Cyberattacken gegen kritische Infrastrukturen

Markus Grimm
Betreuer: Dr. Heiko Niedermayer
Seminar Future Internet SS2013
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: grimmm@in.tum.de

KURZFASSUNG

Kritische Infrastrukturen sind von hoher Bedeutung für das Funktionieren einer Gesellschaft. Bei deren Ausfall können erhebliche Störungen des öffentlichen Lebens auftreten. Die Elektrizitätsversorgung nimmt dabei einen besonderen Stellenwert ein, da sie in gewisser Weise als Basisinfrastruktur gesehen werden kann. Diese Arbeit widmet sich anhand des Beispiels Stromversorgung den Fragen, welche Sicherheitsrisiken diese Infrastruktur aufweist und wie sich diese im Zusammenhang mit Cyberattacken auswirken.

Schlüsselworte

Sicherheit kritische Infrastrukturen, Smart Grid, Stromausfall, Stromversorgung

1. EINLEITUNG

„Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ [1].

Unter diese Definition fallen nach BSI (Bundesamt für Sicherheit in der Informationstechnik) folgende Infrastruktursektoren [1]:

- Transport und Verkehr
- Energie
- Gefahrenstoffe
- Informationstechnik und Telekommunikation
- Finanz-, Geld- und Versicherungswesen
- Versorgung
- Behörden, Verwaltung und Justiz
- Sonstiges (Medien, Großforschungseinrichtungen, Kulturgut)

Einen besonderen Stellenwert nimmt in diesem Zusammenhang die Energieversorgung, im speziellen die Stromversorgung, ein, da ein teilweiser oder vollständiger Ausfall dieser weitreichende Konsequenzen für die anderen Sektoren, die Industrie und das öffentliche Leben im Allgemeinen nach sich zieht (siehe Abschnitt 2) [2]. Die zunehmende Abhängigkeit der Bevölkerung und Wirtschaft von einer reibungslosen Versorgung mit Elektrizität bildet demzufolge eine ernstzunehmende Schwachstelle für die Gesellschaft. Im Hinblick auf die „Stromversorgung der Zukunft“, dem sogenannten intelligenten Stromnetz oder Smart Grid, ergeben sich neben neuen Möglichkeiten auch zusätzliche Risiken für die Energieversorgung.

Ziel dieser Arbeit ist es, bekannte Schwachstellen und Sicherheitsrisiken der Elektrizitätsversorgung zu analysieren. In einem Ausblick wird zudem auf Herausforderungen eingegangen, die sich durch die Einführung des Smart Grids ergeben. Zunächst wird hierfür jedoch die Vulnerabilität der Elektrizitätsversorgung näher betrachtet. Anschließend wird anhand der Analyse vergangener großer Stromausfälle aufgezeigt, wie sich das Zusammenwirken verschiedener Faktoren auf die Stabilität des Stromnetzes auswirken kann. Abschließend werden mögliche Angriffsszenarien gegen die Elektrizitätsinfrastruktur vorgestellt.

2. VERWUNDBARKEIT DER ELEKTRIZITÄTSVERSORGUNG

Ein grundsätzliches Problem der Elektrizitätsversorgung besteht darin, dass Energie im Wesentlichen zur selben Zeit verbraucht werden muss wie sie produziert wird und umgekehrt - Energie zu speichern ist nur in begrenztem Maße möglich. Das Gleichgewicht von Stromerzeugung und Stromabnahme zu halten, ist daher von besonders hoher Bedeutung [9, 13].
Fällt unvorhergesehen ein Kraftwerk oder eine Versorgungsleitung aus, so kommt es in kürzester Zeit zu Spannungsschwankungen im Stromnetz. Wenn diese nicht innerhalb weniger Sekunden ausgeglichen werden können, führt dies durch Sicherheitsabschaltungen bei zu hoher Last auf den Leitungen im ungünstigsten Fall zu einem Dominoeffekt, durch den das gesamte Stromnetz zusammenbrechen kann [5, 13].

Das Wiederanfahren von Kraftwerken und die Wiederherstellung des Netzes unter Einhaltung des Gleichgewichtes von Stromerzeugung und -abnahme ist indes ein komplizierter und langwieriger Prozess, der, wie Ausfälle aus der Vergangenheit zeigen (siehe Abschnitt 3), mehrere Stunden oder sogar Tage in Anspruch nehmen kann. Die mittelbaren und unmittelbaren Auswirkungen auf die Gesellschaft und andere Infrastruktursektoren sind hierbei immens (siehe Abbildung 1). Besonders stark betroffen sind nach [9] unter anderem die Informations- und Kommunikationstechnologien, das Transport- und Verkehrswesen, Industrie- und Produktionsbetriebe, sowie die Trinkwasser- und Nahrungsmittelversorgung. Weitergehende Untersuchungen zu den gesellschaftlichen Auswirkungen eines Stromausfalls finden sich in [5], [6] und [9].

doi: 10.2313/NET-2013-08-1_05

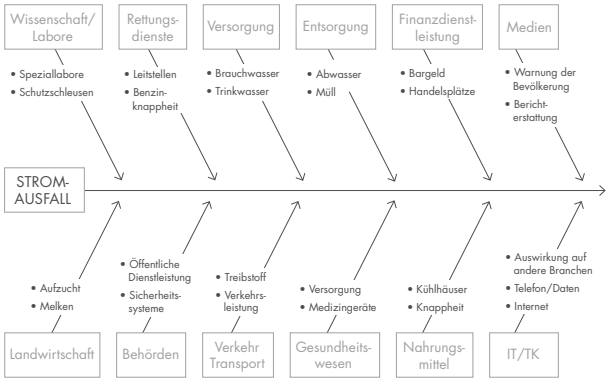

Abbildung 1: Auswirkungen eines Stromausfalls auf andere Infrastrukturen [9]

Im Folgenden wird nun zunächst die Verwundbarkeit der heutigen Elektrizitätsversorgung anhand der Bereiche Exposition (Verwundbarkeit gegenüber äußeren Gefahrenquellen wie Naturereignissen), Anfälligkeit (Systemimmanente Schwachpunkte) und Bewältigungskapazität (Möglichkeiten die Auswirkungen eines Stromausfalls zu reduzieren) nach [5] analysiert.

2.1 Exposition

Zur Analyse der äußeren Gefahrenquellen für kritische Infrastrukturen wird nach [5] zwischen Naturgefahren und von Menschen mutwillig verursachten Gefahren unterschieden.

2.1.1 Naturgefahren

Zu den Naturgefahren zählen sämtliche Einflüsse des Wetters, Erdbeben und Vulkanausbrüche, magnetische Stürme sowie Meteoriteneinschläge. Die Exposition gegenüber diesen Natureinflüssen ist regional unterschiedlich ausgeprägt, in flussnahen Gebieten ist beispielsweise eher mit Hochwasserereignissen zu rechnen. Auch die zeitliche Dimension der Einflüsse variiert stark. Hitzewellen können zum Beispiel mehrere Tage bis Wochen andauern, während Hagelereignisse in der Regel in wenigen Minuten bis Stunden vorüber sind [5].

Naturgefahren sind für die Elektrizitätsversorgung von besonderer Bedeutung. Ein Großteil der wichtigen Hochspannungsleitungen [1] ist oberirdisch verlegt und somit Wind und Wetter ausgesetzt.

2.1.2 Kriminelle Handlungen

Kritische Infrastrukturen sind aufgrund ihrer exponierten Stellung und ihrer gesellschaftlichen Bedeutung in besonderem Maße Gefahren wie Terrorismus, Sabotage, Krieg und sonstiger Kriminalität ausgesetzt [2]. Bereits in der Vergangenheit waren Gas- und Ölpipelines beliebte Ziele für terroristische Anschläge in politisch instabilen Regionen [5]. Ein vergleichbarer Angriff auf Hochspannungsleitungen oder Transformatorstationen stellt daher ein konkretes Bedrohungsszenario dar [10].

[1] `http://de.wikipedia.org/wiki/Stromnetz`

Cyberattacken bilden eine spezielle Form von kriminellen Handlungen gegenüber kritischen Infrastrukturen. Nach [11] lassen sich diese in fünf Kategorien mit steigendem potentiellen Schadensausmaß unterscheiden: Cybervandalismus, Internetkriminalität, Cyberspionage, Cyberterrorismus und Cyberwar.

Für die Stromversorgung von besonderer Bedeutung sind die Felder Cyberterrorismus und Cyberwar [5]. Die Prozesssteuerungssysteme der Energieerzeuger und -versorger (sogenannte SCADA Systeme - *Supervisory Control and Data Acquisition*) bieten hierbei eine große Angriffsfläche, vor allem weil diese zunehmend auch über das Internet vernetzt werden und oftmals nicht ausreichend geschützt sind [3].

Ein bekanntes Beispiel für einen erfolgreichen Angriff über ein SCADA-System ist der im Juni 2010 entdeckte Stuxnet-Wurm. Das mutmaßliche Ziel von Stuxnet war es, Urananreicherungsanlagen im Iran zu zerstören [7]. Weitergehende Informationen zu dem Stuxnet-Wurm und die daraus abzuleitenden Konsequenzen sind in [22] zu finden.

2.2 Anfälligkeit

Im Folgenden werden nach [5] Faktoren beschrieben, die sich maßgeblich auf die Anfälligkeit einer kritischen Infrastruktur wie der Elektrizitätsversorgung auswirken. Diese können als systemimmanente Faktoren aufgefasst werden, die vom System selbst beeinflussbar sind.

2.2.1 Institutionelle Faktoren

Ein wichtiger Faktor zur Beschreibung der Anfälligkeit der Elektrizitätsversorgung ist die Kapazität und die Auslastung des Stromnetzes. Eine zu hohe Belastung des Netzes kann dazu führen, dass selbst kleine Störungen große Schäden verursachen können [5].

Eine weitere Schwachstelle ist die komplexe Organisationsstruktur des Elektrizitätssystems, das sich dadurch auszeichnet, dass eine Vielzahl von Unternehmen national und international zusammenarbeiten, kommunizieren und beispielsweise Wartungsarbeiten koordinieren müssen [5]. Eine unzureichende Kommunikation und Koordination unter den Betreibern war zum Beispiel einer der Hauptgründe für den Stromausfall vom vierten November 2006 (siehe Abschnitt 3).

2.2.2 Gesellschaftliche Faktoren

Die gesellschaftlichen Faktoren beschreiben die Auswirkungen von zum Beispiel Bevölkerungsdichte, Jahres- und Tageszeit und dem Wetter auf die Stromnachfrage [5]. Um das System von Stromverbrauch und Stromproduktion im Gleichgewicht zu halten, sind diese Faktoren von entscheidender Bedeutung.

2.2.3 Systembezogene Faktoren

Ein weiterer problematischer Punkt ist die hohe Komplexität des Elektrizitätssystems, das aus einer Vielzahl unterschiedlicher technischer Systeme besteht [8]. Das Stromnetz ist außerdem ein *gewachsenes* System, sodass das Zusammenwirken verschiedener Komponenten oft nicht von Vorhinein absehbar ist [5].

Große, sprungartige Störungen des Versorgungssystems, verursacht durch den Ausfall von Kraftwerken oder Versorgungsleitungen, führen unmittelbar zu Veränderungen der anliegenden Spannung und Leistungsflüssen. Dadurch kann es zu Überlastungen anderer Komponenten kommen, die daraufhin ebenfalls ausfallen, was wiederum andere Komponenten zum Ausfallen bringen kann [13]. Diese sogenannten Kaskadeneffekte sind Grundlage für großflächige Stromausfälle, wie beispielsweise während des großen Stromausfalls vom 14. August 2003 im Nordosten der USA und in Teilen Kanadas (siehe Abschnitt 3).

2.2.4 Technologische Faktoren

Die Anfälligkeit der Elektrizitätsversorgung wird entscheidend durch das Qualitätsniveau seiner Komponenten beeinflusst. Dazu zählen neben Wartung und Alter auch Schutzmechanismen gegenüber äußeren Gefahren wie zum Beispiel Cyberattacken [5]. Letztere werden in den späteren Abschnitten 4 und 5 genauer betrachtet.

2.2.5 Menschliche Faktoren

Menschliche Fehler stellen einen weiteren Faktor dar, der die Anfälligkeit der Elektrizitätsversorgung beeinflusst. Dazu zählen Unaufmerksamkeit, Fehler aufgrund unzureichender Notfallpläne und Fehler, die durch den Mangel an Echtzeitinformationen im Fehlerfall entstehen [5, 8].

2.3 Bewältigungskapazität

Der dritte Bereich Bewältigungskapazität zur Vulnerabilitätsanalyse einer kritischen Infrastruktur wie der Stromversorgung beschreibt Möglichkeiten und Maßnahmen, die Verwundbarkeit zu reduzieren [5]. Darunter fallen vorbeugende Maßnahmen zur Vermeidung von Störfällen, zur Behandlung von Fehlern und der Retrospektive.

2.3.1 Redundanz

Für die Elektrizitätsinfrastruktur gibt es europaweite Vorschriften für Planung und Betrieb des Netzes. Versorgungsleitungen werden so geplant und betrieben, dass die Stromversorgung bei einem Ausfall eines beliebigen der insgesamt n Versorgungswege aufrecht erhalten werden kann. Man spricht hier vom sogenannten (n-1)-Kriterium [4]. Die Einhaltung des (n-1)-Kriteriums muss von den Übertragungsnetzbetreibern ständig überprüft werden [12]. In der Regel geschieht dies bei den deutschen Netzbetreibern alle 15 Minuten [4].
Bei Nichteinhaltung des (n-1)-Kriteriums können bereits relativ kleine Störungen Kaskadeneffekte auslösen, wie es zum Beispiel 2006 der Fall war (siehe Abschnitt 3).

2.3.2 Engpassmanagement

In einem Wechselspannungs- bzw. Drehstromnetz gibt es eine definierte Netzfrequenz die in engen Grenzen konstant gehalten werden muss. Im öffentlichen Netz in Europa beträgt diese 50 Hz. Steigt die Netzlast ungeplant an oder kommt es zu einer Abnahme der Einspeisung ins Stromnetz, sinkt die Netzfrequenz (*Unterfrequenz*). Im gegenteiligen Fall, also bei zu hoher Einspeisung im Vergleich zum Verbrauch, steigt die Netzfrequenz (*Überfrequenz*). Einer Überfrequenz kann durch Reduzierung der Einspeisung oder Hinzuschalten von Verbrauchern (zum Beispiel Pumpspeicherwerken) entgegengewirkt werden [13].

Um eine Unterfrequenz auszugleichen wird zunächst versucht, zusätzliche Reserven zu aktivieren. Reichen die Reserven nicht aus, ist der Lastabwurf das letzte Mittel zur Wiederherstellung der normalen Netzfrequenz bei Unterfrequenz während eines Störfalls. Dabei werden Teile des Netzes (der Verbraucher) abgespalten, um so die Last zu reduzieren und gleichzeitig die Netzfrequenz zu erhöhen. Bereits ab einer Abweichung von einem Hertz werden durch Lastabwurfrelais 10 bis 15 % der anliegenden Last abgeworfen. Fällt die Frequenz unter 47.5 Hz, so werden Kraftwerke zu ihrem eigenen Schutz vom Netz abgetrennt [13].

2.3.3 Inselbetrieb

Zur Vermeidung des Zusammenbruchs des gesamten Verbundnetzes, zum Beispiel des europäischen UCTE-Netzes, kann das Netz als Notfallmaßnahme auch aufgetrennt werden, sodass Kaskadeneffekte nicht auf andere Regionen übergreifen können. Nach Stabilisierung der Lage in den Inselgebieten werden diese wieder zu einem Verbundnetz zusammengelegt [14].

2.3.4 Transparenz

Im Falle einer Störung ist die Nachvollziehbarkeit der Funktionsweise und der Ereignisse für die betroffenen Akteure von hohem Wert. Ebenfalls unter diesen Punkt fällt die Krisenkommunikation nach Außen über die Medien [5].

3. GROSSE STROMAUSFÄLLE IN DER VERGANGENHEIT

Zur Analyse der Verwundbarkeit der Elektrizitätsversorgung werden im Folgenden vergangene Stromausfälle betrachtet, um Ursachen und Fehlerketten zu identifizieren.

3.1 Nordamerika, 14. August 2003

Im Nordosten der USA und in Teilen Kanadas kam es am 14. August 2003 zu einem weitläufigen und folgenreichen Stromausfall mit etwa 50 Millionen betroffenen Menschen. In einigen Teilen der USA konnte die Stromversorgung erst am vierten Tag wieder vollständig hergestellt werden. Der entstandene wirtschaftliche Schaden wird allein in den USA auf vier bis zehn Milliarden US Dollar geschätzt [15].

Ausgangspunkt waren mehrere Fehler im Umgang mit einem System zur Überwachung und Simulation des Netzzustandes. Dadurch hatten die Operateure in der Leitstelle des Betreibers FirstEnergy von 12:15 bis 16:04 Uhr Ortszeit kein klares Bild der Lage, wodurch notwenige Schritte zur Gefahrenabwehr ausblieben. Zusätzlich verursachte ein Softwarefehler zwischen 14:14 und 15:59 einen Komplettausfall der Alarmfunktion des Systems [15].

Um 13:31 Uhr ging das Kraftwerk Eastlake 5 fehlerbedingt vom Netz, 90 Minuten später fiel, ohne Warnmeldung, auch eine wichtige Hochspannungsleitung aus. Die spätere Untersuchung ergab, dass zu diesem Zeitpunkt das (n-1)-Kriterium nicht mehr erfüllt war. Um 15:32 und 15:41 Uhr fielen zwei weitere Hochspannungsleitungen aus. Bei allen drei Leitungen waren Kurzschlüsse aufgrund des zu hohen Baumbestands in Kombination mit der temperaturbedingten Ausdehnung der Leitungen die Ursache der Ausfälle [15].

Infolge des einsetzenden Spannungsabfalles brach zunächst

das lokale Versorgungsnetz im Norden von Ohio zusammen. Um 16:05 Uhr Ortszeit fiel schließlich eine entscheidende Transportleitung aus, was in den umliegenden Regionen zu Überlastungen der Leitungen führte. Das Verbundnetz zerfiel so in mehrere Inselnetze. Innerhalb von rund 10 Minuten gingen 265 Kraftwerke, darunter 10 Atomkraftwerke, und 508 Generatoren vom Netz [15].

3.2 Europa, 4. November 2006

Am 4. November 2006 ereignete sich ein großflächiger Stromausfall in einigen Teilen Europas mit etwa 15 Millionen betroffenen Menschen. Ausgangspunkt des Stromausfalls war eine planmäßige Abschaltung einer Höchstspannungsleitung im Emsland, welche die Ems überquert, um die Überführung eines Kreuzfahrtschiffes zu ermöglichen. Die ursprünglich geplante Abschaltung für den 5. November um 1:00 Uhr wurde kurzfristig am 3. November auf den 4. November 22:00 Uhr vorverlegt. Wie aus dem Bericht der Bundesnetzagentur hervorgeht erfolgte seitens des Betreibers E.ON keine (n-1)-Berechnung. Durch das Abschalten der Leitung war das E.ON Netz anschließend, auch durch eine andere Wartung bedingt, nicht mehr in einem sicheren Zustand, das (n-1)-Kriterium war also für das gesamte Verbundnetz nicht mehr erfüllt [4].

Hinzu kommt, dass die Lastflussberechnungen zur Bestimmung der Netzsicherheit zu diesem Zeitpunkt falsch waren, da Grenzwerte für eine Hochspannungsleitung zwischen den Betreibern RWE und E.ON nicht korrekt ausgetauscht wurden [4].

Der Auslöser des Stromausfalls war im Anschluss an die Abschaltung der Leitung um 21:38 Uhr ein verhältnismäßig geringer Lastflußanstieg um ca. 160 A auf der Leitung Landesbergen - Wehrendorn zwischen 22:02 Uhr und 22:10 Uhr. Es kam daraufhin zur Überlastung dieser Leitung, die sich automatisch abschaltete. Durch diesen Vorgang fielen kaskadenartig weitere Leitungen in ganz Europa aus, was dazu führte, dass das europäische Netz innerhalb von wenigen Sekunden in 3 Teile mit unterschiedlichen Frequenzen zerfiel (vgl. Abbildung 2) [4].

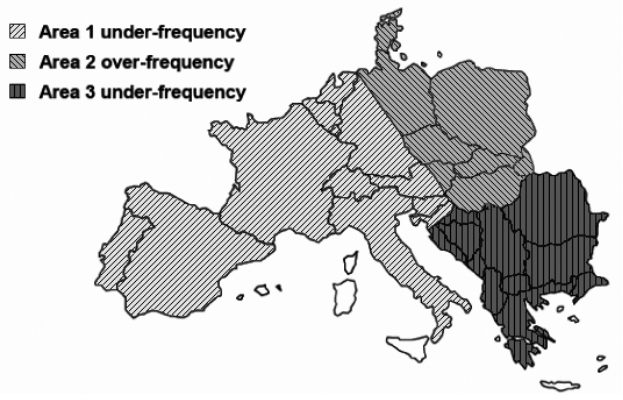

Abbildung 2: Schematische Darstellung der Aufsplittung des UCTE-Netzes [4]

In den Bereichen 1 und 3 sank die Frequenz auf 49.0 Hz bzw. 49.7 Hz. Als Gegenmaßnahme wurden hier automatisch Verbraucher vom Netz getrennt und zusätzliche Erzeugungseinheiten aktiviert. Der nord-östliche Bereich 2 verzeichnete aufgrund eines Energieüberschusses einen Frequenzanstieg auf kurzzeitig bis zu 51.4 Hz. Um dem entgegenzuwirken wurde kurzfristig die Leistung von Erzeugungseinheiten zurückgefahren und Pumpen in Pumpspeicherwerken aktiviert [4].

Um 23:57 Uhr schließlich waren die Teilnetze wieder zum Verbundnetz zusammengeschlossen und alle Verbraucher an das Stromnetz angeschlossen [4].

3.3 Bewertung

Beide Ausfälle zeigen eine Vielzahl von Gefahrenquellen für die Stromversorgung. Der Abschlussbericht der nordamerikanischen Netzaufsicht identifizierte außerdem folgende Probleme auf Seiten der Betreiber des Stromnetzes: Mangelnde Systemkenntnis, unzulängliches Situationsbewusstsein, unzureichendes Vegetationsmanagement und fehlende Unterstützung durch Echtzeitdaten [15]. Besonders kritisch ist bei beiden Ausfällen das Ausbleiben der (n-1)-Rechnung zu sehen [4, 15].

4. SMART GRID SYSTEME

Das Smart Grid unterscheidet sich vom bisherigen Stromnetz in einem wichtigen Punkt: Der Strom soll nicht mehr verbrauchsbasiert geliefert, sondern erzeugungsorientiert verbraucht werden, um so eine effizientere, wirtschaftlichere und nachhaltigere Stromversorgung zu ermöglichen [5]. Es zeichnet sich durch seine dezentrale Struktur aus. Daten über den aktuellen Verbrauch werden direkt beim Verbraucher mit Hilfe der sogenannten Smart Meter erfasst. Über Preissignale sollen Geräte wie Nachtspeicheröfen, Waschmaschinen oder ähnliche zu einem Zeitpunkt mit Energieüberschuss in Betrieb genommen werden, um die vorhandene Energie möglichst optimal nutzen zu können. Die involvierten Systeme werden mit Hilfe von Informations- und Telekommunikationsinfrastrukturen dezentral betrieben und gesteuert. Adäquate Sicherheitsmaßnahmen gegen Angriffe über und auf die Kommunikationsinfrastruktur sind daher von großer Bedeutung für die Versorgungs- und Ausfallsicherheit des Stromnetzes [7].

4.1 Herausforderungen

Das Lastmanagement des Stromnetzes im Smart Grid benötigt aktuelle, korrekte und vollständige Datensätze über den Bedarf an Strom von den Verbrauchern. Die Verbraucher sind dazu über eine Kommunikationsinfrastruktur mit den Netzbetreibern vernetzt. Auf Seiten der Netzbetreiber bedeutet dies, dass vermehrt SCADA-Systeme ans Internet angeschlossen werden, wodurch gezielte Angriffe auf diese Systeme ermöglicht bzw. vereinfacht werden [7].

In [7] werden vier potentielle Angriffsebenen auf Smart Grid Netze im Hinblick auf die Netzsicherheit identifiziert:

- *Hardware*: Viele Hardware Komponenten des Smart Grids wie zum Beispiel Smart Meter sind direkt physikalisch angreifbar. Ein Angreifer könnte so durch Manipulation der vom Smart Meter erhobenen Daten zur Destabilisierung des Stromnetzes beispielsweise einen sehr hohen Energiebedarf vortäuschen [7].

doi: 10.2313/NET-2013-08-1_05

- *Software*: Die verwendeten Softwaresysteme in Smart Metern bieten oft nur ungenügende Schutzmaßnahmen gegenüber Angreifern. Durch Einschleusen von Schadsoftware kann ein Angreifer das Verhalten seines Systems gezielt manipulieren, um sich so zum Beispiel kostenlose Energie zu beschaffen [7].

- *Anwendungen*: Durch manipulierte Anwendungen auf den Smart Metern können andere Systeme, zum Beispiel die SCADA-Systeme der Netzbetreiber, angegriffen oder gestört werden [7].

- *Kommunikationsnetze*: Unter diesen Punkt fallen Angriffe, die über oder auf das Kommunikationsnetz (zum Beispiel Denial of Service Angriffe) stattfinden, mit dem Ziel das Kommunikationsnetz selbst oder angebotene Dienste der Betreiber lahmzulegen [7].

4.2 Sicherheitsmaßnahmen

Das Smart Grid ist ein großes und komplexes System. Um die Sicherheit dieses Systems zu gewährleisten, ist eine Vielzahl von Sicherheitsmaßnahmen vonnöten.
Im Folgenden werden dazu zwei zentrale Maßnahmen vorgestellt. Ein guter Überblick über weitere Schutzmechanismen und aktuelle Forschungsarbeiten wird in [16] gegeben.

4.2.1 Sichere Netze

Für die Kommunikation zwischen den verschiedenen Komponenten des Smart Grids werden eine stabile Kommunikationsinfrastruktur und effiziente, aber auch sichere Kommunikationsprotokolle benötigt [16]. Die Anforderungen an die Kommunikationsprotokolle umfassen zudem Echtzeitfähigkeit, einen effizienten Umgang mit der zur Verfügung stehenden Bandbreite, wenig bis keinen Konfigurationsaufwand sowie sichere Ende-zu-Ende Kommunikation durch Verschlüsselungsmaßnahmen. Ein limitierender Faktor ist die oftmals nur geringe Rechenleistung vieler Komponenten im Smart Grid (zum Beispiel Smart Meter) [7, 16].

4.2.2 Angriffserkennung

Neben der sicheren Kommunikationsinfrastruktur bilden Systeme zur Erkennung von Angriffen (sogenannte *Intrusion Detection Systems*) eine zweite Säule zur Sicherung des Smart Grids. Grundsätzlich gibt es drei unterschiedliche Verfahren zur Erkennung eines Einbruchversuches [17]:

- *Signaturbasierte Erkennung* durch Vergleichen mit bekannten Angriffsmustern,

- *Anomaliebasierte Verfahren*, die durch statistische Verfahren Abweichungen vom normalen Systemverhalten erkennen und

- *Spezifikationsbasierte Verfahren*, die ein unerwartetes Verhalten durch Vergleich des Systemzustandes mit einer logischen Spezifikation des Systems identifizieren können.

Spezifikationsbasierte Verfahren sind nach [17] am besten für die Überwachung einer Smart Grid Infrastruktur geeignet. Das erwünschte Systemverhalten wird dabei mit Hilfe formaler Methoden spezifiziert. Jede Art von Ereignissen oder Ereignisketten, die zu einer Abweichung vom spezifizierten Systemverhalten führen, werden als Verletzung der Sicherheitsbestimmungen angesehen.

Diese Verfahren erzielen idealerweise eine höhere Genauigkeit bei der Erkennung von Angriffen als anomalie- bzw. signaturbasierte Verfahren [17]. Für die formale Beschreibung des Systems und seiner zulässigen Zustände wurden in den vergangenen Jahren verschiedene Formalisierungsmethoden wie zum Beispiel reguläre Ausdrücke für Ereignisse, abstrakte Beschreibungssprachen für Zustandsmaschinen oder gefärbte Petrinetze vorgeschlagen und untersucht [18]. Zusätzlich können zur Überprüfung der Korrektheit und Vollständigkeit einer solchen Systemspezifikation Methoden der formalen Verifikation eingesetzt werden [18]. Die Konzeption und Verifizierung eines solchen Systems ist jedoch vergleichsweise kostenintensiv und noch Gegenstand aktiver Forschung [16, 17, 18].

5. ANGRIFFE AUF DIE STROMVERSORGUNG

Im Folgenden werden kurz zwei mögliche Angriffsszenarien auf die Stromversorgung vorgestellt. Diese betreffen sowohl das Stromnetz von heute, als auch die Smart Grid Infrastruktur.

5.1 Kaskadenbildung

Ein vorsätzlicher Angriff auf die Energieversorgung könnte, um möglichst viel Schaden anzurichten, gezielt versuchen, einen sich kaskadenartig ausbreitenden Ausfall von Komponenten im Stromnetz anzustoßen. In [19] wurden in diesem Zusammenhang zwei unterschiedliche Angriffsstrategien auf Systeme (Knoten) in einem Versorgungs-Netzwerk untersucht und miteinander verglichen:

HL: Gezieltes Ausschalten von Knoten mit der höchsten bzw.
LL: mit der niedrigsten anfänglichen Last.

Die Last L_j eines Knotens j wurde hierfür definiert als Produkt von Knotengrad und Summe der Grade der Nachbarknoten Γ_j: $L_j = [k_j(\sum_{m\in\Gamma_j} k_m)]^\alpha$, wobei k_i den Grad eines Knotens i beschreibt und α ein tunebarer Parameter zur Modifikation der Initiallast ist [19]. Des weiteren wird zur Vereinfachung des Modells ein linearer Zusammenhang zwischen der Last eines Knotens und seiner Kapazität angenommen (siehe unten).

Fällt, wie in Abbildung 3 zu sehen, ein Knoten i aus, wird seine Last auf die umliegenden Knoten verteilt. Die zusätzliche Last für einen benachbarten Knoten j wurde hierfür als proportional zu dessen Initiallast definiert:

$$\Delta L_{ji} = L_i \frac{L_j}{\sum_{n\in\Gamma_i} L_n}$$

Steigt die Last für einen Knoten j dadurch über seine maximal zulässige Last, fällt auch dieser aus. Das Modell benutzt hierfür die Toleranzkonstante T (≥ 1), sodass TL_j die maximal zulässige Last beschreibt. Je größer der Wert von T, desto mehr freie Kapazitäten haben die Knoten, um die zusätzliche Last abzufangen. Der Wert T_c beschreibt nun die

doi: 10.2313/NET-2013-08-1_05

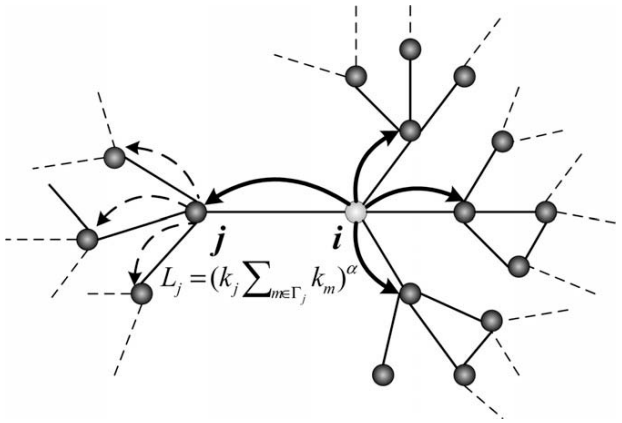

Abbildung 3: Lastumverteilung bei Ausfall von Knoten i [19]

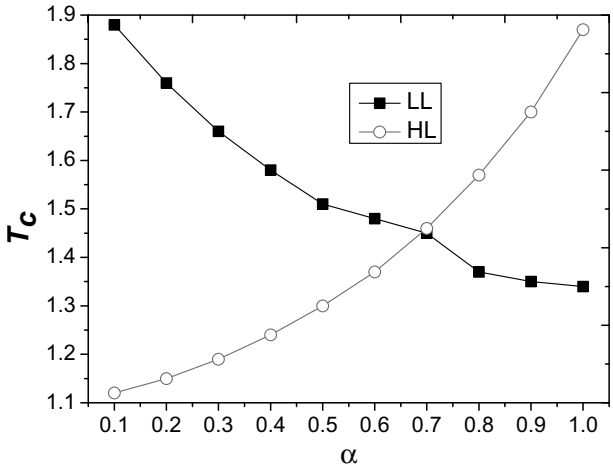

Abbildung 4: Relation zwischen T_c und α unter den beiden Angriffsszenarien [19]

kritische Grenze, ab der für kleinere Werte von T Kaskadeneffekte auftreten [19].

Die Ergebnisse der Untersuchungen in [19], die durch Simulation anhand eines Ausschnitts des amerikanischen Stromnetzes entstanden sind, sind in Abbildung 4 zu sehen. Für $\alpha = 0.7$ sind die Auswirkungen beider Angriffsmethoden in etwa gleich. Für $\alpha \geq 0.7$ sind Angriffe auf Knoten mit hoher Initiallast deutlich effektiver als auf Knoten mit niedriger Last (zum Beispiel für $\alpha = 1.0$ treten für die erste Angriffsmethode erst ab ca. 90 % freie Kapazitäten keine Ausfälle mehr auf). Je größer der Wert α, desto höher ist die Initiallast der Knoten und damit die zusätzliche Last, die im Falle eines künstlich erzeugten Ausfalls auf die benachbarten Knoten übergeht [19].

Für kleinere Werte von α hingegen wäre Angriffsmethode LL effektiver, was bedeutet, dass in diesem Fall Knoten mit niedrigerer Initiallast und damit, aufgrund der Definition von Last, einem niedrigeren „Vernetzungsgrades“ eine wichtigere Rolle im Netz einnehmen als Knoten mit einem hohen Initiallastwert [19].

Die Ergebnisse der Arbeit in [19] können dazu verwendet werden, gezielt Schwachstellen in der Versorgungsinfrastruktur zu identifizieren und diese durch geeignete Maßnahmen wie zusätzliche Überkapazitäten zusätzlich abzusichern.

5.2 Angriffe durch Lastmanipulation

Wie die Stromausfälle aus der Vergangenheit gezeigt haben, ist das Lastmanagement ein ausschlaggebender Faktor für die Stabilität der Elektrizitätsversorgung. Durch die Umstellung auf das Smart Grid eröffnen sich für Angreifer neue Möglichkeiten für Cyberattacken gegen die Elektrizitätsinfrastruktur. Es wäre denkbar, dass ein Angreifer versucht beispielsweise durch falsche Preissignale oder durch Manipulation der Lastdaten der Verbraucher, gezielt eine Überlastung einer Versorgungseinheit herbeizuführen [7, 20, 21].

In [21] wurde versucht, ein Angriffsszenario durch künstliche Veränderung der Lastdaten zu modellieren. Die Ergebnisse zeigen, dass durch gezielte Manipulation der Verbraucherdaten mit einer Abweichung von maximal 50 % von der tatsächlichen Last künstlich Lastabwürfe und Leitungsausfälle herbeigeführt werden könnten.

Neben Angriffen auf das Lastmanagement besteht potenziell auch die Möglichkeit, über Angriffe durch das Internet aktiv den Stromverbrauch auf Seiten des Verbrauchers zu erhöhen. Als Beispiele werden in [20] über das Internet geführte Attacken auf Rechenzentren (Erzeugung von Rechenlast) oder Haussteuerungen in Großwohnanlagen (Aktivieren vieler Energieverbraucher) aufgeführt.

6. ZUSAMMENFASSUNG UND AUSBLICK

Kritische Infrastrukturen wie das Stromnetz sind von wichtiger Bedeutung für das Funktionieren einer Gesellschaft. Große Stromausfälle aus der Vergangenheit haben jedoch deutliche Schwachstellen der Elektrizitätsversorgung aufgezeigt. Durch die Umstellung auf das zukünftige Energie-Versorgungssystem, das Smart Grid, eröffnen sich zusätzliche Möglichkeiten diese, für die Gesellschaft kritische Infrastruktur, durch Cyberattacken anzugreifen. Die Sicherstellung einer stabilen Elektrizitätsversorgung ist Gegenstand aktueller Forschungsarbeiten mit Fokus auf die Sicherung des Smart Grids.

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik: *Analyse Kritischer Infrastrukturen*, 2008

[2] Bundesministerium des Inneren: *Nationale Strategie zum Schutz Kritischer Infrastrukturen*, 2009

[3] Bundesamt für Sicherheit in der Informationstechnik: *Die Lage der IT-Sicherheit in Deutschland 2009*, 2009

[4] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen: *Bericht über die Systemstörung im deutschen und europäischen Verbundsystem am 4. November 2006*, 2007

[5] J. Birkmann, C. Bach, S. Guhl, M. Witting, T. Welle, M. Schmude: *State of the Art der Forschung zur*

Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall, Forschungsforum Öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 2, 2010

[6] D. F. Lorenz: *Kritische Infrastrukturen aus Sicht der Bevölkerung*, Forschungsforum Öffentliche Sicherheit, Schriftenreihe Sicherheit Nr. 3, 2010

[7] C. Eckert, C. Krauß: *Sicherheit im Smart Grid*, In Datenschutz und Datensicherheit, Vol. 35, Nr. 8, 2011

[8] M. Amin: *Energy Infrastructure Defense Systems*, In Proceedings of the IEEE, Vol. 93, No. 5, 2005

[9] R. Göbel, S. S. von Neuforn, G. Reichenbach, H. Wolff: *Risiken und Herausforderungen für die öffentliche Sicherheit in Deutschland*, In Grünbuch des Zukunftsforums, 2008

[10] A. Shull: *Assessment of Terrorist Threats to the Canadian Energy Sector*, In CCISS Critical Energy Infrastructure Protection Policy Research Series, Vol. 1, Nr. 4, 2006

[11] D. Möckli: *Cyberwar: Konzept, Stand und Grenzen*, Center for Security Studies - Analysen zur Sicherheitspolitik, Nr. 71, 2010

[12] European Network of Transmission System Operators for Electricity: *Operation Handbook Part 5*, 2010, `https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/Operation_Handbook/Policy_5_final.pdf`

[13] A. J. Schwab: *Elektroenergiesysteme*, 2009

[14] R. Paschotta: *Das RP-Energielexikon - Verbundnetz*, `http://energie-lexikon.info/verbundnetz.html`

[15] U.S.-Canada Power System Outage Task Force: *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, 2004

[16] T. Baumeister: *Literature Review on Smart Grid Cyber Security*, 2010

[17] R. Berthier, W. H. Sanders, H. Khurana: *Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions*, In First IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010

[18] R. Berthier, W. H. Sanders: *Specification-based Intrusion Detection for Advanced Metering Infrastructures*, In 17th IEEE Pacific Rim International Symposium on Dependable Computing, 2011

[19] J. Wang, L. Rong: *Cascade-based attack vulnerability on the US power grid*, In Safety Science, Vol. 47, Nr. 10, 2009

[20] A. Mohsenian-Rad, A. Leon-Garcia: *Distributed Internet-based Load Altering Attacks against Smart Power Grids*, In IEEE Transactions on Smart Grid, Vol. 2, Ausgabe 4, 2011

[21] Y. Yuan, Z. Li, K. Ren: *Modeling Load Redistribution Attacks in Power Systems*, In IEEE Transactions on Smart Grid, Vol. 2, Ausgabe 2, 2011

[22] M. Brunner, H. Hofinger, C. Krauß, C. Roblee, P. Schoo, S. Todt: *Infiltrating critical infrastructures with next-generation attacks*, Fraunhofer Institute for Secure Information Technology (SIT), 2010