Auswirkungen einer Cyberattacke auf kritische Infrastrukturen am Beispiel des Bundestages

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B.Sc.)“ im Studiengang Wirtschaftswissenschaften der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Heisterhagen Vorname: Robin

[redacted] [redacted] [redacted] [redacted]

Prüfer: Prof. Dr. M. H. Breitner

Hannover, 10.August 2015

Inhaltsverzeichnis

Abstrakt I

Tabellenverzeichnis IV

Abbildungsverzeichnis IV

Abkürzungsverzeichnis V

1. Motivation und Relevanz 1

2. Theoretische Grundlegung 3

2.1. Kritische Infrastrukturen 3

2.2. SCADA Systeme 4

2.3. Smart Grids 7

3. Angriff auf den Bundestag/das Parlakom-Netz 9

3.1. Bestandsaufnahme 9

3.2. Aufbau des Trojaners 11

3.2.2. Werkzeug Nummer 1 12

3.2.3. Werkzeug Nummer 2 12

3.3. Folgen für das Parlakom-Netz des Bundestages 15

3.4. Advanced Persistent Threats 15

3.4.1. Angriffsablauf 16

3.4.2. Social Engineering und seine Möglichkeiten 18

4. Cybercrime, Cybersicherheit und Cyberdefense 24

4.1. Auswirkungen des Bundestag-Hack 24

4.1.1. IT-Sicherheitsgesetz 25

4.1.1.1 ISO/IEC 27001 und damit verbundene Standards 26

4.1.1.2. Meldepflicht von Sicherheitsvorfällen 31

4.2. Cyberattacken und ihre Folgen 31

4.2.1. Stuxnet 32

4.2.2. Baku-Tbilisi-Ceyhan Pipeline 34

4.3. Cyberprotection 35
4.3.1.Honeypots und Honeynets 38
4.3.2.Penetrationstest 39
5. Diskussion 40
6. Zusammenfassung und Ausblick 42
Inhaltsverzeichnis VI
Anhang XIV

1. Motivation und Relevanz

Wir befinden uns mittlerweile im digitalen Zeitalter und die Vernetzung bspw. einzelner Haushaltsgeräte mit unseren Smartphones oder Heizgeräten scheint kein Ende zu nehmen.

Diese Digitalisierung hat natürlich klare Vorteile z.B. im Angesicht gestiegener Energieeffizienz, die mit ihr einhergeht. Jedoch hat sie auch Schattenseiten.

Mit einer schon fast unglaublichen Ignoranz benutzen Menschen ihre an das Internet angeschlossenen Endgeräte, egal ob mobil oder stationär, ohne sich über die Sicherheit ihrer entsandten Daten Gedanken zu machen.

Mittlerweile geht man davon aus, dass etwa 40 Prozent aller internetfähigen Computersysteme in Deutschland mit Schadsoftware belastet sind.[1] Das hat weitreichende Folgen für unser alltägliches Leben.

Die Cyberkriminalität ist im Zeitraum von 2009 bis 2013 von 50.254 auf 64.426 Straftaten nicht nur angestiegen, darüber hinaus werden Schätzungen zu Folge lediglich 9% aller Delikte angezeigt werden. [2]

Neben einzelnen Individuen sind von der steigenden Anzahl an Cyberkriminalität auch ganze Nationen mit den einhergehenden Risiken betroffen. Welche schwerwiegenden Auswirkungen diese Risiken haben können wird deutlich, wenn man der Aussage des Abteilungsleiters für Cybersicherheit der Nato, Ian J. West Glauben schenkt, ein Individuum könne mit einem einzigen Labtop genauso viel oder sogar mehr Verwüstung anrichten könne als eine traditioneller Bombenangriff. [3]

Systeme steuern und überwachen für uns alltägliche Bedürfnisse wie bspw. fließend Wasser zu haben oder auf Bedarf Wärme mit Heizungen zu erzeugen. Diese Systeme sind jedoch kaum vor kriminellen Angreifern geschützt.

In der Vergangenheit kam es vermehrt zu Übergriffen auf diese sogenannten kritischen Infrastrukturen, die mit erheblichen Auswirkungen verbunden sein können wie verschiedene Beispiele deutlich zeigen. Auf zwei davon wird im Kapitel 4.2. eingegangen.

Auch Regierungsnetzwerke können von schwerwiegenden Angriffen betroffen sein, was die deutsche Bevölkerung am Netz des Bundestags nun miterleben musste.

[1] Vgl. Kühne-Hörmann, 2015
[2] Vgl. Bundeskriminalamt, 2013 S.5
[3] Vgl. heise online, 2014

Daraus resultiert die These, dass unsere heutige Gesellschaft noch nicht gegen das Zeitalter der Cyberkriminalität gewappnet ist und somit auch unsere kritischen Infrastrukturen Angreifern schutzlos ausgeliefert sind.

6. Zusammenfassung und Ausblick

Nachdem nun im Zuge dieser Arbeit herausgestellt wurde, durch welche Systeme unsere kritischen Infrastrukturen betrieben werden und welche Auswirkungen auf den berühmten Cyberangriffs des Bundestages folgen, wurden abschließend noch zwei Beispiele von direkten Attacken auf kritische Infrastrukturen aufgezeigt und mögliche Sicherheitsmaßnahmen zum Überwinden von Schwachstellen vorgestellt.

Unsere Gesellschaft ist sich den Ausmaßen der Angreifbarkeit unserer schützenswerten Infrastruktur noch nicht bewusst. Mit der Verabschiedung des IT-Sicherheitsgesetzes wurde bereits die richtige Richtung eingeschlagen, jedoch kratzt das Gesetz nur an der Oberfläche und die verwendeten Formulierungen sind noch sehr ungenau und bedürfen weiterer Auslegungen durch Rechtsverordnungen, die hoffentlich bald folgen.

Es ist zu verzeichnen, dass sich im bisherigen Jahr 2015 einiges zu ändern scheint und nun endlich eine Handlungsakzeptanz der Politik gegeben ist, die ein verstärktes Verantwortungsbewusstsein nach sich zieht.[114]

Möglicherweise wird dieses Jahr zum Wendepunkt in der Cyberwelt, da Regierungen weltweit Regularien und Hilfsmaßnahmen für Angriffsopfer von Cyberattacken vorantreiben.

Wie immens die Auswirkungen von Cyberattacken auf kritische Infrastrukturen sein können. wurde an 2 Beispielen aufgezeigt. Dabei ist festzustellen, dass diese Angriffe noch relativ glimpflich abgelaufen sind, da zwar ein monetärer Schaden entstanden ist, jedoch kein Mensch körperlich zu Schaden kam. Das kann sich in Zukunft jedoch schnell ändern. Mit Hinblick auf die wachsenden Unruhen weltweit, kann das nächste Ziel einer Terrororganisation auch das Trinkwassernetz durch ein gehacktes SCADA System sein.

Im Laufe der Arbeit ist klar geworden, dass die getroffenen Sicherheitsmaßnahmen bei weitem nicht ausreichen. Nicht nur das bestehende kritische Infrastrukturen gefährdet sind, sondern auch, dass die wachsenden Forderungen nach Effizienz und grünerem Strom der Nachfrage nach Sicherheit in unseren Infrastrukturen überwiegen.

Wir sind Cyberattacken nicht hilflos ausgeliefert, jedoch auch bei weitem nicht auf Angriffe dieser Art vorbereitet. Mit Hilfe der in 4.3. vorgestellten Sicherheitsvorkehrungen und einer proaktiven Schwachstellenorientierung, kann man einige Lücken im System füllen, jedoch besteht das Hauptproblem der Sicherheit kritischer Infrastrukturen in dem angesprochenen Fakt, dass diese Systeme zumeist ohne Sicherheitsvorkehrungen gebaut wurden und nachträglich an das Internet angeschlossen wurden. Von daher bedarf es einem

[114] Vgl. Burg, 2015

grundsätzlichem Austausch dieser Systeme mit der heutigen Zeit entsprechend angepassten. Sicherheitslösungen müssen verstärkt eingebaut werden, um dem ständigen Wettlauf von Hackern und Verteidigern gerecht zu werden.[115]
Auch durch die vermehrte Verwendung von Cloud-Infrastrukturen werden Sicherheitsrisiken durch die erhöhte Schnittstellenanzahl mit den Systemen erheblich erhöht.
Abschließend bleibt zu sagen, dass unsere kritischen Infrastrukturen keineswegs sicher sind.
Zur Zeit weiß niemand so recht, wie man Computer wirklich sicher macht, da Angreifer sehr viele Möglichkeiten haben in ein System zu gelangen und Verteidiger meist in der reaktiven Rolle zurück bleiben.[116]
Bis konkrete Lösungsmodelle entstehen, müssen Betreiber kritischer Infrastrukturen, sowie Unternehmen und Privatpersonen allgemein dazu übergehen, die persönliche Kompetenz im Umgang mit Systemen auszubauen. Anomalien müssen sofort bemerkt werden und zu bestimmten Handlungen führen.
Es müssen Best Practice Ansätze für verschiedene Angriffsszenarien sowie Datenbanken mit aggregierten Angriffsdaten geschaffen und in Unternehmen integriert werden. Die verpflichtende Einführung von in Kapitel 4.3.2. angesprochenen regelmäßigen Penetrationstests bietet nützliche Lösungspotentiale.
In Bezug auf das Parlakom-Netz bleibt abzuwarten, ob das Neuaufsetzen der betroffenen Systeme ausreicht, oder sich der Trojaner möglicherweise doch in das BIOS einprogrammiert hat, wodurch ein Austausch des gesamten Systems notwendig werden würde.

Die Auslegung des IT-Sicherheitsgesetzes wird in Zukunft zeigen, ob die Maßnahmen bei den vorgesehenen Unternehmen Wirkung zeigen. Des Weiteren wird im Angesicht der Industrie 4.0 und der Integrierung der dafür vorgesehenen automatisierten Produktions- und Steuerungssysteme gezeigt werden, ob man aus den Fehlern der Vergangenheit gelernt hat. Eine ab Werk-Einführung von Sicherheitslösungen zum Schutz dieser Systeme muss mit einbezogen werden. Hierbei sollte bestenfalls ein Wettbewerb um die Sicherheit der Systeme entstehen, der möglicherweise durch Subventionen der Regierungen gestützt werden muss.

[115] Vgl. Kaminsky, 2015
[116] Vgl. Kaminsky, 2015