Hochschule
Augsburg University of
Applied Sciences

Fakultät für Informatik

Bachelorarbeit

Studienrichtung
Informatik

Michael Jünger

Entwicklung eines Leitfaden zur Unterstützung der forensischen Analyse bei Cybercrimevorfällen in KMU

Prüfer: Prof. Dr. Gordon Rohrmair

Abgabe der Arbeit am: 17.04.2014

Hochschule für angewandte
Wissenschaften Augsburg
University of Applied Sciences

An der Hochschule 1
D-86161 Augsburg

Telefon +49 821 55 86-0
Fax +49 821 55 86-3222
www.hs-augsburg.de
info@hs-augsburg.de

Fakultät für Informatik
Telefon: +49 821 5586-3450
Fax: +49 821 5586-3499

Verfasser der Diplomarbeit:
Michael Jünger
Brunnenbachstraße 4
86157 Augsburg
Telefon:+49 821 24 23 73 06
michael_jünger@arcor.de

Erstellungserklärung:

Hiermit erkläre ich, dass ich die vorgelegte Arbeit selbstständig verfasst, noch nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen oder Hilfsmittel verwendet sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

Name,	Datum,	Unterschrift
Michael Jünger	17.04.2014	

Abstract

Die vorliegende Arbeit wurde in Zusammenarbeit mit der HSASec erstellt. Im Folgenden soll dem Leser das Thema Cybercrime näher erläutert werden, was darunter zu verstehen ist und welche verschiedenen Arten von Angriffen es gibt.

Zunächst wird die juristische Grundlage geklärt und die zuständigen Behörden vorgestellt, die in sicherheitsrelevanten Fragen Ansprechpartner darstellen, und jene, die im Falle eines Angriffes auf die IT-Landschaft kontaktiert werden müssen.

Im weiteren Verlauf wird die aktuelle Sicherheitslage beleuchtet und näher auf die Ziele und das Vorgehen der Angreifer eingegangen.

An einem realen Beispiel wird dargestellt, wie die Sicherheitsvorkehrungen eines Unternehmens aussehen können und welche Techniken dabei zum Einsatz kommen. Außerdem, wie Mitarbeiter in sicherheitsrelevanten Fragen beraten werden und wie diese mittels Dienstanweisungen dazu angeleitet werden können, das Risiko menschlichen Versagens zu minimieren, um ein Optimum an Sicherheit zu gewährleisten.

Schlussendlich bietet diese Arbeit einen Leitfaden mit Verhaltensanweisungen für den Ernstfall.

Vorwort

Technologie im Allgemeinen und allem voran die der Informationsverarbeitung nehmen eine immer größer werdende Rolle in Alltag und Berufsleben ein. Seit Anfang der frühen achtziger Jahre, mit dem Einzug der Personal Computer (PC) in Wohnungen und Büros, hat sich die Abhängigkeit von der elektronischen Datenverarbeitung (EDV) stetig vergrößert. Seither hat sich vieles verändert und auch die Technik hat sich weiterentwickelt. Durch immer komplexer werdende Systeme ist es nunmehr möglich, in so kurzer Zeit wie niemals zuvor die Leistungsfähigkeit datenverarbeitender Systeme kontinuierlich zu steigern. Diese rasante Entwicklung hat allerdings nicht nur positive Aspekte.

Immer komplexer werdende Systeme bedeuten auch eine größere Anfälligkeit für Fehler. Das heißt jedoch nicht in jedem Fall, dass das System schlicht nur nicht mehr funktioniert. Dies wäre angesichts der Folgen, die so ein Systemfehler haben kann, noch die günstigere Variante. Fehler bedeuten auch Sicherheitslücken, die eine Soft- oder Hardware hat. Durch die flächendeckende Vernetzung nahezu aller IT-Systeme via Internet ist es möglich, von einem entfernten Ort auf diese Systeme zuzugreifen und unter Ausnutzung bekannter Sicherheitslücken auch in dieselben einzudringen. Vertrauliche oder persönliche Daten können so schnell in falsche Hände gelangen. Erfolgte der Angriff zudem aus dem Ausland, ist es unter Berücksichtigung der politischen Beziehungen zu dem Land, aus dem der Angriff durchgeführt wurde, nahezu unmöglich, die Täter zu ermitteln, geschweige denn ihrer habhaft zu werden. Nicht selten stellt sich dabei auch die Frage, ob nicht sogar Konkurrenten oder gar ausländische Geheimdienste zum Zweck der Wirtschaftsspionage hinter einem solchen Angriff stecken, und ob die vermeintlichen Hacker nur als Tarnung in ihrem Auftrag handeln.

Sicherheit für IT-Systeme spielt demnach in allen Bereichen der EDV eine immer wichtigere Rolle. Eine Absicherung der IT-Systeme bedeutet nicht nur Schutz der eigenen Privatsphäre oder die der Angestellten. IT-Sicherheit dient vielmehr auch dem Erhalt der Konkurrenzfähigkeit eines Unternehmens durch Wahrung betrieblicher Geheimnisse, und trägt somit zur Sicherheit von Arbeitsplätzen bei. Sie dient dem Erhalt bedeutender Wirtschaftsstandorte und verhindert den Raub von Innovationskraft in ein fremdes Wirtschaftsgebiet. Dies sichert und stärkt nicht zuletzt die Wirtschaftsleistung einzelner Regionen und Staaten. Für die nationale Integrität ist es demzufolge unerlässlich, Bürger, Dienstleistungsgewerbe, Handel und Industrie gegen kriminelle und feindliche äußere Einflüsse zu schützen.

Leider gibt es trotz aller ergriffenen Maßnahmen nie einen Schutz, der zu 100 Prozent für

die Sicherheit garantieren kann. Daher ist es das Ziel dieser Arbeit, darüber aufzuklären, wie sich Opfer einer Cyberattacke verhalten sollten, um am Ende nicht noch mehr Schaden zu verursachen und um möglichen künftigen Angriffen nach gleichem Schema präventiv entgegen wirken zu können.

Inhaltsverzeichnis

Abstract I

Vorwort III

Inhaltsverzeichnis V

Abkürzungsverzeichnis IX

Abbildungsverzeichnis XI

1. Einleitung 1

2. Begriffserklärungen 3
2.1. „Kritische Infrastrukturen“ . . . 3
2.2. Virtual Private Network . . . 3
2.3. Drive-by-Download . . . 3
2.4. Internetprotokoll Adresse . . . 3
2.5. Ports . . . 4
2.6. The Onion Router Network . . . 4
2.7. Sicherungssysteme . . . 5
2.7.1. Antiviren Software . . . 5
2.7.2. Firewall . . . 5
2.7.3. Intrusion Detection Software . . . 6
2.7.4. Persönliche Identifikationsnummer . . . 6
2.7.5. Passwörter . . . 6
2.7.6. Benutzer-Rollen Konzept . . . 7
2.7.7. Verschlüsselung . . . 7
2.8. Malware . . . 8
2.8.1. Computerviren . . . 8
2.8.2. Trojaner . . . 9
2.8.3. Würmer . . . 9
2.8.4. Adware . . . 9
2.8.5. Besondere Ausprägungen vom Malware . . . 10

3. Juristische und organisatorische Grundlagen 11
3.1. Definition von Cybercrime . . . 11

3.2. Gesetze im Zusammenhang mit Cybervergehen . . . 12
3.2.1. Strafgesetze . . . 12
3.2.2. Sonstige Vorschriften . . . 15
3.3. Organisation der Cyberabwehr in der BRD . . . 16
3.3.1. Die Behörden im Gesamtüberblick . . . 17

4. Definition verschiedener Angriffsarten 22
4.1. Gegenwärtige Angriffsszenarien . . . 22
4.1.1. Social Engineering . . . 22
4.1.2. Infektion mit Malware . . . 23
4.1.3. Distributed Denial of Service Attacke . . . 24
4.1.4. Man-in-the-Middle Attacke . . . 24
4.1.5. Phishing . . . 25
4.1.6. Onlineerpressung . . . 27
4.1.7. Diebstahl digitaler Identitäten . . . 28
4.1.8. Spam . . . 29
4.2. Klassifizierung der Angriffsarten . . . 29
4.2.1. Technische Sicht . . . 29
4.2.2. Organisatorische Sicht . . . 30
4.3. Eingrenzung der Tätergruppe . . . 32
4.3.1. Hacker . . . 33
4.3.2. Jugendliche Angreifer . . . 33
4.3.3. Insider . . . 33
4.3.4. Kriminelle Organisationen . . . 34
4.3.5. Politisch motivierte Angriffe . . . 34
4.4. Lokalisation der Angreifer . . . 36

5. Aufbau einer typischen Sicherheitslandschaft 37
5.1. Gängige Sicherheitsvorkehrungen in Firmen . . . 37
5.1.1. Sicherheitspolicen . . . 38
5.1.2. Verwendung externer Datenträger . . . 38
5.1.3. Einsatz von Firewalls . . . 39
5.1.4. Antiviren Software . . . 39
5.1.5. Regelmäßige Updates . . . 40
5.1.6. Restriktiver Zutritt . . . 40
5.1.7. Logische Trennung von Intranet und Internet . . . 41
5.1.8. Wartungsarbeiten durch externe Dienstleister . . . 41
5.1.9. Internetzugang für Gäste . . . 41

6. Aktuelle Gegebenheiten 43
6.1. Fallzahlen in der BRD . . . 43
6.2. Cybervorfälle im Branchenvergleich . . . 44
6.2.1. Systemausfälle . . . 44

6.2.2. Infektionen mit Schadsoftware 44
6.2.3. Spam Mails 44
6.2.4. Versehentliches Verändern von Daten und Datenverlust 45
6.3. Wie hoch ist der jährlich entstehende Schaden 45
6.4. Fazit zu den Fallzahlen 45

7. Leitfaden für das Vorgehen nach einem Angriff **47**
7.1. Erkennen eines Angriffes 47
7.2. Sofortmaßnahmen 48
7.3. Meldung des Vorfalls an die Behörden 49
7.3.1. Wichtige Fragen vorab klären 49
7.3.2. Anzeige des Vorfalls bei einer ermittelnden Stelle 50
7.3.3. Meldung von Datenschutzverstößen 51
7.4. Ziele der Ermittlungen 52
7.4.1. Identifikation des Angreifers 52
7.4.2. Schwachstellen erkennen 53
7.4.3. Prävention und Angriffsabwehr 53
7.4.4. Schadensanalyse 53

8. Schlussteil **54**

Literaturverzeichnis **57**

A. Anhang **A**
A.1. Zugrunde liegende Gesetze . . . . . A
A.2. Informative Links . . . . . M
A.3. Informationssammlung bei Sicherheitskritischen Vorfällen . . . . . O

Abkürzungsverzeichnis

ASCII American Standard Code for Information Interchange 6
BDSG Bundesdatenschutzgesetz 15
BfDI Bundesbeauftragte für Datenschutz und die Informationsfreiheit 15
BfV Bundesamt für Verfassungsschutz 19
BKA Bundeskriminalamt 18
BMWi Bundesministerium für Wirtschaft und Energie 20
BRD Bundesrepublik Deutschland 11
BSI Bundesamt für Sicherheit in der Informationstechnik 16
BS Betriebssystem 5
CAZ Cyber Allianz Zentrum 18
Cyber-AZ Nationale Cyber-Abwehrzentrum 16
DDoS Distributed Denial of Service 24
DV Datenverarbeitung 14
EC3 European Cybercrime Centre 16
EDV Elektronische Datenverarbeitung III
EU Europäische Union 16
E Empfänger 24
IDS Intrusion Detection Software 1
IHK Industrie und Handelskammer 21
IP Internetprotokoll 3
IR Infrarot 23
ISP Internet Service Provider 39
KA Klinikum Augsburg 37
KIS Krankenhaus Informationssystem 40
KRITIS „Kritische Infrastrukturen“ 3
LDA Landesamt für Datenschutzaufsicht 20
LfV Landesamt für Verfassungsschutz 18
LKA Landeskriminalamt 18
MA Mitarbeiter 31
MITM Man-in-the-Middle 24
MIT Bereich Medizinisch/Klinische Kommunikation, Informatik und DV-Technik 38
MPG Medizinproduktgesetz 46
mTAN mobilen Transaktionsnummer 27
PC Personal Computer III

PIN Persönliche Identifikationsnummer 6
PKS Polizeiliche Kriminalstatistik 11
SGB Sozialgesetzbuch 19
SP Spion 24
StGB Strafgesetzbuch 11
S Sender 24
SÜG Sicherheitsüberprüfungsgesetz 19
TKG Telekommunikationsgesetz 15
TOR The Onion Router 4
USB Universal Serial Bus 23
UTF-8 UCS Transformation Format 6
VPN Virtual Private Network 3
WP, StB, RA, Ing. Wirtschaftsprüfer, Steuerberater, Rechtsanwälte, Ingenieure 44
ZAF Zeitarbeitsfirma 31
ZA Zeitarbeiter 31

Abbildungsverzeichnis

3.1. Nationale Cyber-Abwehrzentrum 16
3.2. Behörden auf einen Blick 17

4.1. Distributed Denial of Service Attacke 24
4.2. Man-in-the-Middle Attacke 25
4.3. Beispiel einer Spam Mail 29

7.1. Ablaufkette des Meldevorganges nach einem Angriff 52

1. Einleitung

In den meisten Alltagssituationen, sind wir oft zurecht erst einmal misstrauisch. Kaum jemand würde auf die Idee kommen, einem fremden Menschen von der Straße Zugang zu seiner Arbeitsstelle oder gar Wohnung zu verschaffen. Schon alleine die Frage etwa nach dem Haustürschlüssel dürfte bei den meisten ein ungutes Gefühl auslösen. Wer will schon seine Arbeitsstelle verlieren, weil er derart fahrlässig gehandelt hat, oder möchte, dass jemand in seiner Privatsphäre herum stöbert. In der Realität ist das noch recht einfach. Die Haus- oder Wohnungstüre ist eine klare Grenze zwischen öffentlichem und privatem Lebensraum, die jeder kennt. In aller Regel existiert eine Türklingel, mit deren Hilfe gebetene und ungebetene Gäste auf sich aufmerksam machen können. Hier hat jeder für sich das Recht und die Kontrolle darüber zu entscheiden, wen er in sein privates Umfeld herein bittet.

Überschreitet jemand ohne unsere Zustimmung diese Grenze, ist das zum einen aus strafrechtlicher Sicht ein Einbruch und aus persönlicher Sicht ein klarer Vertrauensbruch. Hier ist wohl jedem klar, wie das weitere Vorgehen aussieht. Die Polizei wird eingeschaltet und es kommt zur Strafanzeige mit anschließendem Gerichtsverfahren. Unter Umständen lassen sich für einen entstandenen Schaden auch zivilrechtlich Ansprüche gegen den Beschuldigten geltend machen. Dass die Polizei an dieser Stelle als Ermittlungsbehörde eine beratende Funktion einnimmt und auch Interessierten vor Ort hilft, die Einbruchssicherheit zu erhöhen, ist wohl ebenso relativ verbreitet.

In der Informationstechnologie ist es im Grunde nicht anders als in der wirklichen Welt. Das Internet ist der öffentliche Raum, der eigene PC - zu Hause oder am Arbeitsplatz - ist der private Lebensbereich. Als Haustüre zwischen dem öffentlichen und privaten Bereich fungiert heutzutage bei den meisten Fällen ein Router. Das Türschloss ist in diesem Vergleich die sogenannten Firewall. Ist diese nicht aktiv oder unzureichend konfiguriert, stehen einem Einbrecher meist Tür und Tor offen, um in das anvisierte System zu gelangen. Weitere Sicherheitsmaßnahmen, wie etwa Antivirenprogramme sorgen zudem dafür, dass ungebetene Gäste enttarnt und ausgeschlossen werden. Zudem übernimmt sogenannte Intrusion Detection Software (IDS) die Funktion einer Alarmanlage.

Die Digitalisierung unserer Welt ist bereits seit einigen Jahrzehnten in vollem Gange. Spätestens mit der Jahrtausendwende hat zudem zunehmend der Einzug des Internet in Büros und Haushalte begonnen. Diese Vernetzung des nicht öffentlichen Bereiches PC mit dem öffentlichen Bereich Internet bietet zahlreiche neue Möglichkeiten. Sie ist jedoch zugleich auch die größte Schwachstelle und stellt die mehr oder weniger technisch versierten Anwender vor immer neue Herausforderungen. Sowohl Unternehmen als auch Privatpersonen sehen sich immer neuen Bedrohungssituationen ausgesetzt. Die Zahl der jährlich festgestellten gezielten Angriffe auf IT-Systeme nimmt zu. Obgleich es zahlreiche Gegenmaßnahmen gibt,

um sich vor den verschiedensten Angriffen zu schützen, bietet keine Sicherungsmaßnahme einen vollkommenen Schutz. Erschwerend kommt hinzu, dass die verfügbaren Maßnahmen nur in Kombination wirksam sind. Durch eine steigende Anzahl notwendiger Sicherheitskomponenten erhöht sich jedoch wiederum das Risiko, dass einer dieser Mechanismen versagt. Folglich ist davon auszugehen, dass es Angreifern auch in Zukunft gelingen wird, in fremde IT-Systeme einzudringen, Daten abzufangen, sie zu manipulieren, und die Informationstechnologie als Ganzes für ihre Zwecke zu missbrauchen.

Ein weiterer Beleg für dieses Szenario ist die derzeitige Abhängigkeit bei der Anschaffung von IT vom US-amerikanischen und chinesischen Markt. Allen voran die Marktführer der Branche aus der Volksrepublik China unterliegen der staatlichen Kontrolle. Es ist demnach nicht auszuschließen, dass unter staatlicher Anleitung Hintertürchen, auch „backdoor“ genannt, in IT-Komponenten eingebaut und von staatlichen Stellen im Zuge der Spionage ausgenutzt werden könnten. Die Enthüllungen durch Edward Snowden aus dem Jahre 2013 zeigen zudem, dass auch Verbündete nicht davor zurückschrecken, das technisch Mögliche für ihre Zwecke zu nutzen.

Um die Risiken für die Zukunft besser abschätzen zu können, ist es unumgänglich, dass so viele Informationen über die Angreifer wie möglich an die entsprechenden Behörden weitergeleitet werden. Nur diese Informationen ermöglichen es, geeignete Gegenmaßnahmen zu entwickeln und schlussendlich auch einzuleiten. Leider kommt es trotz der Notwendigkeit nach wie vor selten zur Anzeige sicherheitskritischer Vorfälle auf IT-Anlagen.

Das Hauptziel dieser Arbeit ist demnach die Klärung der Frage, was im Falle eines erfolgten Cyberangriffes geschehen muss. Sie soll allgemeine Begrifflichkeiten klären sowie die aktuelle Gesetzesgrundlage aufzeigen. Die zuständigen Bundesbehörden sollen vorgestellt und die unterschiedlichen gegenwärtigen Arten von Angriffen erörtert werden. Anhand eines Beispiels soll dargestellt werden, wie eine typische IT-Landschaft eines Unternehmens aufgebaut ist, und welche Maßnahmen zu deren Absicherung ergriffen werden. Schlussendlich ist diese Arbeit ein Leitfaden, der aufzeigt, wie am sinnvollsten weiter verfahren werden soll, nachdem ein Angriff auf ein IT-System erfolgt ist.

2. Begriffserklärungen

Die im Folgenden genannten Begriffe sind Definitionen häufig genannter relevanter Fachbegriffe der IT oder stehen in direktem Zusammenhang mit dem Thema Cybercrime.

2.1. „Kritische Infrastrukturen“

Unter dem Begriff „Kritische Infrastrukturen“ (KRITIS) versteht man sämtliche Einrichtungen mit wesentlicher Bedeutung für das Staats- und Allgemeinwesen. Darunter fallen vor allem wichtige Infrastrukturen für Energie- und Trinkwasserversorgung, Kommunikationseinrichtungen oder Steuerungsanlagen für den Verkehr. Eine Störung solcher Anlagen gefährdet nachhaltig die innere Sicherheit und Versorgung der Zivilbevölkerung.

2.2. Virtual Private Network

Bei einem Virtual Private Network (VPN) handelt es sich um eine verschlüsselte Verbindung zwischen einem Client und einem VPN-Server über ein unsicheres Netzwerk. Häufig ist dabei auch von einem Tunnel die Rede, was den Zweck dieser Verbindung bildlich veranschaulicht. Alle Daten die durch diesen Tunnel gesendet werden, sind durch ihn verschlüsselt und somit von außen geschützt (Werth, 2009, vgl. Kunst d. digitalen Verteidigung, 91).

2.3. Drive-by-Download

Ein sogenannter Drive-by-Download meint die Infektion mit Malware alleine durch das Aufrufen (engl. Drive-by: Im Vorbeifahren) einer Ressource in einem Netzwerk (Bundeskriminalamt, 2012a, vgl. Lagebild, 5).

2.4. Internetprotokoll Adresse

Um gezielt mit einem Computer in einem Netzwerk kommunizieren zu können, braucht dieser eine eindeutige Adresse, so wie auch in der Realität jedes Unternehmen und jede Person eine Postanschrift hat. Die Internetprotokoll (IP) Adresse entspricht dabei der Straße, Hausnummer und Postleitzahl. Es handelt sich um einen numerischen Wert von 32 Bit,

der in Gruppen von je vier Byte dezimal dargestellt wird. Im Heimgebrauch ist eine Adressierung in der Form 192.168.1.1, 192.168.1.2, usw. üblich. Beim normalen Gebrauch von Internetdiensten spielt diese Adresse jedoch keine sichtbare Rolle. Da solche Zahlenpaare für Menschen schwer zu merken sind, erfolgt eine Zuordnung der Adresse auf Namen, wie www.hs-augsburg.de. Wird diese Webadresse aufgerufen, wird der Name auf die numerische Adresse aufgelöst, wovon der Anwender jedoch nichts mitbekommt.

2.5. Ports

Die IP-Adresse dient als Anschrift, um die Netzwerkpakete an den richtigen Computer zu senden. Wie in einem Unternehmen mehrere Personen tätig sind, verrichten auf einem Computer ebenso unterschiedliche Programme ihre Dienste. Einige davon bieten Netzwerkfunktionalitäten an, wie etwa der Webbrowser, E-Mail-Clients oder auch die Windows Update Funktion. Diese Programme lauschen im laufenden Betrieb auf die eingestellte Netzwerkschnittstelle und warten dabei auf eingehende Pakete. Da nun verschiedene Dienste ihre Anfragen und Antworten gleichzeitig über ein und dieselbe Netzwerkschnittstelle senden und empfangen, ist eine Zuordnung der Netzpakete erforderlich. Für die Kommunikation mit dem entfernten Rechner bedienen sich demnach alle netzwerkfähigen Programme sogenannter Ports. Dabei handelt es sich um eine numerische Zuordnung der jeweiligen Dienste, was bei einer Postanschrift dem Namen des Empfängers entspricht. Ein Webserver zum Beispiel lauscht in aller Regel auf Port 80.

2.6. The Onion Router Network

The Onion Router (TOR) Projekt entstammt dem „Onion Routing Project“, welches vom U.S. Naval Research Laboratory und der U.S Navy entwickelt wurde. Ursprünglich sollte es die Kommunikation der US Regierung schützen, inzwischen kann es jedoch von jedermann verwendet werden. Es handelt sich dabei um ein verteiltes anonymes Netzwerk.

Normalerweise wird bei einer Verbindungsanfrage von einem Client an einen Server die IP Adresse des Clients mit übermittelt. Der Server muss schließlich wissen, an wen er welche Antwort zurücksenden soll. Dadurch wird es jedoch möglich, die Aktivitäten eines jeden Clients aufzuzeichnen. Ein online Versandhaus kann dadurch die angesehenen Produkte der IP-Adresse zuordnen, sie speichern, und dem Client bei einem erneuten Besuch entsprechende Produktvorschläge anzeigen. Ziel von TOR ist, diese Rückverfolgung einer Verbindung über das Internet zu verhindern und den Besucher zu anonymisieren.

Die Funktionsweise von TOR ist relativ einfach. Bei einer Anfrage an einen Server wird vom Client zunächst eine Liste der verfügbaren TOR-Server geladen. Aus dieser Menge an

Servern wird anschließend eine zufällige Route zum eigentlichen Ziel gewählt, wobei die Verbindung zwischen den TOR-Servern verschlüsselt ist. Das Entscheidende an der Funktionsweise von TOR ist, dass jeder Server jeweils nur seinen Vorgänger und den Nachfolger kennt, nicht jedoch die Herkunft und das eigentliche Ziel der Anfrage. Das Versandhaus speichert somit nicht die IP-Adresse des Besuchers, sondern die des letzten TOR-Servers. Da TOR bei jeder Verbindungsanfrage eine neue zufällige Route aus der Menge der Server wählt, ist folglich keine eindeutige Zuordnung des Besuchers anhand seiner IP-Adresse mehr möglich, da diese sich mit jeder Anfrage ändert.

2.7. Sicherungssysteme

Hierunter sind gängige Sicherheitsmechanismen zu verstehen, wie sie heute größtenteils eingesetzt werden. Der folgende Überblick dient dem besseren Verständnis der weiteren Arbeit.

2.7.1. Antiviren Software

Antivirenprogramme gibt es in verschiedenen Ausführungen. Es gibt sowohl manuell zu startende Virenscanner, als auch solche, die permanent als Hintergrundprozess im Betriebssystem (BS) laufen. Die sicherste Variante ist, einen Virenscanner als Hintergrundprozess auszuführen. Auf diese Weise wird er automatisch mit dem BS gestartet. Einmal aktiviert, überwacht der Virenscanner die Datenströme des Systems und scannt diese auf bekannte Codesignaturen, die je gezielt einem Schadprogramm zugeordnet werden können. Es ist darauf zu achten, dass kostenfreie Virenscanner in der Regel nicht alle Kanäle überwachen und nur einen rudimentären Schutz bieten.

Sogenannte „manuelle“ Virenscanner sind dabei meistens das letzte Mittel der Wahl, um einer Infektion mit Schadsoftware Herr zu werden. Vor allem, wenn davon auszugehen ist, dass die Infektion ein bereits installiertes Antivirenprodukt korrumpiert hat.

2.7.2. Firewall

Aufgabe einer Firewall ist, den Netzwerkverkehr zu filtern. So können beispielsweise Ports für die Kommunikation entweder komplett gesperrt oder nur für den internen Datenaustausch erlaubt werden. Eine Firewall ist demnach eine Art Pförtner. Pakete, die an diese Port-Nummern gerichtet sind, werden fortan blockiert. Das alleine reicht heutzutage allerdings nicht mehr aus. Gelingt es einem Angreifer den Netzwerkverkehr abzufangen, ist es ihm dadurch möglich, die Daten der Netzwerkpakete nachträglich zu verändern. So auch

die Port-Nummer. Dadurch lassen sich definierte Regeln der Firewall umgehen. Folglich ist eine eingehende Analyse der Netzwerkpakete erforderlich.

2.7.3. Intrusion Detection Software

Eine solche eingehende Analyse der Netzwerkpakete kann durch eine IDS erfolgen. Die IDS sucht dabei nach Mustern, die auf einen möglichen Angriff schließen lassen können. Ein Beispiel: „If the IDS finds that a series of ICMP packets were sent to each port in sequence, this probably indicates that your system is being scanned by network-scanning software... Since this is often a prelude to an attempt to breach your system security...“ (Easttom, 2011, Computer Security, 188). Es geht dabei folglich um das Erkennen untypischer Anfragen eines Clients.

2.7.4. Persönliche Identifikationsnummer

Die Persönliche Identifikationsnummer (PIN) ist eine meist vierstellige Zahlenkombination zur Identifikation. Die PIN fungiert dabei als eine Art Zugangscode, der den Anwender zu nachfolgenden Aktionen autorisiert, wie an einem Bankautomaten. Der Vorteil einer PIN ist, dass sie leichter zu merken ist als ein komplexes Passwort. Dafür ist die PIN jedoch relativ unsicher. Da sie, wie bereits erwähnt, oft vierstellig ist, bietet sie lediglich 10^4 verschiedene Kombinationsmöglichkeiten. Aus diesem Grund bleiben dem Anwender meist nur drei Versuche die richtige Zahlenkombination einzugeben, bevor das System die PIN für den weiteren Zugriff sperrt. Folglich ist die PIN ein Kompromiss aus Sicherheit und Benutzerfreundlichkeit.

2.7.5. Passwörter

Ein Passwort hat die gleiche Aufgabe wie eine PIN, kann jedoch aus einer Kombination von Zahlen, Buchstaben und Sonderzeichen bestehen. Dadurch sind Passwörter grundsätzlich sicherer als PINs. Im Vergleich zur vierstelligen PIN bietet ein vierstelliges Passwort nur aus Kleinbuchstaben bereits $26^4 = 456.976$ verschiedene Möglichkeiten. Enthält das vierstellige Passwort die komplette Bandbreite aller darstellbaren Zeichen der American Standard Code for Information Interchange (ASCII) Tabelle, besteht dieses sogar aus $94^4 = 78.074.896$ verschiedenen Permutationen. Durch die Verwendung eines anderen Zeichensatzes als ASCII, beispielsweise UCS Transformation Format (UTF-8), wäre auch die Verwendung der Zeichen aus dem europäischen Sprachraum möglich, was die Kombinationsmöglichkeiten noch einmal deutlich erhöht. Es existieren demnach zwei Faktoren, welche die Sicherheit eines Passwortes beeinflussen. Dessen Länge und die Anzahl der verwendeten Zeichen.

2.7.6. Benutzer-Rollen Konzept

Die meisten gängigen IT-Systeme erfordern für den Zugriff eine vorherige Authentifizierung. Diese geschieht in der Regel in Kombination eines Benutzernamens mit PIN oder Passwort. Zum einen soll dadurch verhindert werden, dass unberechtigten Personen Zugriff auf das System erlangen. Zusätzlich erlaubt der Benutzername zugleich eine Zuordnung des Anwenders zu einer Gruppe, der sogenannten Rolle. Innerhalb einer Rolle ist es dem Anwender gestattet, lediglich die für die Gruppe autorisierten Aktionen im System durchzuführen. So kann ihm zum Beispiel der Zugriff auf bestimmte Daten verwehrt werden, die für seine spezifische Tätigkeit irrelevant sind.

2.7.7. Verschlüsselung

Gleich welche Sicherungsmaßnahmen Anwendung finden, ohne eine Verschlüsselung der Daten sind diese praktisch nutzlos, wenn jeder die Informationen im Klartext mitlesen kann. Die Idee der Verschlüsselung ist nicht neu und fand bereits in der Antike mit der sogenannten Caesar-Verschlüsselung Anwendung. Dabei handelt es sich um einen einfachen Verschlüsselungsalgorithmus, der lediglich eine Verschiebung der Buchstaben im Alphabet vorsieht. Ein Buchstabe wird so auf einen anderen abgebildet. Eine Verschiebung um den Wert 3 im Uhrzeigersinn ergibt somit: $A \mapsto D, B \mapsto E, C \mapsto F, ..., Z \mapsto C$. Diese Art der Verschlüsselung ist keinesfalls sicher, denn spätestens nach dem 25. Versuch hat der Angreifer diese geknackt. Dennoch zeigt das Beispiel der Caesar-Verschlüsselung anschaulich, was Verschlüsselung bezwecken soll. Sie soll Informationen unkenntlich machen, indem sie diese in eine Form bringt, die für andere keinen Sinn ergibt. Dabei sollen die Informationen jedoch erhalten bleiben, sodass Eingeweihte sie anschließend wiederum entschlüsseln können.

Aktuelle Verschlüsselungsalgorithmen sind weitaus komplexer als noch zu Zeiten der Römer. Ihre Sicherheit liegt vielmehr im Verfahren selbst als in der Anwendung. Aufgrund der Vielfalt der bestehenden Algorithmen sollen im Folgenden jedoch nur die grundsätzlichen Unterschiede behandelt werden.

Der wesentliche Unterschied heutiger Verschlüsselungstechniken sind symmetrische und asymmetrische Verfahren. Bei symmetrischen Verfahren wird das Passwort zur Entschlüsselung, ebenfalls in verschlüsselter Form, übertragen. Bei asymmetrischen Verfahren existieren zwei verschiedene Schlüssel. Der sogenannte private key, der nur dem Eigentümer bekannt ist, und der dazugehörige public key, der den Kommunikationspartnern ausgehändigt wird. Mithilfe des öffentlichen Schlüssels ist es nun möglich, Inhalte zu verschlüsseln, wohingegen die Entschlüsselung nur mittels private key und somit nur dem Eigentümer dieses Schlüssels möglich ist.

2.8. Malware

Malware ist ein Überbegriff für Computersoftware, die darauf ausgelegt ist, dem System, unter dem sie ausgeführt wird, oder dessen Anwender Schaden zuzufügen. In der Gegenwart gibt es viele Arten von Schadsoftware, die sich jedoch alle in die drei Hauptkategorien Viren, Würmer und Trojaner einordnen lassen. Eine sehr ausführliche Beschreibung über das Phänomen Malware bietet das gleichnamige Buch „Malware“ von Eugene Kasperskij. Er beschreibt darin sehr anschaulich die anfängliche Spielerei einzelner Wissenschaftler mit sich selbst replizierenden Programmen in den Großrechenanlagen der Siebziger Jahre. Der Großteil dieses Werkes beschäftigt sich jedoch mit der Ära der Heimcomputer und einer damit einhergehenden Explosion virulenter Software in den Neunzigern bis etwa hin zur Hälfte des ersten Jahrzehnts des neuen Jahrtausends. In dieser allem Anschein nach sehr bewegenden Zeit war der Zweck schadhafter Programme hauptsächlich die mutwillige Zerstörung privater Daten. Vereinzelt verbargen sich auch politische Absichten oder zumindest Botschaften in den eingesetzten Viren, wie etwa dem WANK-Virus aus dem Jahre 1989 (Kasperskij, 2008, vgl. Malware, 110). Erwähnenswert ist auch, dass, wenn die Anzahl auch verschwindend gering ist, nicht jede als schädlich klassifizierte Software zwangsläufig bösartig war. So etwa der Wurm CodeGreen aus dem Jahr 2001. Dieser machte Jagd auf seinen bösen Gegenspieler, den Wurm CodeRed, der ebenfalls 2001 die Bildfläche betreten hatte (Kasperskij, 2008, vgl. Malware, 134). Die Geschichte der Viren und Würmer zeigt deutlich, wie die stetige Weiterentwicklung von Schadprogrammen in den letzten 30 Jahren die aktuelle Sicherheitslage beeinträchtigt hat. Da das Thema Malware sehr umfangreich ist, wird im Folgenden nur auf die wesentlichen Unterschiede eingegangen.

2.8.1. Computerviren

Hierbei handelt es sich um die wohl älteste Form von Schadprogrammen. Ein Computervirus ist seinem Pendant aus der Natur nachempfunden und besitzt die Fähigkeit, sich selbst zu replizieren. Dabei tritt das Virus jedoch nicht aktiv in Erscheinung. So wie das reale Vorbild auf lebendige Zellen angewiesen ist, nistet sich ein Computervirus in ausführbare Dateien ein, die vom Anwender oder dessen BS aufgerufen werden. Werden diese ausgeführt, wird künftig auch das Virus mit gestartet, wodurch es aktiv werden kann.

In späteren Erscheinungen erhielten Computerviren zudem noch die Fähigkeiten, sich zu tarnen und, wie auch sein reales Vorbild, die Fähigkeit, zu mutieren.

2.8.2. Trojaner

Trojaner sind die bislang am weitesten verbreitete Art von Schadsoftware. Dazu zählen Programme, die heimlich unerwünschte Aktionen ausführen, wie das Löschen von Dateien oder die Ausnutzung von Computerressourcen zu anderen Zwecken (Kasperskij, 2008, Malware, 52). Ihre Technologie basiert in der Regel auf Entwicklungen der Computerviren.

2.8.3. Würmer

Wie Computerviren besitzen auch Würmer die Fähigkeit, sich selbst zu replizieren. Der Unterschied zum Computervirus ist jedoch, dass ein Computerwurm aktiv agieren und eigenständig in fremde Systeme eindringen kann. Eine vorhergehende Aktion von Seiten des Anwenders ist nicht mehr zwingend notwendig. Folglich handelt es sich bei einem Computerwurm um eine Software, die das Zielsystem kennt und darauf programmiert ist, gezielt Sicherheitslücken des darunterliegenden BS auszunutzen. Basierend auf ihrer Eigenschaft - dem aktiven Eindringen in Computersysteme - haben Computerwürmer selbst oft keine direkte schädigende Funktion. In den meisten Fällen enthalten sie jedoch zusätzlichen schädlichen Code. Würmer dienen somit Viren und Trojanern als „Transportmittel“, um sie an ihren Bestimmungsort zu bringen und dort zu aktivieren.

2.8.4. Adware

Unter Adware versteht man Programme zum Zweck der Werbeanzeige. Sie wird in der Regel nicht als eigenständige Software ausgeliefert, sondern ist einer anderen beigefügt und wird mit dieser installiert. Solche Anwendungen, die Adware enthalten, sind in der Regel für den Nutzer kostenfrei, da sie mit Hilfe der Adware werbefinanziert werden. In etwa nach dem gleichen Prinzip wie bei heutigen kostenfreien Apps für mobile Geräte. Adware als solche ist demnach nicht grundsätzlich schädlich. Häufig jedoch bleibt deren Vorhandensein im System dem Benutzer, mit Ausnahme der Werbeanzeigen, verborgen, und es fehlen nicht selten Mechanismen zur Deinstallation (Kasperskij, 2008, vgl. Malware, 73). Was jedoch Adware in jedem Fall zu einem potentiellen Sicherheitsrisiko macht, sind die Werbeanzeigen. Es ist oft unklar, woher diese stammen und ob es sich dabei um vertrauenswürdige Quellen handelt. Angreifer könnten die Werbequellen der Adware manipulieren, um über sie gezielt Schadcode auf die Systeme ihrer Opfer zu schleusen.

2.8.5. Besondere Ausprägungen vom Malware

Die vorangegangene Klassifizierung stellt die grundlegenden Arten von Malware dar. Diese Grundarten decken aus technischer Sicht alle Eigenschaften von Malware ab. Einzelne besondere Ausprägungen werden jedoch mit Eigennamen versehen. Einerseits, um sie anhand ihrer Funktion besser von anderen Arten differenzieren zu können, andererseits jedoch auch, weil eine einschlägige Namensgebung auf die Leserschaft von Computermagazinen eine fesselnde Wirkung hat.

Ransomware

Eine erwähnenswerte Ausprägung von Malware ist Ransomware. Dabei handelt es sich um eine Art Schadprogramm, das den PC des Opfers entweder sperrt oder dessen Festplatte verschlüsselt, sodass der Rechner für den Anwender unbrauchbar ist. Die betroffene Person wird anschließend mittels einer eingeblendeten Meldung aufgefordert, ein Lösegeld für die Entsperrung oder die Entschlüsselung zu bezahlen (Funaro, 2013, vgl. Ransomware, 1). Die Bezahlung erfolgt dabei nicht selten über digitale Zahlungsdienstleister, was einen anonymen Geldtransfer zu den Tätern ermöglicht (Bundeskriminalamt, 2012a, vgl. Lagebild, 7).

Dieses Phänomen trat erstmals im Dezember 1989 auf. Ein Trojaner namens „Aids“ wurde von einem Angreifer auf 20.000 Disketten mit der Aufschrift „AIDS Introductory“ an verschiedene Personen in Europa, Afrika und Australien verschickt. Nach 90 Starts des BS wurden alle Dateinamen verschlüsselt und ausgeblendet. Einzig eine lesbare Datei blieb auf dem System sichtbar, welche Zahlungsinformationen enthielt (Kasperskij, 2008, vgl. Malware, 110).

Spyware

Ein weiterer Begriff, der in diesem Zusammenhang in der Vergangenheit häufig anzutreffen war, ist die sogenannte Spyware. Ihre Eigenschaft zur Spionage gehört jedoch zur Definition eines Trojaners. „Damit hat Spyware keine eigenständige technische Bedeutung, sondern ist ausschließlich ein Marketingbegriff“ (Kasperskij, 2008, Malware, 75).

3. Juristische und organisatorische Grundlagen

Dieses Kapitel behandelt nachfolgend alle Themen rund um die gesetzlichen und organisatorischen Gegebenheiten der Bundesrepublik Deutschland (BRD) in Sachen Cyberkriminalität. Der Fokus richtet sich dabei sowohl auf die gesetzliche Grundlage der BRD, die es den hiesigen Strafverfolgungs- und Justizbehörden bei festgestellten Verstößen erlaubt, entsprechende Maßnahmen zu ergreifen, als auch auf die Benennung der verschiedenen Landes- und Bundesbehörden, die zur Thematik informieren, beraten oder die Wirtschaft aktiv in der Abwehr und Aufklärung von Cybervorfällen betreuen.

3.1. Definition von Cybercrime

Die Polizeiliche Kriminalstatistik (PKS) fasst alle Straftaten, welche unter Zuhilfenahme eines Computers begangen wurden, unter dem Begriff Cyberkriminalität zusammen. Dabei handelt es sich um Delikte welche unter „...Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen wurden..." (Bundeskriminalamt, 2012a, Bundeslagebild, 3). Dies ist allerdings eine sehr weit gefasste Erklärung. Um den Tatbestand Cyberkriminalität zu beschreiben und als Ganzes zu erfassen, ist es unumgänglich, die vorherrschende Rechtslage zu betrachten.

Juristisch muss an dieser Stelle differenziert werden. Aus strafrechtlicher Sicht ist eine Straftat, bei der ein Computer lediglich als Tatwerkzeug verwendet wird, keine Straftat im engeren Sinne der Computerkriminalität. Dies kann am Beispiel des Betrugs bzw. des Computerbetrugs veranschaulicht werden. Juristisch gesehen ist ein Betrugsfall auch Betrug gemäß § 263 Strafgesetzbuch (StGB), unabhängig ob er unter Zuhilfenahme von E-Mail, auf postalischem Weg oder direktem Ansprechen auf der Straße erfolgt ist. Eines der Indizien dafür, dass eine Straftat in den Bereich der Computerkriminalität fällt ist, wenn das Begehen einen Eingriff in einen Datenverarbeitungsvorgang notwendig macht.

Im Zuge der Digitalisierung hat der Gesetzgeber darum einige juristische Grundlagen geschaffen, die eine Zuordnung einer Straftat zur Computerkriminalität erlauben. Mithilfe dieser ist es den Behörden nun möglich, solche Vergehen zu ahnden und die Täter entsprechend zu bestrafen. Welche Gesetze hierfür in Frage kommen, wird im Folgenden aufgezeigt.

3.2. Gesetze im Zusammenhang mit Cybervergehen

Aus juristischer Sicht gibt es bei der Auslegung und der Anwendung der Gesetze viele Fallstricke. Demnach kann an dieser Stelle keine vollständig verbindliche juristische Darstellung der Gesetzeslage erfolgen, da immer der konkrete Einzelfall ausschlaggebend ist und für sich betrachtet werden muss. Im Schadensfall sollte daher der Sachverhalt zwingend von einem Rechtsbeistand geprüft werden. Der folgende Inhalt dient demnach vielmehr dazu, die bestehenden Gesetze zu nennen und deren Inhalt zu erörtern.

Diese Gesetze und Verordnungen stellen die aktuelle juristische Grundlage der BRD im Zusammenhang mit Computerkriminalität dar. Cybercrime als solches ist lediglich ein Überbegriff für eine Vielzahl von Vergehen, die im Zusammenhang mit Informationstechnologien stehen. Eine spezifische Erörterung der aktuellen Bedrohungslage findet sich im Anschluss an dieses Kapitel unter Definition verschiedener Angriffsarten auf Seite 22.

3.2.1. Strafgesetze

§ 202a Ausspähen von Daten (StGB)

§ 202a kommt zur Anwendung, wenn der Schutz vor unberechtigtem Zugriff auf Daten umgangen wird, und die Daten nicht für die Person bestimmt sind, die den Schutz umgeht (Fischer u. a., 2014, vgl. § 202a Abs. 1 StGB, 1378). Solche Schutzmaßnahmen sind in der Regel Verschlüsselung, das Ablegen der Daten in einen passwortgeschützten Bereich oder die Blockade von Zugriffen von außerhalb durch sonstige technische Maßnahmen. Umgeht ein Angreifer diese Maßnahmen, ist von Ausspähen die Rede. Ein Beispiel dafür ist das Mitlesen von verschlüsselten Inhalten, die dazu unrechtmäßig entschlüsselt werden mussten.

§ 202b Abfangen von Daten (StGB)

Hier ist in erster Linie das Abhören von Daten gemeint. Strafbar macht sich, „[w]er [sich] unbefugt... Daten... aus einer nicht öffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung... verschafft“ (Fischer u. a., 2014, vgl. § 202b StGB, 1383). Folglich: Wer unberechtigt Daten aus einer Datenübertragung, die nicht an eine undefinierte Personengruppe gerichtet ist, mit-liest, oder sich zu eigen macht. Mit der elektromagnetischen Abstrahlung sind allem voran Datenübertragungen von Funknetzwerken gemeint, es kann sich jedoch beispielsweise auch um die Abstrahlung von Bildinformationen bei alten Röhrenmonitoren handeln.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten (StGB)

Die Vorbereitung von Straftaten im Sinne der §§ 202a, b StGB ist ebenso strafbar. Die Vorbereitung schließt die Anschaffung, Verbreitung oder Erstellung entsprechender Computerprogramme zur Durchführung solcher Straftaten ein (Fischer u. a., 2014, vgl. § 202c Abs. 1 StGB, 1385). Im Volksmund ist § 202c StGB daher auch als der sogenannte Hackerparagraph bekannt.

§ 206 Verletzung des Fernmeldegeheimnisses StGB

Nach § 206 StGB machen sich alle Strafbar, die anderen unbefugt Mitteilung über Tatsachen machen, die dem Post- oder Fernmeldegeheimnis unterliegen. Dies gilt sowohl für Beschäftigte eines Telekommunikationsdienstes, wie für Amtsträger außerhalb des Telekommunikationsbereiches. Das Strafmaß ist mit bis zu fünf Jahren für Beschäftigte von Telekommunikationsdiensten jedoch etwas höher, als für Personen außerhalb dieses Sektors.

Das Post- und Fernmeldegeheimnis ist in § 88 Fernmeldegeheimnis (TKG) definiert. Laut diesem unterliegen der Inhalt, sowie die näheren Umstände, und insbesondere die Tatsache, ob jemand an einer Telekommunikation beteiligt ist oder war, dem Fernmeldegeheimnis. Unter den näheren Umständen einer Telekommunikation sind Verkehrsdaten - wie die Nummer des Telefonanschlusses, Beginn und Ende der Verbindung oder der verwendete Telekommunikationsdienst - gemeint (Miłosz, 2002, vgl. Datenschutzrecht und Fernmeldegeheimnis, 9).

Die Verletzung des Fernmeldegeheimnisses ist zu melden, siehe dazu § 109a Datensicherheit (TKG) auf Seite 15.

§ 263a Computerbetrug (StGB)

Mit § 263a StGB wurde eigens der Tatbestand Computerbetrug definiert. Entscheidend für diesen ist, dass nicht der Mensch getäuscht wurde, sondern die Maschine. Eine E-Mail mit betrügerischem Text ist kein Computerbetrug im Sinne von § 263a Abs. 1 StGB. Damit der Straftatbestand Computerbetrug zu tragen kommt, muss ein Datenverarbeitungsvorgang beeinflusst werden (Fischer u. a., 2014, vgl. § 263a Abs. 1 StGB, 1944).

Das heißt:

1. Die zu verarbeitenden Daten werden von einem Dritten manipuliert, sodass es durch ihre Verarbeitung zu einem falschen Ergebnis kommt.

2. Ein Datenverarbeitungsvorgang wird von einem Dritten ohne die Zustimmung des Nutzers ausgelöst.

§ 263a StGB besagt außerdem: „Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt...“ (Fischer u. a., 2014, § 263a Abs. 1 StGB, 1944). Dem Geschädigten muss demnach zudem ein finanzieller Schaden entstehen.

Darüber hinaus ist die Herstellung, Anschaffung, Bereitstellung, der Besitz und die Übergabe von Programmen, mit denen eine solche Straftat begangen werden kann, ebenso strafbar (Fischer u. a., 2014, vgl. § 263a Abs. 3 StGB, 1944).

§ 269 Fälschung beweiserheblicher Daten (StGB)

Auch die Fälschung beweiserheblicher Daten fällt in die Kategorie Cybercrime. Damit ist im Grunde der Tatbestand der Urkundenfälschung in digitaler Form gemeint.

§ 303a Datenveränderung (StGB)

Eine Datenveränderung im Sinne von löschen, unterdrücken, unbrauchbar machen oder verändern ist ebenso strafbar (Fischer u. a., 2014, vgl. § 303a Abs. 1 StGB, 2247). Die meisten Angriffe auf IT-Systeme dürften hiervon betroffen sein. Wenn an dieser Stelle auch die Veränderung von Logdateien berücksichtigt wird, hat jedes Eindringen in ein System zur Folge, dass mindestens diese verändert werden.

§ 303b Computersabotage (StGB)

Computersabotage meint das Stören einer Datenverarbeitung (DV), die für einen anderen von wesentlicher Bedeutung ist. Absatz eins erfasst dabei sowohl die DV privater Personen als auch die von Unternehmen (Fischer u. a., 2014, vgl. § 303b Abs. 1 StGB, 2251). Es stellt sich jedoch die Frage, wann eine DV von wesentlicher Bedeutung ist. „Das ist der Fall, wenn die jeweilige Aufgabenstellung oder Organisation von der Funktionsfähigkeit der DV ganz oder jedenfalls überwiegend abhängig ist“ (Fischer u. a., 2014, StGB, 2254). Bezogen auf ein Unternehmen ist dies relativ klar. Jeder Arbeitsplatzrechner und nahezu jegliche Peripherie können für den reibungslosen Arbeitsablauf als unentbehrlich angesehen werden. Somit dürfte jedwede Beeinträchtigung der Datenverarbeitungsvorgänge eine Störung von Vorgängen mit wesentlicher Bedeutung sein. Zudem verfügt die Beeinträchtigung der DV von Unternehmen, Behörden oder Betrieben über ein höheres Strafmaß (Fischer u. a., 2014, vgl. § 303b Abs. 2 StGB, 2252).

3.2.2. Sonstige Vorschriften

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten BDSG

§ 42a Bundesdatenschutzgesetz (BDSG) verpflichtet nicht öffentliche Stellen dazu, Verstöße gegen den Datenschutz unverzüglich der Aufsichtsbehörde und den Betroffenen zu melden. Zuständige Behörde ist in der Regel die jeweilige Landesdatenschutzaufsichtsbehörde. Die Meldung an den Geschädigten erfolgt, sobald geeignete Maßnahmen zum Schutz der Daten ergriffen, oder wenn diese zu spät eingeleitet wurden und wenn die Strafverfolgung durch die Meldung nicht mehr gefährdet ist. Der Betroffene muss zudem über die Art der unrechtmäßigen Kenntniserlangung und über Maßnahmen zur Minderung von Nachteilen informiert werden. Die zuständige Aufsichtsbehörde muss über die Folgen des Vorfalls und die ergriffenen Maßnahmen unterrichtet werden. § 42a sieht vor, die Betroffenen in der Öffentlichkeit über den Vorfall zu informieren, wenn zum Beispiel die Anzahl der Geschädigten zu groß ist.

§ 43 Bußgeldvorschriften (BDSG)

Hauptgegenstand der Bußgeldvorschriften sind Verstöße im Zusammenhang mit personenbezogenen Daten. Eine besondere Rolle spielt dabei § 43 BDSG vor allem in Fällen, in denen Anwender durch Täuschung „freiwillig“ dazu gebracht werden, persönliche Daten von sich preis-zu-geben, ohne dass der Angreifer dazu Sicherungsmaßnahmen umgehen muss (Alexander Seidl und Katharina Fuchs, 2010, Strafbarkeit des Phishing).

§ 109a Datensicherheit (TKG)

§ 109a Telekommunikationsgesetz (TKG) verpflichtet Betreiber von Telekommunikationsdiensten dazu, Verstöße gegen den Datenschutz zu melden. Als Betreiber von Kommunikationsdiensten gilt jeder, der personenbezogene Daten verarbeitet oder speichert.

Wird beispielsweise festgestellt, dass ein Unbefugter in ein IT-System eingedrungen ist und dadurch personenbezogene Daten abhanden gekommen sind, muss dies binnen 24 Stunden an die Bundesnetzagentur und die Bundesbeauftragte für Datenschutz und die Informationsfreiheit (BfDI) gemeldet werden. Ein entsprechendes Meldeformular hierzu bietet die Bundesnetzagentur auf ihren Internetseiten an. Siehe dazu auch Anhang A.2

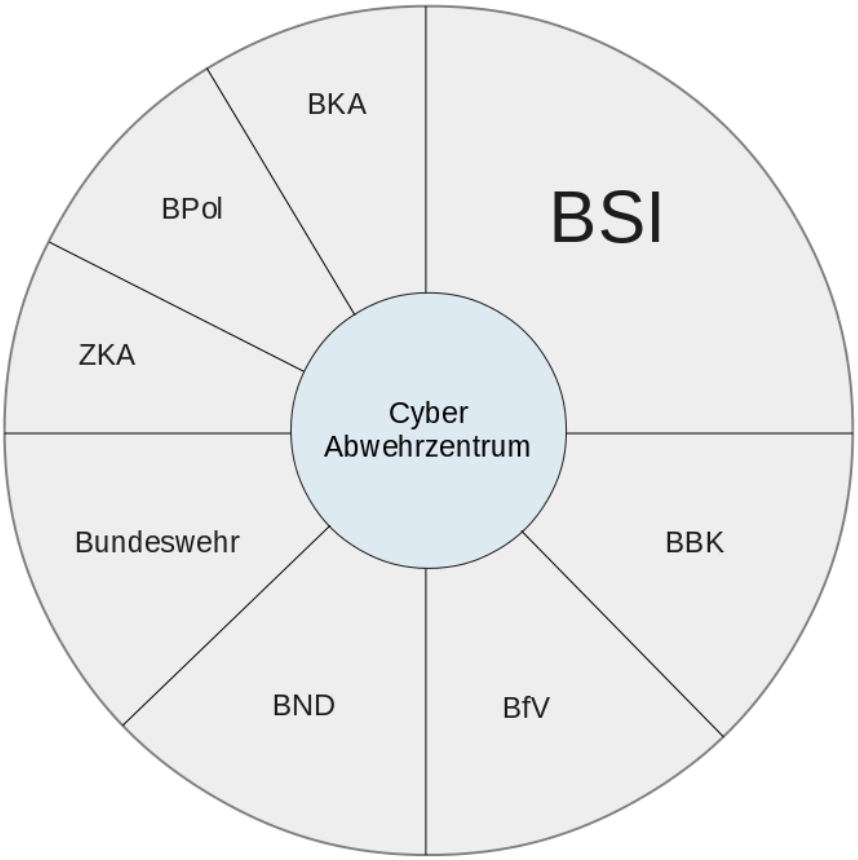
Eine vollständige Ausführung der genannten Gesetze findet sich im Anhang A.1

3.3. Organisation der Cyberabwehr in der BRD

Nach der beschriebenen aktuellen Gesetzesgrundlage, sollen nun die Behörden mit ihren jeweiligen Aufgaben vorgestellt werden. Die Funktionen der verschiedenen Instanzen reichen von Beratung über Prävention, hin zur Aufklärung ganzer Vorfälle. Welches diese Behörden sind und welche Aufgabe sie konkret haben, soll nachfolgend aufgezeigt werden.

Viele Behörden in Deutschland sind in ihrem jeweiligen Aufgabengebiet mit dem Thema Cyberabwehr betraut. An der Spitze steht das Nationale Cyber-Abwehrzentrum (Cyber-AZ), das maßgeblich unter der Führung des Bundesamt für Sicherheit in der Informationstechniks (BSIs) alle diese Stellen vereint. Hauptaufgabe des Cyber-AZ ist das Sammeln und der Austausch von Informationen der Ämter untereinander. Ziel ist es, den Wissensstand der verschiedenen Instanzen im Bezug zu Cybersicherheit auf einem gleichen Niveau zu halten. Seit dem 11. Januar 2013 erhalten die jeweiligen Behörden der Mitgliedsstaaten der Europäischen Union (EU) zudem Unterstützung vom European Cybercrime Centre (EC3). Abbildung 3.1 zeigt, welche Behörden am Cyber-AZ beteiligt sind.

Abbildung 3.1.: Nationale Cyber-Abwehrzentrum



Quelle: (BMI, 2011)

3.3.1. Die Behörden im Gesamtüberblick

Abbildung 3.2 zeigt eine Gesamtübersicht aller Behörden in Abhängigkeit ihrer jeweiligen Funktion.

Abbildung 3.2.: Behörden auf einen Blick

Polizeiliche Behörden

Als direkte Schnittstelle zwischen Geschädigten und Strafverfolgungsbehörden dienen die örtlichen Polizeidienststellen. Hier hängt es von den Begleitumständen des Angriffes ab, wie die Ermittlungen weiter verlaufen. „Bei den Landespolizeien werden Cybercrime-Delikte in der Regel durch örtliche Fachdienststellen bearbeitet oder – z. B. bei schwerwiegenden und überregionalen Fällen – auch durch das jeweilige Landeskriminalamt (LKA). Das Bundeskriminalamt (BKA) unterstützt die Polizeien der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder sonst erheblicher Bedeutung. In bestimmten Fällen kann auch das BKA selbst die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahrnehmen und Ermittlungsverfahren führen.“ (Bundeskriminalamt, 2012b, Handlungsempfehlungen, 7).

Die Ermittlungsbehörden unterliegen dem Legalitätsprinzip. Das bedeutet, dass, ist ein Vorfall einmal zur Anzeige gebracht, die Ermittlungsbehörden gesetzlich dazu verpflichtet sind, diesen aufzuklären.

Stammt der oder die Täter aus dem Ausland, erfolgt die Aufklärung des Falles innerhalb der EU auch unter Mitwirkung des EC3; und über die EU hinaus übernimmt gegebenenfalls Interpol die Ermittlungen.

Verfassungsschutzbehörden

Ähnlich wie die Polizei bietet auch der Verfassungsschutz im Unternehmensbereich eine direkte Schnittstelle für die Betroffenen an. Mit dem Cyber Allianz Zentrum (CAZ) Bayern wurde eigens eine Institution geschaffen, die speziell für Cybervorfälle zuständig ist. Das CAZ ist dabei dem Landesamt für Verfassungsschutz (LfV) untergliedert. Anders als die polizeilichen Behörden untersteht das CAZ nicht dem Legalitätsprinzip. Das bedeutet, ein Unternehmen kann sich zunächst einmal gezielt an das CAZ wenden, ohne befürchten zu müssen, dass es gleich zur Anzeige des Vorfalls mit anschließendem Strafverfahren kommt.

Das CAZ unterstützt Unternehmen und KRITIS bei der Prävention und der Abwehr von Angriffen und ist zugleich vertraulicher Ansprechpartner. Bei konkreten Anhaltspunkten für einen Angriff wird das CAZ jedoch auch selbst aktiv, indem es die betroffenen Unternehmen informiert (Cyber Allianz Zentrum Bayern, 2013, vgl. CAZ Bayern).

Unter bestimmten Voraussetzungen muss der Verfassungsschutz die Verantwortlichkeit in der Aufklärung eines Angriffes übernehmen. „Die Urheber ’Elektronischer Angriffe’ sind oft nicht zweifelsfrei zu identifizieren. Allerdings bedienen sich auch fremde Nachrichtendienste solcher Techniken. In diesen Fällen fällt die Bearbeitung in die Zuständigkeit der Spionageabwehr“ (Bundesamt für Verfassungsschutz, 2012, Verfassungsschutzbericht, 378). Allerdings müssen Anhaltspunkte vorliegen, die eine Beteiligung eines fremden Staates nicht

ausschließen. Weiter wird im Verfassungsschutzbericht auch die Proliferation - die Weitergabe von Atomwaffen, oder Mittel zu deren Herstellung - genannt, was ebenso unter Spionageabwehr fallen dürfte. Zudem sind die Verfassungsschutzbehörden zuständig, wenn sich der Angriff gegen KRITIS richtet. In Bayern übernimmt das CAZ die Steuerung und Koordinierung der Abwehr elektronischer Angriffe für die gesamte bayerische Wirtschaft und KRITIS.

Im CAZ werden alle Meldungen aus der Wirtschaft und der Betreiber von KRITIS gesammelt und in anonymisierter Form an das BSI sowie dem Bundesamt für Verfassungsschutz (BfV) gemeldet. Diese erstellen aus den Daten ein Lagebild der Gesamtsituation, welches die stetige Einschätzung der aktuellen Gegebenheiten, das Entdecken neuer Phänomene, sowie die Entwicklung neuer Abwehrstrategien ermöglicht.

Bundesbeauftragte für Datenschutz und die Informationsfreiheit

Das BfDI berät und kontrolliert hauptsächlich öffentliche Stellen auf Bundesebene, bei Fragen zur Daten- und Informationsverarbeitung, sowie Unternehmen, die unter das Sicherheitsüberprüfungsgesetz (SÜG) fallen. Siehe dazu Anhang A.1. Seit 2011 ist das BfDI auch Aufsichtsbehörde für gemeinsame Einrichtungen nach § 50 Absatz 2 Sozialgesetzbuch (SGB) II.

Der BfDI tritt an Stelle der Aufsichtsbehörde nach § 38 BDSG, wenn bei der geschäftsmäßigen Erbringung von Telekommunikationsdiensten „Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden...“ (BMJV, 2004k, § 115 Abs. 4 TKG). Datenschutzverstöße müssen nicht nur an die Bundesnetzagentur sondern auch an die BfDI gemeldet werden. Der Grund, weshalb eine Meldung sowohl an die Bundesnetzagentur als auch an den BfDI erfolgen muss ist, nach Auskunft der Bundesnetzagentur, „die Entscheidung des Bundesgesetzgebers, die datenschutzrechtlichen Fragen des TK-Rechts nicht durch 16 verschiedene (sonst zuständige!) Landesdatenschutzbehörden, sondern durch den BfDI als zentrale Datenschutzbehörde kontrollieren zu lassen“ (Jan Müller, 2014, Fragen zur Meldepflicht).

Landesbeauftragter für den Datenschutz

Der Landesbeauftragte für Datenschutz ist, wie das Landesamt für Datenschutzaufsicht, für Datenschutzverstöße zuständig, jedoch für den öffentlichen Bereich. Zudem ist er auch Ansprechpartner der Bürger bei Fragen zum Datenschutz in öffentlichen Einrichtungen.

Bundesamt für Sicherheit in der Informationstechnik

Das BSI ist seit 1991 Teil des Innenministeriums und als unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit zuständig. Die Aufgaben des BSI sind vielschichtig und in § 3 im Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes geregelt.

Im Allgemeinen ist die Aufgabe, Bundes-, Polizei- und Verfassungsschutzbehörden, sowie dem Bundesnachrichtendienst beratend und unterstützend zur Seite zu stehen. Darüber hinaus berät und unterstützt das BSI Wirtschaftsunternehmen.

Das BSI bietet Informationsmaterial zu aktuellen Bedrohungssituationen und ist somit wichtige Anlaufstelle für Bundesbehörden, Wirtschaft und Bürger. Zudem werden vom BSI selbst Standards und Verfahren zur Verbesserung der IT-Sicherheit entwickelt.

Bundesnetzagentur

Die Aufgaben der Bundesnetzagentur sind vielschichtig, wie die Regulierung des Telekommunikationsmarktes und anderer infrastruktureller Netze. Sie spielt jedoch auch für Opfer einer Cyberattacke eine Rolle, wenn durch die Attacke personenbezogene Daten verletzt wurden. Entsprechende Vorfälle müssen, wie bereits unter Punkt § 109a Datensicherheit (TKG) erwähnt, an die Bundesnetzagentur gemeldet werden.

Bundesministerium für Wirtschaft und Energie

Das Bundesministerium für Wirtschaft und Energie (BMWi) hat eigens eine Internetseite zum Thema IT-Sicherheit in der Wirtschaft, siehe dazu Anhang A.2. Auf dieser Seite informiert das BMWi über aktuelle Meldungen und bietet verschiedene Angebote zur Verbesserung der IT-Sicherheit in Unternehmen.

Landesamt für Datenschutzaufsicht

Das Landesamt für Datenschutzaufsicht (LDA) ist für die Einhaltung des Datenschutzes im nicht öffentlichen Bereich zuständig. Je nach Bundesland existiert hierfür kein eigenes Amt, sondern übernimmt der Landesbeauftragte diese Funktion. In Bayern jedoch gibt es hierfür ein eigenes Landesamt, mit Sitz in Ansbach. Nach § 42a BDSG in Punkt 3.2.2 müssen Datenschutzverstöße nicht öffentlicher Einrichtungen an das LDA gemeldet werden.

Industrie und Handelskammer

Die Industrie und Handelskammer (IHK) bietet als Organisation des öffentlichen Rechtes ebenso Schulungs- und Beratungsangebote im Bereich IT-Sicherheit für Mitglieder an. Auf den Seiten der IHK finden sich Informationen zur Thematik, auch als Verweise zu anderen Behörden.

4. Definition verschiedener Angriffsarten

In diesem Kapitel richtet sich der Fokus zunächst auf die verschiedenen Angriffsszenarien, denen Unternehmen sowie auch Privatpersonen gegenwärtig ausgesetzt sind, um ein grundlegendes Verständnis für die aktuelle Bedrohungslage zu schaffen. Im Anschluss daran soll das Wesen, welches hinter dem Begriff Cybercrime steckt, anhand unterschiedlicher Perspektiven näher erläutert werden. Ziel dieses Kapitels ist, die möglichen Tätergruppen hinter den Angriffsarten zu identifizieren, sowie ein tiefgreifenderes Verständnis für Computerkriminalität über die juristische und technische Sichtweise hinaus aufzubauen.

4.1. Gegenwärtige Angriffsszenarien

Die folgenden Szenarien sind aktuelle Bedrohungen. Ihre Beschreibung darf jedoch nicht darüber hinwegtäuschen, dass es sich dabei lediglich um Beispiele handelt. Kein Angriff gleicht dem Anderen und es ist durchaus eine Kombination der verschiedenen Techniken denkbar. Zudem kann grundsätzlich von zwei Unterscheidungsmerkmalen ausgegangen werden: Die Vorbereitung und die eigentliche Durchführung.

Vorbereitende Maßnahmen dienen in erster Linie der Informationsbeschaffung. Dabei handelt es sich um Informationen, die benötigt werden, um den eigentlichen Angriff durchführen zu können. Allem voran Social Engineering ist eine solche Maßnahme. Jedoch kann auch die Infektion mit Malware, Phishing oder der Diebstahl digitaler Identitäten eine vorbereitende Maßnahme für einen weiteren Angriff sein, obgleich es sich bei diesen auch um tatsächliche Angriffe handelt.

4.1.1. Social Engineering

Social Engineering ist die Grundlage für eine Vielzahl verschiedener Angriffsszenarien. Für eine erfolgreiche Offensive benötigen die Angreifer zunächst Informationen über die Infrastruktur des Angriffszieles. Im Fokus der Informationsbeschaffung stehen daher vorwiegend technische Mitarbeiter der IT Abteilungen. Die Kontaktaufnahme erfolgt hierfür meist mit Hilfe gefälschter Profile über soziale Netzwerke. Zunächst wird mit der Kontaktperson eine gewisse Vertrauensbasis aufgebaut. Anschließend wird das Opfer nach und nach in Fachgespräche verwickelt. Innerhalb des „freundschaftlichen“ Verhältnisses kommt es zum Fachsimpeln mit dem angeblichen Fachkollegen und es werden unscheinbare technische Details

wie Hersteller oder gar Modellbezeichnungen ausgetauscht. Auch auf dem Profil freigegebene Informationen über den beruflichen Werdegang, wie die Zertifizierung von einem bestimmten Hersteller sind hierbei dienlich. Solche Informationen können bereits Aufschluss darüber geben, welchen Hersteller die IT-Abteilung bevorzugt. Mit diesen Informationen ist es dem Angreifer nun möglich, weitere Recherchen durchzuführen, um die Schwachstellen der IT-Infrastruktur näher zu analysieren. Das Internet bietet hierfür in Form von öffentlichen Foren, Testberichten und Benutzerrezensionen ausreichend Möglichkeiten.

Doch nicht nur soziale Netzwerke und das technische Personal sind Ziel von Social Engineering. Auch direkte Anrufe und persönliches Erscheinen werden nicht gescheut, um an die gewünschten Informationen zu gelangen. So wird dem unbedarften Mitarbeiter eine Notsituation vorgetäuscht und an dessen Hilfsbereitschaft appelliert, schnell ein paar Informationen herauszugeben, weil der zuständige Kollege gerade angeblich nicht erreichbar sei und ohne die ein vermeintliches Problem nicht behoben werden kann.

4.1.2. Infektion mit Malware

Dies ist die wohl häufigste Form eines Angriffes auf ein IT-System und stellt sogleich die Grundlage für nahezu alle Angriffsarten dar. Letztlich bestimmt lediglich der Zweck einer Schadsoftware, um welche Art von Angriff es sich handelt. Die Infektionswege sind dabei so vielfältig, wie die Möglichkeiten, Daten auf ein IT-System zu spielen. Jeder Kanal zur Datenübertragung kann grundsätzlich auch zur Infizierung mit Malware ausgenutzt werden. Die eingesetzten Sicherheitsmechanismen entscheiden, ob es zu einer Infektion kommt. Wenn diese versagen, ist das Sicherheitskonzept des BS ausschlaggebend dafür, wie fatal die Auswirkungen dieser sind.

Der häufigste Infektionsweg ist das Internet. Die Schadsoftware gelangt zumeist über E-Mails oder durch den Besuch von Webseiten auf den Computer. Dabei ist es von Seiten des Anwenders längst nicht mehr erforderlich, einen Anhang aus einer E-Mail oder eine heruntergeladene Datei zu öffnen. Die Infektion kann bereits mittels Drive-by-Download geschehen, ohne das der Anwender hiervon etwas mitbekommt.

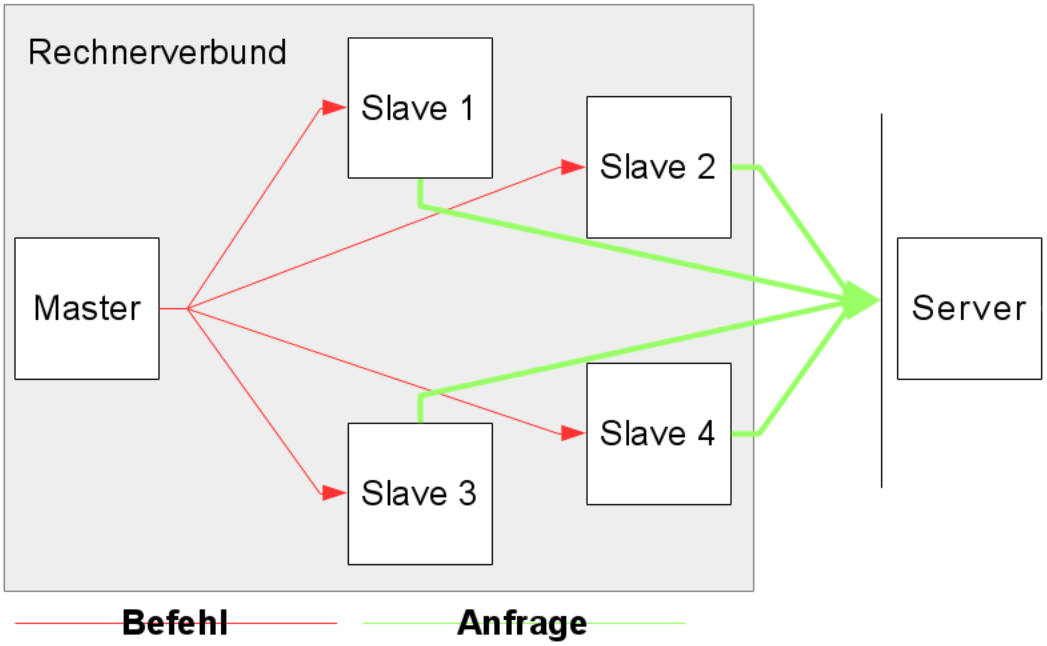
Ein weiterer häufiger Verbreitungsweg sind externe Datenträger, auch Wechselmedien genannt. Allem voran der Datenaustausch mit Hilfe von Universal Serial Bus (USB)-Sticks ist sehr beliebt. Diese sind kompakt, bieten eine hohe Speicherkapazität, sind wiederverwendbar. Der Schadcode befindet sich dabei meist in Dateien, die per Autostartfunktion aufgerufen werden, sobald der Stick am Rechner angeschlossen und vom BS erkannt wurde.

Darüber hinaus sind noch weitere Übertragungswege wie Bluetooth oder eine Infrarot (IR)-Schnittstelle denkbar, wenn dabei Daten übertragen werden, die ebenfalls mit Malware infiziert sind. Sie spielen bei der Verbreitung jedoch eine eher untergeordnete Rolle spielen.

4.1.3. Distributed Denial of Service Attacke

Bei einem Distributed Denial of Service (DDoS) Angriff wird ein Zielsystem durch gleichzeitige Anfragen von einem Rechnerverbund durch Überlastung lahmgelegt. Die Angreifer bedienen sich dabei sogenannter Bot-Netze, welche diesen Rechnerverbund darstellen. Die Teilnehmer eines solchen Bot-Netzes stellen Ihre Dienste dabei nur in den wenigsten Fällen freiwillig zur Verfügung. Vielmehr handelt es sich um Rechner, die mit einem speziellen Trojaner infiziert sind. Ein zentraler Computer - Master - befiehlt den einzelnen Mitgliedern des Rechnerverbunds - Slaves oder auch Zombies - eine Anfrage an den Zielserver zu stellen. Da diese Anfragen nur sehr schwer oder gar nicht von ernst gemeinten zu unterscheiden sind, versucht der Server alle zu beantworten. Ist das Bot-Netz groß genug, reichen die Ressourcen des Servers nun nicht mehr aus um die Anfragen zu beantworten, es kommt in der Folge kaum noch eine Verbindung zustande (Werth, 2009, vgl. Kunst d. digitale Verteidigung, 24). Abbildung 4.1 zeigt den Aufbau eines DDoS Netzes aus Master, Slaves und Angriffsziel.

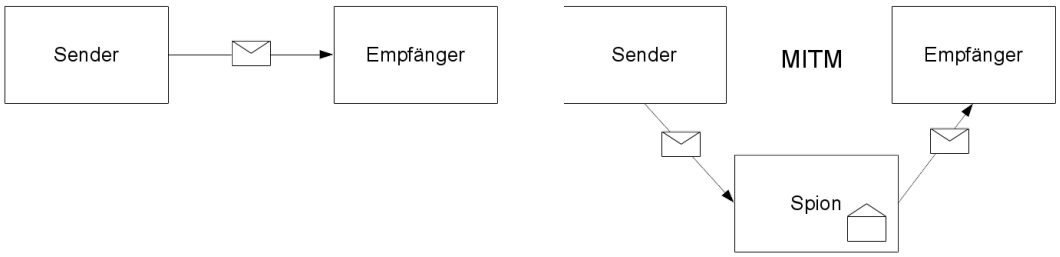
Abbildung 4.1.: Distributed Denial of Service Attacke



4.1.4. Man-in-the-Middle Attacke

In einem Netzwerk werden die gesendeten Pakete normalerweise vom Sender (S) an den Empfänger (E) gesendet. Bei einem Man-in-the-Middle (MITM) Angriff setzt sich jedoch ein unberechtigter Dritter, ein Spion (SP), zwischen diese beiden Kommunikationspartner und fängt deren Datenverkehr ab. Die Kommunikation zwischen Sender und Empfänger verläuft nun folglich von S über SP zu E. Siehe dazu Abbildung 4.2

Abbildung 4.2.: Man-in-the-Middle Attacke



Sender und Empfänger bekommen davon im Normalfall nichts mit. Dem Angreifer stehen dabei mehrere Möglichkeiten offen, eine MITM durchzuführen. Er kann sich im selben Netzwerk befinden wie seine Zielpersonen und den Netzwerkverkehr eigenständig umleiten. Er kann das Umleiten der IP-Pakete jedoch auch von außerhalb durchführen. Die Manipulation der Infrastruktur geschieht in diesem Fall mittels Schadsoftware.

Der Spion erhält nun alle Informationen, die sich Sender und Empfänger senden. Bestenfalls findet der Datenaustausch verschlüsselt statt, so kann der Spion die Informationen zumindest nicht im Klartext mitlesen. Für die Verschlüsselung muss jedoch zuvor zwischen Sender und Empfänger ein Schlüssel ausgehandelt werden. Schafft es der Angreifer sich bereits in diesen Vorgang einzuhängen, kann auch er die Daten entschlüsseln und folglich mitlesen. Um dieses Problem zu lösen benötigen Sender und Empfänger daher einen Dritten, der die Echtheit der beiden Kommunikationspartner garantiert, eine sogenannte Zertifizierungsstelle.

Diese Lösungsansätze existieren zwar bereits seit Längerem, trotzdem ist die Gefahr eines MITM-Angriffes noch immer präsent. Einige Teile des Datenverkehrs werden nach wie vor unverschlüsselt übertragen oder haben eine unzureichende Verschlüsselung. Darüber hinaus muss auch der Schlüssel sicher sein. Ist dieser zu kurz oder besteht aus zu wenigen kombinatorischen Möglichkeiten - enthält er beispielsweise nur Zahlen - ist der Schlüssel nach heutigem Stand der Technik mit relativ wenig Aufwand für den Angreifer entschlüsselbar.

4.1.5. Phishing

Phishing ist die „Beschaffung persönlicher Daten anderer Personen (wie Passwort, Kreditkartennummer o. Ä.) mit gefälschten E-Mails oder Websites“ (Bibliographisches Institut GmbH, 2013, Duden Online). Phishing-Attacken sind zielgerichtete Angriffe. Das heißt, die Angreifer wissen, wonach sie suchen, und richten ihren Angriff entsprechend an eine bestimmte Zielgruppe oder einzelne Person. Diese Angriffsform ist nach wie vor sehr beliebt und wird zum Teil auch mit hoher Effizienz von Geheimdiensten angewendet. Es geht dabei darum, dem Opfer die Authentizität der ihm vorliegenden Daten vorzutäuschen. Gelingt dies, ist der Angriff bereits so gut wie geglückt. In gutem Glauben über die Echtheit der

E-Mail oder Webseite befolgt das Opfer bereitwillig die enthaltenen Anweisungen und gibt relevante Zugangsdaten von sich preis.

Erfolgt der Angriff per E-Mail, wird dazu die Absenderadresse derselben gefälscht und mit einer für den oder die Empfänger vertrauenswürdigen ersetzt. Der Inhalt der E-Mails ist entsprechend auf die Empfänger zugeschnitten. Das Phishing von Daten einer ganzen Zielgruppe ist dabei einfacher durchzuführen, als der Angriff auf eine einzelne Person. Die benötigten Informationen für eine Phishing-Attacke auf eine Personengruppe sind in den meisten Fällen öffentlich zugänglich oder können in Anlehnung an reale Daten entsprechend angepasst werden. Bei einem Angriff auf nur eine Person ist es deutlich schwieriger die Authentizität der Daten zu gewährleisten, da zur Informationsbeschaffung oftmals auch der direkte Kontakt zur Zielperson hergestellt werden muss. An entsprechende Informationen über den Empfänger gelangen die Angreifer daher zum Großteil nur durch Social Engineering. Durch das Öffnen der E-Mail oder deren Anhang aktiviert das Opfer unbewusst eine enthaltene Schadroutine, die sogleich den Rechner infiziert. Ist keine Antiviren Software installiert oder erkennt diese den Eindringling nicht, ist es den Angreifern möglich, Informationen vom nunmehr infizierten Rechner abzufangen. In anderen Fällen werden die Empfänger gebeten, eine Webseite zu besuchen oder dazu aufgefordert, ein Web-Formular auszufüllen, welches direkt in die E-Mail integriert ist.

Zur Darstellung von Links auf eine präparierte Webseite kann ein anderer Zeichensatz Anwendung finden. Durch die Einführung internationaler Domainnamen stehen weit mehr Schriftzeichen für Domains zur Verfügung, als der ASCII-Zeichensatz bietet. Der Angreifer registriert eine Domain, die sich vom Original in nur einem Buchstaben unterscheidet. Er ersetzt dabei dieses Zeichen durch ein Schriftzeichen eines anderen Alphabets, welches dem ursprünglichen gleich sieht. Im kyrillischen Alphabet, um nur ein Beispiel zu nennen, gleichen die Buchstaben (a, e, j, k, o) optisch den lateinischen, wodurch der Unterschied nicht auffällt. Aus technischer Sicht handelt es sich jedoch um eine andere Webadresse als die Ursprüngliche, folglich führt auch der Link auf eine andere Webseite. (Dipl. Phys. Stefan Dieterle und Dr.-Ing. Peer Wichmann, 2003, vgl. Sicherheit für die Top-Level Domain .de, 84)

Im Gegensatz zur E-Mail, die gezielt auch an nur eine bestimmte Person versendet werden kann, richtet sich das Phishing über eine Webseite fast ausschließlich an eine bestimmte Personengruppe. Neben dem gezielten Locken von Personen auf eine Webseite via E-Mail und der Verwendung homographisch identischer Domainnamen, wurden in der Vergangenheit zudem Domains registriert, die sich ebenfalls in nur einem Buchstaben unterscheiden. Hier jedoch liegt der veränderte Buchstabe auf der Tastatur möglichst neben dem Ursprünglichen. Für die Angreifer besteht so eine gewisse Chance, dass sich ein Teil der Besucher bei der Eingabe der Internetadresse im Browser vertippt und dadurch auf die präparierte Seite gelangt. Das Layout der gefälschten Internetseite ist dabei, wie bei der E-Mail, dem Original nachempfunden.

Ob beim Phishing mit Hilfe von E-Mail oder einer Webseite. Einigen Besuchern mag es nicht auffallen, dass sie einer Fälschung zum Opfer fallen und sie geben wie gewohnt ihre Zugangsdaten in die Maske ein. Diese werden nun jedoch an die Angreifer verschickt, die dadurch die digitale Identität ihres Opfers erhalten. Durch die Einführung der mobilen Transaktionsnummer (mTAN) wurde dieses Risiko bislang entschärft. Das Abfangen der mTAN mittels Schadcode ist zwar grundsätzlich möglich, da der Großteil der vor allem privat genutzten mobilen Endgeräte bislang keinen ausreichenden Schutz hat, jedoch ist dies deutlich aufwendiger. Der Angreifer muss nun nicht mehr „nur“ dafür sorgen, dass ein Teil der Opfer auf die gefälschte E-Mail oder Webseite hereinfällt, sondern dass gleichzeitig auch das Empfangsgerät der mTAN entsprechend präpariert ist.

4.1.6. Onlineerpressung

Wie beim Phishing gibt es auch bei der Erpressung unterschiedliche Angriffswege. Richtet sich der Angriff gegen Privatpersonen, erfolgt er vornehmlich durch Ransomware. Soweit die Infektion mit Ransomware nicht mittels E-Mail erfolgt, geschieht dies meist durch den Besuch von Webseiten, die von den Tätern extra für diesen Zweck manipuliert oder eingerichtet wurden. Vor allem Internetseiten, die unsichere, externe Quellen referenzieren, stellen eine Gefahr dar. Der Schadcode befindet sich in diesem Fall in der geladenen externen Ressource. Eine Infektion durch den Besuch einer seriösen Webseite ist derzeit unwahrscheinlich, kann jedoch nicht ausgeschlossen werden.

Dabei werden vor allem Situationen ausgenutzt, in denen sich die Opfer selbst in einer rechtlichen Grauzone befinden, wie etwa beim Besuch eines illegalen Video-Streaming-Portals. Da einige Meldungen über die Sperre des eigenen PCs häufig als angebliche polizeiliche Maßnahme getarnt sind, erhöht dies massiv den Druck auf die Opfer, da sich diese im Moment der Sperre bei ihren eigenen Missetaten ertappt fühlen. Zudem ist die Gefahr einer Anzeige durch eines der Opfer in diesen Fällen sehr gering. Kaum ein Betroffener dürfte einen derartigen Angriff zur Anzeige bringen, wenn er dabei die Gefahr sieht, selbst einer Straftat bezichtigt werden zu können. Die Angreifer setzen folglich nicht mehr nur ihre technische Überlegenheit gegenüber dem Anwender ein, sondern sie spielen nunmehr auch mittels psychologischer Tricks mit ihren Opfern, um eine möglichst hohe Erfolgsquote zu erreichen und, daraus resultierend, den erbeuteten Gewinn zu maximieren.

Zielt der Angriff auf die Erpressung eines Unternehmens, haben sich die Angreifer noch eine weitere Taktik einfallen lassen, um Geld von ihren Opfern zu erpressen. Anders als Privatpersonen sind Firmen beinahe ausnahmslos mit einer Webseite im Internet vertreten. In vielen Fällen wird sogar ein Großteil des Tagesgeschäftes über diese abgewickelt, mindestens jedoch die Kommunikation mittels E-Mail. Alleine der Ausfall dieses Kommunikationsweges hat bereits katastrophale Folgen, da dadurch ganze Arbeitsabläufe massiv gestört werden, wodurch den Betroffenen ein nicht geringer finanzieller Schaden entsteht. Ist zudem das Tagesgeschäft in Teilen oder ganz von einer funktionierenden Webpräsenz abhängig, sind

die Schäden immens, wenn nicht sogar existenziell. Dies ist die sprichwörtliche Achillesferse vieler Unternehmen, die sich Kriminelle zu Nutze machen. Auch hier werden die Opfer dazu aufgefordert, ein Schutzgeld innerhalb eines Zeitraumes zu bezahlen. Andernfalls wird die IT des Unternehmens am genannten Stichtag mittels einer DDoS-Attacke angegriffen, wodurch obiges Szenario eintreten kann. Selbst Branchenriesen haben einer solchen Attacke, wenn diese breit genug angelegt ist, kaum etwas entgegenzusetzen. Da die Angreifer zudem fast ausnahmslos im nicht europäischen Ausland sitzen, ist es den Ermittlungsbehörden kaum möglich, die Täter in absehbarer Zeit zu stellen, weshalb der Angriff häufig statt findet. Doch nicht nur ganze Unternehmen sind der Bedrohung durch Erpressung ausgesetzt. Auch einzelne Mitarbeiter können dieser zum Opfer fallen. Die Möglichkeiten der Täter gehen hierbei über die reine Gelderpressung hinaus. So ist auch die Erpressung vertraulicher Daten ein denkbares Szenario.

4.1.7. Diebstahl digitaler Identitäten

Identitätsdiebstahl ist keine digitale Attacke im klassischen Sinne, sondern vielmehr das Resultat eines zuvor erfolgreich durchgeführten Angriffes. Oftmals steht der Diebstahl einer Identität im Zusammenhang mit Phishing. Erwähnenswert ist diese Form von Cybercrime an dieser Stelle jedoch trotzdem, da mit Hilfe der gestohlenen Identität weitere Angriffe möglich sind. Nahezu alle angebotenen Dienste im Internet sind mit Autorisierungsverfahren vor unbefugten Zugriffen geschützt. Der wachsende Trend, mittels mobiler Endgeräte von überall aus auf die firmeneigene Infrastruktur zugreifen zu können, macht den Identitätsdiebstahl für Angreifer daher zum lohnenswerten Ziel, da mittels dieser Identitäten eine Autorisierung für verschiedenste Dienste möglich wird. Auch die zunehmende Verbreitung des Cloud-Computing und die damit einhergehende Auslagerung von IT-Infrastruktur auf externe Dienstleister werden weiterhin für ein großes Interesse an digitalen Identitäten sorgen. Mit Hilfe der gestohlenen Identität hat ein Angreifer zudem nicht nur Zugang zu Firmeninterna. Ihm steht auch, abhängig von den angewandten Sicherheitsmechanismen, Tür und Tor in das Firmennetzwerk, und somit eine weitere Angriffsfläche, offen. Der Identitätsdiebstahl kann wohl als die fatalste Form aller möglichen Angriffe angesehen werden. Der Angreifer kann durch sie - zumindest solange er im Rahmen dessen agiert, was ihm die Identität erlaubt - beinahe unsichtbar bleiben, und zwar für eine lange Zeit, soweit der Diebstahl nicht auffällt. Durch die scheinbare Autorisierung seiner Handlungen hinterlässt der Angreifer nahezu keine sichtbaren oder auffälligen Spuren im System. Ein autorisierter Lesezugriff auf eine Datei wird wohl keinen Administrator aus der Ruhe bringen. Somit bleibt dem Angreifer genügend Zeit, wertvolle Informationen abzuschöpfen.

4.1.8. Spam

Spam ist eine Form unaufgeforderter elektronischer Werbepost. Spam lockt meist mit dem Versprechen auf schnelles Geld oder anderen Vergünstigungen für den Empfänger. Der Versand dieser Mails erfolgt meist von infizierten Systemen, wodurch den Versendern keine Kosten entstehen, weil sie selbst nicht die notwendige Infrastruktur bereitstellen müssen (Werth, 2009, vgl. Kunst d. digitalen Verteidigung, 26). Gehen die Empfänger auf die E-Mail ein, ist nicht ausschließlich der Betrug das Problem. Eine gut gemachte Spam E-Mail kann auch zum Phishing, Identitätsdiebstahl oder schlicht der Infektion mit Malware dienen. Abbildung 4.3 zeigt eine solche typische Spammail. Sie ist in schlechtem Deutsch geschrieben, was bei Spam häufig der Fall ist. Deshalb kann Spam relativ leicht von seriösen E-Mails unterschieden werden, eine Garantie für die Echtheit der E-Mail ist die sprachliche Qualität jedoch nicht.

Abbildung 4.3.: Beispiel einer Spam Mail


HALLO FREUND

Hallo,

Es tut mir leid, Ihre Privatsphäre zu stören. Es gibt eine gewisse verstorbenen Kunden von meiner Bank, die hinter der Summe von 18 Millionen US-Dollar belassen. Ich suche Ihre Partnerschaft in Empfang dieses Fonds.
Wenn Sie interessiert sind, antworten Sie bitte sofort für detaillierte Informationen. Danke.

Mit freundlichen Grüßen,
Larry.

4.2. Klassifizierung der Angriffsarten

Für ein besseres Verständnis der verschiedenen Angriffsarten ist es notwendig, diese in Kategorien einzuteilen. Zum einen kann auf diese Weise bereits vor dem Angriff eine Bedrohungsanalyse erstellt werden und zum anderen lassen sich dadurch im Ernstfall direkte Gegenmaßnahmen für den laufenden Angriff ableiten. Des Weiteren hilft dies bei der Entscheidungsfindung über das weitere Vorgehen nach einem Angriff. Hier stehen sich jedoch unterschiedliche Sichtweisen gegenüber. Auf der einen Seite die technische Sicht, deren Fokus die Angriffsabwehr durch geeignete Gegenmaßnahmen ist. Auf der anderen Seite die organisatorische Sicht, welche die Konsequenzen nach einem Angriff in den Mittelpunkt stellt. Außerdem, die Frage nach dem Motiv des Angreifers. Dieses erlaubt je nach Branche des Unternehmens Rückschlüsse auf die mögliche Tätergruppe, der das Unternehmen gegenüber steht und somit eine Bedrohungsanalyse.

4.2.1. Technische Sicht

In der gängigen Literatur zum Thema IT-Sicherheit liegt der Fokus häufig auf der Abwehr eines Angriffes. Die Einteilung geschieht hier demnach anhand entsprechender technischer

Kriterien, wie beispielsweise Einbruch, Verfügbarkeitsausfall oder dem Diebstahl von Informationen (Werth, 2009, vgl. Kunst d. digitalen Verteidigung, 23). Diese Art der Einteilung ist richtig, denn ein Verfügbarkeitsausfall erfordert andere Gegenmaßnahmen als dies bei einem Einbruch in das System der Fall ist. Zudem ist es sowohl für die Opfer des Angriffes als auch für die Ermittlungsbehörden entscheidend, ob Daten abhanden gekommen sind, oder ob der Angreifer weiterhin Zugang zum System hat und folglich mit weiteren Angriffen gerechnet werden muss.

Ebenso findet häufig eine Unterteilung nach technischen Kriterien in interne- und externe Angriffe statt. Wobei ersteres vornehmlich die Gefahr eines Angriffes aus dem Intranet durch die eigenen Mitarbeiter thematisiert, während letzteres von Angriffen ausgeht, die über das Internet stattfinden (Werth, 2009, vgl. Kunst d. digitalen Verteidigung, 30). Diese Unterteilung ist insofern ebenso korrekt. Für die Angriffsabwehr ist zunächst lediglich entscheidend, ob der Angreifer von außen oder von innen stammt. Zumal ist aus technischer Sicht nicht ersichtlich, ob es sich bei einem internen Angreifer tatsächlich um einen Mitarbeiter handelt, oder ob Malware den Angriff verursacht.

Die technische Sicht wirft an dieser Stelle jedoch Fragen auf:

1. Ist ein Angriff, der zwar aus dem Intranet heraus, jedoch von einer fremden Person gestartet wurde, dennoch ein interner Vorfall?

2. Kann von einem externen Angriff die Rede sein, wenn dieser zwar über das Internet, jedoch von einem Mitarbeiter durchgeführt wurde?

Für die Sicherheitsverantwortlichen lassen sich beide Fragen mit einem klaren Ja beantworten. Um geeignete Gegenmaßnahmen auf einen Angriff einleiten zu können, ist nur die technische Klassifizierung sowie die Lokalisation des Angriffes von Bedeutung. Da diese Arbeit jedoch einen Leitfaden zur Handlungsweise nach einem Angriff darstellen soll, muss auch die organisatorische Sicht betrachtet werden. Die grobe Einteilung anhand technischer Merkmale und der Lokalisation des Angriffes reicht hier nicht aus, denn diese erlaubt es nicht, geeignete Konsequenzen aus dem Angriff zu ziehen.

4.2.2. Organisatorische Sicht

Bezogen auf die beiden oben genannten Fragen muss das Verhältnis des Angreifers zum Unternehmen betrachtet werden. Um einen Angriff als intern oder extern zu klassifizieren, stellt sich die Frage, wie die Person an das Wissen gelangen konnte, welches für die Ausübung notwendig war. Eine Aufspaltung der Personengruppen lediglich in Mitarbeiter und Nicht-Mitarbeiter ist hier bei weitem nicht ausreichend. Jede Person, die rechtmäßig Zutritt zum Firmengelände oder Gebäude hat, ist während der gesamten Aufenthaltsdauer organisatorischer Teil dieses Unternehmens. Dabei ist es zunächst unerheblich, ob diese Person

Gast, Dienstleister, Zulieferer oder tatsächlich Mitarbeiter ist. Jede dieser Personen hat im Rahmen ihrer Tätigkeit in der Organisation individuelle Befugnisse. Besonders deutlich wird dies am Beispiel eines Zeitarbeiters:

Der Zeitarbeiter (ZA) ist Beschäftigter bei der Zeitarbeitsfirma (ZAF), mit der er ein direktes Beschäftigungsverhältnis hat. Die ZAF wiederum hat mit dem Unternehmen PC-AG einen Dienstleistungsvertrag geschlossen. Der ZA erbringt demnach im Auftrag der ZAF für die PC-AG lediglich eine Dienstleistung. Streng genommen ist der ZA somit kein Mitarbeiter (MA) der PC-AG. Zur Erbringung seiner Dienstleistung benötigt der ZA jedoch Kompetenzen, die ansonsten nur den MA der PC-AG gewährt werden und er ist notwendigerweise in die Geschäftsprozesse eingebunden. Folglich ist der ZA auch organisatorischer Teil der PC-AG. Der ZA steht zudem im Rahmen seiner Tätigkeit wie die MA in einem Vertrauensverhältnis mit der PC-AG und den MA untereinander. Dieses mag nach psychologischen Aspekten weniger stark ausgeprägt sein, als dies zwischen den MA und der PC-AG der Fall ist, was auf ein gesteigertes Zugehörigkeitsgefühl der MA zur PC-AG aufgrund des direkten Beschäftigungsverhältnisses zurückgeführt werden kann. Dennoch unterliegt auch der ZA im Rahmen seiner Tätigkeit in der PC-AG einer Geheimhaltungs- und Sorgfaltspflicht im Umgang mit Ressourcen und Firmeninterna, mit denen er in Berührung kommt oder von denen er aus Versehen Kenntnis erlangt. Wird die PC-AG nun vom ZA angegriffen, muss es sich dabei aus organisatorischer Sicht folglich um einen internen Vorfall handeln, weil dieser auf Wissen beruht, welches der ZA als Teil der PC-AG, und während seiner Tätigkeit für diese, erworben hat. Von wo aus der Angriff gestartet wurde, spielt dabei nur eine untergeordnete Rolle.

Die Konsequenzen sind im Falle eines internen Angriffes aus organisatorischer Sicht in jedem Fall andere, als dies bei einem Angriff durch eine außenstehende Person der Fall wäre. In der Regel wird ein Unternehmen einen internen Vorfall zunächst mit besonderer Diskretion behandeln wollen, da dieser innerhalb der Branche deutlich mehr Aufmerksamkeit erregen dürfte als ein Angriff durch einen Unbekannten. Kann der Angreifer außerdem bereits im Vorfeld von den Sicherheitsverantwortlichen identifiziert werden, kann es durchaus vorkommen, dass die Unternehmensleitung diesen zunächst selbst mit den Vorwürfen konfrontieren möchte, bevor weitere Schritte eingeleitet werden. Aus menschlicher Sicht ist das durchaus verständlich. Eine solche Handlung stellt einen gravierenden Vertrauensbruch dar, vor allem, wenn es sich bei dem Angreifer um einen langjährigen und geschätzten Kollegen handelt. Trotzdem ist dieses Vorgehen nicht zu empfehlen. Konfrontiert mit den Vorwürfen und einer ausweglosen Situation ist die Reaktion des Beschuldigten nicht absehbar. Neben den Konsequenzen für den Angreifer zieht ein interner Vorfall zudem noch weitere, tiefgreifendere Veränderungen für alle Mitarbeiter nach sich. Angriffe auf IT-Systeme sind, wenngleich auch tägliche Realität, häufig ein abstraktes Wesen. Handelt es sich bei einem Vorfall nicht um eine direkte Bedrohung, wie im Falle einer Online-Erpressung oder sind die Auswirkungen nicht direkt sichtbar, wie bei einem DDoS-Angriff, ist es für Laien oftmals schwer vorstellbar, was da vor sich geht. In jedem Fall jedoch hat der Angreifer kein Gesicht. Aufgrund der Anonymität des Internet ist er selbst ein abstraktes Wesen und nicht greifbar. Dadurch fällt

es schwer, die Bedrohung unmittelbar wahrzunehmen. Bei einem internen Vorfall sind die Gegebenheiten anders. Hier hat der Angreifer plötzlich ein Gesicht. Möglicherweise war er gern gesehener Begleiter in der Mittagspause oder saß sogar im selben Büro. Dies hat unbestreitbar auch tiefgreifende psychologische Auswirkungen auf das Betriebsklima und die Vertrauensbasis aller Firmenangehörigen.

Die bloße Einteilung in interne und externe Angriffe anhand technischer und organisatorischer Kriterien bietet ein Grundverständnis für die verschiedenen Angriffsarten. Um die Handlungsweise nach einem Angriff besser verstehen zu können, ist es zusätzlich notwendig zu wissen, wer die Angreifer sind. Der Mitarbeiter mag diesen zwar durchgeführt haben, dennoch ist es ein Unterschied, ob er aus freien Stücken gehandelt hat, oder ob er zu seiner Handlung genötigt wurde. Dementsprechend stellt sich ebenso die Frage nach dem Motiv des Angreifers. Das gibt letzten Endes Aufschluss darüber, wer die tatsächlichen Hintermänner des Angriffes sind.

4.3. Eingrenzung der Tätergruppe

Die Tätergruppen, die heute anzutreffen sind, gab es nicht immer. In der Anfangszeit der Heimcomputer war das Hacken von Computersystemen vielmehr eine Disziplin, die nur eine sehr kleine Gruppe technisch interessierter Menschen betrieben hat. Das notwendige Fachwissen war nicht wie heute üblich von zuhause aus dem Internet abrufbar. Auch gab es zunächst keine vorgefertigten Tools, mit deren Hilfe sich selbst Laien Malware, wie aus einem Baukasten heraus, mit den gewünschten Eigenschaften und mit nur wenigen Mausklicks erstellen können (Kasperskij, 2008, vgl. Malware, 114 u. 115). Ein weiteres Beispiel sind Anwendungen zur Steuerung eines Bot-Netzes, um eine DDoS-Attacke durchzuführen. Solche und ähnliche Programme wurden erst im Laufe der Zeit entwickelt. Bis heute hat sich ein regelrechter Markt rund um entsprechende Software, digitale Identitäten und Computerressourcen entwickelt. Für nur wenige Dollar kann sich ein Interessent auf einschlägigen Märkten bereits gültige Daten einer Kreditkarte kaufen, jedoch ist auch der Erwerb eines ganzen Bot-Netzes möglich.

Folglich ist es in der Gegenwart einfacher, an die notwendigen Ressourcen heranzukommen. Die vorgefertigten Tools erlauben zudem das „Hacken“ eines fremden PCs ohne nennenswertes Fachwissen. Dadurch hat sich das Spektrum der möglichen Täter merklich erweitert.

Aus technischer Sicht bedienen sich alle Angreifer in etwa der gleichen Mittel, jedoch ergeben sich je nach Tätergruppe andere Verhaltensanweisungen für den Geschädigten und unterschiedliche Zuständigkeiten der ermittelnden Behörden. Die Betrachtung der Tätergruppen erlaubt darüber hinaus eine Risikoeinschätzung. Abhängig von der Branche steht ein Unternehmen unterschiedlichen Bedrohungen gegenüber. Ein Online-Versandhaus steht

vermehrt im Visier krimineller Organisationen, während sich ein innovatives Unternehmen der Hightech-Branche zudem gegen Industriespionage anderer Staaten und Marktbegleiter wappnen muss. Versorgungseinrichtungen sowie staatliche Infrastrukturen sehen sich dagegen im Blickfeld von Geheimdiensten und terroristischen Organisationen und können im Kriegsfall außerdem Ziel militärischer Operationen werden.

4.3.1. Hacker

In den Medien ist der Ausdruck Hacker oft negativ dargestellt. Dadurch wird das Wort in der Allgemeinheit oft als Synonym für jegliche Art Angreifer auf IT-Systeme verstanden. Im Grunde ist mit einem Hacker jedoch lediglich eine talentierte Person in einem speziellen Fachgebiet gemeint. In diesem Kontext häufig im Zusammenhang mit Informationstechnologien. Das eigentliche Ziel dieser Personengruppe ist somit in erster Linie die Spezialisierung in einem bestimmten Wissensbereich und die stetige Verbesserung der eigenen Fähigkeiten. In einigen Fällen weisen Personen dieser Gruppe demnach ein sehr hohes Fachwissen auf.

Der Hacker als solches stellt daher pr se keine Gefahr dar. Es kommt vielmehr auf die einzelne Personen an und darauf, wem und wie diese ihr Wissen zur Verfügung stellt bzw. es selbst nutzt. Als Experten auf ihrem jeweiligen Gebiet sind sie in vielen Bereichen hoch angesehen, so auch in der organisierten Kriminalität und in terroristischen Vereinigungen. Bei entsprechender krimineller Energie können sie ihr Wissen jedoch auch für eigene Zwecke missbrauchen. Zudem sind einige der Hacker in Gruppen organisiert, worauf im Punkt Politisch motivierte Angriffe noch näher eingegangen wird.

4.3.2. Jugendliche Angreifer

Hier handelt es sich vornehmlich um Einzeltäter oder kleine Gruppierungen in Form eines Freundeskreises. Tendenziell spielen bei der Motivation der Jugendlichen Sympathien zur Hackerszene eine Rolle. Das technische Know-how dieser Tätergruppe ist meist beschränkt und beruht hauptsächlich auf der Anwendung vorgefertigter Tools und verfügbarer Anleitungen. In der Hackerszene werden sie daher auch abwertend „Skript-Kiddies“ genannt. Ihr Ziel ist es, sich selbst zu beweisen und sich durch erfolgreiche Angriffe in der Szene einen Namen zu machen.

4.3.3. Insider

Insider sind ausschließlich Personen, die organisatorisch dem betroffenen Unternehmen zugeordnet werden können. Auch bei dieser Gruppe kann von einem eher geringen Fach-

wissen ausgegangen werden. Bei einem Großteil der Fälle dieser Tätergruppe handelt es sich um einmalige Vergehen mit dem Hauptziel, Fehler und unerlaubte Handlungen zu verschleiern oder um Vandalismus aus Frust gegen Kollegen und Vorgesetzte. Jedoch ist auch Mobbing eines Mitarbeiters über einen längeren Zeitraum denkbar. Ebenso ist Habgier als Motiv nicht auszuschließen. Diese kann sich auf verschiedene Weise äußern. So ist etwa die Manipulation der Bilanz zur persönlichen Bereicherung denkbar, Bestechung, oder um sich mittels internem Wissen für einen Marktbegleiter zu empfehlen.

4.3.4. Kriminelle Organisationen

Das Motiv hinter Angriffen durch kriminelle Organisationen ist ausnahmslos Geld. Ein großer Teil der Angriffe zielt daher auf Banken- und Kreditkartenbetrug. Die bevorzugten Angriffsmethoden sind der Diebstahl digitaler Identitäten mittels Phishing, entweder zur eigenen Verwendung oder zum Weiterverkauf, sowie Onlineerpressung im Zusammenhang mit einer Distributed Denial of Service Attacke oder der Infektion mit Ransomware als Druckmittel.

Anders als bei den oben genannten Tätergruppen, die vornehmlich Einzeltäter sind, erfolgt die Zusammenarbeit hier in Teams. Dadurch können grundsätzlich weitaus komplexere Angriffe durchgeführt werden als dies mit nur einer Person möglich wäre. Es ist davon auszugehen, dass genügend finanzielle Ressourcen zur Verfügung stehen, um entsprechende Experten, vor allem aus der Hackerszene, anzuheuern.

4.3.5. Politisch motivierte Angriffe

Politisch motivierte Angriffe zielen vor allem darauf, das Weltgeschehen zu Gunsten des Angreifers zu beeinflussen. Es handelt sich nicht um eine homogene Personengruppe, weshalb eine Aufspaltung in Untergruppen erfolgt, die Hauptangriffsziele sind jedoch ähnlich. Vor allem Regierungseinrichtungen, KRITIS und einflussreiche Wirtschaftsunternehmen sind durch politisch motivierte Angriffe bedroht. Die drei aus aktueller Sicht wichtigsten Gruppierungen sind nachfolgend dargestellt.

Hacker-Kollektive

Ein bekanntes Beispiel für ein solches Hacker-Kollektiv ist Anonymous. Dabei handelt es sich meist um eine Art von Jugendbewegungen, die ihre Form von Protest im Cyberspace ausüben. Ihre Aktivitäten richten sich gegen Autoritäten und Unternehmen, wenn diese Praktiken verfolgen, die mit den Ansichten des Kollektivs unvereinbar sind. Auch die Beschaffung geheimer Informationen und deren Veröffentlichung ist ein mögliches Ziel dieser

Tätergruppe. Dies ergibt sich aus dem selbsternannten Grundsatz der Hackerszene, Informationen für alle frei zugänglich zu machen. In diesem Zusammenhang wird daher oft der Begriff „Hacktivisten“ verwendet.

Diese Bewegungen folgen meist keiner inneren Struktur oder Hierarchie. Jeder kann mitmachen, wodurch es für Kriminelle ebenso möglich ist, sich dem Schutz der Anonymität eines solchen Kollektivs zu bedienen und dieses als Deckmantel zu missbrauchen. Mangels innerer Hierarchie ist zudem keine Richtung vorgegeben. Es gibt zwar einige Mitglieder, deren Wort mehr Gehör findet, jedoch ist das nicht verbindlich und kann sich schnell ändern.

Es ist nicht möglich, die Absichten eines jeden Einzelnen innerhalb einer solchen Gruppierung zu kennen. Jeder kann sich im Namen des Kollektivs grundsätzlich gegen alles einsetzen, was von ihm persönlich als ungerecht empfunden wird und um Mitstreiter werben. Eine Erlaubnis der Aktion von höherer Stelle ist nicht erforderlich, obgleich es in Einzelfällen vorkommt, dass sich die einflussreicheren Wortführer von einer Tat distanzieren. Dadurch sind solche Gruppierungen unberechenbar, wovon die größte Gefahr ausgeht.

Terroristische Organisationen

Eine allgemeingültige Definition von Terrorismus gibt es nicht. Die vielen bisher aufgestellten Definitionen werden unter den Experten verschiedener Fachbereiche auch in der Gegenwart noch stark diskutiert (Wikipedia, 2014). Die Grenze zwischen Hacker-Kollektiven und Terroristischen Gruppierungen kann fließend sein, da beide Gruppen politische Ziele verfolgen. In dieser Arbeit erfolgt die Unterscheidung daher anhand der Annahme, dass terroristische Organisationen nicht davor zurückschrecken, willentlich auch die Zivilbevölkerung zu schädigen, während Hacker-Kollektive bewusst davon Abstand nehmen.

Es ist davon auszugehen, dass zukünftig auch terroristische Organisationen versuchen werden, ihren Forderungen Nachdruck zu verleihen, indem sie staatliche Einrichtungen und KRITIS angreifen, stören oder ganz außer Betrieb setzen.

Staatliche Organisationen

Ein weiterer Teil dieser Angriffe geht auf Staaten und deren Geheimdienste zurück. Diese betreiben zum einen Wirtschaftsspionage, um die eigene wirtschaftliche und damit einhergehend auch weltpolitische Lage der Nation zu verbessern. Zum anderen wurde in den letzten Jahren die zunehmende militärische Bedeutung sichtbar, die in der Möglichkeit liegt, IT Systeme anderer Staaten anzugreifen. „Stuxnet“, ein mit hoher Wahrscheinlichkeit von westlichen Militärs entwickelter Computerwurm, wurde dazu konzipiert, das iranische Atomprogramm lahmzulegen. Daran ist deutlich zu erkennen, wie auch Staaten darauf setzen,

ihre politischen Ziele mit Hilfe der Informationstechnologie durchzusetzen. Die jüngsten Enthüllungen durch den Whistleblower Edward Snowden belegen dies zusätzlich.

4.4. Lokalisation der Angreifer

Die Herkunft eines Angreifers zu bestimmen, gestaltet sich meist schwierig. Dass ein Angriff von einem bestimmten Ort aus durchgeführt wurde, heißt nicht zwangsläufig, dass der Angreifer zur selben Zeit auch vor Ort war. Er könnte den Rechner ebenso über das Internet ferngesteuert haben. Woher die Täter stammen, ist demnach nicht eindeutig feststellbar. Durch Anonymisierungswerkzeuge wie dem TOR Netzwerk, ist eine Rückverfolgung der Angreifer schwierig.

Die meisten Attacken auf IT-Systeme laufen jedoch ohnehin automatisiert ab. Eine entsprechende Software führt in regelmäßigen Abständen Angriffe auf Rechner durch, bis ein System gefunden wurde, in welches erfolgreich eingedrungen werden kann. Ein manuelles Prüfen auf Sicherheitslücken wäre viel zu aufwendig und teuer.

Ein auf der CeBIT 2013 vorgestelltes Projekt der Deutschen Telekom veranschaulicht anhand einer Weltkarte grafisch, von wo aus die meisten Angriffe aus technischer Sicht stammen. Siehe dazu Anhang A.2. Den Ergebnissen des Projekts zufolge sind ebenso die USA, Deutschland, und die Niederlande, um nur einige wenige Beispiele zu nennen, Ausgangspunkt der meisten IT-Angriffe, nicht selten noch vor China und der Russischen Föderation.

5. Aufbau einer typischen Sicherheitslandschaft

Welche Sicherheitsmaßnahmen ein Unternehmen für sich einrichtet, ist von verschiedenen Faktoren abhängig. Zum einen spielt die Unternehmensgröße und die Anzahl der Beschäftigten eine wichtige Rolle. Größere Firmen mit mehr Arbeitsplatzrechnern sind grundsätzlich besser abgesichert als beispielsweise kleinere Handwerksbetriebe. Das hat nicht zuletzt den Grund, dass der Handwerker, in aller Regel Laie in Bezug auf die IT, selbst für seinen Bürorechner verantwortlich ist und diesen auch in puncto Sicherheit eigenständig verwaltet. In größeren Unternehmen hingegen übernimmt in den meisten Fällen ein eigens dafür berufener Administrator oder externer Dienstleister diese Aufgabe, was die Qualität der Sicherheit in diesen Betrieben deutlich erhöht.

Zum anderen ist die Vertraulichkeit der Daten für die Wahl der eingesetzten Sicherheitsmechanismen ein entscheidender Aspekt. Zwar sind Kundendaten, wie sie jeder Handwerksbetrieb verwaltet, nicht weniger schützenswert als ein geheimes Fertigungsverfahren, jedoch sind sie trotzdem nicht in jedem Fall der zentrale Angriffsgrund. Vielmehr steht das geistige Eigentum im Fokus gezielter Hackerangriffe. Der Ideenreichtum, welcher eine jeweils spezifische Position am Weltmarkt sichert und von den Marktbegleitern differenziert, hat einen wesentlich höheren Marktwert als der Kundenstamm solcher Unternehmen. Dennoch ist auch der Schutz dieser Daten nach wie vor ausbaufähig.

Ein weiterer zentraler Punkt für den Einsatz spezifischer Sicherheitsmechanismen ist die Architektur der vorherrschenden IT-Landschaft eines Unternehmens. Unterhält eine Firma eigene Server lokal vor Ort, entstehen ganz andere Anforderungen an deren Sicherheit, als wenn die Daten in einer Cloud von einem externen Dienstleister verwaltet werden. Im ersten Fall ist das Unternehmen selbst für die Sicherheit seiner gesamten Systeme verantwortlich, im zweiten Fall werden einige dieser Aufgaben an den Dienstleister übertragen.

5.1. Gängige Sicherheitsvorkehrungen in Firmen

Aus der Vielfalt der Unternehmensstrukturen folgt: Die typische Sicherheitslandschaft lässt sich nicht ohne weiteres beschreiben, da es für jeden Anwendungsfall spezifische Anforderungen zu berücksichtigen gibt. Des Weiteren ist nicht jede Maßnahme für jedes Unternehmen gleichermaßen rentabel und wirtschaftlich tragbar. Soweit Informationen dazu vorliegen, werden einige Sicherheitskonzepte anhand des Klinikum Augsburg (KA) als Beispiel näher erläutert.

5.1.1. Sicherheitspolicen

Die ausgefeiltesten Maßnahmen helfen nichts, wenn sich die eigenen Mitarbeiter nicht an sie halten. Darum sind verbindliche Sicherheitsrichtlinien für alle Mitarbeiter unumgänglich. Diese regeln beispielsweise, ob die private Nutzung des Internets gestattet ist, dass beim Verlassen des Arbeitsplatzes der eigene PC gesperrt werden muss, oder ob es erlaubt ist, eigene Software auf dem Bürorechner zu installieren. Solche Sicherheitspolicen finden in nahezu jedem Unternehmen Anwendung. Diese müssen jedoch auch regelmäßig an die aktuellen Gegebenheiten angepasst werden. Des Weiteren reicht deren alleinige Überarbeitung nicht aus. Die Mitarbeiter müssen zudem über die veränderten Richtlinien informiert werden.

Das KA verwendet hier eine softwaregestützte Lösung. Der Verfasser einer Sicherheitspolice wird in regelmäßigen Abständen auf deren Überarbeitung aufmerksam gemacht. Die Richtlinien lassen sich dabei in zwei Arten unterscheiden. Kenntnisnahmepflichtige Dokumente und solche, die nicht zur Kenntnis genommen werden müssen. Bei ersteren werden nach vollzogener Aktualisierung alle Mitarbeiter per E-Mail auf die veränderte Situation aufmerksam gemacht. Im Anschluss daran registriert die Software über die Benutzerkennung, welcher Mitarbeiter die neue Richtlinie bereits gelesen hat.

5.1.2. Verwendung externer Datenträger

Externe Datenträger stellen eines der größten Sicherheitsrisiken in Unternehmen dar. Wie im Punkt Infektion mit Malware erwähnt, sind sie ein beliebtes Medium zum Datenaustausch. Sie sind in der Beschaffung günstig, jedoch vor allem ein beliebtes Werbegeschenk. Einen USB-Stick als solches an Mitarbeiter zu verteilen, stellt demnach keine besonders auffällige Aktion dar. Die Angreifer müssen lediglich warten, bis einer der Mitarbeiter den Stick an seinem Arbeitsrechner verwendet und dadurch den Schadcode aktiviert. Die kompakte Größe erlaubt zudem den unauffälligen Transport in das Firmengebäude. Die häufig an der Gehäusefront eines PC angebrachte USB-Schnittstelle erleichtert den Zugang zu dieser nicht nur für Mitarbeiter. Ein kurzer, unbeobachteter Moment reicht so für den Angreifer aus, den Datenträger auch selbst an einem System anzubringen.

Abhängig von der Art des Codes ist es dem Angreifer möglich, sich Zugang zum betroffenen System zu verschaffen, Daten nach draußen zu senden oder weitere IT-Systeme zu befallen. Externe Datenträger unbekannter Herkunft sollten demnach nicht oder nur mit hoher Vorsicht zum Einsatz kommen.

Im KA ist die Verwendung externer Datenträger eine besondere Herausforderung. Einerseits ist der Gebrauch von externen Datenträgern, die nicht vom Bereich Medizinisch/Klinische Kommunikation, Informatik und DV-Technik (MIT) herausgegeben wurden, nicht gestattet.

Andererseits sieht sich das KA mit Datenträgern anderer Arztpraxen und Kliniken konfrontiert, die wichtige und für die weitere Behandlung eines Patienten notwendige Daten enthalten. Zwar werden diese Datenträger eingehend vom zuständigen Personal und durch die eingesetzte Antivirensoftware überprüft, einen absoluten Schutz gibt es dennoch nicht. Folglich existiert hier eine Sicherheitslücke, die jedoch zum jetzigen Zeitpunkt aus organisatorischer Sicht nicht schließbar ist. Jedes Unternehmen muss demnach gegebenenfalls Risiken und Nutzen der jeweiligen Verfahrensweise abwägen, um das Höchstmaß an möglicher Sicherheit zu gewährleisten.

5.1.3. Einsatz von Firewalls

Unverzichtbar zur Absicherung der firmeneigenen EDV ist eine Firewall. Nach aktuellem Stand sind diese in nahezu jeder Unternehmensstruktur anzutreffen. Nicht zuletzt deshalb, da bereits die meisten handelsüblichen Router für den privaten Gebrauch, den die Internet Service Provider (ISP) zur Verfügung stellen, eine solche fest integriert hat. Somit sind auch Kleinstunternehmen durch Firewalls geschützt. Auch moderne Betriebssysteme bieten Softwaretechnisch einen - wenn auch rudimentären - Schutz, wie die Windows Firewall.

5.1.4. Antiviren Software

Nicht weniger zu vernachlässigen ist eine Antiviren-Software auf jedem Arbeitsrechner. Diese spürt nicht nur schadhaften Code auf den Clients auf, sondern verhindern zugleich auch den Befall von außerhalb. Einige ISP bieten ihren Kunden bereits seit einiger Zeit als zusätzliche Dienstleistung Sicherheitspakete, bestehend aus Software-Firewall und Antivirenprogramm, an.

Somit setzt auch das KA eine entsprechende Software zur Abwehr von schadhaftem Code ein. Diese ist auf jedem Client installiert und prüft zum einen neue Dateien auf bekannte Signaturen. Zum anderen wird der Rechner in regelmäßigen Abständen einer Systemprüfung unterzogen. Das bedeutet, dass alle Dateien auf den Datenträgern nach schädlichem Inhalt überprüft werden.

Alleine das Vorhandensein eines Virenscanners reicht jedoch nicht aus. Da heute pro Tag hunderte neue schadhafte Programme entdeckt werden, müssen auch die Virendefinitionen regelmäßig aktualisiert werden. Der Virenschutz kann sonst nicht auf aktuelle Bedrohungen reagieren, da er diese nicht kennt.

5.1.5. Regelmäßige Updates

Wie schon zuvor bei den Virendefinitionen erwähnt, so muss auch die Software als solches regelmäßig aktualisiert werden. Vor allem bei Anwendungen mit Zugriff auf Inhalte des Internets sind diese zwingend erforderlich, werden jedoch allzu gerne aufgeschoben. Bei der Häufigkeit, mit der Updates erscheinen, ist es in der Praxis jedoch nicht immer möglich, Updates sofort auf allen Arbeitsplatzrechnern bereitzustellen. Neben Fehlerbehebungen und Verbesserungen der Bedienbarkeit werden häufig auch Sicherheitslücken von Updates geschlossen, die Angreifern den Zugang auf ein fremdes System erst ermöglichen würden.

5.1.6. Restriktiver Zutritt

Nicht jeder Mitarbeiter braucht Zugang zu allen Bereichen. Selbst in kleineren Unternehmen muss nicht jeder Angestellte Zutritt zum Serverraum haben. Dies ist weniger eine Frage des Vertrauens an die eigenen Mitarbeiter, sondern vielmehr an die Besucher. Häufig sind Gäste, Kunden oder externe Dienstleister im Haus. Darum muss niemand unter Generalverdacht gestellt werden. Trotzdem erspart es viele Unannehmlichkeiten, wenn nicht jeder Besucher des Hauses überwacht werden muss, weil grundsätzlich die Möglichkeit besteht, dass er in Bereiche eintreten könnte, zu denen er keinen Zugang haben sollte. Zutrittskontrollen erhöhen demnach nicht nur die eigene Sicherheit, sie ermöglichen auch einen entspannten Umgang mit Besuchern.

Doch ist nicht nur eine Absicherung der örtlichen Gegebenheiten geboten, sondern auch eine Zugangsbeschränkung auf die IT selbst. Nicht jedem Mitarbeiter sollte Einsicht in interne Dokumente über Netzwerkfreigaben gewährt werden. Um das zu realisieren, ist ein Benutzer-Rollen Konzept erforderlich. Zum eigenen Schutz sollte zudem jeder PC mit einem Passwort versehen sein, welches in seiner Länge und den zu verwendenden Zeichen - Klein- und Großbuchstaben, Sonderzeichen und Ziffern - gewissen Mindestanforderungen entspricht. Siehe dazu Passwörter auf Seite 6.

Das KA verwendet zwei verschiedene Benutzerverwaltungen. Zum einen den in Windows integrierten Domaincontroller. Dieser greift bei der Anmeldung am PC für die Mitarbeiter aller Abteilungen. Zusätzlich bietet das Krankenhaus Informationssystem (KIS) noch eine weitere Benutzerverwaltung, die jedoch nur das medizinische Personal einbezieht. So hat ein Mitarbeiter der Personalabteilung zwar Zugriff auf seinen Arbeitsrechner, nicht jedoch auf patientenbezogene Daten über das KIS. Aus datenschutzrechtlichen Gründen darf zudem nicht jede Rolle Zugriff auf alle Daten eines Patienten erhalten, sondern nur auf die, welche für die Ausübung der Tätigkeit relevant sind. So kann ein Mitarbeiter an der Information zwar Auskunft darüber geben, in welchem Zimmer ein Patient liegt, er hat jedoch keinen Einblick auf die gestellten Diagnosen.

5.1.7. Logische Trennung von Intranet und Internet

Im KA ist das Intranet logisch von außen getrennt. Die Clients selbst haben keinen direkten Zugang zum Internet. Eine Verbindung nach draußen ist nur über eine virtuelle Umgebung möglich. Dazu existiert ein eigener Server. Ausschließlich dieser kann Verbindungen zum Internet herstellen. Will ein Client externe Informationen abrufen, so muss er zunächst eine virtuelle Umgebung auf dem Server starten. Nur aus dieser heraus kann er an die gewünschten Informationen gelangen. Die Verbindung zum Server ist dabei verschlüsselt. Ein Angreifer von außen greift somit nur die virtuelle Umgebung an und nicht den dahinter liegenden physikalischen Client. Dadurch besteht erst einmal weder Zugang zu den Daten, welche auf dem Client gespeichert sind, noch auf das Intranet.

5.1.8. Wartungsarbeiten durch externe Dienstleister

Sind Wartungsarbeiten durchzuführen, die keinen direkten Eingriff in die Hardware erfordern, so werden diese häufig von außerhalb durchgeführt. Das ist deutlich effizienter, da kein Servicemitarbeiter vor Ort erscheinen muss. Der Zugriff von außerhalb erfolgt dabei mittels VPN-Tunnel.

Im KA unterliegen die Softwaresysteme einer regelmäßigen Wartung. Die externen Dienstleister haben jedoch nicht beliebig Zugriff von außerhalb auf die Infrastruktur. Um den Zugang zu Wartungsarbeiten zu ermöglichen, wird der VPN-Tunnel erst von einem Mitarbeiter des MIT geöffnet. Der Tunnel selbst ist dabei nur für eine begrenzte Zeit offen.

5.1.9. Internetzugang für Gäste

Gerade mittelständische und größere Unternehmen haben häufig für einen längeren Zeitraum Besucher im Haus. Sei es, weil längere Gespräche mit wichtigen Geschäftspartnern anstehen oder weil sie neben dem eigentlichen Produkt als zusätzliche Dienstleistung Schulungen für ihre Kunden anbieten. Daraus ergibt sich häufig die Notwendigkeit, den Gästen für die Dauer ihres Aufenthaltes Zugang zum Internet zu gewähren. Dabei ist es jedoch wenig empfehlenswert, die Zugangsdaten für das Hausinterne WLAN herauszugeben. Die Gefahr, dass ein angeblicher Kunde etwas ganz anderes im Sinn hat, als seinem Tagesgeschäft nachzukommen, ist viel zu groß. Es empfiehlt sich daher, ein eigenes, extra für diesen Zweck eingerichtetes WLAN bereitzustellen. Dieses darf keine logische Verbindung zum hausinternen Netzwerk haben.

So ist dies auch im KA gelöst. Um Besuchern und Patienten den Aufenthalt angenehmer zu gestalten, bietet das Klinikum einen WLAN-Zugang an. Diesen kann jeder Gast nach Belieben nutzen. Dabei handelt es sich jedoch um ein eigenständiges Netz, welches in

keiner Verbindung zum Intranet des KA steht. Somit ist gewährleistet, dass sich niemand von außerhalb unbefugt Zugang zu sensiblen Daten verschaffen oder das Intranet in irgendeiner Weise infiltrieren kann.

6. Aktuelle Gegebenheiten

Dieses Kapitel soll die aktuellen Statistiken zu Cybervorfällen in der BRD näher betrachten. Das Augenmerk liegt dabei sowohl auf den Fallzahlen der Angriffe im zeitlichen Verlauf, als auch auf den Erfahrungen verschiedener Branchen mit sicherheitskritischen Vorfällen. Ebenso ist die momentane Schadensbilanz von Interesse.

6.1. Fallzahlen in der BRD

Laut dem Bundeslagebild des BKA aus dem Jahre 2012 hat sich die Zahl der unter Cybercrime fallenden Delikte von 2008 bis 2012 stark erhöht. Während sich jedoch zwischen 2008 und 2010 noch ein deutlicher Anstieg zum Vorjahr beobachten lässt, fällt dieser seit 2010 sichtlich flacher aus. Mit 63.959 Fällen pro Jahr erreichte die Anzahl der registrierten Cybervergehen 2012 ihren neuen Höchststand (Bundeskriminalamt, 2012a, Lagebild, 3). Der Großteil aller Vergehen fällt dabei mit rund 40 % auf Computerbetrug, gefolgt von Datenspionage (26,3 %) und Datenveränderung (17 %). Die Fälschung beweiserheblicher Daten schlägt mit noch rund 13,4 % zu Buche und schlussendlich der Betrug durch Identitätsdiebstahl mit 4,6 %.

Es ist jedoch von einer großen Dunkelziffer nicht zur Anzeige gebrachter Angriffe auszugehen. In einer Studie der IHK Nord aus dem Jahre 2013 wollten 28,9 % der Befragten keine Angaben über ihren Umgang mit Cybervorfällen innerhalb der letzten 12 Monate machen. Mehr als die Hälfte - 57,8 % - gab an, keinen der Vorfälle der letzten 12 Monate angezeigt zu haben, 4,4 % haben weniger als die Hälfte zur Anzeige gebracht und nur 2,9 % mehr als 50 % der Vorfälle. Lediglich 5,9 % haben alle Angriffe an die Behörden weitergeleitet (IHK Nord, 2013, Umfrageauswertung, 10).

Zudem zeigt die Studie auf, dass 54,4 % der befragten Unternehmen den Arbeitsaufwand für eine Anzeige zu groß sähen. Etwa ein Drittel, 30,1 %, zweifelten gar am Erfolg der Ermittlungen und 22,1 % gaben an, nicht zu wissen, an wen sie sich wenden müssten. Etwa 5 % der Unternehmen befürchte gar einen Imageschaden und immerhin gut jedes vierte sogar eine starke Beeinträchtigung des laufenden Betriebes durch die Ermittlungen (IHK Nord, 2013, Umfrageauswertung, 11). Zwar bezieht sich diese Erhebung ausschließlich auf den norddeutschen Raum, dennoch ist davon auszugehen, dass dieses Bild zumindest in Teilen die Gesamtsituation in der BRD widerspiegelt.

6.2. Cybervorfälle im Branchenvergleich

Eine Studie im Auftrag des BMWi zum IT Sicherheitsniveau aus dem Jahr 2012 stellte unter anderem die Erfahrungen verschiedener Branchen mit kritischen Vorfällen dar. Befragt wurden Finanz- und Versicherungsdienstleister, Gastgewerbe, Gesundheits- und Sozialwesen, Wirtschaftsprüfer, Steuerberater, Rechtsanwälte, Ingenieure (WP, StB, RA, Ing.), sowie Handwerksbetriebe (Franz Büllingen und Annette Hillebrand , 2012, IT-Sicherheitsniveau im Branchenvergleich, 55).

6.2.1. Systemausfälle

Branchenübergreifend gaben rund 79 % der befragten Unternehmen an, mit Ausfällen der IT konfrontiert zu sein. Obgleich hier alle Geschäftszweige hohe Erfahrungswerte verzeichnen, liegen Betriebe der Branchen WP, StB, RA, Ing., sowie Handwerksbetriebe 5 bis 10 % über den Erfahrungswerten der anderen Branchen.

Auffällig ist, dass sich das Gastgewerbe in den meisten Punkten zum Teil deutlich von den anderen Branchen unterscheidet. Bei den Systemausfällen liegen Gastronomiebetriebe 10 % unter dem Durchschnitt.

6.2.2. Infektionen mit Schadsoftware

Deutlich geringer scheinen die Erfahrungen der Unternehmen mit Malware. Nur etwa die Hälfte aller Befragten gab an, schon einmal mit Schadsoftware konfrontiert worden zu sein. Auch hier heben sich die Branchen WP, StB, RA, Ing. mit 63,4 % und Handwerk mit 73 % deutlich von den anderen Sektoren und dem Durchschnitt ab.

Ebenso die Gastronomiebetriebe, die mit 46,8 % von weniger Erfahrung mit Schadsoftware berichten, und damit etwa 5 % unter dem Durchschnitt liegen.

6.2.3. Spam Mails

Ebenfalls knapp die Hälfte, 47 % aller Unternehmen, hat Erfahrungen mit Spam. Das Gesundheitswesen sticht hier mit einem besonders hohen Erfahrungswert heraus. Dieser liegt mit 60 % deutlich über dem Durchschnitt.

Mit 38,3 % signifikant unter dem Durchschnitt liegt abermals das Gastgewerbe.

6.2.4. Versehentliches Verändern von Daten und Datenverlust

Gut 40 % der Betriebe aller Branchen hat mit fahrlässigen, destruktiven Dateioperationen Erfahrung. Erneut liegen WP, StB, RA, Ing. und Handwerksbetriebe knapp 10 % über dem Durchschnitt, während die Gastronomie mit 27,7 % von weit weniger Vorfällen zu berichten weiß.

6.3. Wie hoch ist der jährlich entstehende Schaden

Derzeit scheinen die verursachten Schäden durch Cybercrime rückläufig. Erreichten diese 2010 61,5 Mrd. Euro und 2011 mit 71,2 Mrd. Euro ihren bisherigen Höchststand, so lag der entstandene Schaden 2012 bei 42,5 Mrd. Euro (Bundeskriminalamt, 2012a, Lagebild, 4). Doch können diese Zahlen auch täuschen. Wie bereits erwähnt, gibt es eine unbekannte Größe nicht angezeigter Vorkommnisse von Cybercrime, welche dieses Bild etwas verzerren. Dennoch ist davon auszugehen, dass die stetige Sensibilisierung der Bürger und Unternehmen durch staatliche Behörden und Sicherheitsunternehmen dazu beigetragen hat, die Situation zu verbessern. Die Gefahren gerade von Phishing und E-Mails unbekannter Herkunft sind nun weitestgehend bekannt.

6.4. Fazit zu den Fallzahlen

Insgesamt betrachtet ist es wenig überraschend, dass alle Branchen in ähnlicher Weise den gleichen Bedrohungen ausgesetzt sind. Auffällig ist, dass die Zweige WP, StB, RA, Ing. und Handwerk fast ausnahmslos deutlich stärker betroffen sind, während das Gastgewerbe scheinbar mit signifikant weniger sicherheitskritischen Vorfällen konfrontiert ist.

Bei diesen drei Branchen handelt es sich in vielen Fällen um Klein- und Kleinstbetriebe, die ihre IT in Eigenregie verwalten, ohne dafür über das notwendige Fachwissen zu verfügen. Dass das Gastgewerbe hierbei mit deutlich weniger Vorfällen konfrontiert wird, lässt darauf schließen, dass im Gastbetrieb, Hotels wie auch kleinen Gaststätten, IT eine untergeordnete Rolle spielt bzw. anders zum Einsatz kommt als in den anderen Branchen.

Im Gesundheits- und Sozialwesen gestaltet sich die Struktur ähnlich wie im Gastgewerbe. Auch hier gibt es viele Kleinstbetriebe wie Ärzte und größere Organisationen wie Krankenkassen und Krankenhäuser. Da Arztpraxen ihrer Größe wegen in der Regel ebenso keinen eigenen Sachverständigen vor Ort haben, sind auch diese für die Sicherheit ihrer IT selbst verantwortlich. Weil in Arztpraxen Computer eine weitaus größere Rolle spielen als im Gastgewerbe, wären faktisch deutlich höhere Erfahrungswerte mit sicherheitskritischen Vorfällen

zu erwarten, die denen im Handwerk ähneln. Medizin-technische Produkte unterliegen jedoch nach dem Medizinproduktgesetz (MPG) deutlich strengeren Anforderungen als Systeme anderer Branchen und sind dadurch merklich besser vor Angreifern geschützt. Dies wirkt sich positiv auf die Statistik aus. Zum anderen entfällt auf die großen Organisationen der Gesundheitsbranche eine deutlich umfangreichere IT, da diese einen höheren Verwaltungsaufwand haben. Dies wirkt sich wiederum in einem Plus auf die Erfahrungswerte mit sicherheitskritischen Vorfällen aus.

Die Branche der Finanzdienstleister ist von Natur aus mit einer relativ hohen Anzahl von Angriffen konfrontiert, da die Angreifer hier entsprechend viel Geld wittern. An diese Situation angepasst fallen jedoch auch die Sicherheitsmaßnahmen des Finanzsektors aus, wodurch keine signifikanten Abweichungen von Durchschnitt zu beobachten sind.

Dass die jährlich verursachten Schäden geringer ausfallen, ist zwar zunächst erfreulich, Grund zur Entspannung ist dies jedoch nicht. Es ist nur eine Frage der Zeit, bis sich findige Köpfe neue Angriffsstrategien ausgedacht haben, auf die es die breite Masse abermals zu sensibilisieren gilt. Es kann davon ausgegangen werden, dass bei Auftreten neuer, unbekannter Gefahren auch der jährlich verursachte Schaden wieder zunehmen wird.

Die Zahlen aus der Studie der IHK Nord sprechen eine deutliche Sprache. Dass 22 % der befragten Unternehmen angeben nicht zu wissen, an wen sie sich nach einem Angriff wenden sollen, zeigt die Notwendigkeit eines Leitfadens, wie er in dieser Arbeit entwickelt werden soll. Dass allerdings rund 30 % den Erfolg der Ermittlungen anzweifeln, und etwas mehr als die Hälfte den Aufwand für eine Anzeige zu groß sehen, zeigt deutlichen Handlungsbedarf, nicht nur von Seiten der Unternehmen, worauf jedoch im Schlussteil auf Seite 54 noch ausführlicher eingegangen wird.

7. Leitfaden für das Vorgehen nach einem Angriff

In diesem Kapitel soll aufgezeigt werden, welche Behörden nach einem Cyberangriff kontaktiert werden können und sogar müssen. Zur Beschreibung des weiteren Vorgehens nach einem Cyberangriff wird davon ausgegangen, dass das betroffene Unternehmen daran interessiert ist, mit den Bundesbehörden zu kooperieren. Es ist nicht ratsam, auf eigene Faust oder ausschließlich unter Zuhilfenahme privater Dienstleister den Tathergang zu ermitteln, oder ihn ganz unter den Tisch fallen zu lassen.

Die Zusammenarbeit mit den Bundesbehörden ist von entscheidender Bedeutung. Nur dadurch können genaue Fallzahlen erfasst werden. Mit Hilfe derer ist es zum einen möglich, eine exakte Abschätzung der Sicherheitslage durchzuführen, und zum anderen können dadurch die richtigen Entscheidungen im Hinblick auf Prävention und geeigneter Abwehrmechanismen getroffen werden.

Darüber hinaus werden einige grundlegende Verhaltensempfehlungen genannt. Zusätzlich findet sich im Anhang A.3 eine Checkliste mit den wichtigsten Fragen, um vor der Kontaktaufnahme mit den Behörden bereits die notwendigsten Informationen zu sammeln.

7.1. Erkennen eines Angriffes

Ein wichtiger Punkt für das weitere Vorgehen ist, zu erkennen, dass ein Angriff stattgefunden hat. Im Gegensatz zu einer DDoS Attacke, oder bei dem Befall des Rechners mit Ransomware, sind die Auswirkungen nicht in jedem Fall offensichtlich. Zielt der Angriff nicht auf schnelles Geld, sondern auf Informationen, möchten die Angreifer die gewünschten Daten nachhaltig abgreifen können. Dazu müssen sie ihr Eindringen und ihren Aufenthalt im System tarnen und unkenntlich machen. Zur Datenspionage kommen daher überwiegend Trojaner zum Einsatz, die entsprechende Eigenschaften zur Tarnung besitzen. So kann es oft Monate oder Jahre dauern, bis die Schädlinge erkannt werden.

Datenübertragungen an unerwartete und ungewöhnliche Ziele können ein Indiz dafür sein, dass unautorisiert Daten versendet werden. Bei der Menge der anfallenden Datenübertragungen, können solch einzelne Meldungen in der Masse jedoch leicht untergehen. Anhand der Vielzahl der verschiedenen Unternehmensstrukturen und der Konfigurationsmöglichkeiten einer IT-Landschaft kann eine Aufzählung möglicher Anzeichen für einen Angriff nur in einem theoretischen Rahmen erfolgen. Weil die Thematik der Computerforensik dazu sehr komplex ist, können an dieser Stelle auch nur einige Beispiele genannt werden.

Mögliche Indizien für einen Eindringling im System sind:

- Unstimmigkeiten in den Logdateien.
- Aktivitäten zu ungewöhnliche Zeiten.
- Hohe Anzahl fehlgeschlagener Authentifizierungen.
- Auffallend hohe Zahl übertragener Daten.
- Laufende Dienste unbekannter Herkunft.
- Auslastung von Ressourcen ohne erkennbaren Grund.

7.2. Sofortmaßnahmen

Wurde ein Angriff festgestellt, ist es wichtig, erst einmal Ruhe zu bewahren. Nur wenige Mitarbeiter sollten über die Details des erfolgten Angriffs informiert werden. Sie kennen einen Notfallplan und leiten die entsprechenden Schritte ein. Da bei einem internen Angriff auch die Möglichkeit besteht, dass sich der Täter in dem Personenkreis der Sicherheitsverantwortlichen befindet, dürfen hier keine Alleingänge passieren. Jeder Eingriff in die IT muss von mindestens einer weiteren Person überwacht werden.

Liegt ein interner Angriff vor, muss davon ausgegangen werden, dass der Täter noch im Haus ist. Dadurch besteht die Gefahr weiterer Attacken und die damit einhergehende Vernichtung wertvoller Beweismaterialien. Die Belegschaft darf deshalb die betroffene EDV nicht mehr benutzen und sollte auf weitere Anweisungen warten. Soweit die Arbeit ohne PC erledigt werden kann, können diese Tätigkeiten fortgesetzt werden.

Kann mit Sicherheit davon ausgegangen werden, dass der Angriff von außerhalb erfolgt ist, sind die eigenen Mitarbeiter zunächst einmal entlastet. Wenngleich auch Teile der Belegschaft zu einer gewissen Wahrscheinlichkeit mitverantwortlich für den Angriff sein könnten, ist diese Gefahr eher gering zu bewerten.

In beiden Fällen ist es ratsam, die betroffenen Systeme zumindest teilweise stillzulegen, um ein Ausbreiten eventuell eingeschleuster Schadsoftware auf die noch intakten Systeme zu vermeiden. Da die Lokalisation eines Angriffs jedoch einige Zeit in Anspruch nehmen kann, muss über Kosten und Nutzen der Abschaltung im Einzelfall abgewogen werden. Sind noch Datenübertragungen von den befallenen Geräten aus festzustellen, sind diese umgehend zu unterbinden. Handelt es sich dabei um personenbezogene Daten, ist dies laut § 42a BDSG, siehe Punkt 3.2.2, sogar gesetzlich vorgeschrieben. Außer diesen Schritten dürfen an den betroffenen Systemen keine weiteren Veränderungen mehr vorgenommen werden, um nicht

versehentlich wertvolles Beweismaterial zu vernichten. Im Zweifelsfall die Stromzufuhr zu den betroffenen Geräten unterbrechen. Dadurch gehen zwar flüchtige Daten verloren, die Daten, die auf der Festplatte gespeichert waren, bleiben jedoch erhalten und können wiederhergestellt werden. Die angegriffenen Systeme dürfen nur noch von fachkundigem Personal oder unter Anleitung eines Sachverständigen bedient werden.

Übersicht der Sofortmaßnahmen:

- Sicherheits-Taskforce aktivieren.
- Die Arbeiten an den betroffenen Geräten einstellen.
- Noch aktive Datenübertragungen abbrechen.
- Sind personenbezogene Daten durch den Angriff betroffen, umgehend Maßnahmen zu deren Schutz ergreifen.
- Das betroffene Gerät vom Netzwerk trennen, um eine Ausweitung des Vorfalls zu verhindern.
- Bei einem internen Angriff ist sicherzustellen, dass kein unbefugter an die betroffene IT herankommt.
- Keine Änderungen am System mehr vornehmen.
- Im Zweifelsfall die Stromzufuhr unterbrechen.

7.3. Meldung des Vorfalls an die Behörden

Ein sicherheitskritischer Vorfall muss an die Behörden gemeldet werden. Wie bereits erwähnt, benötigen die zuständigen Stellen verlässliche Fallzahlen, um daraus ihr weiteres Handeln ableiten zu können. Die Meldung erfolgt dabei unter zwei verschiedenen Aspekten. Der Anzeige des Vorfalles an eine ermittelnde Stelle mit dem Ziel des Strafvollzugs, sowie der Anzeige von Verstößen des Datenschutzes an die Aufsichtsbehörden zum Schutz der Betroffenen.

7.3.1. Wichtige Fragen vorab klären

Wie im Allgemeinen üblich, sind auch bei der Anzeige von sicherheitskritischen Vorfällen die bekannten W-Fragen zu beantworten. Sie helfen den Behörden, Art und Umfang des Vorfalls im Voraus abschätzen zu können, um sogleich eine Entscheidung über das weitere

Vorgehen treffen zu können. Über diese Fragen hinaus findet sich im Anhang A.3 noch eine Checkliste mit zusätzlich benötigten Informationen, die für die Ermittler im weiteren Verlauf der Aufklärung von Bedeutung sein können.

Die folgenden Fragen sind für den Erstkontakt mit den Behörden wichtig und sollten bereits vor der Kontaktaufnahme bereitgestellt werden.

- Was ist geschehen?
- Wann passierte der Vorfall?
- Wie konnte der Angreifer vorgehen?
- Welche Systeme sind betroffen?
- Warum wurde das System angegriffen: Mögliches Motiv?
- Was passierte nach dem Angriff?
- Wo wird der Täter vermutet?
- Welche Schäden sind entstanden?
- Sind Spuren vorhanden oder wurden bereits welche verwischt?

(Prof. Dr. Gordon Rohrmair, 2013, Anwendungen der IT-Sicherheit 2, 12)

7.3.2. Anzeige des Vorfalls bei einer ermittelnden Stelle

Da die Identität der Täter eines Cybervorfalles oft nicht auf Anhieb mit Sicherheit bestimmt werden kann, ist auch nicht ersichtlich, ob es sich bei dem Vorfall um eine Straftat handelt oder um eine nachrichtendienstliche Tätigkeit. Darum bleibt zunächst einmal offen, wer für die Aufklärung des Vorfalls zuständig ist.

1. Direkte Anzeige des Vergehens bei der Polizei.
2. Meldung des Vorfalls an das CAZ.
3. Beauftragung eines privaten Unternehmens, in Kooperation mit der Polizei oder dem CAZ.

Da der Großteil der Angriffe von organisierten Banden durchgeführt wird, sind in den meisten Fällen die Polizeien die richtigen Ansprechpartner. Diese sind jedoch in zweierlei Hin-

sicht gezwungen, ein Ermittlungsverfahren einzuleiten. Zum einen unterliegen sie dem Legalitätsprinzip, wodurch sie gesetzlich dazu verpflichtet sind, den Vorfall zu ermitteln. Zum anderen müssen die Ermittlungsbehörden, um in dem Fall handlungsfähig zu bleiben, ein Ermittlungsverfahren eröffnen. Ein laufendes Verfahren auf Dauer vor der Öffentlichkeit zu verbergen ist jedoch kaum möglich. Aus Gründen der Vertraulichkeit ist es einigen Unternehmen daher lieber, einen diskreteren Weg einzuschlagen.

Den bietet an dieser Stelle das CAZ, als Teil des LfV. Im Rahmen der Abwehr von Wirtschaftsspionage ist es die Aufgabe des LfV, Bedrohungen auf IT Anlagen präventiv und defensiv entgegenzuwirken. Firmen können das CAZ Bayern direkt kontaktieren. Ein Einschalten der Ermittlungsbehörden erfolgt nur in enger Kooperation mit dem LfV und nur mit dem Einverständnis des betroffenen Unternehmens. Der Vorteil davon ist, dass die Unternehmen sich nicht gezwungenermaßen in der Situation sehen, ein Ermittlungsverfahren einleiten zu müssen, was für einige Unternehmen eine eher abschreckende Wirkung hat.

Neben den staatlichen Behörden hat sich zusätzlich eine Zahl privater Unternehmen auf den Sektor der Computerforensik spezialisiert. Diese agieren als Detekteien in beratender sowie ermittelnder Funktion hauptsächlich für Unternehmen. Aufgrund des hohen technologischen Know-hows solcher Firmen, das nach aktuellem Stand jenes staatlicher Behörden teilweise übersteigt, werden diese auch von den Polizeien konsultiert. Grundsätzlich spricht nichts dagegen, einen Vorfall von einem privaten Unternehmen untersuchen zu lassen. Er sollte jedoch zwecks Datenerhebung auch an das CAZ gemeldet werden.

7.3.3. Meldung von Datenschutzverstößen

Bei Verstößen gegen das Bundesdatenschutzgesetz ist das weitere Vorgehen von der Art des Unternehmens abhängig.

Nicht öffentliche Einrichtungen nach § 2 Abs. 4 BDSG müssen zuerst Maßnahmen ergreifen, welche der Sicherung und dem Schutz der Daten dienen. Gegebenenfalls hat auch eine Meldung an den Softwarehersteller zu erfolgen, damit dieser seinerseits die verursachenden Sicherheitslücken beheben kann, um weitere Schäden abzuwenden. Im Anschluss muss der Vorfall an das jeweilige LDA gemeldet werden. Soweit es die Umstände erlauben und die laufenden Ermittlungen dadurch nicht gefährdet sind, müssen ebenso die betroffenen Personen über den Verlust ihrer Daten informiert werden. Ist davon auszugehen, dass der Vorfall wegen seiner besonderen Tragweite in der Presse erscheint, kann es sinnvoll sein, die Betroffenen erst später zu benachrichtigen. Die Täter könnten sonst dadurch ungewollt alarmiert werden und ihrerseits wichtige Beweise vernichten. Die Entscheidung darüber obliegt jedoch den Ermittlungsbehörden.

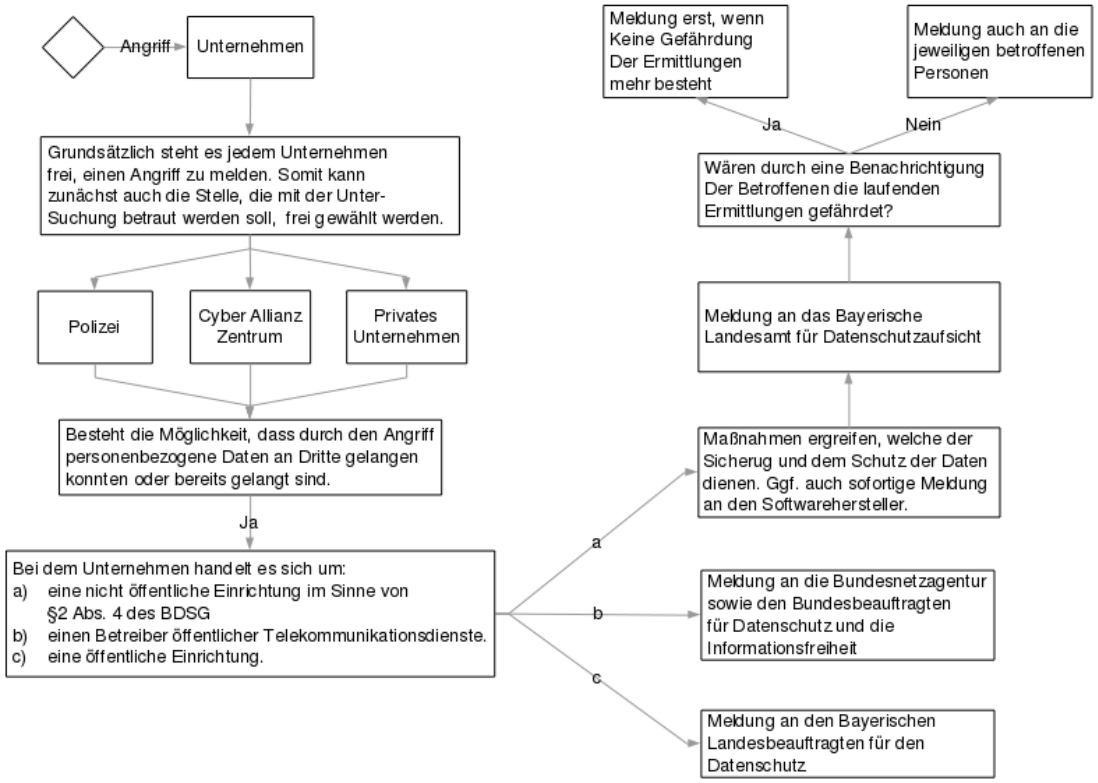
Betreiber von öffentlichen Telekommunikationsdiensten sind nach § 109a Datensicherheit (TKG) dazu verpflichtet, einen Vorfall, auch einen kleineren, binnen 24 Stunden an die Bun-

desnetzagentur sowie den BfDI zu melden. Ein entsprechendes Meldeformular findet sich auf den Internetseiten der Bundesnetzagentur, siehe Anhang A.2.

Für Datenschutzverstöße im öffentlichen Dienst ist der Landesdatenschutzbeauftragte zuständig.

Abbildung 7.1 zeigt den gesamten Meldevorgang in Form eines Entscheidungsbaumes.

Abbildung 7.1.: Ablaufkette des Meldevorganges nach einem Angriff



7.4. Ziele der Ermittlungen

In Punkt 6.1, Fallzahlen in der BRD, wurde bereits auf das Anzeigeverhalten von Unternehmen eingegangen. Dieses ist nach aktuellem Stand verbesserungswürdig, obgleich die Ziele der Ermittlungen im Interesse der Unternehmen liegen.

7.4.1. Identifikation des Angreifers

Der Täter kann zivil- und strafrechtlich nicht belangt werden, wenn nicht bekannt ist, wo er sich aufhält und wer er ist. Zum einen ist den Geschädigten durch die Identifizierung des Täters möglich, Schadensersatzansprüche gegen ihn geltend zu machen. Dies hätte

eine abschreckende Wirkung auf andere mögliche Täter zur Folge. Wichtiger ist jedoch der konsequente Vollzug der Strafe des Vergehens. Herrscht hier beinahe Straffreiheit, weil ein Großteil der Vorfälle nicht zur Anzeige gebracht wird, ist das ein Freibrief für alle Angreifer, ihre Machenschaften fortzusetzen. Dass die Strafe gegen das begangene Verbrechen vollzogen wird, ist folglich von größter Wichtigkeit. Nicht nur für das betroffene Unternehmen, sondern ebenso für die gesamte Wirtschaft und den privaten Sektor. Eine funktionierende Strafverfolgung im IT-Bereich stärkt das Vertrauen in die Informationstechnologien, die andernfalls nicht ohne Vorbehalte genutzt und dadurch nicht ihr wahres Potential entfalten kann.

7.4.2. Schwachstellen erkennen

Ein weiteres Ziel der Ermittlungen ist das Erkennen von Sicherheitslücken. Dies ermöglicht zum einen eine Risikoanalyse der Systemlandschaft, mit der Folge, die gegenwärtigen Risiken besser abschätzen zu können. Zum anderen hilft dies bei der Prävention und der Abwehr von Angriffen, durch das Entwickeln geeigneter Gegenmaßnahmen.

7.4.3. Prävention und Angriffsabwehr

Prävention und Abwehr von Angriffen können nur funktionieren, wenn so viele Schwachstellen wie möglichen von den verschiedenen Systemen bekannt sind. Informationen über neue Sicherheitsrisiken müssen daher umgehend ausgetauscht werden, um den Sicherheitsstandard zu maximieren, und, damit einhergehend, den möglichen Schaden zu minimieren.

7.4.4. Schadensanalyse

Die Ermittlung der entstandenen Schäden ermöglicht eine Abschätzung der Budgetplanung für die Abteilungen der IT-Sicherheit. Somit können die eingesetzten Sicherheitsmaßnahmen entsprechend der aktuellen Sicherheitslage angepasst werden. Das ermöglicht zu jeder Zeit ein Höchstmaß an Sicherheit. Des Weiteren werden dadurch Ressourcen nicht unnötig verschwendet, sondern dort eingesetzt, wo sie gebraucht werden.

8. Schlussteil

Die Arbeit gliedert sich grundlegend in einen theorie- und einen praxisbezogenen Teil. Im theoretischen Teil wurden zunächst allgemeine Begrifflichkeiten erläutert, die im Zusammenhang mit der Fragestellung auftreten. Anschließend wurden die juristischen und organisatorischen Grundlagen zum Thema Computerkriminalität in der BRD betrachtet. Der Fokus lag dabei darauf, die relevanten Gesetze zu nennen und ihren Inhalt zu erörtern, sowie die zuständigen Behörden und ihr jeweiliges Aufgabengebiet vorzustellen. Des Weiteren wurde auf die Definition der verschiedenen Angriffsarten eingegangen.

Im praxisbezogenen Teil wurde zu Beginn der mögliche Aufbau einer Sicherheitslandschaft erläutert. Die Ausführungen dazu erfolgten dabei sowohl auf theoretischer Basis als auch anhand eines konkreten Beispiels. Anschließend wurden die aktuellen Gegebenheiten näher beleuchtet, wie sich die Fallzahlen in der BRD entwickelt haben, und wie hoch diese aktuell sind. Auch die Unternehmen und deren Erfahrungen mit sicherheitskritischen Vorfällen, sowie ihr Anzeigeverhalten wurde betrachtet. Schlussendlich finden sich in einem Leitfaden Handlungsempfehlungen für das Vorgehen nach einem Angriff. Dies soll den Betroffenen von sicherheitskritischen Vorfällen bei der Orientierung helfen. Ihnen soll ein Weg aufgezeigt werden, wie sie sich im Schadensfall optimal verhalten sollen und an wen sie sich wenden müssen.

In einer Informationsgesellschaft ist die Computersicherheit ein zentraler Punkt, der in den Bereichen Politik, Wirtschaft und Privatleben Einzug erhalten hat. Dadurch ist auch das Thema Computerkriminalität ein sehr vielschichtiger Bereich. Ihn gänzlich zu erfassen, ist mit einer rein technischen Sichtweise nicht möglich. Darum wurden im Rahmen dieser Arbeit neben den technischen Aspekten ebenso juristische und organisatorische, jedoch auch gesellschaftspolitische Punkte beleuchtet.

Um möglichst alle diese Aspekte zu erfassen, gab es im Zuge der Bearbeitung viele Konversationen mit unterschiedlichen Personengruppen. Frau Birgit Maneth von der Rechtsanwaltskanzlei Sonntag & Partner hat die Arbeit mit ihrem juristischen Fachwissen betreut, mit dem Ergebnis einer Aufstellung der relevanten Gesetze in Verbindung mit Computerkriminalität. Herr Björn Stelte vom CAZ hat überwiegend zum Verständnis der Arbeit der Verfassungsschutzbehörden und allem Voran des CAZ beigetragen, auch bezogen auf den Unterschied zu den Ermittlungsbehörden. Ebenso Herr Peter Hirsch von der Kriminalpolizeiinspektion Neu-Ulm, jedoch speziell im Hinblick auf den Aufgabenbereich der Polizeilichen Behörden und dem juristischen Hintergrund im Zusammenhang mit den Ermittlungen der Strafverfolgungsbehörden. Herr Dr. Gerhard Rammel, Leiter der Medizintechnik am Zentralklinikum Augsburg, hat anschaulich aufgezeigt, wie die Sicherheitslandschaft in einem größeren Unternehmen aussehen kann. Innerhalb dieses Gespräches fand ebenso ein Austausch über allgemeine Belange der IT-Sicherheit statt, was auch in anderen Punkten zu ei-

nem besseren Verständnis beigetragen hat. Herr Jan Müller von der Bundesnetzagentur half bei der Erläuterung der Meldevorschriften nach § 109a TKG. Darüber hinaus fanden noch weitere Gespräche mit Vertretern verschiedener Branchen statt, die sich nicht direkt im Inhalt dieser Arbeit widerspiegeln, die jedoch geholfen haben, das Bild, welches diese Arbeit formt, zu formen. Herr Andreas Defet von der Firma IT-Architekten in Nürnberg, schilderte seine über Jahre gesammelten Erfahrungen als selbstständiger IT-Dienstleister. Frau Jennifer Ball half mit ihrer langjährigen Erfahrung in verschiedenen Gastronomiebetrieben beim Verständnis des Branchenvergleiches, in Bezug auf die Nutzung der IT im Gastgewerbe.

Die für die Arbeit notwendige Recherche sowie die verschiedenen Gespräche haben letzten Endes dazu beigetragen, ein Verständnis für Computerkriminalität aufzubauen, ohne das es nicht möglich gewesen wäre, einen Leitfaden mit Handlungsempfehlungen zu entwickeln. Dass ein solcher dringend notwendig ist, hat die Arbeit ebenfalls gezeigt. Die Unwissenheit der Unternehmen über das Vorgehen nach einem Angriff steht jedoch lediglich an dritter Stelle. Deutlich mehr Unternehmen bezweifeln den Erfolg der Ermittlungen und sehen sogar den Aufwand für eine Anzeige zu hoch. Neben der Entwicklung eines Leitfadens wäre es somit auch interessant gewesen zu erfahren, worin diese Meinungen begründet sind. Das hätte allerdings den Umfang dieser Arbeit weit überstiegen. Eine zukünftige Untersuchung könnte sich jedoch näher mit diesen Aspekten beschäftigen. Die Kritik und Skepsis einiger Unternehmen im Hinblick auf den Aufwand und Erfolg der Ermittlungen implizieren einen Handlungsbedarf von Seiten der Behörden und der Politik. Ein Leitfaden zum Vorgehen nach sicherheitskritischen Vorfällen kann sein volles Potential erst entfalten, wenn auch das Vorgehen, welches er beschreibt, von den Betroffenen angenommen wird.

Insgesamt betrachtet baut diese Arbeit für den Leser ein tiefgreifenderes Verständnis des Themas Computerkriminalität auf. Dies ermöglicht es ihm, auch eigene Schlussfolgerungen zu ziehen, was ein Ziel des Definitionsteils ist, denn kaum eine Branche unterliegt einer so rasanten Entwicklung wie der IT-Sektor. Durch den schnellen und stetigen Wandel der Gegebenheiten ändern sich auch die Sicherheitsanforderungen kontinuierlich. Um sich in möglichst kurzer Zeit an neue Umstände anpassen zu können, ist ein Grundverständnis unerlässlich. Der Leitfaden zeigt zudem auf, wie sich der Leser nach einem Cyberangriff verhallten soll, was letztlich Thema dieser Untersuchung ist.

Literaturverzeichnis

[Alexander Seidl und Katharina Fuchs 2010] ALEXANDER SEIDL UND KATHARINA FUCHS: Die Strafbarkeit des Phishing nach Inkrafttreten des 41. Strafrechtsänderungsgesetzes. In: *HRRS* (2010), Februar, Nr. 2. – URL http://www.hrr-strafrecht.de/hrr/archiv/10-02/index.php?sz=7

[Bibliographisches Institut GmbH 2013] BIBLIOGRAPHISCHES INSTITUT GMBH: *Duden Online*. http://www.duden.de/node/678628/revisions/1177425/view. Januar 2013. – Aufgerufen: 16.03.2014

[BMI 2011] BMI: *Nationales Cyber-Abwehrzentrum*. http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html. 2011. – Aufgerufen: 10.04.2014

[BMJV 2004a] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Bundesdatenschutzgesetz*. http://www.gesetze-im-internet.de/bdsg_1990/__42a.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004b] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Bundesdatenschutzgesetz*. http://www.gesetze-im-internet.de/bdsg_1990/__43.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004c] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Sicherheitsüberprüfungsgesetz*. http://www.bfdi.bund.de/DE/Dienststelle/Aufgaben/Aufgaben_node.html. 2004. – Aufgerufen: 11.04.2014

[BMJV 2004d] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Strafgesetzbuch*. http://www.gesetze-im-internet.de/stgb/__202a.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004e] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Strafgesetzbuch*. http://www.gesetze-im-internet.de/stgb/__202b.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004f] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Strafgesetzbuch*. http://www.gesetze-im-internet.de/stgb/__202c.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004g] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Strafgesetzbuch*. http://www.gesetze-im-internet.de/stgb/__263a.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004h] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Strafgesetzbuch*. http://www.gesetze-im-internet.de/stgb/__269.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004i] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Strafgesetzbuch*. http://www.gesetze-im-internet.de/stgb/__303a.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004j] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Strafgesetzbuch*. http://www.gesetze-im-internet.de/stgb/__303b.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004k] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Telekommunikationsgesetz*. http://www.gesetze-im-internet.de/tkg_2004/__115.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004l] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Telekommunikationsgesetz*. http://www.gesetze-im-internet.de/tkg_2004/__88.html. 2004. – Aufgerufen: 16.03.2014

[BMJV 2004m] BMJV, Bundesministerium der Justiz und für Verbraucherschutz: *Gesetze im Internet, Telekommunikationsgesetz*. http://www.gesetze-im-internet.de/tkg_2004/__109a.html. 2004. – Aufgerufen: 16.03.2014

[Bundesamt für Verfassungsschutz 2012] BUNDESAMT FÜR VERFASSUNGSSCHUTZ: *Verfassungsschutzbericht 2012*. Fehlt 2012. – URL http://www.verfassungsschutz.de/embed/vsbericht-2012.pdf

[Bundeskriminalamt 2012a] BUNDESKRIMINALAMT: *Bundeslagebild Cybercrime*. Fehlt 2012. – URL http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2012,templateId=raw,property=publicationFile.pdf/cybercrimeBundeslagebild2012.pdf

[Bundeskriminalamt 2012b] BUNDESKRIMINALAMT: *Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime*. Fehlt 2012. – URL http://www.bka.de/nn_238144/SharedDocs/Downloads/DE/ThemenABisZ/InternetKriminalitaet/handlungsempfehlungenWirtschaft,templateId=raw,property=publicationFile.pdf/handlungsempfehlungenWirtschaft.pdf

[Cyber Allianz Zentrum Bayern 2013] CYBER ALLIANZ ZENTRUM BAYERN: *Cyber Allianz Zentrum Bayern ist Anlaufstelle für die bayerische Wirtschaft und Betreiber kritischer Infrastruktur*. http://www.verfassungsschutz.bayern.de/service/spionage/09666/index.php. Januar 2013. – Aufgerufen: 11.04.2014

[Dipl. Phys. Stefan Dieterle und Dr.-Ing. Peer Wichmann 2003] DIPL. PHYS. STEFAN DIETERLE UND DR.-ING. PEER WICHMANN: *Sicherheitfür die Top-Level Domain .de durch Secure DNS*. Mai 2003. – URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/SecureDNS/Studiesecdns_pdf.pdf?__blob=publicationFile. – FZI Forschungszentrum Informatik: Im Auftrag des Bundesamt für Sicherheit in der Informationstechnik (BSI)

[Easttom 2011] EASTTOM, C.: *Computer Security Fundamentals*. Pearson Education, Limited, 2011. – URL http://books.google.de/books?id=qpUfKQEACAAJ. – ISBN 9780789748904

[Fischer u. a. 2014] FISCHER, T. ; SCHWARZ, O. ; DREHER, E. ; TRÖNDLE, H.: *Strafgesetzbuch: mit Nebengesetzen*. Beck C. H., 2014 (Beck Kurzkommentare). – URL http://books.google.de/books?id=hxiXmwEACAAJ. – ISBN 9783406652349

[Franz Büllingen und Annette Hillebrand 2012] FRANZ BÜLLINGEN UND ANNETTE HILLEBRAND : *IT-Sicherheitsniveau in kleinen und mittleren Unternehmen*. September 2012. – URL https://docs.google.com/viewer?url=http%3A%2F%2Fwww.bmwi.de%2FBMWi%2FRedaktion%2FPDF%2FS-T%2Fstudie-it-sicherheit%2Cproperty%3Dpdf%2Cbereich%3Dbmwi2012%2Csprache%3Dde%2Crwb%3Dtrue.pdf. – WIK-Consult GmbH: Im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi)

[Funaro 2013] FUNARO, Greg: *Ransomware & Cyber-Erpressung: Computer unter Belagerung*. http://blog.kaspersky.de/ransomware-cyber-erpressung-computer-unter-belagerung. Juli 2013. – Aufgerufen: 16.03.2014

[IHK Nord 2013] IHK NORD: *Unternehmensbefragung zur Betroffenheit der norddeutschen Wirtschaft von Cybercrime*. Juni 2013. – URL http://www.ihk-nord.de/linkableblob/ihknord/downloads/2455988/.6./data/Cybercrime_Umfrageauswertung_18062013-data.pdf. – Arbeitsgemeinschaft Norddeutscher Industrie- und Handelskammern

[Jan Müller 2014] JAN MÜLLER: *Fragen zur Meldepflicht nach § 109a TKG*. April 2014. – E-Mail-Verkehr mit der Bundesnetzagentur: Fragen zur Meldepflicht nach § 109a TKG

[Kasperskij 2008] KASPERSKIJ, E.V.: *Malware: von Viren, Würmern, Hackern und Trojanern und wie man sich vor ihnen schützt ; [inkl. 90-Tage-Testversion Kaspersky Internet*

Security 7.0]. Hanser, 2008. – URL http://books.google.de/books?id=5LR5yV-GEJkC. – ISBN 9783446415003

[Miłosz 2002] MIŁOSZ, Adam: *Datenschutzrecht und Fernmeldegeheimnis nach Art. 10 GG, § 85 TKG*. Mai 2002. – URL http://www.uni-kiel.de/eastlaw/ws0001/Seminararbeiten1/Milosz.doc. – Seminar „Datenschutz im elektronischen Rechtsverkehr“, Prof. Alexander Trunk, Christian-Albrechts-Universität zu Kiel

[Prof. Dr. Gordon Rohrmair 2013] PROF. DR. GORDON ROHRMAIR: *Anwendungen der IT-Sicherheit 2 - Ermittlung*. Mai 2013. – Skript der Vorlesung: Anwendungen der IT-Sicherheit 2

[Werth 2009] WERTH, T.: *Die Kunst der digitalen Verteidigung*. C & L, Computer- und Literaturverl., 2009 (Computer & Literatur). – URL http://books.google.de/books?id=vAZSPgAACAAJ. – ISBN 9783936546590

[Wikipedia 2014] WIKIPEDIA: *Terrorismus*. http://de.wikipedia.org/wiki/Terrorismus#Definitionen. März 2014. – Aufgerufen: 04.04.2014

A. Anhang

A.1. Zugrunde liegende Gesetze

§ 202a Ausspähen von Daten (StGB)

„(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.“ (BMJV, 2004d, StGB, § 202a)

§ 202b Abfangen von Daten (StGB)

„Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.“ (BMJV, 2004e, StGB, § 202b)

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten (StGB)

„(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.“ (BMJV, 2004f, StGB, § 202c)

§ 206 Verletzung des Post- oder Fernmeldegeheimnisses (StGB)

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt
1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die
1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 263a Computerbetrug (StGB)

„(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 7 gilt entsprechend.

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.“ (BMJV, 2004g, StGB, § 263a)

§ 269 Fälschung beweiserheblicher Daten (StGB)

„(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend.“ (BMJV, 2004h, StGB, § 269)

§ 303a Datenveränderung (StGB)

„(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.“ (BMJV, 2004i, StGB, § 303a)

§ 303b Computersabotage (StGB)

„(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er
1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar

macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter
1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.“ (BMJV, 2004j, StGB, § 303b)

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten BDSG

Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte
1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten
unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten.

Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden. (BMJV, 2004a, BDSG, § 42a)

§ 43 Bußgeldvorschriften (BDSG)

„(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,
2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,
2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,
3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,
3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,
4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,
4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,
7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt, 7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,
7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,
8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,
8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,
8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,
9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,
10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder
11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.
(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,
5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,
5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,
6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder
7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.
(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.“ (BMJV, 2004b, BDSG, § 43)

§ 88 Fernmeldegeheimnis (TKG)

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.

(4) Befindet sich die Telekommunikationsanlage an Bord eines Wasser- oder Luftfahrzeugs, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber ihrer Stellvertretung. (BMJV, 2004l, TKG, § 88)

§ 109a Datensicherheit (TKG)

„(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen. Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten Teilnehmer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden, hat der Anbieter des Telekommunikationsdienstes zusätzlich die Betroffenen unverzüglich von dieser Verletzung zu benachrichtigen. In Fällen, in denen in dem Sicherheitskonzept nachgewiesen wurde, dass die von der Verletzung betroffenen personenbezogenen Daten durch geeignete technische Vorkehrungen gesichert, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gespeichert wurden, ist eine Benachrichtigung nicht erforderlich. Unabhängig von Satz 3 kann die Bundesnetzagentur den Anbieter des Telekommunikationsdienstes unter Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten zu einer Benachrichtigung der Betroffenen verpflich-

ten. Im Übrigen gilt § 42a Satz 6 des Bundesdatenschutzgesetzes entsprechend.

(2) Die Benachrichtigung an die Betroffenen muss mindestens enthalten:
1. die Art der Verletzung des Schutzes personenbezogener Daten,
2. Angaben zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind, und
3. Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen. In der Benachrichtigung an die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat der Anbieter des Telekommunikationsdienstes zusätzlich zu den Angaben nach Satz 1 die Folgen der Verletzung des Schutzes personenbezogener Daten und die beabsichtigten oder ergriffenen Maßnahmen darzulegen.

(3) Die Anbieter der Telekommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen, das Angaben zu Folgendem enthält:
1. zu den Umständen der Verletzungen,
2. zu den Auswirkungen der Verletzungen und
3. zu den ergriffenen Abhilfemaßnahmen. Diese Angaben müssen ausreichend sein, um der Bundesnetzagentur und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Prüfung zu ermöglichen, ob die Bestimmungen der Absätze 1 und 2 eingehalten wurden. Das Verzeichnis enthält nur die zu diesem Zweck erforderlichen Informationen und muss nicht Verletzungen berücksichtigen, die mehr als fünf Jahre zurückliegen.

(4) Vorbehaltlich technischer Durchführungsmaßnahmen der Europäischen Kommission nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG kann die Bundesnetzagentur Leitlinien vorgeben bezüglich des Formats, der Verfahrensweise und der Umstände, unter denen eine Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten erforderlich ist.“ (BMJV, 2004m, TKG, § 109a)

§ 115 Kontrolle und Durchsetzung von Verpflichtungen (TKG)

(1) Die Bundesnetzagentur kann Anordnungen und andere Maßnahmen treffen, um die Einhaltung der Vorschriften des Teils 7 und der auf Grund dieses Teils ergangenen Rechtsverordnungen sowie der jeweils anzuwendenden Technischen Richtlinien sicherzustellen. Der Verpflichtete muss auf Anforderung der Bundesnetzagentur die hierzu erforderlichen Auskünfte erteilen. Die Bundesnetzagentur ist zur Überprüfung der Einhaltung der Verpflichtungen befugt, die Geschäfts- und Betriebsräume während der üblichen Betriebs- oder Geschäftszeiten zu betreten und zu besichtigen.

(2) Die Bundesnetzagentur kann nach Maßgabe des Verwaltungsvollstreckungsgesetzes Zwangsgelder wie folgt festsetzen:

1. bis zu 500 000 Euro zur Durchsetzung der Verpflichtungen nach § 108 Abs. 1, § 110 Abs. 1, 5 oder Abs. 6, einer Rechtsverordnung nach § 108 Absatz 3, einer Rechtsverordnung nach § 110 Abs. 2, einer Rechtsverordnung nach § 112 Abs. 3 Satz 1, der Technischen Richtlinie nach § 108 Absatz 4, der Technischen Richtlinie nach § 110 Abs. 3 oder der Technischen Richtlinie nach § 112 Abs. 3 Satz 3, 2. bis zu 100 000 Euro zur Durchsetzung der Verpflichtungen nach den §§ 109, 109a, 112 Absatz 1, 3 Satz 4, Absatz 5 Satz 1 und 2, § 113 Absatz 5 Satz 2 und 3 oder § 114 Absatz 1 und 3. bis zu 20 000 Euro zur Durchsetzung der Verpflichtungen nach § 111 Abs. 1, 2 und 4 oder § 113 Absatz 4 und 5 Satz 1.

Bei wiederholten Verstößen gegen § 111 Abs. 1, 2 oder Abs. 4, § 112 Abs. 1, 3 Satz 4, Abs. 5 Satz 1 und 2 oder § 113 Absatz 4 und 5 Satz 1 kann die Tätigkeit des Verpflichteten durch Anordnung der Bundesnetzagentur dahin gehend eingeschränkt werden, dass der Kundenstamm bis zur Erfüllung der sich aus diesen Vorschriften ergebenden Verpflichtungen außer durch Vertragsablauf oder Kündigung nicht verändert werden darf.

(3) Darüber hinaus kann die Bundesnetzagentur bei Nichterfüllung von Verpflichtungen des Teils 7 den Betrieb der betreffenden Telekommunikationsanlage oder das geschäftsmäßige Erbringen des betreffenden Telekommunikationsdienstes ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen.

(4) Soweit für die geschäftsmäßige Erbringung von Telekommunikationsdiensten Daten von natürlichen oder juristischen Personen erhoben, verarbeitet oder genutzt werden, tritt bei den Unternehmen an die Stelle der Kontrolle nach § 38 des Bundesdatenschutzgesetzes eine Kontrolle durch den Bundesbeauftragten für den Datenschutz entsprechend den §§ 21 und 24 bis 26 Abs. 1 bis 4 des Bundesdatenschutzgesetzes. Der Bundesbeauftragte für den Datenschutz richtet seine Beanstandungen an die Bundesnetzagentur und übermittelt dieser nach pflichtgemäßem Ermessen weitere Ergebnisse seiner Kontrolle.

(5) Das Fernmeldegeheimnis des Artikels 10 des Grundgesetzes wird eingeschränkt, soweit dies die Kontrollen nach Absatz 1 oder 4 erfordern. (BMJV, 2004k, TKG, § 115)

§ 1 Zweck und Anwendungsbereich des Gesetzes (SÜG)

(1) Dieses Gesetz regelt die Voraussetzungen und das Verfahren zur Überprüfung einer Person, die von der zuständigen Stelle mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll (Sicherheitsüberprüfung) oder bereits betraut worden ist (Wiederholungsüberprüfung).
(2) Eine sicherheitsempfindliche Tätigkeit übt aus, wer

1. Zugang zu Verschlußsachen hat oder ihn sich verschaffen kann, die STRENG GEHEIM, GEHEIM ODER VS-VERTRAULICH eingestuft sind,

2. Zugang zu Verschlußsachen überstaatlicher Einrichtungen und Stellen hat oder ihn sich verschaffen kann, wenn die Bundesrepublik Deutschland verpflichtet ist, nur sicherheitsüberprüfte Personen hierzu zuzulassen,

3. in einer Behörde oder einer sonstigen öffentlichen Stelle des Bundes oder in einem Teil von ihr tätig ist, die auf Grund des Umfanges und der Bedeutung dort anfallender Verschlußsachen von der jeweils zuständigen obersten Bundesbehörde im Einvernehmen mit dem Bundesministerium des Innern als Nationale Sicherheitsbehörde zum Sicherheitsbereich erklärt worden ist,

4. nach anderen Vorschriften einer Sicherheitsüberprüfung unterliegt, soweit auf dieses Gesetz verwiesen wird.

(3) Verpflichten sich Stellen der Bundesrepublik Deutschland gegenüber Stellen anderer Staaten durch Übereinkünfte, bei Personen, die Zugang zu Verschlußsachen ausländischer Staaten haben oder sich verschaffen können, zuvor Sicherheitsüberprüfungen nach deutschem Recht durchzuführen, ist in diesen Übereinkünften festzulegen, welche Verschlußsachengrade des Vertragspartners Verschlußsachengraden nach diesem Gesetz vergleichbar sind. Derartige Festlegungen müssen sich im Rahmen der Bewertungen dieses Gesetzes halten und insbesondere den Maßstäben des § 4 entsprechen.
(4) Eine sicherheitsempfindliche Tätigkeit übt auch aus, wer an einer sicherheitsempfindlichen Stelle innerhalb einer lebens- oder verteidigungswichtigen Einrichtung oder wer innerhalb einer besonders sicherheitsempfindlichen Stelle des Geschäftsbereiches des Bundesministeriums der Verteidigung ("Militärischer Sicherheitsbereich") beschäftigt ist oder werden soll (vorbeugender personeller Sabotageschutz).Ziel des vorbeugenden personellen Sabotageschutzes ist es, potenzielle Saboteure (Innentäter) von sicherheitsempfindlichen Stellen fernzuhalten, um den Schutz der in Absatz 5 Satz 1 und 2 genannten Schutzgüter sicherzustellen.
(5) Lebenswichtig sind solche Einrichtungen,

1. deren Beeinträchtigung auf Grund der ihnen anhaftenden betrieblichen Eigengefahr die Gesundheit oder das Leben großer Teile der Bevölkerung erheblich gefährden kann oder

2. die für das Funktionieren des Gemeinwesens unverzichtbar sind und deren Beeinträchtigung erhebliche Unruhe in großen Teilen der Bevölkerung und somit Gefahren für die öffentliche Sicherheit oder Ordnung entstehen lassen würde.

Verteidigungswichtig sind außerhalb des Geschäftsbereiches des Bundesministeriums der Verteidigung solche Einrichtungen, die der Herstellung oder Erhaltung der Verteidigungsbereitschaft dienen und deren Beeinträchtigung auf Grund

1. fehlender kurzfristiger Ersetzbarkeit die Funktionsfähigkeit, insbesondere die Ausrüstung, Führung und Unterstützung der Bundeswehr und verbündeter Streitkräfte sowie der Zivilen Verteidigung, oder

2. der ihnen anhaftenden betrieblichen Eigengefahr die Gesundheit oder das Leben großer Teile der Bevölkerung erheblich gefährden kann. Sicherheitsempfindliche Stelle ist die kleinste selbständig handelnde Organisationseinheit innerhalb einer lebens- oder verteidigungswichtigen Einrichtung, die vor unberechtigtem Zugang geschützt ist und von der im Falle der Beeinträchtigung eine erhebliche Gefahr für die in den Sätzen 1 und 2 genannten Schutzgüter ausgeht (BMJV, 2004c, SÜG, § 1).

A.2. Informative Links

Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/DE/Home/home_node.html

Allianz für Cybersicherheit (BSI)
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html

IT-Sicherheit in der Wirtschaft (BMWi)
http://www.it-sicherheit-in-der-wirtschaft.de/

Bundesnetzagentur
http://www.bundesnetzagentur.de/cln_1912/DE/Home/home_node.html

Meldeformular der Bundesnetzagentur
http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Datenschutz/Meldeformular.pdf?__blob=publicationFile&v=2

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
http://www.bfdi.bund.de/Vorschaltseite_DE_node.html

Landesamt für Datenschutzaufsicht Bayern
http://www.lda.bayern.de/index.htm

Landesbeauftragte für den Datenschutz Bayern
https://www.datenschutz-bayern.de/

Internetplattform zum Schutz kritischer Infrastrukturen
http://www.kritis.bund.de/SubSites/Kritis/DE/Home/home_node.html

European Cybercrime Centre
https://www.europol.europa.eu/ec3

Nationales Cyber-Abwehrzentrum der BRD
http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategi
Cyberabwehrzentrum/cyberabwehrzentrum_node.html

Cyber Allianz Zentrum Bayern
http://www.verfassungsschutz.bayern.de/service/spionage/09666/index.php

Sicherheitstacho der Deutschen Telekom
http://www.sicherheitstacho.eu/

The Onion Router

https://www.torproject.org/index.html.en

A.3. Informationssammlung bei Sicherheitskritischen Vorfällen

Fragen bei Erstkontakt:

Wer meldet den Vorfall:	
Was ist passiert:	
Wann geschah der Vorfall:	
Wie ging der Angreifer vor:	
Welche Systeme sind betroffen:	
Gibt es ein erkennbares Motiv:	
Wo wird der Täter vermutet:	
Welche Schäden sind entstanden:	
Sind Spuren vorhanden oder verwischt:	
Auswirkungen auf den Anwender:	

Informationen zum System:

Betriebssystem:	
IP-Adresse:	
Hauptbenutzer des Systems:	
Zuständiger Administrator:	

Vorgenommene Tätigkeiten:

Stecker gezogen:	
Remote oder lokaler Zugriff:	
Änderungen am System:	
Wer wurde informiert:	

Informationen zum Angreifer:

Angreifer noch aktiv:	
Quell IP-Adresse:	
Möglicherweise Intern:	

Sonstiges:

Optionale Angaben:	