Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung

IT-Sicherheit in der Wasserversorgung

Schutz kritischer Infrastrukturen

Stefan Schumacher

Informationstechnische Systeme werden in immer mehr industriellen Bereichen eingesetzt. Seien es klassische Regelungstechnische Systeme, SCADA oder Industrie 4.0 und das Internet der Dinge. Auch in der Wasserversorgung gewinnen Automatisierungstechnik und Informationstechnik immer mehr Bedeutung. Trotz des Einsatzes in dieser kritischen Infrastruktur kommt der IT-Sicherheit hier häufig nicht die notwendige Bedeutung zu.

Dies ist eine überarbeite Fassung des Artikels zum Tagungsband der Trinkwassertagung Sachsen-Anhalt 2014 (Schumacher 2014b)

Citation: Schumacher, S. (2016). IT-Sicherheit in der Wasserversorgung: Schutz kritischer Infrastrukturen. *Magdeburger Journal zur Sicherheitsforschung*, *11*, 667–685. Zugriff 1. März 2016, unter http : / / www . sicherheitsforschung-magdeburg.de/publikationen/journal.html

Version 2016/03/08 13:08

1 Einführung

Weder aus Unternehmen noch aus den Haushalten sind Computer und Internet wegzudenken. So nutzen nach einer Statistik[1] des Branchenverbandes BITKOM bereits mehr als drei Viertel aller deutschen Haushalte einen Internetzugang, wobei zwei Drittel aller Haushalte Breitbandinternet und jeder vierte Deutsche mobile Internetzugänge via Laptop oder Handy nutzen. Ebenso nutzen in Deutschland 61% aller Beschäftigten einen Computer am Arbeitsplatz. Es ist also heute schon fast unnormal geworden *keinen* Computer zu benutzen, zumindest wenn man zu den Jugendlichen oder Erwerbstätigen gehört.

Im Rahmen der Verbreitung von Computern, IT und Internetzugängen wurden und werden immer mehr Tätigkeiten via Internet angeboten. Seien es soziale Netzwerke wie Facebook oder Xing, die ohne PCs und Internet gar nicht möglich wären oder Business-2-Comsumer-Angebote (B2C) wie Internetbanking oder Handelsplattformen à la Ebay und Amazon. Auch in der Wirtschaftswelt sind viele Dienste nur noch via Internet verfügbar, zum Beispiel die sogenannten Business-2-Business-Dienste (B2B) wie die weltweite Kooperation von Softwareentwicklern oder der Datenaustausch zwischen Automobilherstellern und Zulieferern, der fast ausnahmslos virtuell stattfindet. Auch Produktionsanlagen[2] und Geräte kommunizieren inzwischen immer mehr über das Internet miteinander, so sollen beispielsweise nach dem Willen der EU sogenannte Smart Meter[3], also »intelligente« Stromzähler eingeführt werden, die den Verbrauch der Haushalte direkt und in Echtzeit an die Stadtwerke und Kraftwerke melden. Die Stromerzeuger sind auch interessiert daran, den Jahresverbrauch online auszulesen um die Kosten für menschliche Ableser einzusparen. Außerdem sollen aus Kostengründen die Smart Meter per Remote-Zugang abschaltbar sein, damit im Falle des Zahlungsverzugs oder Auszugs eines Kunden der Stromzugang sofort und bequem gekappt werden kann.

Unter den Stichwörtern »Industrie 4.0« sowie »Internet der Dinge« wird der Einsatz von Informationstechnologie noch weiter vorangetrieben. Dazu soll zukünftige Automatisierungstechnik in die Lage versetzt werden, sich selbst zu diagnostizieren, zu konfigurieren und zu optimieren.

Auf Managementebene gewinnen Konzepte wie Big Data und damit einhergehend Entscheidungsunterstützungsysteme an Bedeutung. Durch den Einsatz vielerlei Sensoren können Daten erfasst und algorithmisiert ausgewertet werden. Die Auswertung bildet dann die Grundlage für Managemententscheidungen.

All diese Szenarien birgen jedoch ein entscheidendes Problem – dass der Sicherheit.

Neben »einfachen« Sicherheitsproblemen, wie den verbreiteten Viren, Würmern und Trojanern sowie Spam- und Phishing-Mails, gibt es tagtäglich wenig elaborierte aber automatisierbare Angriffe gegen Internetbanking, die zwar eine geringe Erfolgsquote haben, in der Masse aber zu erklecklichen Gewinnen bzw. Schäden führen. Das CERT Coordination Center der Carnegie Mellon University katalogisiert Sicherheitslücken in Software. Sie stiegen von 171 im Jahre 1995 auf 7236 im Jahre 2007.

Allen u. a. (2000, Seite 43) zeigen die steigende Raffinesse von Angriffen auf IT-Sicherheitssysteme. Waren die ersten Angriffsmethoden wie Passwörter erraten in den 1980ern noch recht simpel, sind diese in den 2000ern wesentlich komplexer geworden. Dafür sanken die Fertigkeiten der Angreifer, da viele technische Angriffe inzwischen mittels vorhandener Software (»Skript«) von sogenannten Skript-Kiddies ausgeführt, die sich lediglich die fertigen Skripte verschaffen, um sie einzusetzen. Dadurch steigt die Zahl der Angriffe und Sicherheitsvorfälle von Jahr zu Jahr an, während gleichzeitig die technischen Voraussetzungen und intellektuellen Fähigkeiten auf Angreiferseite immer niedriger werden.

In der Wirtschaft spielt die IT-Sicherheit inzwischen auch eine große Rolle. Seien es Vorgänge wie Wirtschaftsspionage[4] oder Sabotage durch verärgerte Mitarbeiter. Auch Sicherheitsfehler in technischen Anlagen können zum Beispiel in Kernkraftwerken, Flugzeugen oder in der Raumfahrt[5] zu massiven, mitunter tödlichen, Konsequenzen führen.

Ebenso werden in der Politik und dem Militär seit einiger Zeit technische Sicherheitsprobleme antizipiert. So ist es theoretisch möglich über Sicherheitslücken[6] in den geplanten Smart Metern in einer konzertierten Aktion alle angschlossenen Haushalte aus dem Stromnetz herauszuschießen. Dies würde in der Folge aufgrund auftretender Überlastung der Stromnetze zum kaskadierenden Ausfall der Stromerzeuger führen. Da die Kraftwerke europaweit im Europäischen Verbundnetz zusammengeschlossen sind, könnten die Ausfälle kaskadieren und im Endeffekt die Stromversorgung in allen angeschlossenen Ländern ausschalten. Das heißt, dass ein einziger Implementierungsfehler in den Smart Metern halb Europa über Nacht in das »finstere Mittelalter der Stromlosigkeit« zurückkatapultieren könnte.

Gegenwärtig läuft daher getrieben von Stuxnet[7]

1 http://www.bitkom.org/de/markt_statistik/64003.aspx r. 2014-03-11

2 http://www.heise.de/security/meldung/Stuxnet-Wurm-kann-Industrieanlagen-steuern-1080584.html r. 2014-03-11

3 http://www.heise.de/security/meldung/Intelligente-Stromzaehler-Entwurf-fuer-Schutzprofil-zur-Diskussion-gestellt-1180901.html r. 2014-03-11

4 http://www.heise.de/newsticker/meldung/Verfassungsschutz-registriert-zunehmende-Wirtschaftsspionage-uebers-Internet-219591.html r. 2014-03-11

5 http://en.wikipedia.org/w/index.php?title=Death_by_PowerPoint&oldid=415751189 r. 2014-03-11

6 Siehe dazu Sambleben und Schumacher (2012) und Schumacher (2011, 2014a)

7 http://www.heise.de/thema/Stuxnet r. 2014-03-11

und diversen Spionagevorfällen[8] eine internationale Cyberwar-Debatte, in der viele Akteure von einem Krieg im Cyberspace ausgehen. Es zeigt sich also, dass der Einsatz von Informationstechnologie nicht nur Vorteile bietet, sondern insbesondere im Bereich der Sicherheit noch viele Probleme bestehen.

2 Assettanalyse

Um die Sicherheit eines IT-Systems einschätzen zu können, muss eine Gefährdungsanalyse der potenziellen Opfersysteme durchgeführt werden. Derartige Gefährdungsanalysen kann man zum einen als Organisation selbst durchführen, beispielsweise in dem man die ISO 27001[9] anwendet. Vereinfacht stellt man dazu eine Übersicht möglicher Angriffsziele auf und berechnet mögliche Schadensfälle und deren Eintrittswahrscheinlichkeit. Anschließend gewichtet man die Abhängigkeit bzw. Wichtigkeit des Angriffsziel und priorisiert entsprechende Schutzmaßnahmen. Die zentrale Frage ist daher: »Wie hoch ist die Wahrscheinlichkeit, dass ein Asset ausfällt und was passiert wenn es ausfällt?«.

Eine weitere beliebte Möglichkeit ist ein sogenannter Penetration Test (kurz Pen-Test). Diese Tests werden in der Regel von externen Sicherheitsberatern durchgeführt. Die Sicherheitsberater nutzen dabei in der Regel alle Werkzeuge und Methoden die echten Angreifern auch zur Verfügung stehen und versuchen damit, die Systeme einer Organisation anzugreifen und zu übernehmen. Gelingt es ihnen in ein System einzudringen, wird der Angriffsweg dokumentiert und die Dokumentation dem Auftraggeber zur Verfügung gestellt. Dieser kann mit den Informationen Sicherheitslücken identifizieren und Gegenmaßnahmen einleiten.

Dieses Vorgehen ist die einzige praktizierbare Möglichkeit um die Sicherheit eines Systems zu überprüfen. Zwar besteht in der Theorie noch die Variante die Sicherheit oder Fehlerfreiheit eines technischen Systems mathematisch zu berechnen, also zu verifizieren, dies ist aber praktisch unmöglich. Zum einen bestehen Systeme nicht nur aus technischen Anlagen, die theoretisch noch berechenbar wären, sondern auch aus Menschen bzw. Interaktionen von und mit Menschen. Diese sind dann aber nicht mehr sicher berechenbar (vgl. Schumacher 2011, 2012). Außerdem ist die Komplexität eines technischen Systems nicht mehr berechenbar, da der Rechenaufwand zu hoch ist. Man kann theoretische jeden Quellcode, den ein Programmierer schreibt um ein Programm zu entwickeln in ein mathematisches Gleichungssystem umwandeln und dieses lösen, um seine Fehlerfreiheit zu zeigen. Ein derartiges Gleichungssystem ist in der Praxis aber aufgrund der schieren Größe der Gleichungen und der Anzahl der unbekannten Variablen nicht mehr in vertretbarem Zeitaufwand lösbar. Allein das Gleichungssystem um die Fehlerfreiheit eines Betriebssystems zu berechnen ist größer als das Gleichungssystem, das der Wetterdienst lösen muss um das Wetter für die nächsten Monate zu berechnen.

Daher ist es in der Regel nur praktikabel ein technisches System durch Belastungsstests im Labor zu validieren, wie dies beispielsweise die Automobilhersteller mit Crashtests tun, oder ein System im Feld beispielsweise durch einen Pen-Test anzugreifen und so Schwachstellen aufzuspüren.

Um einen Pen-Test durchzuführen einigt man sich mit dem Auftraggeber auf ein Ziel. Dann versucht man alle notwendigen Assets zu identifizieren, die dazu genutzt werden können ein solches Ziel zu erreichen. Diese Assets untersucht man dann auf sogenannte Angriffsvektoren. Ein Angriffsvektor ist ein »Einfallstor« für einen Angreifer um Rechte auf einem System zu erlangen. In den mittelalterlichen Städten waren beispielsweise Schwachstellen in der Stadtmauer, die Stadttore oder die Wasserversorgung Angriffsvektoren. In modernen IT-Systemen sind es in der Regel Authentifikationsmechanismen (Passwörter, PINs, ID-Karten und ähnliches) oder Sicherheitslücken in Anwendungsprogrammen. Diese Sicherheitslücken, sogenannte Vulnerabilities, also Verwundbarkeiten, können ausgenutzt werden um beispielsweise Administratorenrechte in einem System zu erlangen. Programme die eine solche Vulnerability ausnutzen nennt man »Exploit«, was von ausnutzen, ausbeuten abgeleitet ist.

Die Schwierigkeit des Pen-Tests besteht in der Praxis vor allem darin, die geeigneten Assets zu identifizieren und diese auf Sicherheitslücken hin zu untersuchen. Beliebte Angriffsziele von kriminellen und politisch motivierten Angreifern sind unter anderem:

- Stromversorgung
- Versorgung mit Erdöl, Erdgas, Heizöl, Treibstoffen, Kraftstoffen, Schmierstoffen etc.
- Trinkwasserversorgung
- nationale Kommunikationsnetze (Telefon-Netze, GSM, Funknetze, BOS-Funk)
- Vernetzung der Banken, Geldautomaten, EC-Kartensysteme, Kreditkarten etc.
- Smart-Meter in Haushalten
- Steuerungssysteme in intelligenten Häusern (Smart Homes)
- vernetzte Computersysteme (das ominöse »Internet«)
- Industriesteuerungsanlagen (SCADA)
- Satelliten
- Geo-Positionssysteme (GPS, Glonass, Galileo)

Nachdem man eine solche Liste erstellt hat, kann man die identifizierten Assets gewichten und priorisieren. Nach der Priorisierung untersucht man die Assets systematisch auf Schwachstellen, welche dann wiederum selbst gewichtet und priorisiert werden und idealerweise geschlossen werden. Leider werden in

8 http://www.spiegel.de/politik/ausland/0,1518,502118,00.html r. 2014-03-11

9 Siehe hierzu das Kapitel »Eine DIN für IT-Sicherheit?« von Dr. Hubert Feyrer

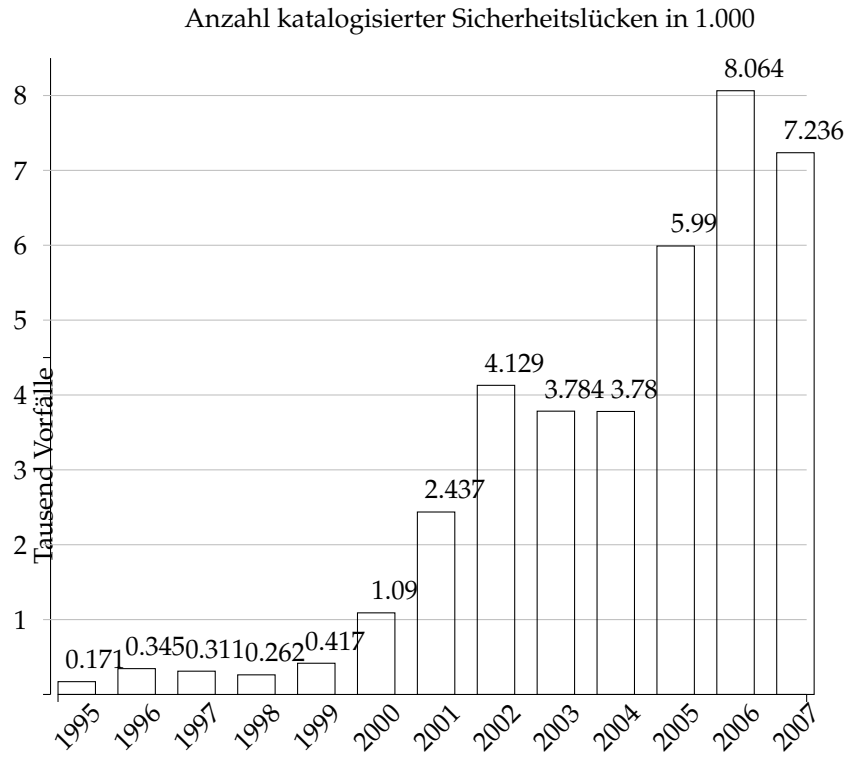

Abbildung 1: Beim CERT/CC katalogisierte Sicherheitslücken

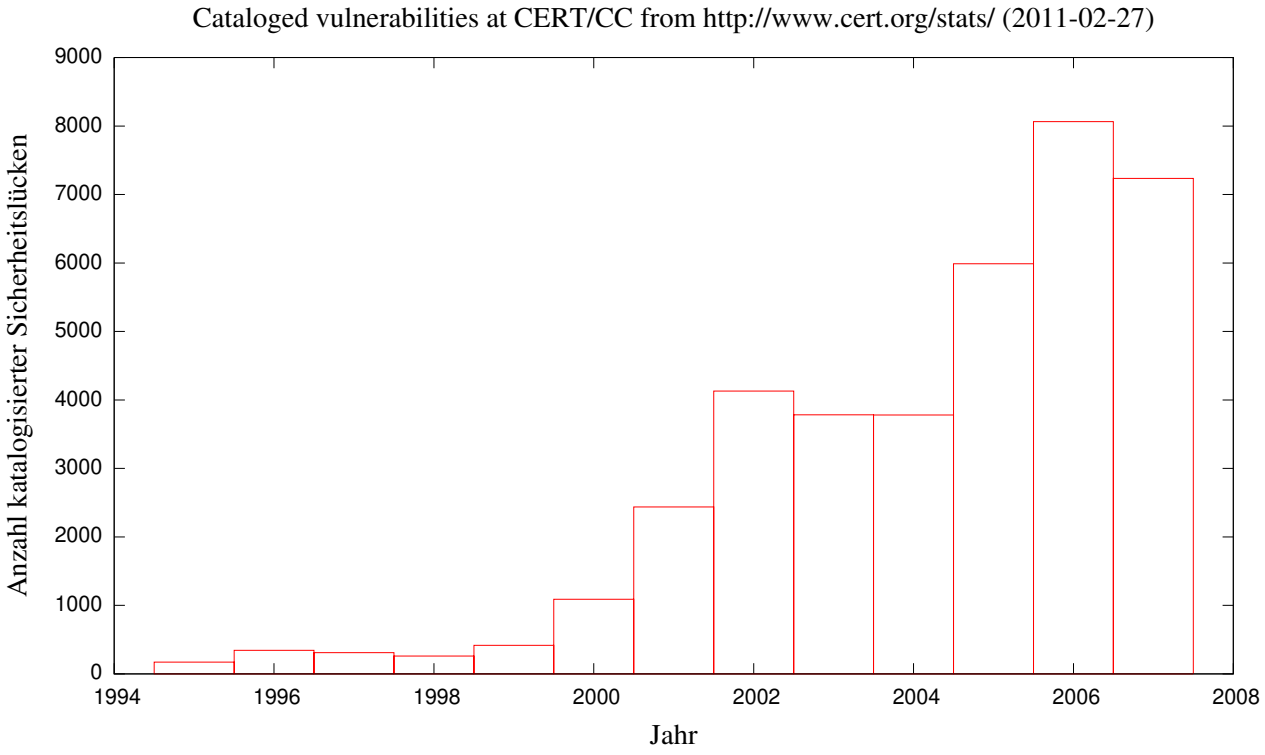

Abbildung 2: Beim CERT/CC katalogisierte Sicherheitslücken

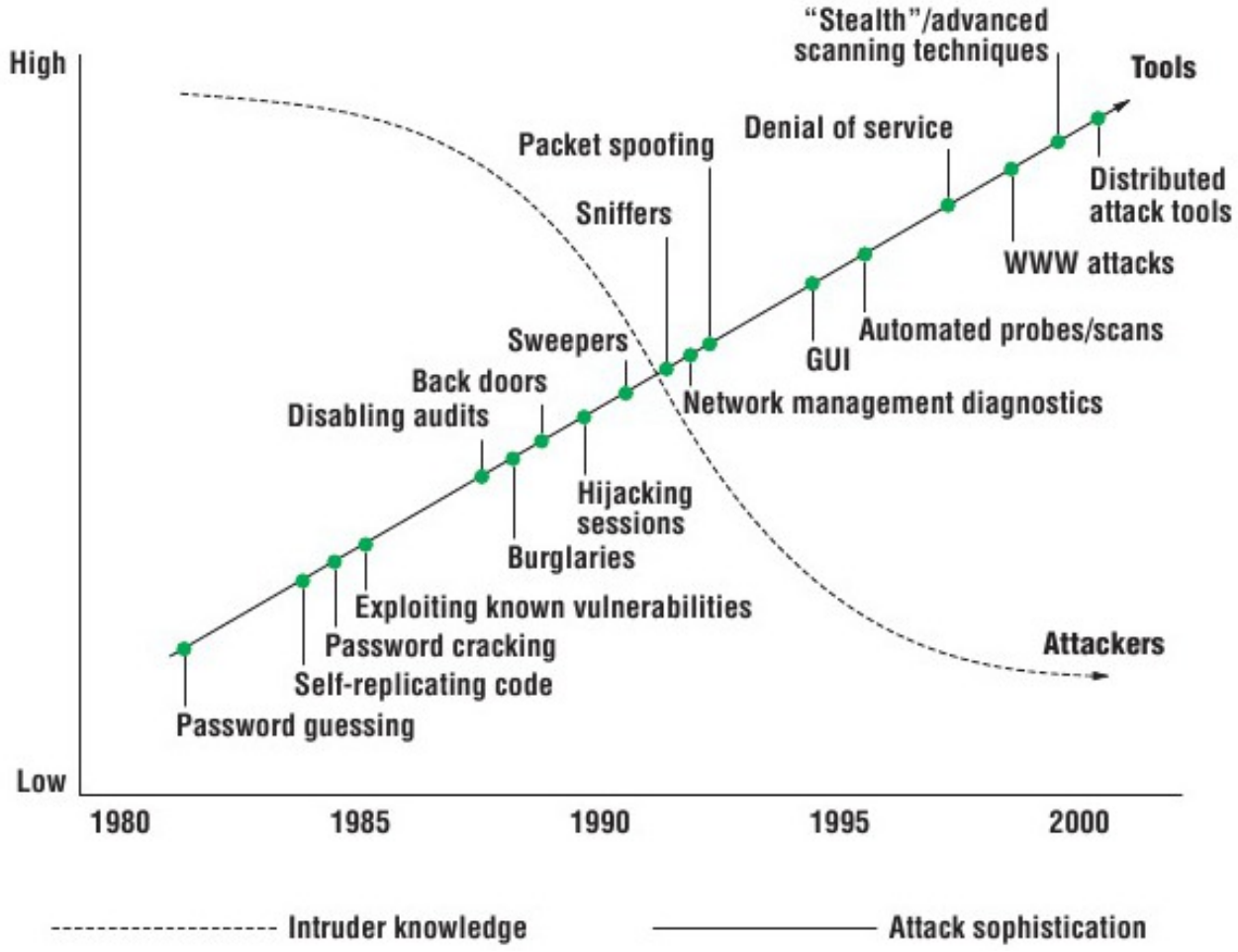

Abbildung 3: Angriffs-Komplexität und Angreiferfertigkeiten
Quelle: Allen u. a. (2000, Seite 43)

der Praxis nicht alle bekannten Sicherheitslücken in akzeptabler Zeit geschlossen, einige aus verschiedenen Gründen auch nie. Ein Problem bei dieser Analyse ist, dass Unternehmen und andere Organisationen kaum oder gar keine Daten zu Sicherheitsvorfällen oder Analysen veröffentlichen. Daher ist es kaum bis gar nicht möglich den gegenwärtigen Sicherheitszustand einzelner Systeme einzuschätzen und verlässlich zu bestimmen. Hier sind gegebenenfalls rechtliche Maßnahmen sowie empirische Untersuchungen notwendig.

Shukla (2015) beschreibt unter anderem die vom Carna-Botnet kompromittierten Geräte, Sauder (2015) zeigt wie einfach man Virenscanner aushebeln kann und Lukas (2015) bzw. Ullrich u. a. (2015) zeigen Sicherheitslücken in Jave bzw. IPv6 auf.

3 Mögliche Angriffsvektoren

Besonders interessant sind hierbei die sogenannten Smartmeter: also intelligente Stromzähler. Diese intelligenten Stromzähler sind keine einfachen Geräte mehr die nur den Strom messen, sondern netzwerkfähige Computer, die auch den Stromverbrauch messen können. Smartmeter können beispielsweise dazu eingesetzt werden, um den Stromverbrauch eines Haushalts zu protokollieren und auszuwerten. Diese Möglichkeit kann sinnvoll im Rahmen der Energiewende eingesetzt werden, da das Smartmeter hier über die Protokollierung des Verbrauchs Feedback für die Benutzer geben kann, beispielsweise um den Stromverbrauch und damit die Kosten zu senken.

Die gewünschten Smartmeter verfügen darüberhinaus auch über Netzwerkfunktionen, so können die Verbrauche an die Energieversorger oder Stadtwerke quasi in Echtzeit gemeldet werden. Es ist daher nicht mehr notwendig einen Mitarbeiter zum Ablesen des Stromverbrauchs in die Haushalte zu schicken. Außerdem wünschen viele Stromversorger eine Abschalt-Funktionalität, das heisst sie möchten von der zentralen Leitwarte aus bestimmte Smartmeter abschalten und damit die angeschlossenen Haushalte vom Stromnetz abkoppeln.

Genau diese Funktionalität kann zu schweren Sicherheitsproblemen führen. Wird ein Smartmeter ausgerollt, das Sicherheitslücken hat, kann diese von einem Angreifer ausgenutzt werden. Gelingt es über die Sicherheitslücke den Smartmeter abzuschalten bzw. die Stromversorgung abzuschalten, können unter Umständen Stromnetze oder Kraftwerke überlastet werden und damit die Stromversorgung in bestimmten Gebieten zusammenbrechen. Stellt man sich nun vor es ist der 24. Dezember 18 Uhr, es schneit bei -17°C und die Stromversorgung bricht zusammen. Wenn dann noch die Erdgaslieferungen ausbleiben, kann man sich einige der potenziellen Auswirkungen ausmalen.

Ein weiteres interessantes Phänomen ist Stuxnet. Stuxnet wird im Kapitel zu Malware von mir näher und vor allem auf technischer Ebene beschrieben. In diesem Aufsatz spielt jedoch die strategische Ebene eine größere Rolle, daher werde ich hier Stuxnet auch nur aus strategischer Sicht besprechen.

Es wird vermutet[10], dass Stuxnet von israelischen und/oder amerikanischen Diensten entwickelt wurde, um das iranische Atomprogramm zu stören. Die Analysen der Schadsoftware gehen davon aus, dass die Urananreicherungsanlagen in Natanz oder das Kernkraftwerk in Buschehr gestört werden sollten.

Auffällig an Stuxnet ist, dass es mehrere Programmierer bzw. Programmierteams gab und diese koordiniert werden mussten. Es handelt sich also nicht um einen einzelnen Täter, sondern um mehrere, die generalstabsmäßig koordiniert wurden. Desweiteren verfügten die Stuxnet-Entwickler über eine Testgestellung des SCADA-Systems samt Frequenzumrichter, die genutzt werden können um Zentrifugen zur Urananreicherung zu steuern. Vereinfacht gesagt ist ein Frequenzumrichter eine Anlage, in die Wechselstrom eingespeist wird. Der Wechselstrom wird intern in Gleichstrom gerichtet und wieder als Wechselstrom zur Verfügung stellt, welcher in Frequenz und Amplitude moduliert werden kann. Der Frequenzumrichter kann beispielsweise vor einen Elektromoter geschaltet werden um diesen mit einer niedrigeren Drehzahl laufen zu lassen. Ein Frequenzumrichter wird auch eingesetzt, um in Zentrifugen die Drehzahl anzupassen und konstante Werte sicherzustellen. In der Praxis werden dazu Frequenzumrichter über Feldbusse (CAN, EtherCAT, Profibus, EtherNET/IP) miteinander und mit Steuerungsrechner gekoppelt, die eine automatische Rückkopplung beziehungsweise computergesteuerte Programmierungen erlaubt. Manipuliert ein Angreifer die SCADA-Steuerungsanlage (Supervisory Control and Data Acquisition) kann er die Ausgangsfrequenz der Frequenzumrichter und damit die Drehfrequenz der Zentrifugen manipulieren. Ist die Abweichung der Frequenz zu gering um mit dem bloßen Auge erkannt zu werden und hat der Angreifer neben der Steuerung auch die Überwachung im SCADA-System manipuliert, haben die Opfer in der Regel keine Chance die Manipulation zu entdecken.

Stuxnet nutzte mehrere sogenannte Zero-Day-Exploits aus, also Exploits, die dem Hersteller der Software und anderen Sicherheitsforschern nicht bekannt ist. Damit hatten die Entwickler und Anwender des Systemes keine Möglichkeit es durch ein Softwareupdate zu schützen. Desweiteren wurde Stuxnet über mehrere Angriffsvektoren ausgerollt, darunter auch über USB-Sticks, was voraussetzt, dass eine Person physisch in das Zielgebiet der zu kontaminierenden Rechner eindringt und den Stick dort verteilt oder einsetzt. Dies ist eine klassische

10 http://www.heise.de/thema/Stuxnet v. 19.04.2012; http://www.zeit.de/2010/34/T-Stuxnet-Trojaner v. 19.04.2012; http://www.spiegel.de/netzwelt/gadgets/spektakulaere-virus-analyse-stuxnet-sollte-irans-uran-anreicherung-stoeren-a-729329.html v. 19.04.2012; http://www.faz.net/aktuell/feuilleton/debatten/digitales-denken/trojaner-stuxnet-der-digitale-erstschlag-ist-erfolgt-1578889.html v. 19.04.2012

Geheimdienstaufgabe.

Man kann davon ausgehen, dass Stuxnet ein organisierter Akt der »Gewalt« ist, allerdings ist fraglich, ob der Urheber seinen Gegner zur Erfüllung seines Willens zwingen konnte. Es ist weder offiziell bekannt wer der Urheber ist, noch sind seine Forderungen und damit Ziele bekannt. Es ist daher müßig über den Erfolg des Unternehmens Stuxnet zu spekulieren. Fakt ist lediglich, dass Stuxnet enttarnt wurde, was definitiv keinen Erfolg der Schadsoftware darstellt.

Ein weiterer Zwischenfall ist der Absturz bzw. die Entführung des »Beast of Kandahar«, einer Drohne vom Typ Lockheed Martin RQ-170 Sentinel im Iran. Bei der Drohne handelt es sich um ein unbemanntes Flugobjekt (Unmanned Aerial Vehicle UAV) welches zu Überwachungszwecken selbständig über ein definiertes Zielgebiet kreist und Video- oder Photoaufnahmen erstellt. Da das UAV unbemannt ist, benötigt es einen Steuerungsmechanismus. Entweder wird es per Funk von einem Piloten ferngesteuert oder es navigiert selbständig. Die selbständige Navigation kann über ein Trägheitsnavigationssystem und/oder GPS erfolgen. Trägheitsnavigationssysteme existieren bereits seit 1910 und wurden unter anderem im deutschen Aggregat 4 - der V2 - oder auf der USS Nautilus (SSN-571) eingesetzt. Diese Systeme haben aber den bekannten Nachteil einen Positionsfehler bzw. Kreiselfehler aufgrund der Erdkrümmung zu entwickeln. Um diese Messfehler zu minimieren werden in der Praxis neben Trägheitsnavigationssysteme auch GPS-Systeme oder ähnliches eingesetzt, meist auch gekoppelt.

Vorteil des GPS ist die hohe Genauigkeit - Nachteil ist aber die Angreifbarkeit des Signals bzw. des Systems. Ein GPS-Navigationsgerät peilt den eigenen Standort über die Triangulation (Dreieckspeilung) gegenüber 4 Satelliten (je einen für die Länge, Breite und Höhe sowie die Zeit). Dazu empfängt es die Daten der Satelliten und berechnet deren Signallaufzeit um die eigenen Koordinaten zu bestimmen. Diese Signale zwischen Satellit und Navigationssystem können wie jedes andere Funksignal auch gestört oder mit falschen Daten überschrieben werden. Dies ist sogar relativ einfach möglich, da der Leistungspegel nur -155 dBW beträgt[11]. Um dieser Gefahr vorzubeugen, gibt es neben dem offenen zivilen GPS noch ein verschlüsseltes System mit höherer Genauigkeit und Schutz vor Manipulationen. In der Praxis nutzen militärische Systeme nur das militärische GPS. Allerdings besteht oftmals die Möglichkeit auf das zivile Signal zurückzufallen, wenn das militärische gestört ist. Das zivile Signal kann aber mit einem gefälschten Signal überschrieben werden und falsche Daten liefern. So wäre es in der Praxis möglich die Signale zwischen Satellit und Drohne zu stören, so dass die Drone auf die zivile Version zurückfällt. Die zivilen Signale können dann mit falschen Daten überschrieben werden und der Drohne so falsche Positionen vorspiegeln, die sie zur Landung zwingen. Der Iran behauptet die Drohne so erbeutet zu haben. Die USA bestreiten den Einsatz von GPS in der Drohne. China fälscht GPS-Signale auf dem chinesischen Festland um die Positionierung zu erschweren. Man könnte sich auch vorstellen, dass die USA die Drohne gezielt in iranische Hände gespielt hat um den Iranern falsche Technik oder sonstige »rote Heringe« unterzuspielen.

11 http://www.phrack.org/issues.html?issue=60&id=13#article v. 12.05.2008

4 Routing und Resilienz des Netzes

Im Jahre 1962 startete die Advanced Research Project Agency des US Verteidigungsministeriums ein Entwicklungsprojekt, welches ein neues Kommunikationsnetz hervorbringen sollte. Dieses sogenannte Arpanet entwickelte sich im Laufe der Zeit über verschiedene Zwischenschritte zum sogenannten »Internet« weiter.

Bei der Entwicklung des Netzes wurde Wert auf Ausfallsicherheit gelegt, so dass eine hierarchische Vermittlung in Bäumen nicht in Betracht gezogen wurde. Stattdessen wurde das Routing paketvermittelnd implementiert. Das Routing legt dabei fest, wie ein Paket vom Absender zum Empfänger vermittelt wird, also welchen Weg es nehmen soll. Ist das Netzwerk als Baum implementiert, existiert nur genau ein Weg vom Absender zum Empfänger, die Route wird also schon durch das Netz selbst festgelegt.

Gibt es allerdings mehrere mögliche Routen, muss das Paket oder die Vermittlungsstation eine bestimmte Route nach definierten Kriterien auswählen. Es führen schließlich viele Wege nach Rom, so dass ein Navigationssystem oder Routenplaner verschiedene Strecken nach Länge, Stauwahrscheinlichkeit oder Sehenswürdigkeiten auswählen kann. Analog dazu muss in einem paketvermittelnden Netz der jeweilige Router entscheiden, über welche Route ein Paket weitervermittelt werden soll.

Der Vorteil der Paektvermittlung liegt in der erhöhten Resilienz des Netzwerkes, denn es stellt die Erreichbarkeit verschiedener Knoten auch dann sicher, wenn ein oder mehrere Knoten ausgefallen sind.

Aufgrund dieser von Anfang gewollten und implementierten Ausfallsicherheit ist es fast unmöglich das Internet (oder Teile davon) auszuschalten. Fällt ein Knotenpunkt aus, können immer noch genügend Routen über andere Knoten gefunden werden. Um einen Knoten komplett aus dem Netz zu entfernen, müssen alle inzidenten Kanten zerstört werden, das selbe gilt auch für ein beliebiges Subnetz (mehrere Knoten). Ebenso ist es problematisch Netzwerkpakete zu ihrem Ursprungsort zurückzuverfolgen, da jedes Paket einen anderen Weg durch das Netzwerk nehmen kann und Absenderadressen auch gefälscht werden können. Daher ist es äußerst problematisch mögliche Angreifer zu identifizieren und zur Rechenschaft zu ziehen. Im schlimmsten Falle hat ein Angreifer dutzende Rechner in verschiedenen Staaten unter seine Kontrolle gebracht und für den Angriff ge-

nutzt. Davon muss jeder Einzelne forensisch untersucht werden - wenn er denn überhaupt identifiziert werden kann und die lokalen Strafverfolgungsbehörden dazu in der Lage sind.

5 Distributed Denial of Service

Eine Denial-of-Service-Attacke ist eine Angriffsform, bei der ein Server, der einen bestimmten Dienst anbieten soll durch Überlastung ausser Gefecht gesetzt wird. Dazu wird der Server derart mit Anfragen bombardiert, dass er entweder abstürzt oder aber nicht mehr erreichbar ist, da das Netzwerk bzw. die Hardware des Servers überlastet wird. Dies kann der Angreifer erreichen, in dem er beispielsweise mit seinem eigenen Rechner den angebotenen Dienst (zum Beispiel eine Webseite) immer wieder abruft. Da heutzutage ein einzelner Rechner mit einer Endkunden-Internetanbindung nicht mehr ausreicht um einen ordentlich dimensionierten Server lahmzulegen, wurden sogenannte distributed-Denial-of-Service-Attacken (dDoS) entwickelt. Dazu greifen viele verteilte (distributed) Rechner den Zielserver an und überlasten ihn so gemeinsam.

Die verteilten Rechner werden dabei entweder von ihren Benutzern koordiniert gesteuert - beispielsweise über die bei Anonymous Script Kiddies beliebte Low Orbit Ion Cannon, LOIC[12] - oder in dem ein Angreifer fremde Rechner unter seine Kontrolle bringt.

Dazu nutzt ein Angreifer Schadsoftware aus um Rechner mit Sicherheitslücken unter seine Kontrolle zu bringen. Die Opferrechner, im Jargon Zombie genannt, werden zentral gesteuert und können auf Geheiß ihres Meisters bestimmte Befehle ausführen, beispielsweise einen Zielserver mit Anfragen bombardieren. Die Gesamtheit der Zombies nennt man dann Bot-Netz, abgeleitet von Roboter.

Rechtlich problematisch ist hier die Herrschaft über den Rechner der unter Umständen ein Zombie ist. Selbst wenn es gelingt den Angreifer (also Zombierechner) zu identifizieren, ist noch nicht sichergestellt das der Inhaber des Internet-Anschlusses auch Urheber der Attacke ist. Es ist ebenso möglich, dass der Rechner von einer anderen Person trojanisiert und zum Zombie gemacht wurde, so dass schon rein rechtlich gesehen hier einige Probleme entstehen.

Aus Sicht der IT-Sicherheit sind derartige Attacken besonders problematisch, da deren Ausführung relativ simpel ist, während die Verteidigung beliebig komplex und damit teuer werden kann. Praktisch wurden diese Attacken schon mehrfach umgesetzt, beispielsweise im Jahre 2000, als der 15-jährige kanadische Schüler mit dem Alias *Mafiaboy* mehrere US-Amerikanische Server mit dem deutschen dDoS-Tool *Stacheldraht*[13] lahmlegte und nach Medienberichten Schaden in Höhe von 1,7 Milliarden kanadischen Dollarn anrichtete. Bei Mafiaboy handelt es sich übrigens nicht um einen Hacker, sondern um ein Script Kiddie. Hacker frönen dem kreativen Umgang mit der Technik und verfügen über umfangreiche technische Handlungskompetenz. Script Kiddies hingegen nutzen vorgefertigte Programme (sogenannte Scripte, hier Stacheldraht) ohne überhaupt zu wissen was sie tun. Damit können sie unter Umständen extrem gefährlich werden.

Auch die Angriffe auf Estland[14] im Jahr 2007 und Georgien[15] 2008 waren dDoS-Attacken, die insbesondere im estnischen Fall weitreichende Konsequenzen hatten.

In der Informatik bzw. der IT-Sicherheit werden verschiedene Diagnosekriterien festgelegt, die der Sicherheitsdiagnose von Software, Hardware und ganzen IT-Systemen dienen. Ein derartiges Verfahren ist auch als forensische Analyse notwendig, um zu überprüfen ob ein Angriff von einer bestimmten IP-Adresse stammt.

Die bekanntesten Sicherheitskriterien im deutschsprachigen Raum sind die sogenannten VIVA-Kriterien, also Vertraulichkeit, Verfügbarkeit, Integrität und Authentisierung, welche unter anderem vom Bundesamt für Sicherheit in der Informationstechnik (2006) wie folgt definiert werden:

Vertraulichkeit Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

Integrität Die Daten sind vollständig und unverändert. Der Begriff »Information» wird in der Informationstechnik für »Daten« verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.

Verfügbarkeit Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.

Authentisierung Bei der Anmeldung an einem System wird im Rahmen der Authentisierung die Identität der Person, die sich anmeldet, geprüft und verifiziert. Der Begriff wird auch verwendet, wenn die Identität von IT-Komponenten oder Anwendungen geprüft wird. Ist die Authentisierung erfolgreich, spricht man auch davon, dass die Person oder ein Datum authentisch ist bzw. die Authentizität gewährleistet ist.

Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein anderer Begriff dafür ist »IT-Sicherheit« (Bundesamt

12 http://www.scip.ch/?labs.20101219, Zugriff am 22.04.2011

13 http://www.sans.org/security-resources/malwarefaq/stacheldraht.php, 19.04.2008

14 http://en.wikipedia.org/w/index.php?title=2007_cyberattacks_on_Estonia&oldid=514966602, 15.10.2012

15 http://en.wikipedia.org/w/index.php?title=Cyberattacks_during_the_2008_South_Ossetia_war&oldid=481694597, 15.10.2012

für Sicherheit in der Informationstechnik 2006, S. 8).

Möchte man beispielsweise elektronische Sensoren in einem kybernetischen System einsetzen um bestimmte Parameter zu überwachen, muss deren Kommunikation durch Kryptographie gesichert werden. Jede Form der elektronischen Datenverbindung unabhängig vom Protokoll bzw. der Sprache (http, xml, ftp, snmp, xmpp) und der physikalischen Verbindung (Kabel, WLAN, Richtfunk, Satellitentelefon, GSM) kann durch eine Man-in-the-Middle-Attacke angegriffen werden. Dies ist ein Angriff, bei dem die Datenübertragung mitgeschnitten und abgehört und/oder manipuliert wird. So lässt sich jedes beliebiges Datenpaket auf dem Übertragungsweg zwischen den Teilnehmern abfangen und lesen oder verändern und weiterleiten. Dabei wird die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten gefährdet. Um eine derartige Attacke zu verhindern, können die Kommunikationspartner ihre Kommunikation untereinander verschlüsseln. Danach ist es einem Angreifer zwar möglich, die Daten weiterhin abzufangen, er kann sie aufgrund der Verschlüsselung und Signatur nicht mehr lesen und manipulieren, ebensowenig kann er sich als ein anderer Kommunikationspartner ausgeben. Leider implementieren viele Überwachungs- und Steuerungssysteme in der Industrie bzw. Regelungstechnik keine kryptographischen Methoden um die Kommunikation zu sichern.

Ein weiteres Problem der Angriffe in der Zuordnung der Urheberschaft von Attacken ist die technische Herrschaft über einen Rechner. Selbst wenn die Quelle einer Attacke zweifelsfrei identifiziert werden kann, heißt das nicht dass der Eigentümer des Rechners auch der Angreifer ist. Schließlich ist es für einen Angreifer notwendig, nicht identifiziert werden zu können. Daher werden nicht nur Verschleierungstechniken verwendet, sondern auch sogenannte Proxies benutzt. Das heißt ein Angreifer greift nicht direkt von seinem Rechner aus das Zielsystem an, sondern benutzt Zwischenstationen, um seine Herkunft zu verschleiern. Dazu bieten sich schlecht gesicherte Rechner in Staaten an, deren Polizei mit der Aufklärung von Internetkriminalität überfordert ist und die mit den Staaten, in denen das Zielsystem bzw. der Angreifer sitzt nicht kooperieren. Das heißt der Angreifer übernimmt zuerst Rechner in der Ukraine, Südafrika, Mexiko, China und Serbien, bevor er den Zielrechner in Wien attackiert.

Wird der Angriff auf das Zielsystem erkannt, können die lokalen Strafverfolgungsbehörden lediglich den letzten genutzten Proxy in Serbien identifizieren. Sie können aber nicht zweifeslfrei belegen, dass der Eigentümer des serbischen Rechners (beziehungsweise der Inhaber des Internetsanschlusses von dem aus die Attacke zur Angriffszeit begangen wurde) auch wirklich der Angreifer ist und sein Rechner nicht durch einen anderen Hacker oder Trojaner missbraucht wurde. Dazu müssten hier die österreichischen Strafverfolgungsbehörden mit den serbischen kooperieren und den missbrauchten Rechner forensisch untersuchen. Sind die serbischen Behörden dazu nicht bereit, bleibt den österreichischen Behörden keine Möglichkeit, den Angreifer zu identifizieren.

Kooperieren die österreichischen und serbischen Behörden und es gelingt ihnen den Angriff auf das Proxysystem aufzukären, stehen sie wieder vor dem selben Problem: der Angreifer ist über einen chinesischen Rechner in den serbischen eingedrungen. Das heißt die österreichischen und serbischen Behörden müssen nun gemeinsam mit den chinesischen den Einbruch in das chinesische System aufklären. Um dann den Proxy in Mexiko zu enttarnen und das selbe Verfahren von vorne zu beginnen.

6 Aufwand der Verteidigung

Die Absicherung von IT-Systemen ist ungleich komplexer als der Angriff. Bereits eine einfache stochastische Überlegung belegt dies: der Angreifer muss nur eine einzige geeignete Sicherheitslücke finden und ausnutzen. Der Verteidiger muss jede Sicherheitslücke identifizieren und stopfen.

Dabei gilt auch zu beachten, dass es praktisch unmöglich ist, die Sicherheit von IT-Systemen mathematisch zu verifizieren. Es ist zwar theoretisch möglich, ein Computerprogramm wie ein Betriebssystem in ein mathematisches Gleichungssystem zu überführen und zu berechnen um Fehler zu entdecken. Ein derartiges Gleichungssystem ist allerdings so komplex, dass es praktisch nicht mehr zu berechnen ist. Zum Vergleich ein paar Daten zur Größe des Betriebssystems NetBSD, Version 5.0: es besteht aus 163 000 Quelldateien, 57 228 442 Codezeilen und 1 991 091 842 Zeichen. Zum Vergleich: Goethes Faust I besteht »nur« aus ca. 4 600 Zeilen mit 200 000 Zeichen. Es ist daher praktisch unmöglich, dass eine Person den gesamten Überblick über das NetBSD-System hat. Und in der Praxis läuft auf einem Computer nicht nur das Betriebssystem sondern meist noch wesentlich komplexere Anwendungsprogramme. Allein durch den Einsatz von IT-Systemen wird hier eine Komplexitätsstufe eröffnet, die kaum noch beherrschbar ist.

Schließlich gibt es auch noch eine zentrale Frage, die jede elektronische Attacke ins Leere laufen lassen kann. Das potenzielle Opfer muss sich nur fragen, wie abhängig es vom angegriffenen System ist. Es kann sich selbst aussuchen, ob es dieses System einsetzen will oder ob Alternativen genutzt werden sollen. Oder ob es im Konfliktfall das System nicht einfach abschaltet und auf eine Alternative ausweicht. Damit wird die Kampfkraft einer »Cyber-Waffe« fast ausschließlich vom angegriffenen System bestimmt. Eine Situation, die für konventionelle Waffen nicht so einfach gilt. Zwar kann die Bevölkerung eine Stadt vor einem Bombenangriff verlassen oder in Bunkern unterziehen, die materiellen Werte wie Häuser, Strassen und Fabriken können aber nicht einfach versetzt oder versteckt werden.

Problematisch ist allerdings zur Zeit, dass sich unsere Gesellschaft immer weiter von IT-Systemen ab-

hängig macht. Der Einsatz von Smartmetern ist nur ein Punkt. Ein normaler Drehstromzähler kann nicht über das Internet angegriffen werden, damit ist auch Sicherheitsanalyse oder Alternative nicht notwendig. Trotzdem werden die potenziellen Sicherheitsprobleme kaum dezidiert diskutiert.

7 Angriffsziele in der Wasserversorgung

Auch in der Trinkwasseraufbereitung und Versorgung werden vielerlei IT-Systeme eingesetzt. Dies können normale Büro-PCs für die klassischen Verwaltungsaufgaben (E-Mail, Office, Abrechnungen etc.) sein, aber auch spezialisierte Steuerungs- und Regelungsanlagen sein.

Die verbreiteten Office-PCs lassen sich mit etwas Sicherheitssoftware vergleichsweise einfach absichern. Dabei kann man eine ausgewogene Balance zwischen der Beuntzbarkeit und den Sicherungsmaßnahmen finden, so dass der Bedienkomfort nicht übermäßig leidet.

Regelungsanlagen hingegen verfügen oftmals nicht über entsprechend sichere Software wie bspw. kryptogrpahische Bibliotheken zur Absicherung der Kommunikation. Oftmals werden auch extrem einfache und relative Leistungsschwache Rechner eingesetzt, die eine Verschlüsselung der Kommunikation oder andere Integritätssicherungsmaßnahmen gar nicht erst ermöglichen.

Hier gilt es die Hersteller der entsprechenden Regelungstechnik in die Pflicht zu nehmen und entsprechende Funktionalität einzufordern, beispielsweise über die Einbindung von kryptographischen Bibliotheken wie OpenSSL, OpenSWAN, OpenVPN oder OpenSSH.

Eine Anbindung ungesicherter Systeme in das Internet ist schlichtweg verantwortungslos, da man damit diese Rechner dem weltweiten Zugriff aussetzt. So kann auch ein gelangweilter 15-jähriger kanadischer High-School-Schüler diese Systeme mit vorgefertigter Software finden und vollautomatisch Angreifen. So geschehen bereits im Februar 2000 mit *MafiaBoy*, einem 15-jährigen Kanadier der mit vorgefertigter Software die Webserver von eBay, Microsoft, Amazon, CNN und einigen anderen lahmgelegt hat.

Dabei nutzte er die Software *Stacheldraht*, die ein deutscher Hacker entwickelt hat. Er musste dazu nur die Software finden und installieren und die entsprechenden Zieladressen eingeben. 15 Jahre späte existiert mit Kali-Linux gar eine komplette Linuxdistribution die dutzende von Sicherheitsprogrammen bündelt - darunter auch Metasploit(vgl. Kohl 2012). Damit kann selbst ein technisch völlig unbegabter Laie automatisierte Angriffe auf Systeme fahren. Und derzeit werden insbesondere Regelungstechnische Systeme (sogenannte SCADA-Systeme) bzw. deren Software angegriffen und erforscht. Die gefundenen Sicherheitslücken lassen sich mit etwas krimineller Engergie auf dem Schwarzmarkt im Internet gewinnbringend veräußern und von kriminellen Banden einkaufen.

Besonders zielführend sind auch Angriffe auf die eingesetzten Kommunikationsverfahren wie GSM oder Bluetooth (vgl. Hofmann 2012; Kafka und Pfeiffer 2012; Valeros und García 2013, 2015; Wendzel und Keller 2012), die insbesondere durch die Integration von eingebetteten Geräte und mobilen Endgeräten (Smartphone, Tablets) vorangetrieben wird.

Diese kommt insbesondere dann zum Tragen wenn größe Systeme implementiert werden wie Entscheidungsunterstützungssysteme. Diese vereinen unter anderem Sensoren zur Messung verschiedener Parameter. Diese werden häufig im großen Stil erfasst und über längere Zeiträume in Datenbanken gespeichert. Data-Warehousing-Systeme nutzen diese Daten damm um algorithmisiert Lagebilder zu erstellen die der Entscheidungsfindung dienen. Derartige Entscheidungsunterstützungsysteme sind in der Regel recht umfangreich, da sie eine erhebliche Menge an erfassten Daten benötigen. Darüberhinaus ist die eingesetzte Software komplex und es sind meist viele Rechner angeschlossen. Daher sind hier meist viele potenzielle Angriffsvektoren und Sicherheitslücken vorhanden. Außerdem werden Entscheidungsunterstützungssysteme oft auf strategischer Entscheidungsebene mit entpsprechend weitreichenden Konsequenzen eingesetzt, so dass ein längerfristiger Angriff mit sogenannten Advanced Persistent Threats und hohem finanziellen Aufwand lohnender ist.

Auch hier fehlen nach unserer bisherigen Erfahrung bisher entsprechend sinnvolle Sicherungsmaßnahmen auf technischer und sozialer Ebene.

Literaturverzeichnis

Allen, J., Christie, A. & McHugh, J. (2000 September). Defending Yourself: The Role of Intrusion Detection Systems. Zugriff 4. Januar 2005, unter http://www.cert.org/archive/pdf/IEEE_IDS.pdf

Bundesamt für Sicherheit in der Informationstechnik (Herausgeber). (2006). Leitfaden IT-Sicherheit IT-Grundschutz kompakt. Zugriff 16. Oktober 2006, unter http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

Hofmann, F. (2012). Sichere Benutzer-Authentifikation an sensiblen IT-Systemen. In J. Sambleben & S. Schumacher (Herausgeber), *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* (Seiten 103–118). Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung. Norderstedt: BoD.

Kafka, M. & Pfeiffer, R. (2012). Angriffe und Verteidigungsstrategien für vertrauliche Kommunikation über Funkdienste. In J. Sambleben & S. Schumacher (Herausgeber), *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im*

Internet ausgetragen? (Seiten 119–136). Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung. Norderstedt: BoD.

Kohl, M. (2012). Penetrationstests mit Metasploit. In J. Sambleben & S. Schumacher (Herausgeber), *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* (Seiten 137–152). Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung. Norderstedt: BoD.

Lukas, G. (2015). Java's SSLSocket: How Bad APIs Compromise Security. *Magdeburger Journal zur Sicherheitsforschung*, *9*, 506–513. Zugriff 20. März 2015, unter http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Sambleben, J. & Schumacher, S. (Herausgeber). (2012). *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung. Norderstedt: BoD.

Sauder, D. (2015). Why Anti-virus Software Fails. *Magdeburger Journal zur Sicherheitsforschung*, *10*, 540–546. Zugriff 19. Juli 2015, unter http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Schumacher, S. (2011). Sicherheit messen: Eine Operationalisierung als latentes soziales Konstrukt. In S. Adorf, J.-F. Schaffeld & D. Schössler (Herausgeber), *Die sicherheitspolitische Streitkultur in der Bundesrepublik Deutschland: Beiträge zum 1. akademischen Nachwuchsförderpreis Goldene Eule des Bundesverbandes Sicherheitspolitik an Hochschulen (BSH)* (Seiten 1–38). Magdeburg: Meine Verlag.

Schumacher, S. (2012). Zum Verhältnis von psychischen, sozialen und technischen Dimensionen des Einsatzes von IT-Systemen. Bachelor-Arbeit. Otto-von-Guericke-Universität Magdeburg.

Schumacher, S. (2014a). Cyber-Terrorismus: Reale Bedrohung oder Mythos? In S. Hansen & J. Krause (Herausgeber), *Jahrbuch Terrorismus 2013/2014* (Seiten 159–177). Opladen: Verlag Barbara Budrich.

Schumacher, S. (2014b). IT-Sicherheit in der Wasserversorgung: Schutz kritischer Infrastrukturen. In *Trinkwassertagung Sachsen-Anhalt* (Seiten 25–38). HS Magdeburg Stendal. Magdeburg: Hochschule Magdeburg-Stendal.

Schumacher, S. (2016). IT-Sicherheit in der Wasserversorgung: Schutz kritischer Infrastrukturen. *Magdeburger Journal zur Sicherheitsforschung*, *11*, 667–685. Zugriff 1. März 2016, unter http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Shukla, P. (2015). The Compromised Devices of the Carna Botnet: As used for the Internet Census 2012. *Magdeburger Journal zur Sicherheitsforschung*, *10*, 547–627. Zugriff 22. Oktober 2015, unter http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Ullrich, J., Krombholz, K., Hobel, H., Dabrowski, A. & Weippl, E. (2015). IPv6 Security: Attacks and Countermeasures in a Nutshell. *Magdeburger Journal zur Sicherheitsforschung*, *9*, 514–529. Zugriff 30. März 2015, unter http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Valeros, V. & García, S. (2013). How bluetooth may jeopardize your privacy. An analysis of people behavioral patterns in the street. *Magdeburger Journal zur Sicherheitsforschung*, *6*, 394–405. Zugriff 26. Dezember 2013, unter http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

Valeros, V. & García, S. (2015). How bluetooth may jeopardize your privacy: An analysis of people behavioral patterns in the street. In S. Schumacher & R. Pfeiffer (Herausgeber), *In Depth Security: Proceedings of the DeepSec Conferences* (Seiten 315–334). Magdeburg: Magdeburger Institut für Sicherheitsforschung.

Wendzel, S. & Keller, J. (2012). Einführung in die Forschungsthematik der verdeckten Kanäle. In J. Sambleben & S. Schumacher (Herausgeber), *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* (Seiten 91–102). Reihe Sicherheitsforschung des Magdeburger Instituts für Sicherheitsforschung. Norderstedt: BoD.