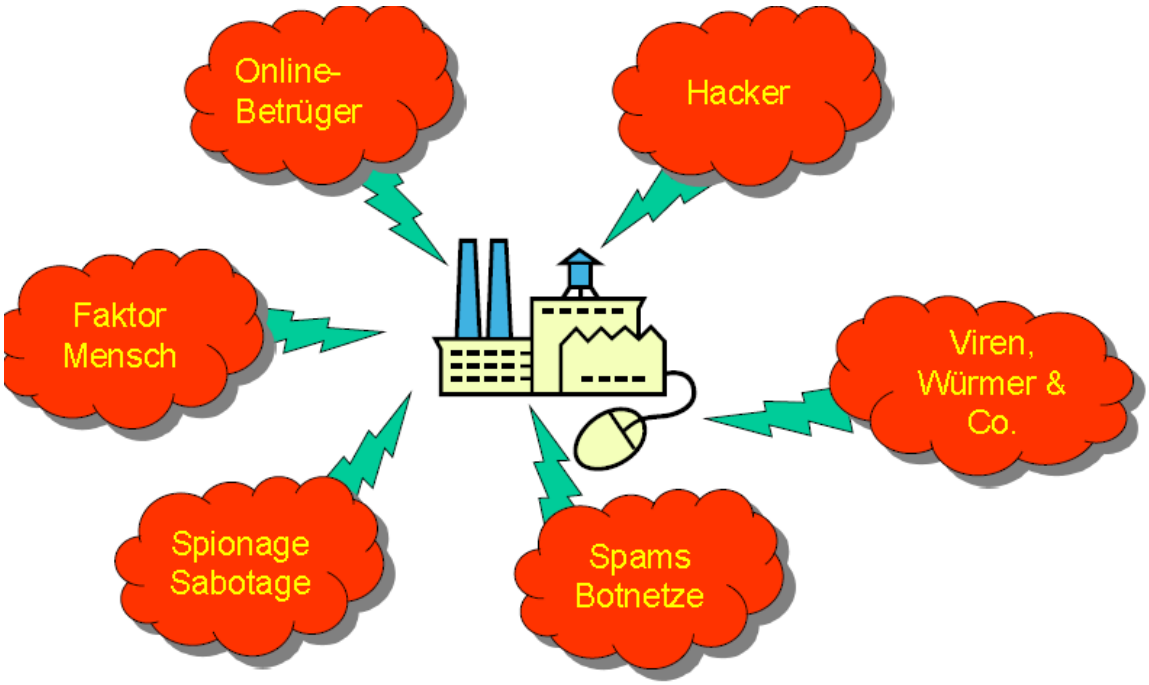

Abbildung: Bedrohungsszenarien

Wie sehen die konkreten Bedrohungs-Szenarien aus?

Wirtschaftsspionage, staatliche Ermittlungen, militärische Interessen, kriminelle Internetkonzerne, Neugier, „spielerische Herausforderung“, Langeweile und Frust sind als Motivatoren auszumachen. Dabei sprechen laut Eugene Kaspersky vom gleichnamigen Anti-Viren-SW-Anbieter „die meisten Schadprogramme Chinesisch!“

Es gibt eine Vielzahl von Bedrohungsszenarien, die sich grafisch wie folgt darstellen lassen:

Vor diesem Hintergrund stellt sich insbesondere die Frage nach der IT-Sicherheit beim Thema „Cloud Computing"? Dabei werden die Probleme beim Megathema Cloud-Computing z. B. von Amazon, Google, IBM, Microsoft am sichtbarsten.

Für den Betrieb von (Public)-Clouds fehlt es bisher an tragfähigen Konzepten zu Datenschutz und -sicherheit. Dabei gibt es insbesondere bei Schnittstellen gefühlte Sicherheitsbedenken. Ein wünschenswerter „Cloud-Datenschutz“ gilt derzeit aufgrund globalisierungsbedingter Durchsetzungsdefizite grundsätzlich als problematisch.

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) weist in seinem Lagebericht 2011darauf hin, dass international anerkannte Standards zu erarbeiten und zu etablieren sind, auf deren Grundlage Cloud Computing-Plattformen sicherer genutzt und betrieben sowie überprüft und zertifiziert werden können. „Wer heute in einer Public Cloud Personendaten verarbeitet, handelt regelmäßig unverantwortlich und rechtswidrig“, so auch Thilo Weichert, Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD).

Im Gegensatz zur Public Cloud betreiben heute Einrichtungen wie das krz bereits Private Clouds („private Clouds“). Im Prinzip greifen die kommunalen Rechenzentren damit auf Erfahrungen zurück, die über 40 Jahre zurückreichen. So unterstützt der Lemgoer IT-Dienstleister wirtschaftlich und sicher die betreuten Kommunen mit Fachanwendungen und Querschnittslösungen aus einem geschlossenen Netz.

Wichtig dabei ist, dass anerkannte Standards der IT-Sicherheit nicht nur proklamiert, sondern auch zertifiziert sind. Dazu gehört aber auch, dass die Datenhoheit öffentlich-rechtlich organisiert ist, entsprechend integriert (Single Point of Contact) und konsequent am standardisierten IT Service Management (ITSM am Rahmenwerk IT Infrastructure Library V3 -ITIL) ausgerichtet ist. Vor allem aber sind dadurch die Mitarbeiterinnen und Mitarbeiter sensibilisiert, und werden permanent bei den Themen Datenschutz und IT-Sicherheit weitergebildet.

Welche Maßnahmen sind notwendig?

Die bereits angeführten Angriffe auf die IT-Sicherheit führen auf allen staatlichen Ebenen zu Konsequenzen. Dabei muss berücksichtigt werden, dass wichtige IT-Komponenten aktuell im Ausland hergestellt werden wie z. B. Betriebssysteme, Internet-Router, Computerchips und Netzausrüstungen.

Ist dieser Vorsprung der globalen Anbieter noch aufholbar und kann die Kontrolle über diese wichtigen Komponenten zurück gewonnen werden? Nationale Arbeitskreise sollen Antworten auf diese Frage finden. Der Bund richtet Kompetenzzentren für IT-Sicherheit in Saarbrücken, Darmstadt und Karlsruhe ein. Das BSI baut das Cyber-Abwehrzentrum mit

derzeit 10 Mitarbeitern auf; das NRW-Cybercrime-Kompetenzzentrum LKA mit 100 Mitarbeitern befindet sich ebenfalls in der Entstehung.

Ferner stellt der Bund 30 Millionen für Forschung im Bereich IT-Sicherheit bereit und richtet die Task-Force „IT-Sicherheit in der Wirtschaft“ ein. Dabei sind laut BITKOM, dem Branchenverband der IT-Wirtschaft, rund drei Viertel der kritischen Infrastrukturen sind in privater Hand.

Dazu erklärt Horst Flätgen, Vizepräsident des BSI: Das BSI betreibt mit seinem Computer-Emergency-Response-Team (CERT) und dem Nationalen Cyber-Abwehrzentrum in Bonn eine Art Frühwarnsystem des Bundes. Er macht aber auch darauf aufmerksam, dass eine vergleichbare Institution auf Länderebene nicht existiert. Einen „direkten Draht“ zu den Kommunen gibt es erst recht nicht.

Auch Franz-Reinhard Habbel, Sprecher des Deutschen Städte- und Gemeindebundes, schätzt die Gefahr realistisch ein: Der Bund ist für viele internationale „Bedroher“ interessant, wobei unterschiedlichste Gefährdungstatbestände existieren. Einheitliche Sicherheitsstandards für ebenübergreifende Fachanwendungen und ein einheitliches IT-Sicherheitsmanagement durch Etablierung von Verantwortlichen für die Umsetzung der Sicherheitsziele auf allen Ebenen ist erforderlich. Wir können nicht jede kleinste Kommune wie Fort Knox sichern. Deshalb verlangen die Kommunen bei der Verabschiedung von Leitlinien zur IT-Sicherheit auch ein Mitspracherecht ihrer Verbände.

Es gibt drei Ebenen, auf denen IT-Sicherheit umzusetzen ist.

Auf der Bundesebene beschäftigt sich der IT-Planungsrat mit den Schwerpunkt-Themen „IT-Sicherheit“ und „Nationale E-Government-Strategie“. Auf Landesebene (hier am Beispiel NRW) gibt es verschiedene Projekte wie z. B. IDV (Integriertes Datenverarbeitungssystem Verbraucherschutz).

In Berlin und Düsseldorf werden die IT-Grundschutzhandbücher des BSI bei den entsprechenden Ausarbeitungen zugrunde gelegt. Auch IT.NRW, der IT-Dienstleister des Landes, wendet bei der technischen Administration grundsätzlich die empfohlenen BSI-Maßnahmen an. Im Übrigen empfehlen auch die Datenschutzbeauftragten der Länder die Anwendung von BSI-Grundschutz.

Schwierig wird die Situation auf der kommunalen Ebene. Dazu Dr. Marianne Wulff, Geschäftsführerin von VITAKO, der Bundesarbeitsgemeinschaft der kommunalen IT-Dienstleister: „Im kommunalen Bereich sind die Folgen von Gesetzen und Verordnungen in der Regel am stärksten spürbar. Doch werden im legislativen Prozess weder die Konsequenzen für die Arbeitsprozesse noch die hochkomplexen IT-Infrastrukturen berücksichtigt“.

Entsprechend hat VITAKO in der Facharbeitsgemeinschaft IT-Sicherheit und Datenschutz u.a. einen generellen Fahrplan für die Einführung eines Informationsmanagementsystems (ISMS) nach BSI-Standards und IT-Grundschutz erarbeitet.

Kommunale IT-Dienstleister wie das krz bieten ihren Kunden Beratungs- und Auditangebote zur Informationssicherheit und Basis-Workshop-Pakete zum IT-Grundschutz als Einstieg in ein rechtssicheres Informations-Sicherheits-Management-System an. Begleitet wird das Vorgehen nach BSI-Grundschutz bei leistungsfähigen IT-Dienstleister durch ei-

ne entsprechende Infrastruktur mit den Komponenten:

- 2-Häuser-Konzept
- Notstromversorgung
- Verschlüsselung
- Virenschutz
- Spamfilter
- URL-Filter
- Firewalls und Applikation-Firewalls
- Mobile Device Management

Das hört sich alles kompliziert an – und ist es auch. Wenn man sich allein vor Augen führt, dass z. B. das krz täglich über 160.000 Spam-Mails abwehrt, wird deutlich, das nur eine Konzentration der Kräfte zu einer ausreichenden IT-Sicherheit führt. Nicht umsonst stellt Prof. Andreas Engel, Geschäftsführer des KDN, fest: „Wir erleben eine Renaissance der IT-Dienstleister“.

Fazit

Der Aufbau eines föderalen verwaltungsinternen Warn- und Informationsdienstes (Cert-Verbund) ist für die IT-Sicherheit von besonderer Bedeutung. Das Vorgehen nach BSI-Grundschutz ist der richtige Weg für ein Mindestsicherheitsniveau und bietet damit die Möglichkeit auf einer ersten Stufe für unterschiedliche Ebenen einheitliche Sicherheitsstandards zu erreichen.

Eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz stellt für Rechenzentren nicht nur ein wichtiges Qualitätsmerkmal dar, sondern gilt z. B. als Voraussetzung für den Betrieb eines eID-Servers. Auch die elektronischen Funktionserweiterungen des neuen Personalausweises (nPA) werden nur von Bürgern und Unternehmen angenommen, wenn ihre Daten sicher sind.

Zwar hat Joachim Ringelnatz, deutscher Schriftsteller und Kabarettist, einmal formuliert „Sicher ist, dass nichts sicher ist. Selbst das nicht!“ Durch gemeinsames Handeln wird es aber gelingen, ein Höchstmaß an Sicherheit zu gewährleisten. Im Interesse der Bürgerinnen und Bürger, der Verwaltungen und der Wirtschaft.

Reinhold Harnisch *ist Geschäftsführer des Kommunalen Rechenzentrums Minden-Ravensberg/Lippe (krz), Lemgo und stellvertretender Vorstandsvorsitzender der Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e.V. VITAKO, Berlin*

Sicherheit im Smart Grid

Claudia Eckert

Zusammenfassung

Der Artikel stellt ein Vorgehen zur Entwicklung von Sicherheitsarchitekturen vor, in dem die unterschiedlichen Sichten und Bedürfnisse von Beteiligten eines Smart Grids systematisch in Domänen erfasst werden. Für jede Domäne werden dann anhand ausgewählter Anwendungsfälle die wichtigsten Rollen der beteiligten Akteure mit ihren jeweiligen Rechten und Pflichten beschrieben. Dies ermöglicht es, die Sicherheitsanforderungen aus den verschiedenen Sichten der Beteiligten systematisch abzuleiten. Dies bildet die Basis für die Entwicklung von Sicherheits-Referenzarchitekturen, die auf diese domänenspezifischen Anforderungen zugeschnitten sind. Diese Referenzarchitekturen können spezifizieren, an welchen Stellen, welche Verfahren und Kontrollen notwendig sind, um die erfassten Sicherheitsanforderungen durchzusetzen, ohne jedoch bereits dedizierte Technologien festzuschreiben. Mit den Referenzarchitekturen für Subsysteme der verschiedenen Domänen können zudem die Schnittstellen für den Domänenübergang auf einem geeigneten Abstraktionsniveau festgelegt werden. Die vorgestellte Methodik verfolgt den Ansatz, Sicherheitsbasismechanismen und Kontrolldienste qua Design in Sicherheitsarchitekturen zu integrieren, aber über eine klare Trennung von Mechanismus und Regelwerk Freiheitsgrade zu belassen, so dass diese Mechanismen flexibel, angepasst und anpassbar genutzt werden können, um unterschiedliche Sicherheitsanforderungen zu erfüllen. Anhand der Domäne Privatkunde und Verteilnetze wird die vorgeschlagene Vorgehensweise anhand von Beispielen erläutert. Der Artikel basiert auf Arbeiten im Rahmen des NEWISE-Projekts der Alcatel-Lucent Stiftung. Eine ausführliche Darstellung des Ansatzes wurde in der Schriftenreihe der Stiftung veröffentlicht[1].

1 Einleitung

Die Verknappung der fossilen Energiequellen und die ungelöste Umweltproblematik der Nuklearenergie erfordern nachhaltig wirkende Lösungen, um den steigenden Energiebedarf zu befriedigen und gleichzeitig die Umwelt zu schonen. Notwendig sind Energie-Systeme zur breitflächigen Nutzbarmachung erneuerbarer Energien und die systematische Umsetzung von Energiesparmaßnahmen. Im Gegensatz zu konventionellen Energiequellen weisen aber erneuerbare Energiequellen wie Wind, Sonne oder Wasserkraft ein stark Zeit variantes Verhalten auf und können nur gekoppelt mit Energiespeicherverfahren zum Einsatz kommen. Die klassische Lösung eines Verbundes von Grundlast- und zugeschalteten Spitzenlast-Kraftwerken mit einer hierarchischen Verteilung von Energie zur Verteilnetzebene muss strukturell verändert werden, da erneuerbare Energien beispielsweise durch Photovoltaikanlagen auch auf Verteilnetzebene eingespeist werden und damit die Energiegewinnung nicht mehr hierarchisch, sondern dezentral erfolgt. Dies erfordert eine geeignete IKT-Infrastruktur zur Steuerung des Energietransports. Die Kombination der Energietechnik mit der IKT wird auch als Energieinformationsnetz oder im Englischen als Smart Grid bezeichnet.

[1] Bericht Nr. 93 unter http://www.stiftungaktuell.de

Das Energieinformationsnetz ist eine sicherheitskritische Infrastruktur, deren Ausfall oder (partielle) Störung gravierende gesellschaftliche und volkswirtschaftliche Schäden nach sich zieht. Neben den erforderlichen Netzen, um Daten rechtzeitig, korrekt, Privatsphären-bewahrend, vertraulich, vollständig (aus Sicht des Dienstes, der die Daten benötigt) und sicher zwischen allen beteiligten Parteien auszutauschen, werden auch dezentral betriebene, kooperative Managementsysteme zur sicheren Steuerung von Netzkomponenten und dem Informationsaustausch über Betreibergrenzen hinweg benötigt. In einem Smart Grid müssen verschiedene Teilsysteme, wie Kraftwerke, Energiemanagementsysteme oder auch Abrechnungssysteme mittels Kommunikationstechnologien in einem Kommunikationsnetz zusammengeführt werden. Wie das bekannte Internet verbindet dieses Kommunikationsnetz somit verschiedene Teilnetze. Um Sicherheit und Stabilität des Energieinformationsnetzes zu gewährleisten, wäre es wünschenswert, wenn dieses Kommunikationsnetz zumindest logisch getrennt vom bekannten Internet aufgebaut würde, auch wenn auf der physikalischen Ebene allein schon aus ökonomischen Gesichtspunkten in weiten Bereichen auf bestehende Kommunikationsnetze zurückgegriffen werden wird.

Komplexe vernetzte Systeme sind bereits heute einer Vielzahl von Angriffen ausgesetzt. Dies gilt zunehmend auch für Industrielle Kontroll-Systeme, wie der Stuxnet Wurm [1] Mitte 2010 gezeigt hat. Im Kontext von Smart Grids sind hier insbesondere die Supervisory Control and Data Acquisition (SCADA) Systeme als mögliche Schwachstellen zu nennen. Solche SCADA Systeme sind auch in der Leittechnik und der Prozesssteuerung von Energienetzen sehr viel im Einsatz. Um Smart Grids angemessen vor Störungen und Missbrauch zu schützen, ist ein sicheres Energieinformationsnetz unerlässlich. Das Energieinformationsnetz kann dabei sowohl Angriffsziel als auch Mittel zur Durchführung eines Angriffs, also eine Art Tatwaffe sein. Ist das Energieinformationsnetz selbst Ziel von Angriffen, so kann es zu Störungen und Manipulationen bei der Datenübertragung kommen, so dass beispielsweise falsche Steuerdaten oder veraltete Steuerdaten eingespeist werden können und es zu einer Störung der Betriebs- bis hin zur Versorgungssicherheit kommen kann. Als Tatwaffe kann das Netz verwendet werden, um unter falscher Identität kriminelle Angriffe auf Versorger durchzuführen oder z.B. physische Anlagen zu schädigen. Eine wichtige Komponente im Smart Grid ist der digitale Zähler, der Smart Meter, der die Verbrauchsdaten in Haushalten und gewerblichen Gebäuden erfasst und an den Stromversorger übermittelt. Die korrekte Erfassung dieser Daten und die Möglichkeiten, zur Steuerung, um Lastspitzen zu vermeiden und um Lasten gezielt verschieben zu können, ist essenziell für eine zukünftige stabile und beherrschbare Energieversorgung. Im Hardwarelabor des Fraunhofer AISEC (vgl. www.aisec.-fraunhofer.de) in München wurden deshalb Sicherheitsanalysen an handelsüblichen Smart Metern durchgeführt. Die durchgeführten Angriffe auf Smart Meter haben gezeigt, dass digitale Zähler bereits durch sehr einfache Angriffe so manipuliert werden können, dass Daten eingeschleust, verändert, abgehört oder unterdrückt werden. So ist es leicht möglich, die Firmware inklusive aller gespeicherten kryptographischen Schlüssel auszulesen und beliebige Manipulationen vorzunehmen. Somit könnte sich beispielsweise ein Angreifer leicht kostenlose Energie ver-

schaffen oder mit einem gezielten Angriff einen sehr hohen Energiebedarf vorspiegeln und damit die Versorgungssicherheit eines ganzen Segments gefährden.

In einem Smart Grid agieren unterschiedliche Akteure mit sehr unterschiedlichen Aufgaben und Sicherheitsanforderungen, die zum Teil auch konträr sind. Aus Kundensicht ergeben sich beispielsweise Fragestellungen in Bezug auf dessen Privatsphäre, wenn sich aus den erhobenen Energieverbrauchsdaten sein Nutzungsverhalten ablesen lässt [8, 13]. Demgegenüber basieren neuere Geschäftsmodelle von Anbietern von Energie-Mehrwertdiensten häufig darauf, möglichst exakte Informationen über das Verbrauchsverhalten von Nutzern zu besitzen, um zugeschnittene Services anbieten zu können. Dies könnte damit auch für den Nutzer von Vorteil sein, wenn er solche personalisierten Dienstleistungen wünscht. Erforderlich sind somit Sicherheitsarchitekturen, die einen Interessensausgleich zwischen den unterschiedlichen Marktteilnehmern und deren Individualinteressen ermöglichen. Sicherheit muss von Beginn an („Secure by Design“) und auch während der Laufzeit („Secure during Operation“) elementarer Bestandteil von Smart Grids sein [6, 5].

Der Artikel ist wie folgt strukturiert. Kapitel 2 motiviert die Domänen-bezogene Sicht, die es ermöglicht, die unterschiedlichen Sichten und Bedürfnisse von Teilnehmern des Energiemarktes systematisch zu erfassen und damit die Komplexität der Aufgabenstellung zu reduzieren. In den Kapiteln 3 und 4 werden beispielhaft die Domänen Privatkunde und Verteilnetz betrachtet. Hierzu werden zunächst Grundlagen und die relevanten Anwendungsfälle vorgestellt, Sicherheitsanforderungen abgeleitet und abschließend eine mögliche Sicherheitsarchitektur beschrieben. Der Schwerpunkt liegt auf technischen Fragestellungen; betriebswirtschaftliche Fragestellungen wie Bilanzkreismanagement sind nicht Gegenstand des Artikels. In Kapitel 5 werden die wichtigsten Ergebnisse noch einmal zusammengefasst.

2. Domänen

Smart Grids sind in Bereiche aufgeteilt, in denen jeweils spezifische technische und ökonomische Geschäftsprozesse und Anwendungsfälle ablaufen. Solche Bereiche bezeichnen wir im Folgenden als **Domänen** (vgl Abbildung 1).

Unterschieden werden in der Regel die Domänen Erzeugung, Übertragung, Verteilung, Kunde, Märkte, Betrieb und Service [3]. Diese lassen sich noch in weitere Subdomänen unterteilen. Beispielsweise kann die Domäne „Kunde“ in Privat- / Haushaltskunde, Gewerbekunde oder Industriekunde untergliedert werden.

Jede der Marktteilnehmer ist in einer oder mehreren Domänen bzw. Sub-Domänen aktiv, wobei er in den verschiedenen Domänen unterschiedliche Aufgaben und Verpflichtungen haben kann. Um dies geeignet zu erfassen, führen wir **Rollen** ein. Mit jeder Rolle sind spezifische Sicherheitsanforderungen, sowie weitere, meist ökonomische Anforderungen verbunden. So möchte ein Endkunde in seiner Rolle als Energienutzer in der Domäne Privatkunde beispielsweise seine Privatsphäre gewahrt haben, während das Unternehmen, das in der Rolle Energielieferant in dieser Domäne aktiv ist, vordringlich an einer möglichst kostengünstigen Gesamtlösung interessiert ist. Dazu könnte auch gehören,

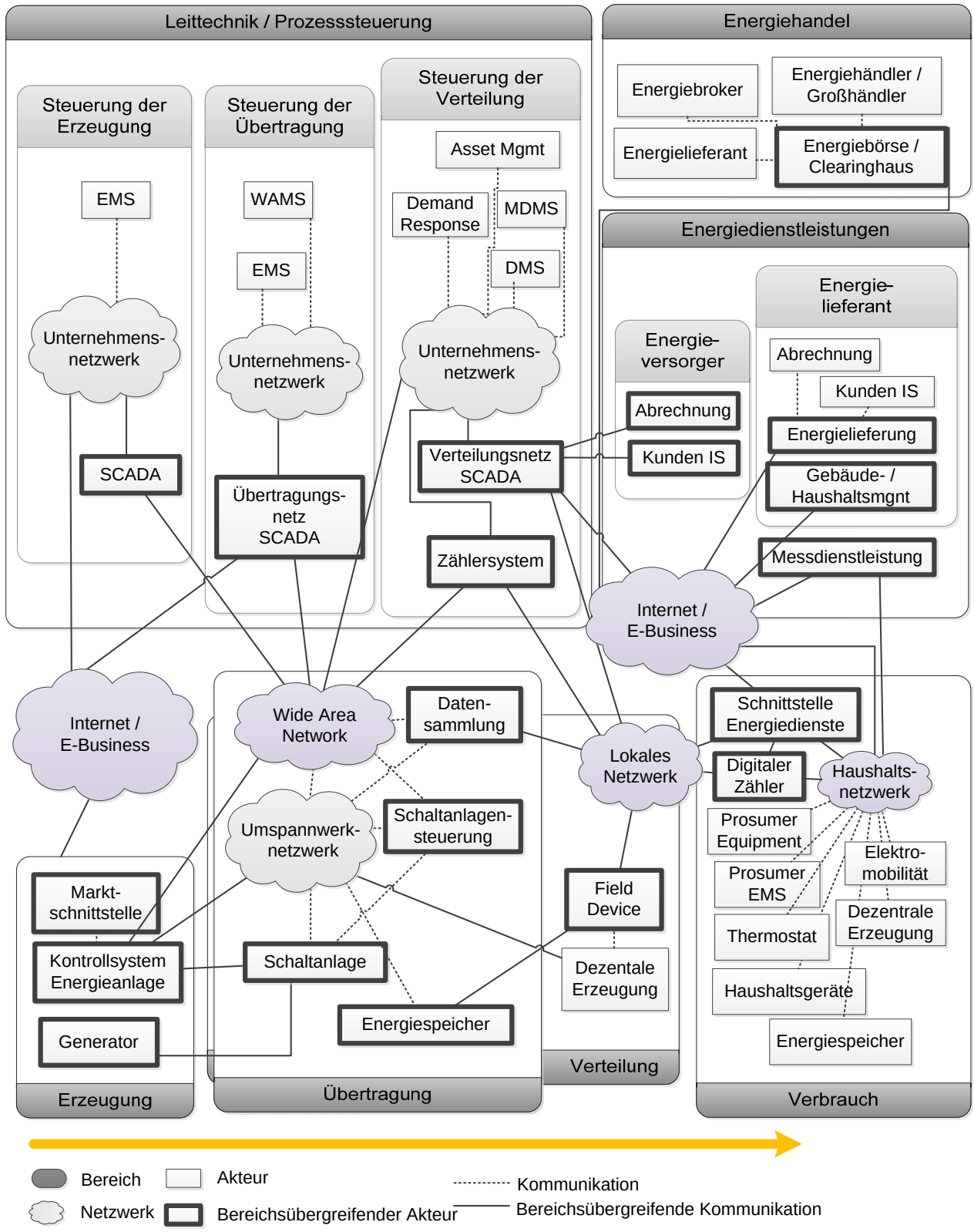

Abbildung 1 Konzeptuelles Modell eines Smart Grid[1]

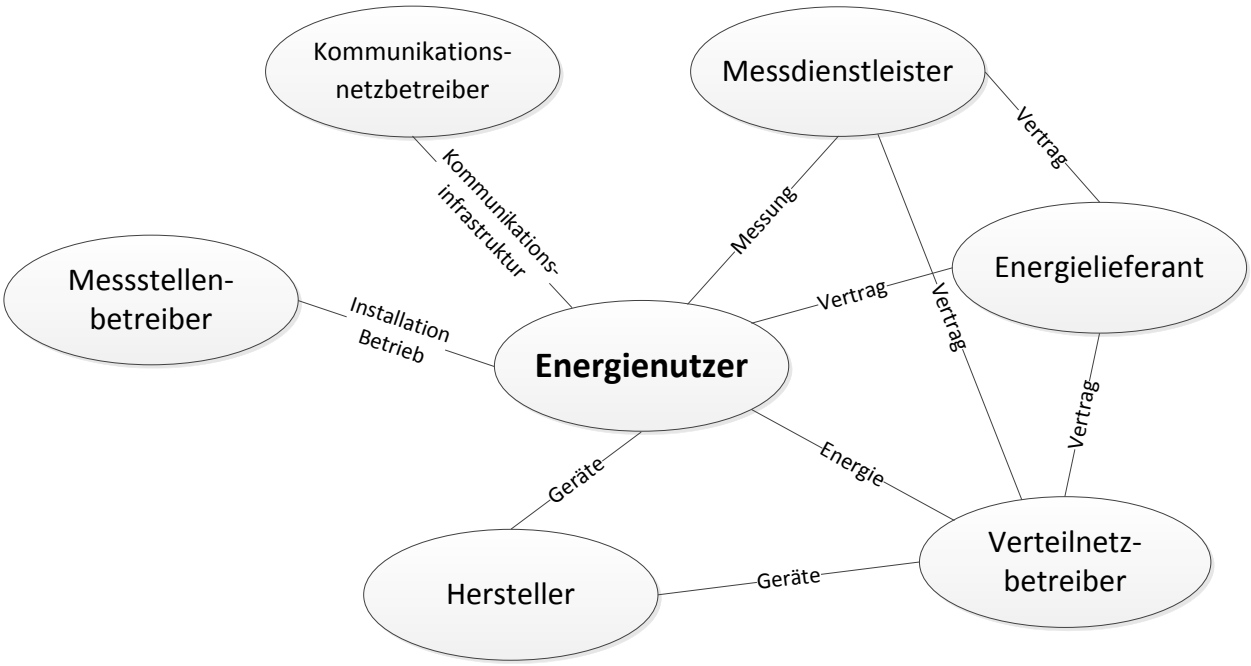

Abbildung 2: Rollen in der Domäne Privatkunde und deren Beziehungen

dass der Energielieferant zugeschnittene Mehrwertdienste anbieten möchte, wofür er ggf. detaillierte Informationen über das Nutzungsverhalten des Energienutzers benötigt. Dies könnte im Widerspruch zu dessen Wünschen stehen, dass seine Privatsphäre geschützt wird. Die Umsetzung der oftmals entgegen gesetzten (Sicherheits-) Anforderungen stellt eine große Herausforderung bei der Entwicklung von Sicherheitsarchitekturen in Smart Grids dar.

Um die Komplexität der Aufgabenstellung zu reduzieren, schlagen wir vor, die einzelnen Domänen differenziert zu betrachten und für jede Domäne generische Muster für Sicherheitsarchitekturen zu entwerfen, so dass auf dieser Basis systematisch Handlungsempfehlungen für die verschiedenen Marktteilnehmer eines Smart Grid abgeleitet werden können. Insbesondere in den Domänen *Privatkunde* (als Sub-Domäne der Domäne Kunde) und *Verteilnetz* wird ein großer Wandel vollzogen werden. Dies ist darin begründet, dass in Zukunft Energie vermehrt durch erneuerbare Energien und verteilt durch viele Produzenten erzeugt wird. Um mit der dezentralen Verarbeitung und den zu erwartenden höheren Schwankungen umgehen zu können und eine kontinuierliche Stromversorgung zu garantieren, ist ein vermehrter Einsatz von IKT notwendig. Es müssen Messungen von Angebot und Nachfrage von Energie durchgeführt werden und entsprechende Steuerungen durchgeführt werden. Im Folgenden skizzieren wir die Vorgehensweise auszugsweise an den Beispielen der Domänen Privatkunde und Verteilnetz.

3 Domäne Privatkunde

Die Subdomäne Privatkunde[2] der Domäne Kunde stellt aufgrund der vielen Hausanschlüsse eine wesentliche Komponente von Smart Grids dar. In der Domäne Privatkunde sind die folgenden Rollen relevant und können auch gleichzeitig in ihr aktiv sein: Energienutzer, Verteilnetzbetreiber, Energielieferant, Kommunikationsnetzbetreiber, Messstellenbetreiber, Messdienstleister, Hersteller und ggf. weitere Energiedienstleister. Abbildung 2 stellt die Rollen und deren Beziehungen untereinander vergröbert dar. Der Fokus liegt dabei auf dem Energienutzer, da dieser im Mittelpunkt der Domäne Privatkunde steht. Nicht direkt relevante Beziehungen werden der besseren Übersicht halber nicht dargestellt.

Der Privatkunde steht in der Rolle *Energienutzer* im Mittelpunkt dieser Domäne. In seinem häuslichen Umfeld sind Smart Meter und Gateways installiert. Diese Installation zählt zu dem Aufgabenbereich der Rolle *Messstellenbetreiber,* die auch den Betrieb gewährleisten und deren Rollenmitglieder, also die Mitarbeiter des jeweiligen Messstellenbetreibers, Wartungsarbeiten an den Smart Metern und Gateways durchführen. Im Rahmen der Aufgabenerledigung in der Rolle Messstellenbetreiber können beispielsweise für Wartungszwecke mittels Fernzugriff regelmäßig System-Updates auf die digitalen Zähler, die Smart Meter, in den Haushalten aufgespielt werden, so dass eine zeit- und kostenaufwändige Vorort-Wartung durch einen Servicetechniker weitestgehend entfallen kann. Die durch die Smart Meter erfassten Messwerte werden über ein Gateway an eine in der Rolle *Messdienstleisteragierende* Instanz gesendet, die diese einer in der Rolle *Energielieferanten* agierenden Instanz zu Abrechnungszwecken zur Verfügung stellt. Zwischen dem Energielieferanten und dem Energienutzer besteht ein Vertragsverhältnis über den Bezug von Energie. Hierbei tritt der Energielieferant als eine Art Wiederverkäufer auf, so dass auch ein Vertragsverhältnis mit einem *Verteilnetzbetreiber* besteht, welcher die Energie an den Energienutzer liefert. Alternativ könnte der Privatkunde auch direkt einen Vertrag mit einem Verteilnetzbetreiber abschließen, z.B. einem Stadtwerk, von dem er die Energie bezieht. Auch ist denkbar, dass der Messdienstleister dem Verteilnetzbetreiber direkt Messwerte zur Verfügung stellt, die dieser für interne Zwecke verwendet. Die Kommunikation aller Rollen untereinander wird durch einen oder mehrere *Kommunikationsnetzbetreiber* realisiert, die entsprechende Kommunikationsinfrastrukturen bereitstellen. Relevante Mitglieder der Rolle *Hersteller* sind beispielsweise Hersteller von Smart Metern oder von Geräten zur Heimautomatisierung.

Eine mögliche Netztopologie der Domäne Privathaushalt ist in Abbildung 3 dargestellt. Die linke Seite stellt einen Privatkunden in den beiden Rollen Energienutzer und Energielieferant, also als Prosumer, dar.

Beim Privatkunden sind Energieverbrauchs-Geräte (z.B. eine Waschmaschine), Energieerzeuger (z.B. die o.g. Photovoltaik-Anlage), Speicher (nicht dargestellt), Smart Meter, ein Gateway und ein internetfähiges Gerät, wie beispielsweise ein PC, installiert. Der Energieversorger repräsentiert zur Vereinfachung die Rollen Energielieferant, Verteilnetzbetrei-

[2] Im Folgenden sprechen wir als Vereinfachung auch häufig von der Domäne Privatkunde, auch wenn wir sie als eine Subdomäne der übergeordneten Domäne Kunde betrachten. Diese Unterscheidung ist aber für die weiteren Ausführungen unerheblich, so dass wir darauf verzichten.

ber, Messstellenbetreiber und Messdienstleister. Mit dem Energieversorger hat der Privatkunde einen Vertrag und bezieht über das Stromnetz Energie.

Die Messwerte über die verbrauchte und erzeugte Energie werden durch Smart Meter erfasst, an das Gateway gesendet und von dort zum Energieversorger weitergeleitet. In einem Mehrfamilienhaus kann beispielsweise ein einzelnes Gateway die Daten vieler Smart Meter bündeln und weiterleiten [11]. Alternativ können beispielsweise in einem Einfamilienhaus auch Smart Meter direkt in das Gateway integriert sein [2]. Das Gateway kann zusätzlich auch Funktionalitäten eines Energie-Management Gateways zur Heimautomatisierung bereitstellen. Neben Stromzählern können auch weitere Zähler wie Gas- oder Wasser-Zähler an ein Multi-Utility-Gateway angeschlossen sein, das die Messwerte von

zes auf die so genannten Hybridnetze wird derzeit intensiv diskutiert, da erhebliche Synergien zu erwarten sind, wenn man die verschiedenen Versorgungsnetze (Gas, Wasser etc.) gemeinsam betrachtet. Hybridnetze werden in diesem Artikel nicht weiter betrachtet.

Daten wie z.B. Messwerte oder Steuersignale werden zwischen Gateway und Energieversorger über das Energieinformationsnetz ausgetauscht, das von einem oder mehreren Kommunikationsnetzbetreibern betrieben wird. Der Energieversorger sorgt dafür, dass der Energienutzer mit Strom versorgt wird, Messwerte erfasst werden und Rechnungen gestellt werden. Er empfängt aktuelle Messwert oder sendet Daten wie aktuelle Verbrauchswerte oder Preisinformationen über das Energieinformationsnetz oder über das Internet an den Energienutzer.

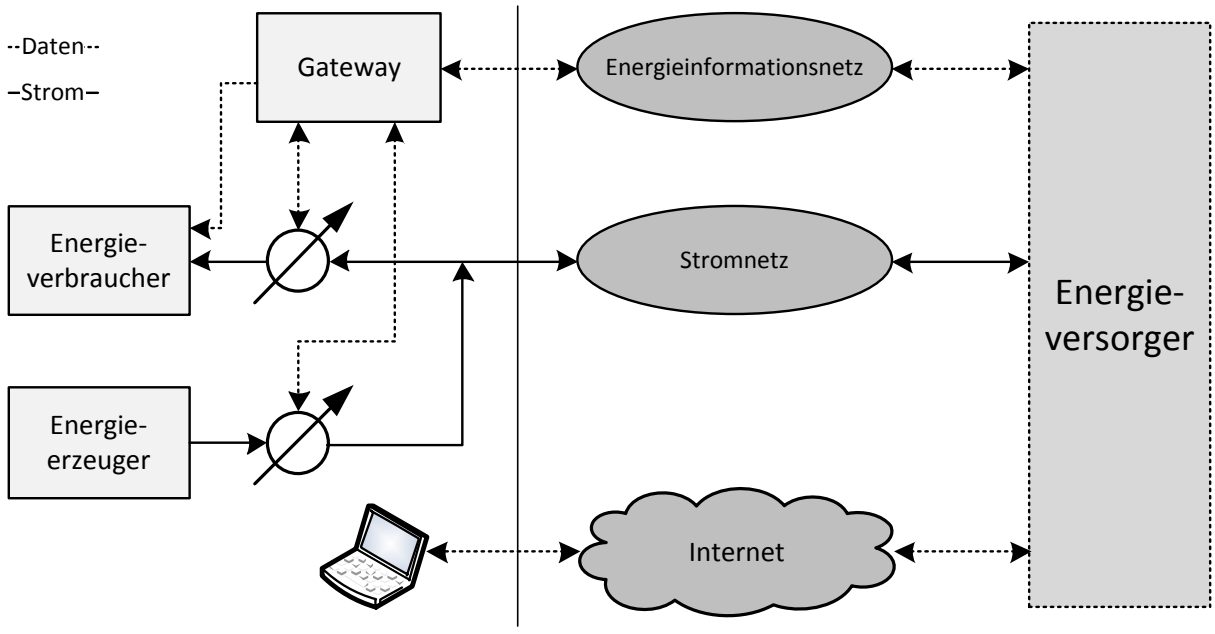

Abbildung 3: Netztopologie der Domäne Privathaushalt

Strom, Gas und Wasser sammelt und weiterleitet. Die Ausweitung des Smart Grid Ansat-

Anwendungsfälle

Im Folgenden werden mit der Messwerterfassung, der (Fern)-Wartung und der Tarifierung drei Beispiele für Anwendungsfälle (engl. Use Cases) (vgl. auch [10]) für die Domäne Privatkunde beschrieben und relevante Schutzziele identifiziert, um daraus anschließend die Sicherheitsanforderungen relevanter Rollen abzuleiten. In den Anwendungsfällen muss berücksichtigt werden, dass den Rollen auch gewisse Rechte und Pflichten zugeordnet sind, die sie erfüllen müssen. Beispielsweise sind gewisse Datenschutzanforderungen oder Protokollierungen gesetzlich vorgeschrieben.

Use Case: Messwerterfassung und -übertragung

Dieser Anwendungsfall beschreibt das Auslesen der Messwerte, um Rechnungen stellen zu können. Zu schützen ist die Vertraulichkeit der beim Kunden erfassten Messwerte (z.B. im Gateway), während der Übertragung und in den verschiedenen Datenbanken (Rechnungsdatenbanken). Hierbei sind insbesondere auch Datenschutzanforderungen zu erfüllen. Für eine korrekte Abrechnung müssen die Daten authentifiziert und integer sein. Das heißt, es ist sicher zu stellen, dass die Daten von einer eindeutig identifizierbaren Instanz stammen und nicht manipuliert wurden. Weiterhin muss eine gewisse Verbindlichkeit gewährleistet sein, so dass der Kunde die Korrektheit der Daten, auf deren Basis dann Rechnungen über den Stromverbrauch erstellt werden, nicht abstreiten kann. Grundsätzlich muss auch die Verfügbarkeit der Daten gegeben sein. Die entsprechenden Anforderungen sind jedoch nicht sehr hoch, da für einen korrekten Betrieb keine dauerhafte Verfügbarkeit der Daten oder eine Bereitstellung der Daten in Echtzeit erforderlich ist. Im Zusammenhang mit dem weiter unten angesprochenen Use Case Echtzeit-Tarifierung ist jedoch wichtig, dass die Messwerte korrekt dem bei der Nutzung gültigen Tarif zugeordnet werden.

Use Case: Fernwartung

Um die Managementkosten zu reduzieren, streben die Energieversorger eine Wartung von Geräten mittels Fernzugriffen an. Anstatt durch einen Mitarbeiter vor Ort soll die Energieversorgung unter Nutzung der installierten Smart Meter über das Energieinformationsnetz aktiviert oder aber auch deaktiviert werden können, z.B. wenn ein Mieter neu in ein Haus ein- oder auszieht. Hierzu werden entsprechende Steuernachrichten durch den Messstellenbetreiber an das Smart Meter bzw. Gateway gesendet. Es ist offensichtlich, dass derartige Aktivitäten, die einen direkten Einfluss auf die Energieversorgung eines Privatkunden haben, so zu schützen sind, dass kein unberechtigter Dritter gefälschte Aktivierungs- oder Deaktivierungsnachrichten an den Meter senden darf.

Smart Meter und Gateways müssen regelmäßig gewartet werden, z.B. müssen Firmware-Updates oder Patches installiert werden. Hierzu sendet der Messstellenbetreiber Steuersignale sowie Wartungsdaten wie Updates und Patches an die Geräte, um beispielsweise Sicherheitslücken zu schließen oder Konfigurationen an sich geänderte Bedingungen anzupassen.

Use-Case: Echtzeit-Tarifierung

Entsprechend der Angebots- und Nachfragesituation werden Energie-Preise variabel gestaltet und diese Preisinformationen über das Energieinformationsnetz, Internet oder andere Datenkanäle an den Kunden gesendet.

Dadurch erhält der Kunde die Möglichkeit, seine Energienutzung an den aktuellen Preis zu koppeln und seine Kosten zu reduzieren. Dieser Use-Case muss seit 30. Dezember 2010 nach dem Energiewirtschaftsgesetz (EnWG) [21] gemäß § 40 (5) EnWG[3] von Energieversorgungsunternehmen umgesetzt werden.

Insbesondere für den Verteilnetzbetreiber kann dieser Anwendungsfall relevant sein, um das Nutzungsverhalten des Energienutzers entsprechend der verfügbaren Energie zu beeinflussen. Für den Privatkunden können sich finanzielle Vorteile ergeben. Derzeit sind diese Vorteile zwar noch relativ gering [14], durch Einbindung von Elektrofahrzeugen ist aber zu erwarten, dass sich dies ändern wird. Bei der Abrechnung muss berücksichtigt werden, dass der Energielieferant den jeweiligen Messwerten die korrekten Preisinformationen zu Grunde legt. Hierzu ist es ggf. nicht mehr ausreichend, dass der Messdienstleister dem Energielieferanten aggregierte Messwerte zur Verfügung stellt. Dies muss in der Sicherheitsarchitektur bei der Umsetzung eines Datenschutzkonzeptes entsprechend berücksichtigt werden.

Rollen und deren Sicherheitsanforderungen

Basierend auf den sicherheitsrelevanten Anwendungsfällen, werden nun die Sicherheitsanforderungen für zwei ausgewählte Rollen beschrieben.

(1) Rolle: Energienutzer

Der Privatkunde in der Rolle als Energienutzer hat in der Regel hohe Anforderungen an den Datenschutz und an die Wahrung seiner Privatsphäre. Somit müssen Vertraulichkeit und der Schutz aller personenbezogenen bzw. personenbeziehbaren (Energie)-Daten gewährleistet sein, um die Erstellung von Nutzungsprofilen zu verhindern. Dies umfasst die Messwerte, Daten zur Abrechnung wie die Adaption an geänderte Preisinformationen, aktuelle Verbrauchsdaten, Statusmeldungen und Rechnungsdaten. Zum einen müssen die Daten gegen unberechtigte externe Dritte geschützt werden, angefangen bei der Erfassung, über die Übertragung, bis zur (ggf. langfristigen) Speicherung und Verarbeitung der Daten in (Rechnungs-) Datenbanken des Energielieferanten oder Messdienstleisters. Zum anderen sollten auch der Energielieferant und der Messdienstleister nicht in der Lage sein, Personenbezogene bzw. Personenbeziehbare Daten des Energienutzers auszuwerten. Diese Anforderung erscheint jedoch sehr restriktiv und erschwert oder verhindert zukünftige Geschäftsmodelle, die auch einen interessanten Nutzwert für Kunden haben könnten. So sind Szenarien denkbar, in denen der Energienutzer seinem Lieferanten ganz bewusst Personenbeziehbare Daten verfügbar macht und damit Profilbildungen durch diesen Lieferanten nicht nur in Kauf nimmt, sondern sogar unterstützt, weil für den Kunden damit Anreize wie Rabattierungs-Modelle etc. verbunden sind. Damit ergibt sich die Anforderung nach Maßnahmen und Dienstleistung, die eine nutzerkontrollierbare Weitergabe von personenbeziehbaren Energiedaten ermöglichen. Dies stellt besondere Anforderungen an das Design von Smart-Metern bzw. Gateways und den Zugangsgeräten zu diesen Komponenten. Es muss auf einfache Weise möglich sein, Datenschutz-Regeln zu formulieren und

[3] In der Fassung vom 04.08.2011 (geändert durch Artikel 1 G. v. 26.07.2011 BGBl. I S. 1554)

deren Einhaltung nachvollziehbar zu kontrollieren.

Eine weitere zentrale Anforderung der Rolle Energienutzer betrifft die Korrektheit der Abrechnungen. D.h. Messwerte müssen korrekt erfasst und ebenso wie Daten zur Abrechnung unverändert und vollständig, sowie zeitlich korrekt an den Energielieferanten oder Messdienstleister übertragen werden. Auch müssen die vom Kunden empfangenen Preisinformationen korrekt, aktuell und verbindlich sein. Alle Daten müssen eindeutig dem richtigen Kunden zugeordnet werden können. Die beim Energienutzer installierten IKT-Komponenten wie Smart Meter und Gateways müssen hierfür vor Manipulationen geschützt werden, d.h. die Integrität dieser Systeme muss gewährleistet sein. So muss die genutzte Software nachweislich unverfälscht über die gesamte Lebenszeit der Komponenten ihre Aufgaben erfüllen. Das bedeutet, dass die Komponenten insbesondere geeignete, nicht umgehbare Konzepte zur Abwehr von Manipulationsangriffen umfassen müssen, sowie auch die Möglichkeit unterstützen müssen, dass man die Fehlerfreiheit und Unverfälschtheit der Komponenten jederzeit, auch über Fernzugriffe, überprüfen kann. Die erforderlichen Schutzmaßnahmen müssen auch Angriffe, die einen physischen Zugriff erfordern, abwehren können, da ein solcher Zugriff u.a. für die Kunden stets möglich ist. Die Forderung der Unverfälschtheit erstreckt sich über die gesamte Zeit des Einsatzes der Komponenten und schließt natürlich die korrekte Installation und Wartung durch den Messstellenbetreiber mit ein.

Zusätzlich ist zu fordern, dass die Daten sicher zu autorisierten Empfängern übertragen werden. Dazu ist wiederum erforderlich, dass geeignete Maßnahmen ergriffen werden, die sicherstellen, dass die Daten unverfälscht, vollständig und rechtzeitig bei den korrekten Empfängern ankommen und dass der Datenursprung überprüfbar ist. Eine absichtlich oder unabsichtlich erfolgte, erneute Einspielung korrekter Datensätze muss ebenfalls erkannt und abgewehrt werden.

Die Forderung nach Authentizität und Integrität der Datenkommunikation bezieht sich nicht nur auf die von den Smart Metern bzw. Gateways gesendeten Daten, sondern natürlich auch auf die Daten, die vom Energieversorger an die Smart Meter bzw. Gateways oder über das Internet an Rechner des Kunden gesendet werden. Dies umfasst die aktuellen Verbrauchsdaten, Rechnungsdaten aber auch insbesondere kritische Steuernachrichten, bei denen ggf. auch noch die Aktualität wichtig ist, um beispielsweise Smart Meter zu aktivieren bzw. zu deaktivieren. Auch Wartungsdaten wie Firmware-Updates und Patches, die der Messstellenbetreiber oder der Energielieferant an die Geräte sendet und installiert, müssen einen Ursprungsnachweis führen und unverfälscht sein, damit Manipulationsversuche durch absichtlich oder unabsichtlich eingeschleuste Schadsoftware frühzeitig erkannt und abgewehrt werden können.

Neben den IKT-Komponenten von Smart Grids muss auch das eigentliche Stromnetz geschützt und die Versorgungssicherheit gewährleistet sein. Seit Jahren werden hierfür in der Energiewirtschaft etablierte Verfahren eingesetzt, auf die in diesem Artikel jedoch nicht weiter eingegangen wird. Durch die sehr starke Durchdringung der klassischen Energieversorgungsnetze mit IKT Komponenten zur Steuerung und Überwachung der Energieverteilnetze unterliegt jedoch auch die Bedrohungs- und Risikolage dieser Netze einem starken Wandel. So kann die eingesetz-

te IKT nicht nur angegriffen werden, sondern sogar als Tatwaffe gezielt missbraucht werden, um die Energieversorgung zu unterbrechen oder sogar mittelfristig zu gefährden. Das bedeutet, dass der Absicherung der eingesetzten IKT Komponenten in Zukunft ein sehr hoher Stellenwert zukommen wird, da es durch Angriffe auf die IKT-Komponenten bzw. durch die missbräuchliche Nutzung dieser IKT Komponenten potentiell zu Ausfällen oder Fehlsteuerungen der Energieversorgung für einzelne Regionen oder ggf. sogar kaskadierend für weite Landstriche kommen kann. Hierauf wird weiter unten noch einmal eingegangen.

(2) Rolle: Verteilnetzbetreiber

Wichtigste Anforderung eines Verteilnetzbetreibers ist sicherlich die Gewährleistung der Versorgungssicherheit, um die Energieversorgung im vertraglich zugesicherten Umfang sicherzustellen. Neben den etablierten Verfahren der Energiewirtschaft müssen auch Verfahren der IT-Sicherheit etabliert werden, um den neuen und erweiterten Angriffsmöglichkeiten, die sich aus der genutzten IKT ergeben können, Rechnung zu tragen.

Eine korrekt arbeitende IKT ist essentiell, um die notwendigen Steuerungen im Verteilnetz und allgemein in Smart Grids durchzuführen. Zum einen umfasst dies die Steuerungen von Systemen wie Umspannwerken innerhalb des Verteilnetzes. Hierzu kann der Verteilnetzbetreiber Messstellen innerhalb seines Verteilnetzes nutzen, um Messungen durchzuführen und auf deren Basis Steuerungen vorzunehmen. Alternativ könnten auch Messwerte der Smart Meter für Steuerungen verwendet werden. Zum anderen wird der Verteilnetzbetreiber auch verstärkt mit Energienutzern bzw. Energieerzeugern (Prosumer) kommunizieren, um angemessen auf Angebot und Nachfrage reagieren zu können. Beispielsweise können Preismodelle und das Dienstleistungsangebot an das aktuelle Angebot bzw. die aktuelle oder absehbare Nachfrage angepasst werden, um Verbraucher mit überzeugenden Mehrwertdiensten dazu anzuregen, ihr Energieverbrauchsverhalten dem verfügbaren Stromangebot anzupassen. Auch ist vorstellbar, dass Netzbetreiber mit den Kunden spezielle Service-Verträge abschließen, die es den Betreibern unter speziellen Rahmenbedingungen erlauben, selber, zum Beispiel durch Fernabschaltung von Geräten, in den Verbrauch beim Kunden regulierend einzugreifen. Hierzu könnten beispielsweise Nachrichten mit Preisinformationen an den Energienutzer gesendet werden und dieser kann z.B. mit der Annahme eines passenden Tarifs antworten. Da kaum zu erwarten ist, dass ein Endkunde derartige Entscheidungen explizit in Realzeit selber treffen möchte, werden Konzepte wie der smarte Energiebutler, wie sie derzeit in den E-Energy-Modellregionen erprobt werden, umzusetzen sein, um eine regelbasierte, automatisierte Entscheidung zu ermöglichen. Auch ist zu erwarten, dass der Kunde (natürlich nicht der Endkunde selber, sondern dies erfolgt automatisiert durch seine IKT Komponenten) Statusmeldungen über den Zustand von vorhandenen Speichern und Erzeugungsanlagen an den Verteilnetzbetreiber sendet, so dieser beispielsweise seine Lastflusssteuerung an die von den Prosumern eingespeiste Energie anpasst. Somit muss die Authentizität, Integrität, Verfügbarkeit und Aktualität von Steuerdaten und Statusmeldungen sichergestellt sein.

Weiterhin hat der Verteilnetzbetreiber die Anforderung, dass die Abrechnung mit dem

Energielieferanten bzw. direkt mit dem Energienutzer korrekt erfolgt. Hierzu erhält der Verteilnetzbetreiber vom Messdienstleister die notwendigen Daten. Aus Sicht des Datenschutzes muss hier geklärt werden, welche Daten für Abrechnungszwecke nötig sind. So sind sicherlich keine sekundengenauen Messwerte individueller Kunden notwendig. Jedoch muss bei variablen Preisen gewährleistet sein, dass die jeweils aktuellen Preise für die Abrechnung verwendet werden. Hier ließen sich beispielsweise Messwerte für einzelne Preisstufen monatlich aggregieren. Auch müssen diese Daten, genauso wie weitere Daten zur Abrechnung, wie sie beispielsweise zur Annahme eines Tarifs gesendet werden, korrekt, vollständig und vom richtigen Kommunikationspartner stammen.

Gleiches gilt für Rechnungsdaten, die an den Kunden gesendet werden. Zur Erstellung von Abrechnungen müssen diese Daten zwar verfügbar sein, aber die Erfüllung von Echtzeitanforderungen ist nicht erforderlich. Wenn bestimmte Daten jedoch dazu führen, dass in die Steuerung der Verteilnetze koordinierend eingegriffen wird, um z.B. Angebot und Nachfrage besser aufeinander abzustimmen, so ist die Aktualität und Vollständigkeit der Daten besonders wichtig, d.h. solche Daten unterliegen gewissen Echtzeitanforderungen. Welche Daten dem Verteilnetzbetreiber hierfür zur Verfügung gestellt werden, sollte der Energienutzer entsprechend der oben erwähnten Datenschutz-Regeln entscheiden können. Beispielsweise kann der Verteilnetzbetreiber sekundengenaue Messwerte erhalten, deren Ursprung aber anonymisiert wurde, so dass sie nur noch dem entsprechenden Netzsegment zuordenbar sind und nicht mehr dem individuellen Energienutzer.

Da Smart Meter und Gateways direkt beim Kunden installiert sind, können diese theoretisch leicht manipuliert werden. Somit ist für eine korrekte Abrechnung, wie bereits oben erwähnt, ebenfalls wieder die Integrität von Smart Metern und Gateways sowie Authentizität und Integrität von Wartungsdaten erforderlich.

Sicherheitsarchitektur

Im Folgenden wird eine generische Sicherheitsarchitektur für die Domäne Privatkunde vorgestellt. Abbildung 4 zeigt das Referenzmodell der Domäne Privathaushalt. Dargestellt sind die Komponenten Verbraucher, Smart Meter, Gateway, PC[4] und der Energieversorger, sowie deren Beziehungen zueinander. Die Verbraucher stehen repräsentativ auch für Speicher und Erzeugungsanlagen, die potentiell bei einem Kunden installiert sein können, da die Sicherheitsbetrachtungen auf dem hier betrachteten Niveau analog sind. An den Referenzpunkten 1 bis 7 identifizieren charakteristische Punkte, an denen auf jeden Fall geeignete Sicherheitsmechanismen in die Architektur integriert werden müssen. Im Folgenden werden beispielsweise zwei der Punkte beschrieben.

Referenzpunkt 1 beschreibt die Kommunikation zwischen Verbrauchern (bzw. Speicher oder Erzeuger) und Gateway, z.B. wenn das Gateway aufgrund eines niedrigen Preises entscheidet, einen Verbraucher einzuschalten. Hier müssen Zugriffskontrollen etabliert werden, so dass dies nur die dazu berechtigten Komponenten durchführen dürfen. Die erforderlichen Steuerdaten müssen authentifi-

[4] Als Platzhalter für andere Präsentationsgeräte beim Nutzer

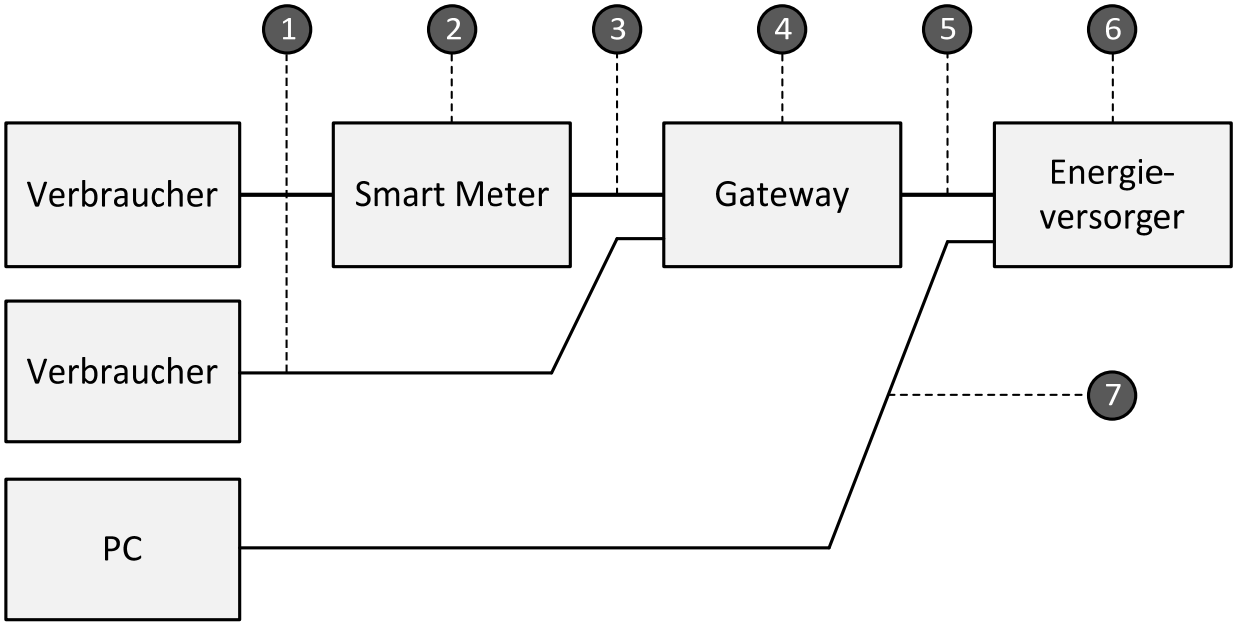

Abbildung 4: Referenzmodell der Subdomäne Privathaushalt mit Referenzpunkten

ziert, autorisiert und integer sein. Dies gilt ebenfalls für die andere Kommunikationsrichtung. Falls Speicher oder Erzeuger Statusmeldungen über das Gateway an den Energieversorger senden, sollten diese auch auf diesem Kommunikationsabschnitt geschützt sein, d.h. die Authentizität und Integrität sollte gewährleistet sein. Somit sind die umzusetzenden Sicherheitsmechanismen:

- Mechanismen zur Authentifizierung, Autorisierung und zum Integritätsschutz von Steuerdaten.
- Mechanismen zur Authentifizierung und zum Integritätsschutz von Statusmeldungen.

Die Umsetzung der Authentifizierung und Autorisierung wird an dieser Stelle voraussichtlich mit relativ einfachen Mechanismen realisiert, da die eingebetteten Systeme in den Verbrauchern stark in ihren Ressourcen (z.B. Rechenleistung, Speicher) eingeschränkt sein werden. Hier bieten sich Verfahren basierend auf symmetrischer Kryptographie wie Message Authentication Codes (MAC) an (vgl [4]), um Daten zu authentifizieren. Dies würde gleichzeitig die Integrität der Daten sicherstellen. Ein noch zu lösendes Problem ist hierbei die Frage der sicheren und effizienten Verteilung der benötigten symmetrischen Schlüssel. Während die Frage der Authentisierung bereits relativ konkret diskutiert wird, erscheint derzeit die Problematik der Autorisierung, also der Überprüfung von Zugriffsberechtigungen, noch weitestgehend offen zu sein. Aufgrund der beschränkten Ressourcen der beteiligten Komponenten erscheint es derzeit eher fraglich, ob Maßnahmen zur Autorisierung überhaupt umgesetzt werden sollten.

Referenzpunkt 3 beschreibt die Kommunikation zwischen Smart Meter und Gateway. Hier können unterschiedliche drahtgebundene (z.B. M-Bus [9], Power Line Communication (PLC)[5]) oder drahtlose (z.B. Wireless M-Bus, Bluetooth, IEEE 802.15.4 Zigbee) Kommunikationstechnologien verwendet werden. Entsprechend der identifizierten Sicherheitsanforderungen sind bei dieser Kommunikation die übertragenen Messwerte gegen (Wieder-) Einspielen, Manipulation und Abhören zu schützen. Bei der Übertragung von Steuerdaten sowie Wartungsdaten für Smart Meter sind Mechanismen zum Schutz gegen (Wieder-) Einspielen und Manipulationen ausreichend. Grundsätzlich sollte auch die Verfügbarkeit der gesamten Kommunikation in angemessenem Maße gegeben sein. Solange die Messwerte der Smart Meter nur zu Abrechnungszwecken genutzt werden, sind zwischenzeitliche Ausfälle jedoch kein größeres Problem. Falls jedoch Steuerungen im Verteilnetz auf Smart Meter Daten basieren, sind hier höhere Ansprüche an die Verfügbarkeit und die Aktualität der Daten zu stellen. Wobei auch hier das Ausbleiben von Daten einzelner Smart Meter keine größeren Auswirkungen haben sollten, da die Beeinflussung der Steuerungen durch einzelne Smart Meter eher gering. bzw. durch Messstellen des Verteilnetzbetreibers leicht kompensiert werden können. Derartige Messstellen könnten beispielsweise in Ortsnetzstationen oder Umspannwerke integriert werden. Die umzusetzenden Sicherheitsmechanismen sind somit:

- Mechanismen zum Schutz der Authentizität, Integrität und Vertraulichkeit der übertragenen Messwerte.
- Mechanismen zum Schutz der Authentizität und Integrität der übertragenen Steuerdaten und Wartungsdaten.
- Mechanismen zur Sicherstellung einer gewissen Verfügbarkeit der Kommunikation.

Zum Schutz der Authentizität, Integrität und Vertraulichkeit der Kommunikation zwischen Smart Meter und Gateway können beispielsweise die in die die jeweilige Technologie integrierten Sicherheitsmechanismen wie Verschlüsselungsverfahren direkt verwendet werden. So spezifiziert beispielsweise IEEE 802.15.4 Zigbee derartige Mechanismen und viele PLC Geräte haben ebenfalls entsprechende Mechanismen integriert. Aber auch bei einer direkten, kabelgebunden Verbindung zwischen Smart Meter und Gateway sollten die Daten geschützt werden. Eine kabelgebundene Verbindung ist zwar in der Regel etwas weniger bedroht, als eine drahtlose, dennoch sollten auch hier bekannte Techniken, wie digitale Signaturen, Zeitstempel, und Verschlüsselung eingesetzt werden, um Manipulationen und das Einschleusen falscher Messwerte sowie das Abhören durch Dritte zu verhindern.

Die Sicherstellung der Verfügbarkeit, insbesondere bei drahtloser Kommunikation, ist grundsätzlich schwierig zu realisieren. So gibt es gegen gezielte Jamming-Angriffe auf einen drahtlosen Kanal keine Schutzmöglichkeiten. Selbst bei kabelgebundener Kommunikation sind Angriffe auf die Verfügbarkeit nicht ausgeschlossen. So kann der Energienutzer selbst versuchen die Kommunikation zu stören, so dass keine Messwerte versendet werden und er seinen Stromverbrauch nicht bezahlen muss. Da man solche Angriffe nicht a priori verhindern kann, sollten diese zumindest a posteriori erkannt werden, in-

[5] z.B. nach IEEE 1901, HomePlug AV oder ITU-T G.hn

dem, ähnlich zu Keep-alive-Signalen, regelmäßig Daten versendet werden und deren Ausbleiben eine Unterbrechung der Verbindung oder einen Ausfall des Kommunikationspartners anzeigt.

4 Verteilnetz

Ein Verteilnetz wird von einem Verteilnetzbetreiber (engl. Distribution System Operator (DSO)) betrieben und unterhält Stromnetze im Nieder- und Mittelspannungs-Bereich (vgl. Abbildung 5).

Da ein großer Teil der Energie verbrauchenden Geräte Niederspannungsgeräte in den privaten Haushalten sind, stellen die Niederspannungsnetze die zentralen Energieverteilnetze für die Domäne Privathaushalt dar. An Niederspannungsnetze werden einphasige Geräte angeschlossen. In Mitteleuropa werden solche Niederspannungsnetze üblicherweise mit Spannungen zwischen 230 V / 400 V (einphasig / dreiphasig) und 1000 V betrieben. Derartige Netze sind in der Regel räumlich begrenzt und überspannen einen Bereich von einigen 100 m bis zu einigen wenigen Kilometern. Diese räumliche Beschränkung ist notwendig, um Spannungsverluste zu vermeiden. Üblicherweise bestehen Niederspannungsnetze aus mehreren Kabelsträngen, die einzelne Häuser oder Häusergruppen in räumlich naher Umgebung in einer sternförmigen Topologie versorgen. Im Haus erfolgt die Unterverteilung ebenfalls in der Regel sternförmig zu den Steckdosen und sonstigen Verbrauchern. Niederspannungsnetze werden über regionale Transformatorenstationen aus einem Mittelspannungsnetz bzw. von einem Übertragungsnetzbetreiber (engl. Transmission System Operator, (TSO)) versorgt.

Ein Übertragungsnetzbetreiber erhält Strom von großen Erzeugern wie Kohle- oder Atomkraftwerken und überträgt den Strom über große Entfernungen in Hochspannungsnetzen. Ein Verteilnetzbetreiber kann aber auch selbst Strom erzeugen, z.B. durch eigene Windparks oder Blockheizkraftwerke. Üblicherweise gehören Verteilnetzbetreiber zu einem lokalen bzw. kommunalen Energieversorgungsunternehmen wie einem Stadtwerk. In Deutschland werden Verteilnetze von über 720 Stadtwerken, ca. 70 regionalen Netzbetreibern und über 100 privaten Versorgern betrieben [11]. Eine detaillierte Einführung in Verteilnetze findet sich in [12].

In zukünftigen Smart Grids wird erwartet, dass sowohl zwischen den Komponenten und Mitglieder, die sich innerhalb eines Verteilnetzes befinden, als auch mit Mitgliedern weiterer Rollen erheblich mehr als jetzt kommuniziert werden muss, um eine Steuerungen wie Lastflusssteuerung oder Netzüberwachungen durchzuführen. Derzeit wird im Verteilnetz noch überwiegend manuell gesteuert und in vielen Bereichen kommt man noch ohne Kommunikation aus. So agieren beispielsweise Ortsnetzstationen meist autonom. Durch die ansteigende Nutzung von erneuerbaren Energien ist aber zu erwarten, dass sich dies in Zukunft ändern wird.

Im Verteilnetz sind die folgende Rollen relevant (vgl. auch [12]): Verteilnetzbetreiber, Produzent, Kommunikationsnetzbetreiber, Übertragungsnetzbetreiber, Energielieferant, Messdienstleister, Energienutzer und Messstellenbetreiber. Abbildung 4 stellt die Zusammenhänge zwischen den einzelnen Rollen graphisch dar. Der Fokus liegt dabei auf dem Verteilnetzbetreiber. Nicht direkt relevante Beziehungen werden zur besseren Übersicht nicht dargestellt.

Beispielhaft werden im Folgenden die Rollen *Verteilnetz-* und Übertragungsnetzbetreiber sowie *Produzent* betrachtet.

Der *Verteilnetzbetreiber* betreibt, wie bereits oben erwähnt, Niederspannungsnetze bzw. Mittelspannungsnetze auf regionaler Ebene und sorgt für die Stromversorgung der Endverbraucher, d.h. er liefert Energie an den Energienutzer. In Zukunft wird es zur Steuerung von Verteilnetzen zu einer vermehrten Kommunikation kommen. So müssen zur Überwachung und Steuerung Messwerte und Statusdaten erfasst und übertragen werden sowie mittels Steuerdaten Steuerungen durchgeführt werden. Dies muss zum einen innerhalb des Verteilnetzes erfolgen, z.B. zur Überwachung und Steuerung von Ortsnetzstationen oder Umspannwerken. Zum anderen werden auch mit anderen Rollen vermehrt Daten ausgetauscht werden müssen, um die Verteilnetze versorgungssicher zu betreiben. Hierzu können z.B. Energieverbraucher ferngesteuert werden, um den Verbrauch an das Angebot anzupassen, wofür entsprechende Steuerdaten übertragen werden müssen.

Mit dem *Übertragungsnetzbetreiber* findet sowohl Kommunikation zur Herstellung eines Lastausgleichs als auch zur Abwicklung des Energiehandels statt. Hierzu werden Daten, wie das aktuelle Angebot und die aktuelle Nachfrage nach Energie, sowie Abrechnungsdaten auszutauschen sein. Der Übertragungsnetzbetreiber ist mit Produzenten verbunden, die mittels Großkraftwerken in das Höchstspannungsnetz einspeisen. Eine direkte Verbindung zwischen Verteilnetzbetreiber und Produzenten auf Höchstspannungsebene gibt es somit nicht.

Die *Produzenten,* mit denen der Verteilnetzbetreiber kommuniziert, sind verantwortlich dafür, Energie ins Niederspannungsnetz oder ins Mittelspannungsnetz des Verteilnetzbetreibers einzuspeisen. Dies kann beispielsweise ein Prosumer sein, der mittels ei-

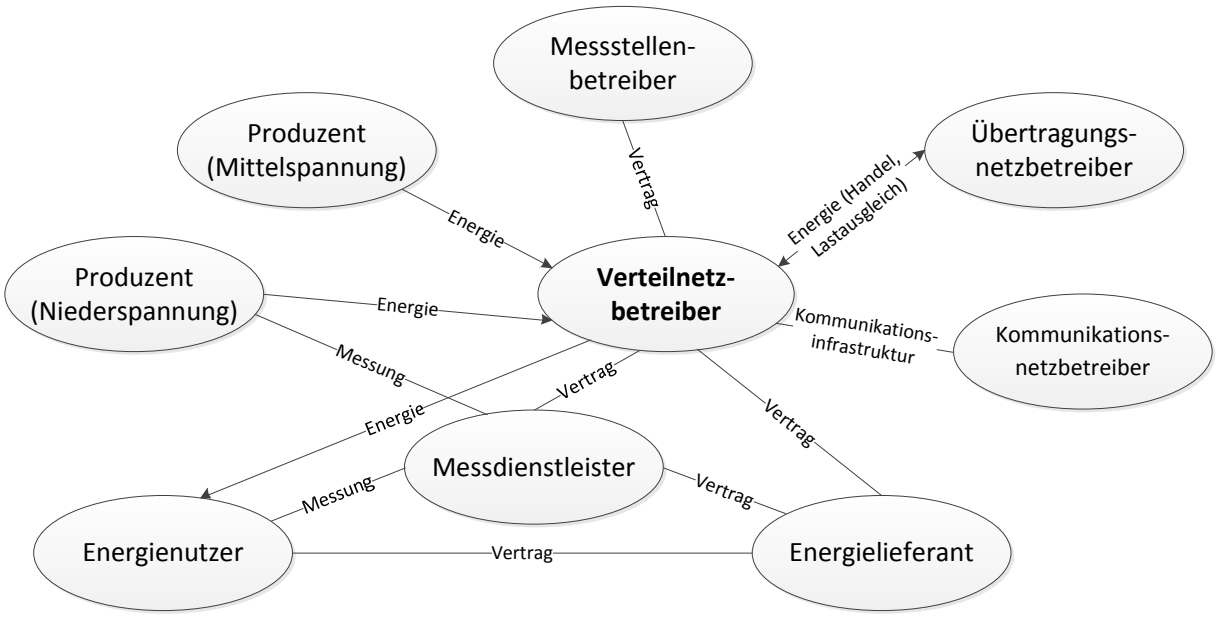

Abbildung 5: Rollen in der Domäne Verteilnetz und deren Beziehungen

ner Photovoltaikanlage ins Niederspannungsnetz einspeist. Falls der Verteilnetzbetreiber ein überregionales Verteilnetz mit eigenen Erzeugungsanlagen betreibt, wird auch mit diesen Produzenten, die ins Hochspannungsnetz einspeisen, kommuniziert. Hier müssen ebenfalls Messwerte über die eingespeiste Energie und ggf. weitere Statusdaten übertragen werden. Auch wird der Verteilnetzbetreiber eigene Energieerzeugungsanlagen überwachen und steuern und hierzu Steuerdaten sowie Statusdaten übertragen. Eventuell werden auch Prognosedaten über die erwartete Energiekapazität übertragen. Dies ist insbesondere für die Erzeugung mittels erneuerbarer Energien relevant.

Eine mögliche Referenzarchitektur der Netztopologie der Domäne Verteilnetz und deren Anbindung an das Übertragungsnetz und an Energienutzer wie Privatkunden sind in Abbildung 5 dargestellt. Die Abbildung beschreibt die funktionalen Elemente im Verteilnetz und die Strom bzw. Datenverbindungen darin. Das Verteilnetz ist an das Übertragungsnetz angeschlossen und bezieht von dort Strom, der von Produzenten in Großkraftwerken erzeugt wird. Betreibt der Verteilnetzbetreiber ein überregionales Verteilnetz, so wird der über Höchstspannungsnetze empfangene Strom zunächst in einem *Umspannwerk* auf Hochspannung transformiert. Zur Transformation zwischen den verschiedenen Spannungsebenen der Höchst-, Hoch- und Mittelspannung betreibt der Verteilnetzbetreiber verschiedene *Umspannwerke* und zur Transformation zwischen der Mittelspannungsebene und der Niederspannungsebene betreibt er *Ortsnetzstationen* (Trafostationen).

In Zukunft werden viel mehr verteilte *Erzeuger* auf den verschiedenen Spannungsebenen an das Verteilnetz angebunden sein. Dies umfasst mittlere Erzeuger wie On-shore Windparks, kleine Erzeuger wie Geothermie oder Biogasanlagen, sowie kleinste Erzeugungsanlagen wie Photovoltaikanlagen beim Privatkunden oder Blockheizkraftwerke. Zum Ausgleich von Schwankungen in der Verfügbarkeit der Energie können *Speicher* auf den verschiedenen Spannungsebenen eingesetzt werden. *Verbraucher* sind auf Mittelspannungsebene meist Industriebetriebe und auf Niederspannungsebene Privatkunden oder kleine Gewerbebetriebe.

Die Kommunikation findet zentral mit einer *Netzleitstelle* statt. Derzeit existieren Kommunikationsbeziehungen vorwiegend zwischen Umspannstationen und der Leitstelle. Dagegen arbeiten die Ortsnetzstationen in der Regel autonom ohne Kommunikation. Hier ist aber im Zuge des Ausbaus von Smart Grids zu erwarten, dass auch Ortsnetzstationen kommunizieren werden. Die Kommunikation umfasst die Überwachung, Steuerung und Wartung der Anlagen, wozu Messwerte, Steuerdaten sowie Wartungsdaten ausgetauscht werden können. Die Kommunikation mit den Verbrauchern umfasst den Austausch von Messwerten, aktuellen Verbrauchsdaten, Preisinformationen, Steuerdaten, Wartungsdaten etc. Mit Erzeugern müssen Messwerte zur Abrechnung, Statusdaten, Steuersignale zur Überwachung und Steuerung sowie Wartungsdaten zur Wartung ausgetauscht werden. Mit Energie-Speichern werden ebenfalls Messwerte zur Abrechnung ausgetauscht sowie Statusdaten z.B. zur Anzeige der verfügbaren Speicherkapazität oder gespeicherten Energie. Zur besseren Übersichtlichkeit sind in Abbildung 6 einige Kommunikationsbeziehungen vereinfacht dargestellt. So wird aufgrund der gesetzlich vorgeschriebenen Rollentrennung beispielsweise

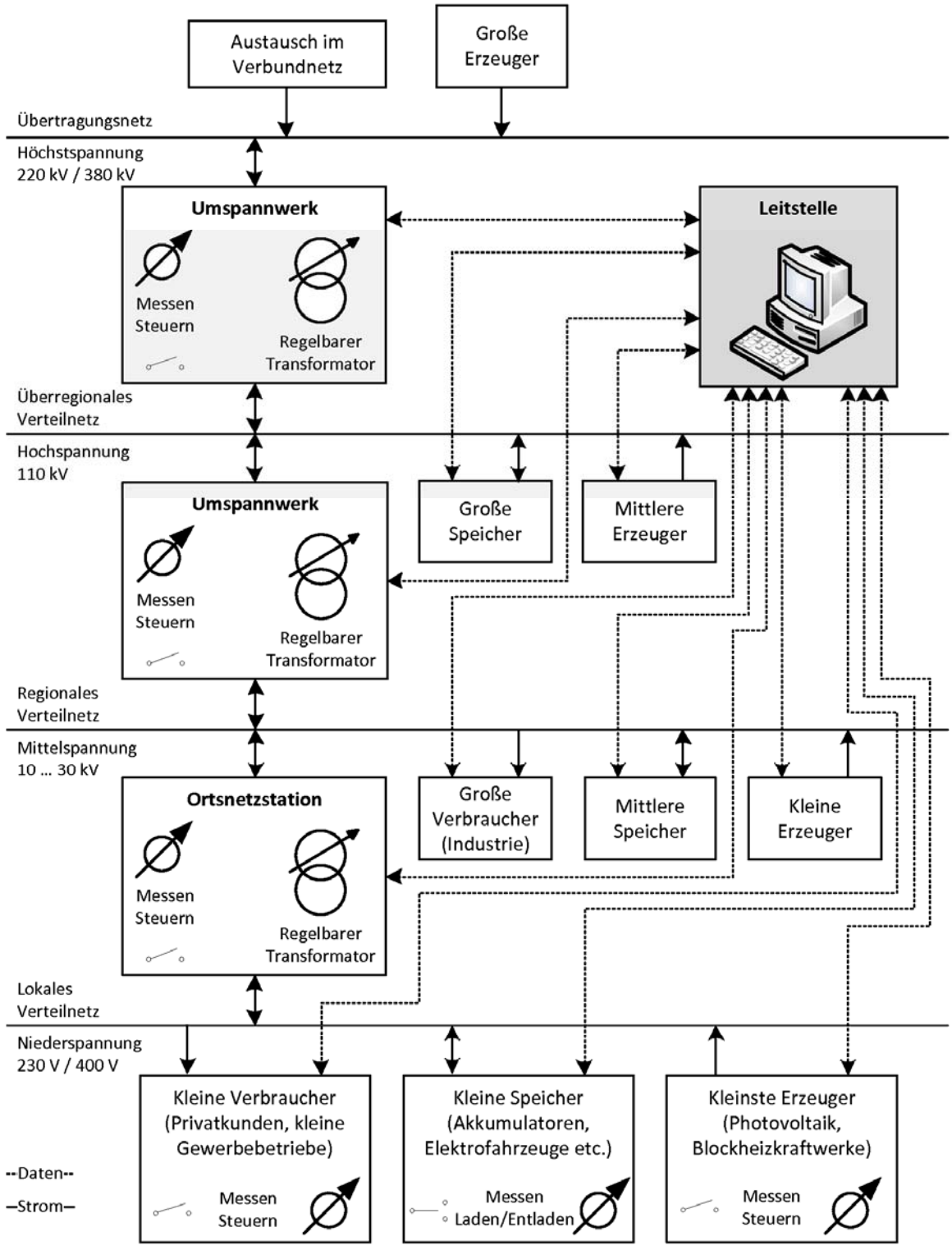

Abbildung 6: Repräsentative Topologie der Domäne Verteilnetz

die Leitstelle des Verteilnetzbetreibers keine Messwerte der Smart Meter direkt erhalten, sondern diese über den Messdienstleister, der diese Daten ggf. aggregiert oder anonymisiert, empfangen.

Anwendungsfälle

Da die beiden Domänen Privatkunde und Verteilnetz direkt zusammen hängen, sind Anwendungsfälle der Domäne Privatkunde größtenteils ebenfalls für die Domäne Verteilnetz relevant. So ist der Anwendungsfall *Fernwartung* von Smart Metern für den Verteilnetzbetreiber insofern interessant, dass er aufgrund der Informationen, die er vom Messstellenbetreiber über die Art und Anzahl der angeschlossenen Kunden erhält, Lastprofile zur Prognose des Energiebedarfs erstellen kann. Als Beispiel für einen weiteren Anwendungsfall betrachten wir im Folgenden das *Einspeisen von Energie.*

Use-Case: Einspeisen von Energie

Der Privatkunde kann Energie, die in installierten Erzeugungsanlagen erzeugt wurde, oder die in Speichern, wie den Batterien von Elektrofahrzeugen gespeichert wurde, in das Verteilnetz einspeisen. Die Erfassung der Messwerte über die eingespeiste Energie erfolgt über Smart Meter. Der Verteilnetzbetreiber kann aber auch selbst mittels eigener Erzeugungsanlagen Energie erzeugen und in sein Verteilnetz einspeisen. Für das Netzmanagement, die Abrechnung und auch die Wartung ist die Erfassung und Kommunikation von Informationen zur Energienutzung, -erzeugung und -speicherung notwendig. Diese Informationen sind insbesondere für den Verteilnetzbetreiber für das Netzmanagement wichtig, um die Versorgungssicherheit zu gewährleisten. So müssen beispielsweise für die einzelnen Netzsegmente (aggregierte) Messwerte z.B. durch den Messdienstleister oder eigene Messstellen im Verteilnetz über Energieverbrauch und durch Energieerzeuger und Speicher eingespeiste Energie erfasst werden. Auch müssen (ggf. aggregierte) Statusinformationen zu verfügbaren Erzeugungsressourcen, gespeicherten Energien, verfügbaren Speicherkapazitäten etc. erfasst werden. Basierend auf diesen Daten kann der Verteilnetzbetreiber dann entsprechende Steuerungen in den einzelnen Netzsegmenten seines Verteilnetzes vornehmen, um auf Spitzen in Angebot und Nachfrage zu reagieren.

Rollen und Sicherheitsanforderungen

Im Folgenden werden beispielhaft die Sicherheitsanforderungen der Rollen *Verteilnetzbetreiber* und *Übertragungsnetzbetreiber* beschrieben.

(1) Rolle: Verteilnetzbetreiber

Zusätzlich zu den bereits beschriebenen Sicherheitsanforderungen muss die Authentizität, Integrität, Verfügbarkeit und Aktualität sowohl von Statusdaten von Systemen beim Kunden als auch von Systemen im Verteilnetz gewährleistet werden. Damit wird sichergestellt, dass die Daten von der besagten Stelle stammen, während der Übertragung nicht verändert wurden und rechtzeitig eintreffen. Um zu gewährleisten, dass die empfangenen Daten auch von einem vertrauenswürdigen System stammen, welches nicht manipuliert wurde, ist weiterhin die Integrität der Systeme, also von IKT-Komponenten von Energie-Speichern, -Erzeugern, Ortsnetzstationen, Umspannwerken etc. sicherzustellen. Bei der Umsetzung dieser Anforderungen ist zu beachten, dass die

Schutzanforderungen für die Systeme im Verteilnetz wesentlich höher sind als in der Domäne Privatkunde, da deren Ausfall wesentlich schwerwiegendere Folgen hätte als die Störung der Versorgung eines einzelnen Kunden.

(2) Rolle: Übertragungsnetzbetreiber

Der Übertragungsnetzbetreiber hat genauso wie der Verteilnetzbetreiber die Hauptanforderung, dass sein Netz verfügbar ist. Hierzu muss die Leittechnik zur Steuerung des Netzes korrekt funktionieren und die übertragenen Steuernachrichten müssen authentifiziert, gegen Manipulation geschützt, verfügbar und aktuell sein. Gleiches gilt für Statusdaten sowie Steuerdaten, die mit angeschlossenen Verteilnetzbetreibern ausgetauscht werden. Diese werden zum korrekten Betrieb des Übertragungsnetzes benötigt, z.B. zur Lastflussoptimierung oder für Schutzfunktionen wie der Sicherstellung der Frequenzstabilität.

Auf weitere Anforderungen des Übertragungsnetzbetreibers, wie beispielsweise nach korrekter Abrechnung der Netznutzung, soll hier nicht weiter eingegangen werden, da der Fokus dieses Artikels der Privatkunde und das Verteilnetz ist.

Sicherheitsarchitektur

Abbildung 7 zeigt ein Referenzmodell der Domäne Verteilnetz basierend auf der Architektur aus Abbildung 5 mit einer Leitstelle. Da die Sicherheitsarchitektur hier nur auf einem relativ hohem Abstraktionsniveau beschrieben wird, sind einige Komponenten und Schnittstellen zur besseren Übersichtlichkeit

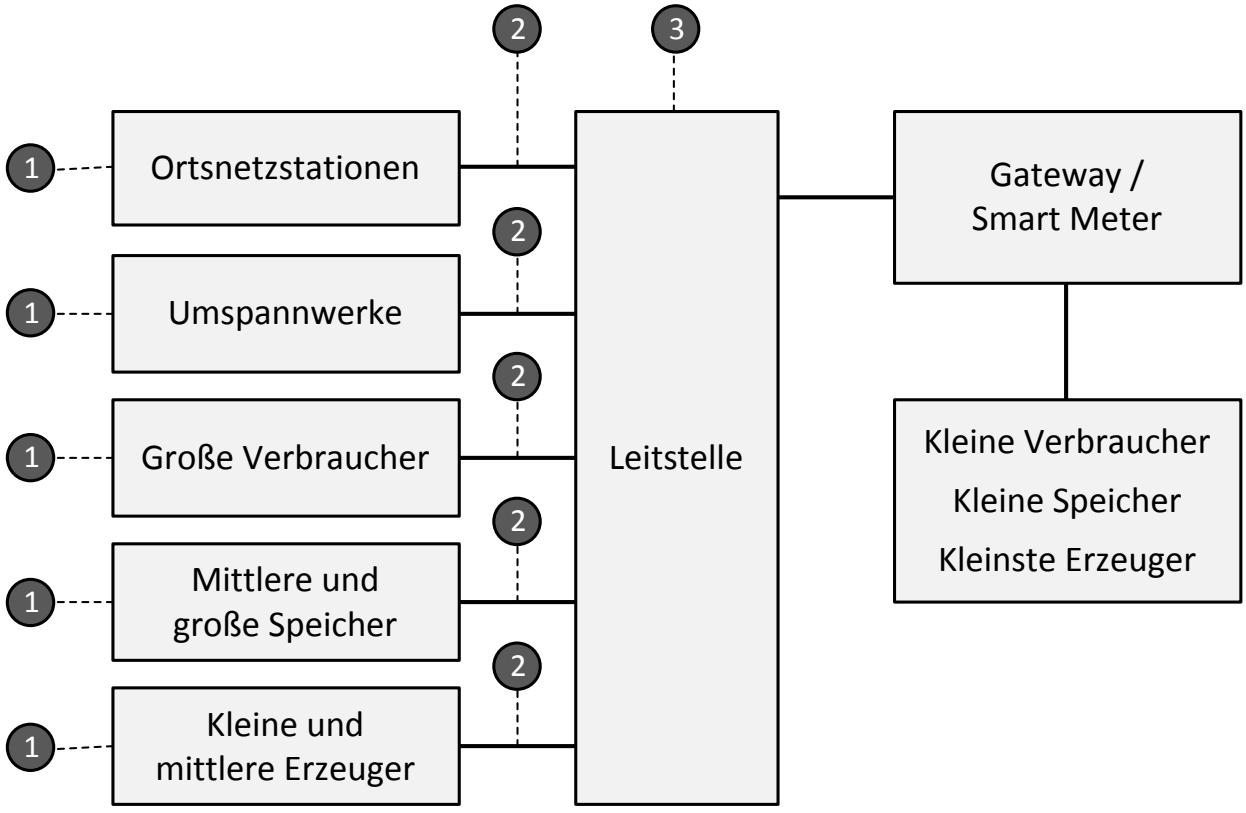

Abbildung 7: Referenzmodell der Domäne Verteilnetz mit Referenzpunkten

zusammengefasst. Beispielhaft wird nachfolgend der Referenzpunkt 1 etwas genauer beschrieben.

Der Referenzpunkt 1 beschreibt die erforderlichen Sicherheitsmechanismen zur Absicherung der IKT-Systeme von Ortsnetzstationen, Umspannwerken, großen Verbrauchern wie Industrieunternehmen sowie den verschiedenen Speichern und Erzeugern. Es müssen Mechanismen zum Schutz gegen Manipulationen etabliert werden, um eine korrekte Funktionsweise der IKT-Systeme zu gewährleisten. Dies geht einher mit geeigneten Mechanismen zur Authentifizierung und Autorisierung von Mitgliedern der verschiedenen Rollen zum Schutz gegen unberechtigte Zugriffe. Für den Verteilnetzbetreiber ist besonders die Verfügbarkeit der IKT-Systeme wichtig. Dies gilt in besonderem Maße für Ortsnetzstationen und Umspannwerke, da ein Ausfall der IKT-Systeme eine entfernte Überwachung und Steuerung verhindert. Diese Systeme müssen auch garantieren, dass bestimmte Daten innerhalb gewisser Zeiten verarbeitet werden, z.B. Statusmeldungen über Ausfälle. Aber auch Ausfälle der IKT-Systeme von Energie-Speichern, -Erzeugern und -Verbrauchern können Auswirkungen auf das Verteilnetz und die Verteilnetzautomatisierung haben, da die Netzsteuerung auf aktuelle Daten zum Energieverbrauch oder zu Einspeisekapazitäten zurückgreifen wird.

Die Umsetzung der Sicherheitsmechanismen zum Schutz gegen Manipulationen wird insbesondere bei Ortsnetzstationen und Umspannwerken voraussichtlich wie bisher durch physische Sicherheit, wie z.B. abgeschlossene Gebäude sichergestellt. Authentifizieren müssen sich sowohl Personen wie Administratoren der Systeme als auch IKT-Systeme . Die Authentifizierung kann wie bereits beschrieben mit Hilfe von kryptographischen Protokollen umgesetzt werden; die Autorisierung kann mittels Zugriffskontrolllisten zusammen mit Rollen-basierter Zugriffskontrolle realisiert werden. Zur Sicherstellung der Verfügbarkeit und zur Einhaltung gewisser Zeitschranken sind zum einen derzeit schon eingesetzte klassische Safety-Mechanismen wie die redundante Auslegung von IKT-Systemen, um Fehlertoleranz zu erzielen, nötig. Damit ließen sich Ausfälle einzelner IKT-Komponenten kompensieren. Eine weitere Möglichkeit besteht in der Priorisierung von Aktivitäten, so dass bei partiellen Ausfällen nur noch die Kernfunktionen aufrecht erhalten werden. Damit Angreifer derartige Situationen nicht gezielt herbeiführen können, und damit einen Denial-of-Service-Angriff provozieren, werden Erkennungsverfahren benötigt, um übliches und unübliches Kommunikationsverhalten unterscheiden zu können.

Maßnahmen zur Gewährleistung der Betriebssicherheit müssen durch IT-Sicherheits-Maßnahmen ergänzt werden. Beispielsweise können vorgeschaltete Firewall-Systeme den Zugriff auf IKT-Komponenten des Verteilnetzes kontrollieren, so dass diese nicht durch zu viele Zugriffe überlastet werden. Die Wechselwirkungen zwischen Betriebssicherheit und IT-Sicherheit sind bei der Entwicklung und Umsetzung geeigneter Sicherheitsmechanismen (im Sinne von Safety und Security) zu beachten. Beispielsweise sollten abgestufte Sicherheitszonen eingeführt werden, so dass Kontrollen nur an Zonenübergängen durch ressourcenstarke Komponenten erfolgen.

5 Zusammenfassung

In diesem Artikel wurde ein domänenbasierter Ansatz zur Beherrschung der Komplexität von Smart Grid Sicherheitsarchitekturen vorgestellt. Am Beispiel der Domänen Privatkunde und Verteilnetz wurde die Vorgehensweise skizziert, Rollen und Anwendungsfälle zu identifizieren, auf dieser Basis differenzierte Sicherheitsanforderungen abzuleiten und domänenspezifische Referenzarchitekturen zu konzipieren. Sobald konkret abzusehen ist wie die zukünftigen Smart Grids konkret realisiert werden, können die vorgestellten Sicherheits-Referenzarchitekturen entsprechend angepasst und die umzusetzenden Sicherheitsmechanismen weiter konkretisiert werden. Die vorgestellten Domänen-bezogenen Referenzarchitekturen, Rollenmodellierungen und abgeleiteten Sicherheitsanforderungen sowie Umsetzungshinweise verstehen wir als einen ersten Schritt in Richtung auf die Erstellung eines umfassenden Sicherheitskonzepts für Smart Grids.

Danksagung

Die hier vorgestellten Ergebnisse sind Ausschnitte aus einer Studie, die für die Alcatel-Lucent Stiftung von der Autorin zusammen mit Herrn Dr. Christoph Krauß durchgeführt wurde. Die ausführliche Darstellung der Ergebnisse dieser Studie ist als Bericht Nr. 93 unter http://www.stiftungaktuell.de zu finden.

Literatur

[1] M. Brunner, H. Hofinger, C. Krauß, C. Roblee, P. Schoo, S. Todt. Infiltrating critical infrastructures with next-generation attacks: W32.Stuxnet as a showcase threat. Technical Report, Fraunhofer AISEC, December 2010.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI). Protection Profile for the Gateway of a Smart Metering System, 2011.

[3] Deutsche Kommission Elektrotechnik Informationstechnik im DIN und VDE. Die deutsche Normungsroadmap E-Energy / Smart Grid, Version 1.0. Technical report, DKE, März 2010.

[4] C. Eckert. *IT-Sicherheit: Konzepte, Verfahren, Protokolle*. Oldenbourg-Verlag, 2011.

[5] C. Eckert, C. Krauß. Sicherheit im Smart Grid – Herausforderungen und Handlungsempfehlungen. *Datenschutz und Datensicherheit*, 8:535–541, 2011.

[6] C. Eckert, C. Krauß, P. Schoo. Sicherheit im Smart Grid – Eckpunkte für ein Energieinformationsnetz, . Stiftungsreihe Nr. 90, 2011.

[7] D. Ferraiolo, D. Kuhn. Role-based access control. In *15th National Computer Security Conference*, 1992.

[8] Heise Online. Meldung vom 19.11.2009. Intelligente Stromnetze: Ich weiß, ob du gestern geduscht hast. http://www.heise.de/security/meldung/Intelligente-Stromnetze-Ich-weiss-ob-du-gestern-geduscht-hast-864221.html.

[9] M-Bus standard. EN 13757. http://www.m-bus.com.

[10] NIST. Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References. NISTIR 7628, August 2010.

[11] H. Orlamünder. Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen – ein nachhaltiges Energieinformationsnetz, Stiftungsreihe Nr. 85, 2009.

[12] H. Orlamünder. Der Einsatz von Informations- und Kommunikationstechnik in Stromnetzen – ein nachhaltiges Energieinformationsnetz, Stiftungsreihe Nr. 93, 2011.

[13] D. L. U. Greveler, B. Justus. Hintergrund und experimentelle Ergebnisse zum Thema “Smart Meter und Datenschutz”. Technical report, FH Münster, September 2011.

[14] J. Schleich, M. Klobasa, M. Brunner, S. Gölz, K. Götz, G. Sunderer. Smart metering in Germany and Austria – results of providing feedback information in a field trial. Working Paper Sustainability and Innovation, No. S6/2011.

[15] eTelligence Projekt. http://www.etelligence.

[16] Telekommunikationsgesetz. http://www.gesetze-im-internet.de-/tkg_2004/index.html

[17] Information and Privacy Commissioner, Ontario, Canada. SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation. November, 2009. http://www.futureofprivacy.org/wp-content/uploads/2009/11/smartprivacy-for-the-smart-grid.pdf

[18] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO), 1996.

[19] P. Kocher, J. Jaffe, B. Jun: Differential Power Analysis, Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO), 1999.

[20] Miele Pressemitteilung Nr. 095/2010. http://www.miele-presse.de/media/presse/media/2010-095_Miele_praesentiert_die_ersten_Smart-Grid-faehigen_Hausgeraete.pdf

[21] Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz – EnWG) http://www.gesetze-im-internet.de/-bundesrecht/enwg_2005/gesamt.pdf

Prof. Dr. Claudia Eckert *ist Leiterin der Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit (AISEC) in Garching bei München sowie Leiterin des Fachgebiets Sicherheit in der Informationstechnik des Fachbereichs Informatik an der Technischen Universität in München.*

Sicherheitsdomänen im Energieinformationsnetz

Andreas Memmert

Es kommt immer wieder zu lang anhaltenden und teilweise großflächigen Stromausfällen in Deutschland. Die spektakulärsten Fälle der letzen Jahre hat der NDR in seinem Bericht vom 14. Juli 2011 dokumentiert. Zu erwähnen sind die großflächigen Stromausfälle infolge des Elbe- und Oderhochwassers 2002 / 2005, der Stromausfall im Münsterland 2005 und die Folgen von „Kyrill“ 2007. Die Auswirkungen auf die gesamten Lebensumstände der Menschen und Unternehmen sind katastrophal. Die deutschen Städte, Gemeinden und Landkreise, der Bund und die Länder sind bisher nicht auf das dazu erforderliche Krisenmanagement vorbereitet. Für die kommunale Ebene gibt es bisher keine Handlungsempfehlungen für solche Szenarien in Deutschland. Lediglich der Bundesstaat Kalifornien hat im April 2004 ein Local Government Emergency Planning Handbook durch die California Energy Commission im Auftrag von Governor Arnold Schwarzenegger herausgegeben.

Der Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung des Deutschen Bundestages (18. Ausschuss) vom 27. April 2011 (Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/5672, S. 3) – Technikfolgenabschätzung (TA) „Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und lang andauernder Ausfalls der Stromversorgung“ beschreibt für den Fall dieses Ereignisses die Lage in Deutschland mit folgenden Aussagen:

1. „Aufgrund der großen Abhängigkeit nahezu aller kritischen Infrastrukturen von der Stromversorgung kommt dem Szenario eines großflächigen und längerfristigen Stromausfalls mit der Folge massiver Versorgungsstörungen, wirtschaftlicher Schäden sowie Gefährdungen der öffentlichen Sicherheit eine zentrale Bedeutung zu.“

2. „Die im Jahr 2004 durchgeführte Bund-Länder-Krisenmanagementübung (LÜKEX) hat die problematischen Folgen und Folgenketten sowie die enormen Schwierigkeiten, eine solche Krisen- und Gefahrenlage ohne Vorwarnung in den föderalen Strukturen zu bewältigen, deutlich gemacht.“

3. „Gleichwohl sind – soweit erkennbar – die möglichen Folgen eines solchen Ereignisses in der Literatur ebenso wie in offiziellen behördlichen Dokumenten noch nicht intensiv und systematisch durchdacht worden.“

4. „Die Analysen des TAB zeigen, dass die Folgen eines solchen Stromausfalls einer nationalen Katastrophe zumindest nahekommen könnten. Es bedürfte einer Mobilisierung aller internen und externen Kräfte des Bevölkerungsschutzes, um die Auswirkungen zumindest zu mildern.“

Der Bericht kommt zu folgenden Ergebnissen:

- Die Informations- und Kommunikationsinfrastruktur bricht teils sofort, teils nach wenigen Tagen zusammen (Telefon, Handy, Internet)
- Im Sektor Transport- und Verkehr fallen die elektrisch betriebenen Elemente der Verkehrsträger Straße, Schiene; Luft und

Wasser sofort oder nach wenigen Stunden aus

- das Gesundheitssystem einschließlich Not- und Rettungswesen ist erheblich gestört und bricht teilweise zusammen
- die Versorgung mit Trinkwasser fällt bereits nach kürzester Zeit aus, da alle Trinkwasserstruktursysteme elektrisch betrieben werden – die Folgen für die Versorgung der Bevölkerung wären katastrophal
- die Nahrungsmittelversorgung ist erheblich gestört
- die Entsorgung von Abwasser und Müll bricht unmittelbar zusammen (Hochhäuser müssten wegen Seuchengefahr evakuiert werden)
- die Behörden und Verwaltungen können nur noch eingeschränkt handeln
- Tankstellen fallen sofort aus, da nur fünf deutsche Tankstellen mit einer Notstromversorgung ausgestattet sind, der Individualverkehr bricht nach kurzer Zeit zusammen.

Fazit

„Die Folgenanalysen haben gezeigt, dass bereits nach wenigen Tagen im betroffenen Gebiet die flächendeckende und bedarfsgerechte Versorgung der Bevölkerung mit (lebens)notwendigen Gütern und Dienstleistungen nicht mehr sicherzustellen ist. Die öffentliche Sicherheit ist gefährdet, der grundgesetzlich verankerten Schutzpflicht für Leib und Leben seiner Bürger kann der Staat nicht mehr gerecht werden“. (Ausschussbericht S. 15)

Umgesetzt wurde bisher noch nichts. Offenkundig ist der Bericht in der Schublade verschwunden. Dabei wird im letzten Absatz des Vorwortes des Ausschusses folgendes festgestellt:

„Der TAB-Bericht gibt Hinweise darauf, wie die Robustheit Kritischer Infrastrukturen gestärkt und die Handlungsmöglichkeiten des nationalen Systems des Katastrophenmanagements verbessert werden könnten. Der Bericht leistet damit einen wertvollen Beitrag, die Sensibilität in Wirtschaft und Gesellschaft für diese Thematik zu erhöhen und bietet für die Fachausschüsse des Deutschen Bundestages eine gute Grundlage für die weitere Befassung.“ (Bericht S. 3)

Welche Lösungsansätze sind erkennbar bzw. denkbar?

1. Ich fordere die Erstellung eines Kommunalen Planungshandbuches zum Schutz kritischer Infrastrukturen bei Notfällen nach dem Vorbild des kalifornischen „Local Government Emergency Planning Handbook“ von 2004

2. Es müssen dezentrale Inselnetze zur Aufrechterhaltung der Versorgung in Krisenfällen geschaffen werden. Dabei müssen lokale Bioenergieverbünde (Wind, Biogas-BHKWs und Photovoltaik) die insgesamt erzeugte Strommenge lokal einspeisen. Dies bringt auch eine deutliche Steigerung der regionalen Wertschöpfung.

3. Das BMBF hat verschiedene Forschungsprojekte zum Schutz kritischer Infrastrukturen (GRASB, InfoStrom, SES², Simkas-3D) in Auftrag gegeben.

Die Ergebnisse müssen abgewartet und umgesetzt werden.

Andreas Memmert *ist Bürgermeister der Samtgemeinde Schladen.*

Alcatel-Lucent Stiftung

Die Alcatel-Lucent Stiftung für Kommunikationsforschung ist eine gemeinnützige Förderstiftung für Wissenschaft insbesondere auf allen Themengebieten einer „Informationsgesellschaft“, neben allen Aspekten der neuen breitbandigen Medien speziell der Mensch-Technik-Interaktion, des E-Government, dem Medien- und Informationsrecht, dem Datenschutz, der Datensicherheit, der Sicherheits-kommunikation sowie der Mobilitätskommunikation. Alle mitwirkenden Disziplinen sind angesprochen, von Naturwissenschaft und Technik über die Ökonomie bis hin zur Technikphilosophie.

Die Stiftung vergibt jährlich den interdisziplinären „Forschungspreis Technische Kommunikation“, Dissertationsauszeichnungen für WirtschaftswissenschaftlerInnen sowie Sonderauszeichnungen für herausragende wissenschaftliche Leistungen.

Die 1979 eingerichtete gemeinnützige Stiftung unterstützt mit Veranstaltungen, Publikationen und Expertisen ein eng mit der Praxis verbundenes pluridisziplinäres wissenschaftliches Netzwerk, in dem wichtige Fragestellungen der Informations- und Wissensgesellschaft frühzeitig aufgenommen und behandelt werden.

www.stiftungaktuell.de

Kontakt

Alcatel-Lucent Stiftung
Lorenzstraße 10, 70435 Stuttgart
Telefon 0711-821-45002
Telefax 0711-821-42253
E-Mail office@stiftungaktuell.de
URL: http://www.stiftungaktuell.de