FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

Identitätsdiebstahl und Identitätsmissbrauch im Internet

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Wirtschaftsingenieurwesen Informatik

eingereicht von

Felix Meindl
Matrikelnummer 0125871

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer: Ao.Univ.Prof. Dr.iur. Markus Haslinger

Wien, 12.01.2012

(Felix Meindl, Bakk. techn.)

(Dr. Markus Haslinger)

Erklärung

Felix Meindl, Mariatheresienstraße 30/15, 1010 Wien, Österreich

„Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe."

Wien, 12.01.2012 _____

(Felix Meindl, Bakk. techn.)

Danksagung

Besonderer Dank geht an meine Eltern Hans und Eva Meindl, die mich mein gesamtes Studium bis zum Abschluss meiner Diplomarbeit immer unterstützt haben.

Zusätzlicher Dank gebührt meinem Betreuer, Dr. Markus Haslinger, der mich während der Arbeit an meiner Diplomarbeit ausgezeichnet und zuverlässig betreut hat.

Abkürzungsverzeichnis

ABGB	Allgemeines Bürgerliches Gesetzbuch
ABN	Australian Business Number
ACK	Acknowledgement
AG	Amtsgericht
APWG	Anti-Phishing Working Group
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BDSG	Bundesdatenschutzgesetz
BGBl	Bundesgesetzblatt
BIOS	Basic Input/Output System
BK	Bundeskriminalamt(Österreich)
BKA	Bundeskriminalamt(Deutschland)
BKU	Bürgerkartenumgebung
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BWG	Bankwesengesetz
CA	Certification Authority
CD	Compact Disk
CIPPIC	Canadian Internet Policy and Public Interest Clinic
CMS	Content-Management-System
CSN	Consumer Sentinel Network
DDoS	Distributed Denial of Service
DNA	Desoxyribonukleinsäure
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
DRDoS	Distributed Reflection Denial of Service
DSG	Datenschutzgesetz
DSL	Digital Subscriber Line
E	Elektronisch
EG	Europäische Gemeinschaft
ENISA	European Network and Information Security Agency
EU	Europäische Union
FBI	Federal Bureau of Investigation
FH	Fachhochschule
FIDIS	Future of Identity in the Information Society
FIN	Finish
FPEG	Fraud Prevention Expert Group
FRA	Försvarets Radioanstalt
FTC	Federal Trade Commission
G	Gesetz
HSTS	Hypertext Transfer Protocol Strict Transport Security
HTML	Hypertext Markup Language

HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICQ	I Seek You
ID	Identifikator
IHL	Internetprotokoll Header Length
ICANN	Internet Corporation for Assigned Names and Numbers
IP	Internetprotokoll
IRC	Internet Relay Chat
ISO	International Organisation for Standardization
ISP	Internet Service Provider
IT	Informationstechnik
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LLC	Logical Link Control
LSO	Local Shared Objects
MAC	Media Access Control
MCLOC	Model Criminal Law Officers Committee
MitM	Man-in-the-Middle
NCVS-ITS	National Crime Victimization Survey – Identity Theft
OPM	Office of Personnel Management
OSI	Open Systems Interconnection
OTP	One Time Password
OWASP	Open Web Application Security Project
PDF	Portable Document Format
PIN	Personal Identification Number
PIPEDA	Personal Information Protection and Electronic Documents Act
PHP	Hypertext Preprocessor
PKI	Public-Key-Infrastruktur
PRADO	Public Register of Authentic Identity and Travel Documents
PRIME	Privacy and Identity Management for Europe
PSH	Push
RCMP	Royal Canadian Mounted Police
RECOL	Reporting Economic Crime On-line
RFI	Remote File Inclusion
RPC	Remote Procedure Call
RST	Reset
S	Section
SCTP	Stream Control Transmission Protocol
SEPA	Single Europe Payments Area
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSN	Social Security Number
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SYN	Synchronize

TAN	Transaktionsnummer
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TLS	Transport Layer Security
UDP	User Datagram Protocol
URG	Urgent
URL	Uniform Resource Locator
USB	Universal Serial Bus
U.S.C.	United States Code
WAN	Wide Area Network
WET	Web Exploit Toolkit
WLAN	Wireless Local Area Network
XSRF	Cross-Site-Request-Forgery
XSS	Cross-Site-Scripting
ZKA	Zentraler Kreditausschuss

Inhaltsverzeichnis

1 Einleitung

Wir leben heute in einem Zeitalter zunehmender digitaler Vernetzung. Egal ob im Bereich des Online-Banking, des E-Commerce, des E-Government oder des Internethandels, der Trend geht dahin, immer mehr Alltagsgeschäfte von zuhause aus zu erledigen. Im Jahr 2012 haben bereits über 70% aller EU-Haushalte Zugang zum Internet[1], allein in Österreich haben 79% aller privaten Haushalte einen Internetanschluss[2].

Um konkurrenzfähig zu bleiben, versuchen die Anbieter diverser elektronischer Dienste den privaten Nutzern immer mehr technische Funktionalität bei gleichzeitig immer einfacherer Benutzung zu bieten. Damit erweitert sich aber auch die Angriffsfläche gegenüber modernen Bedrohungen wie elektronischem Identitätsdiebstahl und Identitätsmissbrauch, denn noch nie war es so einfach, mittels verhältnismäßig niedrigem Aufwand an personenbezogene Daten zu kommen.

Identitätsdiebstahl und Identitätsmissbrauch mithilfe des Internet sind eine ernstzunehmende und stetig zunehmende Bedrohung für die Sicherheit von Nutzern und Unternehmen in einer modernen und immer stärker vernetzten Gesellschaft. Diese Form der Internetkriminalität ist bereits seit einigen Jahren durch Angriffsmethoden wie Phishing oder Pharming vor allem im Bereich des Online-Banking bekannt, allerdings werden die Methoden der Angreifer im Hinblick auf ihre technische Ausführung immer professioneller und raffinierter. Nach Studien der FTC (Federal Trade Commission) in den USA und des BSI (Bundesamt für Sicherheit in der Informationstechnik) in Deutschland werden elektronischer Identitätsdiebstahl und Identitätsmissbrauch zunehmend professioneller im Rahmen organisierter Internetkriminalität durchgeführt. Die Täter sind mittlerweile ausschließlich finanziell motiviert, denn Identitätsdaten von Personen sind auf diversen Schwarzmärkten im Internet ein Vermögen wert. Hier wurde ein neuer Markt geschaffen, und zwar ein Markt für die Identität von Personen. Daher muss im Rahmen dieser Arbeit ein nicht unerheblicher Teil den gängigsten Methoden der Angreifer und vor allem neuen Trends auf diesem Gebiet gewidmet werden.

Elektronischer Identitätsdiebstahl und Identitätsmissbrauch ist aktuell der am stärksten wachsende Bereich der Internetkriminalität und ein Ende des Wachstums ist mit November 2012 noch nicht abzusehen. Die verursachten Schäden liegen in Milliardenhöhe; entsprechend wichtig ist eine genauere Betrachtung dieses verhältnismäßig neuen Phänomens. Um diesem Problem entgegenzuwirken, sind Maßnahmen rechtlicher und technischer Natur notwendig. Der technische Teil der Arbeit behandelt ausschließlich die IT-basierten Werkzeuge und Methoden der Angreifer. Darüber hinaus werden die gängigsten den Nutzern und Unternehmen zur Verfügung stehenden

1 http://derstandard.at/1291455064176/70-Prozent-der-EU-Haushalte-haben-Zugang-zum-Internet (11.01.2012).
2 http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_haushalten/index.html (17.01.2012).

Verteidigungsmöglichkeiten im Hinblick auf ihre Effizienz überprüft. Rechtlich gesehen ist Identitätsdiebstahl und Identitätsmissbrauch eine Kriminalform, die innerhalb der EU verschiedene Rechtsmaterien betrifft, darunter etwa das Datenschutzrecht, das E-Commerce-Recht, das Strafrecht, aber oft auch das Zivilrecht. Daher liegt der Fokus des rechtlichen Teils der Arbeit auf bestehenden Gesetzen gegen Identitätsdiebstahl in diversen Ländern wie etwa den USA sowie einem länderübergreifenden Vergleich. Dabei ist nicht nur die Frage, ob und wie Identitätsdiebstahl strafrechtlich sanktioniert wird, von Bedeutung; auch die Effizienz und Wirkung dieser Gesetze wird geprüft.

Den Abschluss der Arbeit bildet eine Auflistung von Handlungsempfehlungen, die teils von führenden Experten auf dem Gebiet der Technik und des Rechts bezüglich Identitätsdiebstahl und Identitätsmissbrauch erstellt wurden, und die teils mithilfe der Ergebnisse der Untersuchungen des technischen und rechtlichen Abschnittes der Diplomarbeit ausgearbeitet werden konnten.

Auswertung der Quellen bis Stichtag 30.12.2012.

1.1 Fragestellung und Ziel

Im Rahmen dieser Arbeit sollen 2 Fragen beantwortet werden:

- Wie führen die Täter einen Identitätsdiebstahl oder Identitätsmissbrauch mithilfe von Informationstechnologie aus?
- Welche rechtlichen Bestimmungen und technischen Schutzmechanismen existieren, um dieser Bedrohung entgegenzuwirken und wie effizient sind diese?

Ziel der Arbeit ist es, zu ermitteln, wie groß die von Identitätsdiebstahl und Identitätsmissbrauch ausgehende Gefahr für die Informationsgesellschaft im Jahr 2012 ist und welche rechtlichen und technischen Schutzmaßnahmen einen erfolgversprechenden Ansatz zur Bekämpfung dieser Kriminalitätsform darstellen.

Es wird aufgezeigt, welche Maßnahmen der Gesetzgeber, IT-Sicherheitsfirmen, Experten aus Recht und Technik sowie die Politik bereits getroffen haben, um Identitätsdiebstahl und Identitätsmissbrauch entgegenzuwirken. Diesbezüglich sind sowohl präventive Maßnahmen von Bedeutung als auch Maßnahmen, die erst wirksam werden, wenn der Identitätsdiebstahl bereits erfolgreich ausgeführt wurde.

Um einen möglichst guten Schutz vor allem für technisch weniger versierte Nutzer zu bieten, ist es auch notwendig, sämtliche in dieser Arbeit behandelten technischen Schutzmechanismen auf ihre Komplexität zu überprüfen. Darüber hinaus muss die Frage beantwortet werden, ob und welche

Mindeststandards für Sicherheit an heimischen Rechnern gelten sollten. Zu diesem Zweck muss geprüft werden, ob zentrale Anlaufstellen im Netz für die Opfer von Identitätsdiebstahl existieren sollten, die diese mit notwendigen Informationen versorgen.

1.3 Struktur der Arbeit und wissenschaftliche Methode

Die Arbeit enthält 3 Teile:

- Begriffsdefinitionen;
- technischer Teil;
- rechtlicher Teil.

Der erste Teil der Arbeit beschäftigt sich im wesentlichen mit dem Identitätsbegriff sowie den Begriffen des Identitätsdiebstahls und des Identitätsmissbrauchs. Den Kern der Arbeit bilden der technische und der rechtliche Teil zusammen. Diese enthalten eine genaue Betrachtung der jeweiligen technischen Methoden, derer sich die Täter bedienen, eine Auflistung potentieller Schutzmaßnahmen für die Opfer und eine Darstellung der rechtlichen Regelungen zu diesem Delikt in verschiedenen Ländern.

Als wissenschaftliche Methoden wurden sowohl die traditionelle Recherche in der entsprechenden fachlichen Literatur gepflegt als auch Internetquellen recherchiert und ausgewertet.

Für den juristischen Teil der Arbeit wurden unter anderem bestehende Gesetzestexte, entsprechende EU–Richtlinien, diverse Studien, die unter anderem durch die deutsche Regierung oder die Federal Trade Commission in den USA eingeholt wurden sowie die Stellungnahmen anerkannter Experten auf diesem Gebiet verwendet. Im Rahmen der Prüfung von Gesetzestexten und EU-Richtlinien wurden nicht nur spezielle Normen zu Identitätsdiebstahl und Identitätsmissbrauch untersucht, sondern auch Gesetze aus angrenzenden Rechtsmaterien, wie beispielsweise das österreichische Datenschutzgesetz. Auch aktuelle Projekte der EU, die für diese Thematik von Bedeutung sind, wurden einbezogen.

Als Grundlage für jenen Teil der Arbeit, der sich vor allem mit den technischen Methoden der Täter und den Schutzmaßnahmen für die Opfer beschäftigt, dienten in erster Linie entsprechend fachkundige Plattformen im Internet, Security-Reports namhafter Sicherheitsfirmen sowie möglichst aktuelle wissenschaftliche Beiträge von IT-Sicherheitsexperten.

2 Der Identitätsbegriff

Bevor man sich tiefer mit der Problematik des Identitätsdiebstahls und Identitätsmissbrauchs auseinandersetzt, ist es zunächst notwendig, einige wichtige Fragen zu klären:

- Wie genau ist eigentlich der Identitätsbegriff definiert?

- Was kann man unter einer Identität im technischen Sinne verstehen?

- Was ist eine Identität nach geltendem Recht?

Es ist schlicht und ergreifend unerlässlich, vor der Definition der Begriffe Identitätsdiebstahl und -missbrauch zunächst ein grundlegendes Verständnis zu entwickeln.

2.1 Der Identitätsbegriff

Der Identitätsbegriff an sich kann je nach Disziplin bzw Betrachtungswinkel relativ stark divergieren. Trotz seiner geradezu inflationären Verwendung in der modernen Zeit sind es speziell die Human- und Sozialwissenschaften, die sich eingehend mit ihm beschäftigen und auch die meisten Kommentare dazu verfasst haben. Die Psychologie und die Philosophie waren streng genommen die ersten Wissenschaften, die sich mit der Identität an sich sowie der Definition eines Identitätsbegriffs befasst haben:

- Was genau ist nun eigentlich eine Identität?
- Welche Unterschiede zwischen Begriffen aus verschiedenen Disziplinen sind zu beachten?

Geht man rein vom psychologischen Konzept aus, so variiert die Definition je nach Wissenschaftler beziehungsweise Ansatz. Zunächst gäbe es da das Konzept des Psychoanalytikers Erik Homburger Erikson, welcher die Identität wie folgt definiert:

„Ein Zuwachs an Persönlichkeitsreife, den das Individuum am Ende der Adoleszenz der Fülle seiner Kindheitserfahrungen entnommen haben muss, um für die Aufgaben des Erwachsenenlebens gerüstet zu sein.“ Es handelt sich um das Gefühl für ein inneres Sich-Selbst-Gleichsein, ein Wissen um die eigene Unverwechselbarkeit und deren Bejahung.“[3]

Erikson geht also, vereinfacht gesagt, davon aus, dass jedes Individuum im Zuge des Alterungsprozesses unterschiedliche Stufen durchlebt, und nach Abschluss einer Stufe Erfahrungen gewonnen hat, die sich als einzelne Teile sukzessive zu etwas, das man als Identität versteht, zusammenfügen. Dem entgegen steht der Identitätsbegriff nach George Herbert Mead:

3 http://ods3.schule.de/aseminar/entwicklung/identkrise.htm (23.01.2012).

„Identität entwickelt sich; sie ist bei der Geburt anfänglich nicht vorhanden, entsteht aber innerhalb des gesellschaftlichen Erfahrungs- und Tätigkeitsprozesses, das heißt im jeweiligen Individuum als Ergebnis seiner Beziehungen zu diesem Prozess als Ganzem und zu anderen Individuen innerhalb dieses Prozesses.“[4]

Man erkennt also bereits anhand der verschiedenen Konzepte der Psychologie, dass der Begriff Identität gar nicht so selbstverständlich und einfach zu definieren ist, wie man es sich zunächst vielleicht denken mag. Ebenfalls interessant ist der Ansatz des Philosophen Gottfried Wilhelm Leibniz:

„Zwei Dinge sind identisch, wenn sie in allen ihren Eigenschaften ununterscheidbar sind.“ [5]

Nach der Definition von Leibniz wird Identität, vereinfacht ausgedrückt, dadurch geschaffen, dass es keine Gegenstände oder Lebewesen gibt, die sich in all ihren Eigenschaften und Merkmalen gleichen.

Durch diese Ansätze wird verdeutlicht, dass sogar in jenen Disziplinen, in denen der Identitätsbegriff seinen Ursprung hat, keinesfalls eine interdisziplinär einheitliche Definition des Begriffs „Identität“ vorhanden ist. Bereits in den Wissenschaften der Psychologie und der Philosophie herrscht aufgrund disziplinspezifischer Unterschiede ein teilweise komplett unterschiedliches Verständnis der Identität. Umso wichtiger ist es, zu betrachten, was unter einer Identität nach den Maßstäben der Technik und des Rechts verstanden werden kann.

2.2 Die juristische Identität

Eine Definition des Begriffes Identität im juristischen Sinne existiert nicht. Im Kontext des Rechts wird das Wort meist im Zusammenhang mit der Identitätsfeststellung verwendet. Sinn einer solchen Identitätsfeststellung ist der Abgleich der in Ausweisdokumenten enthaltenen personenbezogenen Daten einer natürlichen Person mit der natürlichen Person selbst. Man könnte also eben das Ergebnis jenes Abgleichs noch am ehesten mit dem Begriff „juristische Identität“ gleichsetzen. Im Zusammenhang mit dem österreichischen Strafrecht finden sich die Richtlinien für die Identitätsfeststellung in §118 StPO. Die essentiellen Passagen des §118 StPO im Wortlaut:

„(1) Identitätsfeststellung ist zulässig, wenn auf Grund bestimmter Tatsachen angenommen werden kann, dass eine Person an einer Straftat beteiligt ist, über die Umstände der Begehung Auskunft geben kann oder Spuren hinterlassen hat, die der Aufklärung dienen könnten.

4 http://www.praxisphilosophie.de/mead.htm (30.01.2012).
5 http://www.uni-muenster.de/Leibniz/seite2.html (30.01.2012).

(2) Die Kriminalpolizei ist ermächtigt, zur Identitätsfeststellung die Namen einer Person, ihr Geschlecht, ihr Geburtsdatum, ihren Geburtsort, ihren Beruf und ihre Wohnanschrift zu ermitteln. Die Kriminalpolizei ist auch ermächtigt, die Größe einer Person festzustellen, sie zu fotografieren, ihre Stimme aufzunehmen und ihre Papillarlinienabdrücke abzunehmen, soweit dies zur Identitätsfeststellung erforderlich ist."[6]

Im Rahmen des Strafverfahrens bezeichnet der Begriff Identität also in erster Linie den Namen einer natürlichen Person, ihr Geschlecht, ihr Geburtsdatum, ihren Geburtsort, ihren Beruf und ihre Wohnanschrift. Im Zivilrecht werden die Begriffe Identität und Identitätsfeststellung in Zusammenhang mit der sogenannten Legitimationsprüfung verwendet. Diese umfasst die Prüfung der Identität von Personen und der Echtheit von Unterschriften im Banken- und Kreditwesen, beispielsweise bei der Eröffnung von Konten oder Depots; sie kann aber auch bei zivilrechtlichen Verträgen aller Art durchgeführt werden. Auch bei Beglaubigungen und Beurkundungen durch Notare ist eine solche Prüfung notwendig, im deutschen Beurkungsgesetz etwa wäre dies in § 40 Abs. 4 geregelt.[7] Diese Verifizierung geschieht anhand sogenannter Legitimationspapiere. In Frage kommen dafür nur der Personalausweis oder der Reisepass einer Person, da nur diese alle für die Legitimation notwendigen personenbezogenen Daten enthalten; in diesem Fall den vollständigen Namen, den Geburtstag, den Geburtsort, die Staatsangehörigkeit sowie die Wohnanschrift. Von Institutionen, die dem Geldwäschegesetz unterliegen, müssen zudem die ausstellende Behörde, die Art des Dokuments sowie die Ausweisnummer vermerkt werden[8]. Für Banken ist die Legitimationsprüfung deswegen von enormer Wichtigkeit, weil gerade bei der Verwaltung von Konten die Gefahr von Missbrauch relativ hoch ist; es müssen daher geeignete Maßnahmen getroffen werden, um die Identität sowohl des Kontoinhabers als auch sämtlicher Verfügungsberechtigter zweifelsfrei festzustellen. Banken und Kreditinstitute unterliegen zusätzlich den sehr strengen gesetzlichen Vorgaben des Geldwäschegesetzes. Durch dieses werden Finanzinstitute gezwungen, Angaben zu einer Person zu erheben und deren Identität genauestens zu überprüfen, wie dies etwa in § 40 des österreichischen Bankwesengesetz, kurz BWG, geregelt ist.[9] Ähnlich wie beim Strafrecht, lässt sich also auch im Zivilrecht die Identität am ehesten durch eindeutige personenbezogene Daten definieren, also Namen, Geburtstag, Geburtsort, Staatszugehörigkeit und Wohnanschrift. Zusätzlich aber ist im Zivilrecht die Unterschrift einer Person ein entscheidender Nachweis für deren Identität, was dadurch begründet ist, dass es hierbei auch öfter um Schriftstücke geht, die durch diese Unterschrift erst ihre Rechtswirksamkeit erlangen

6 https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326 (08.02.2012).
7 http://www.gesetze-im-internet.de/beurkg/__40.html (08.02. 2012).
8 http://dejure.org/gesetze/GwG/3.html (08.02.2012).
9 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827 (09.02.2012).

bzw Rechte und Pflichten begründen. Anzumerken ist weiters: Der Begriff der Identität muss sich im Recht nicht nur auf Personen beziehen, er kann sich auch auf Marken oder Internetdomains beziehen. Er kommt also nicht nur im Strafrecht und Zivilrecht vor, sondern auch im Markenrecht -dort aber in einem völlig anderen Kontext. Dieser Rechtsbereich ist ein ausgezeichnetes Beispiel dafür, dass Identitätsdiebstahl und -missbrauch nicht nur auf die Identität natürlicher Personen limitiert ist. Auch die Identität von Marken kann ein durchaus attraktives und lohnendes Ziel darstellen. Daher an dieser Stelle ein kurzer Exkurs ins österreichische Markenschutzgesetz: Was versteht man eigentlich unter einer Marke im rechtlichen Sinn? Gemäß § 1 österreichisches Markenschutzgesetz gilt:

„Marken können alle Zeichen sein, die sich graphisch darstellen lassen, insbesondere Wörter einschließlich Personennamen, Abbildungen, Buchstaben, Zahlen und die Form oder Aufmachung der Ware, soweit solche Zeichen geeignet sind, Waren oder Dienstleistungen eines Unternehmens von denjenigen anderer Unternehmen zu unterscheiden.“[10]

Das bedeutet also, ähnlich wie beispielsweise im Strafrecht oder Zivilrecht steht auch hier im Markenrecht die Einzigartigkeit und Unverwechselbarkeit im Vordergrund. Hier muss es sich nicht nur um den Namen oder die entsprechenden Daten einer natürlichen Person handeln; der Spielraum ist weit größer. Dies zeigt sich auch sehr schön in § 4 Abs. 1 und Abs. 2 des österreichischen Markenschutzgesetzes:

„(1) Von der Registrierung ausgeschlossen sind Zeichen, die:

.....3. keine Unterscheidungskraft haben;

(2) Die Registrierung wird jedoch in den Fällen des Abs. 1 Z 3, 4 und 5 zugelassen, wenn das Zeichen innerhalb der beteiligten Verkehrskreise vor der Anmeldung infolge seiner Benutzung Unterscheidungskraft im Inland erworben hat.“[11]

Das Markenschutzgesetz in Österreich und auch in Deutschland kennt nun seinerseits entsprechende Bestimmungen, um den Identitätsschutz der Marke zu gewährleisten, geregelt in § 14 Abs. 2 Nr. 1 des MarkenG Deutschland[12] oder auch § 10 des österreichischen Markenschutzgesetzes.

Die wichtigen Passagen des § 10 des österreichischen Markenschutzgesetzes im Auszug:

„(1) Vorbehaltlich der Wahrung älterer Rechte gewährt die eingetragene Marke ihrem Inhaber das ausschließliche Recht, Dritten zu verbieten, ohne seine Zustimmung im geschäftlichen Verkehr

10 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827 (09.02.2012).
11 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827 (09.02.2012).
12 http://www.gesetze-im-internet.de/markeng/__14.html (10.02.2012).

1. ein mit der Marke gleiches Zeichen für Waren oder Dienstleistungen zu benutzen (§10a), die mit denjenigen gleich sind, für die die Marke eingetragen ist;
2. ein mit der Marke gleiches oder ähnliches Zeichen für gleiche oder ähnliche Waren oder Dienstleistungen zu benutzen (§10a), wenn dadurch für das Publikum die Gefahr von Verwechslungen besteht, die die Gefahr einschließt, daß das Zeichen mit der Marke gedanklich in Verbindung gebracht wird.“[13]

Doch nicht nur für Marken existieren entsprechende Bestimmungen, um den Schutz ihrer Identität zu gewährleisten, sondern zB. auch für Internet Domains. Rein technisch gesehen, ist eine Domain nichts anderes als die Umwandlung der IP-Adresse eines Internet Servers in eine Zeichenkette, die oftmals eine beliebige Kombination aus Buchstaben und Zahlen ist. Die Domain lässt sich ihrerseits unterscheiden in Top Level Domain und Second Level Domain. Bei der Top Level Domain handelt es sich um die Endung der Domain Zeichenkette. Sie ist normalerweise stellvertretend für ein Land (wie etwa .at für Österreich) oder für einen bestimmten Zweck (wie .com für kommerzielle Angebote). Die für diesen Abschnitt wichtigere Domain ist die Second Level Domain, welche den Mittelteil der Zeichenkette bildet, da diese für die eindeutige und unverwechselbare Identifizierung des Unternehmens oder der Organisation, die die Domain verwendet, verantwortlich ist. Durch die Second Level Domain kann die Domain ihrem Besitzer zugeordnet werden, man kann sie also praktisch als eine Art von Identität ansehen. Kann also die Identität einer Domain ebenfalls „gestohlen“ oder „missbraucht“ werden? Dies ist zu bejahen. Wie sich noch in den späteren Kapiteln der Arbeit zeigen wird, ist auch der „Diebstahl“ von Domain Namen, also der Identität von Domains, ein überaus lukratives Geschäft, das bereits in höchst professionellem Ausmaß betrieben wird. Der rechtliche Schutz von Domain Namen ist etwas schwieriger zu bewirken als bei natürlichen Personen oder auch Marken. Man betrachte die Lage zum Domainrecht in Deutschland:

„Domainrecht ist (noch) Richterrecht - ähnlich dem Wettbewerbsrecht, dem jedoch noch ein schmales Gesetz - das Gesetz gegen den unlauteren Wettbewerb zugrunde liegt. Richterrecht bedeutet auch im Domainrecht, dass aufgrund fehlender gesetzlicher Bestimmungen die Auslegungen den Gerichten überlassen bleiben.“[14]

In nahezu allen europäischen Staaten, so auch in Österreich, ergibt sich der Rechtsschutz einer Domain aus dem Namensrecht, dem Wettbewerbsrecht und auch dem Markenrecht. Darüber hinaus erfordert eine Verfolgung der Täter meistens eine grenzübergreifende Zusammenarbeit mit jenen Ländern, aus denen die Täter operieren. Bestes Beispiel für den Identitätsdiebstahl bei Domains wäre das Phishing, dem im Rahmen dieser Arbeit ein eigenes Kapitel gewidmet wurde.

13 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827 (10.02.2012).
14 http://www.domainrecht-aktuell.de/domainrecht_einleitung.htm (10.02.2012).

Zusammenfassend lässt sich sagen, dass trotz der fehlenden Existenz einer eindeutigen Definition des Identitätsbegriffs im Bereich des Rechts jedenfalls einige Gesetze existieren, aus deren Regelungen sich eine Art rechtliche Identität ableiten lässt. Die Identität wird nach den Maßstäben des Rechts aus jenen personenbezogenen Daten gebildet, die nach den jeweiligen Gesetzen für eine Identitätsfeststellung oder Legitimationsprüfung zur Identifizierung einer natürlichen Person herangezogen werden. Darüber hinaus besitzen nicht nur exklusiv natürliche Personen eine schützenswerte Identität, sondern auch Marken oder Domains, die selber das Ziel von Angriffsformen(wie etwa Phishing) werden können.

2.3 Die Identität im Bereich der Informationstechnologie

Wie auch schon im Recht, so kann auch in den Bereichen Technik und Internet eine Identität als etwas interpretiert werden, das in erster Linie für eine Unterscheidbarkeit und Abgrenzung zwischen Personen sorgt. Vermutlich ein Paradebeispiel für eine Art von Identität im Bereich der Informationstechnologie stellen die sogenannten personenbezogenen Daten dar, die eine Art Schnittstelle zwischen Recht und Technik bilden. Dabei muss es sich nicht zwingend um Daten in digitaler Form handeln. Gemeint sind in diesem Kontext Daten beziehungsweise Informationen, die einer Person eindeutig zugeordnet werden können und dank derer eine Bestimmung und Identifizierung dieser Person möglich ist. Geht es nach dem österreichischen Datenschutzgesetz, kurz DSG 2000, so sind personenbezogene Daten gemäß § 4 Zif. 1:

„1. „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;“[15]

Während im österreichischen Datenschutzgesetz der Begriff „personenbezogene Daten“ mit der Umschreibung „Angaben über Betroffene“ sehr allgemein gefasst ist, ist er im deutschen Bundesdatenschutzgesetz durch die Formulierung „Einzelangaben über persönliche und sachliche Verhältnisse“ schon deutlich klarer definiert.

Der entsprechende Auszug aus § 3 Abs. 1 des deutschen Bundesdatenschutzgesetzes zum Vergleich:

„(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“[16]

15 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (14.02.2012).
16 http://www.gesetze-im-internet.de/bdsg_1990/__3.html (18.02.2012).

Nach Artikel 2 lit. a der Datenschutzrichtlinie 95/46/EG sind personenbezogene Daten „a*lle Informationen über eine bestimmte oder bestimmbare natürliche Person ("betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.“*[17]

Basierend auf der EU Richtlinie für Datenschutz sollen also personenbezogene Daten in erster Linie zur Identifizierung einer Person beitragen, wobei in diesem Zusammenhang Identifizierung als Zuordnung dieser Informationen zu dieser Person verstanden werden kann. Die Angaben stehen also in direktem Zusammenhang zur Identität einer Person. Ein einfaches Beispiel: Man nehme an, zu der Person mit dem Namen Max Mustermann existieren folgende Angaben: Email-Adresse, Geburtsdatum, Geburtsort, Auto, Adresse, Augenfarbe, Telefonnummer, Körpergröße, Gewicht. Gemäß der bereits aufgelisteten Definition von personenbezogenen Daten in diversen Datenschutzgesetzen, würden diese Angaben als personenbezogene Daten gelten und könnten somit in diesem Zusammenhang als Identität der konkreten Person Max Mustermann verstanden werden. Die Identifizierung erfolgt durch die Zuordnung dieser Informationen zu der jeweiligen Person. Dabei wird nicht unterschieden, ob es sich um allgemeine Angaben wie etwa Namen und Geburtsdatum oder um Besitzverhältnisse wie etwa das Auto der Person handelt oder um rein technische Daten wie etwa die Email-Adresse und die Handynummer. Sie alle zusammen bilden die Identität des Max Mustermann und tragen maßgeblich zu seiner Identifizierung bei.

Da die meisten dieser Angaben eher in den Bereich der juristischen Identität fallen(also beispielsweise Namen, Geburtsdatum, Sozialversicherungsnummer oder ähnliche Informationen), die auch ohne die Unterstützung von Informationstechnologie einer Person eindeutig zugewiesen werden können und zu deren Unterscheidbarkeit maßgeblich beitragen, stellt sich nun die Frage, inwieweit sich die technische Identität und vor allem die Identität im Internet von der juristischen Identität unterscheiden. Als technische Identität beziehungsweise als Identität im Internet werden in dieser Arbeit Daten oder Datensätze verstanden, die mit den personenbezogenen Daten oder eben der juristischen Identität einer natürlichen oder juristischen Person untrennbar verbunden sind und die dieser Person durch die Verwendung von Informationstechnologie eindeutig zugewiesen werden können. Beispiele für Elemente einer technische Identität im Sinne dieser Arbeit wären etwa E-Mail-Adresse und E-Mail-Account, Telefonnummer, Mobilfunknummer, Diverse Chipkarten, Kreditkarten, die IP-Adresse eines Rechners, Benutzernamen und Passwörter auf diversen Internetseiten und Plattformen sowie Domainnamen, die von einer Person im Internet registriert

17 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT (18.02.2012).

werden. Es gibt aber aber noch eine Reihe weiterer Datensätze, die speziell in Zusammenhang mit dem Internet als Identität verstanden werden können. So kann auch der von Personen als Alias verwendete Nickname bei diversen Kommunikationsprogrammen im Internet, wie etwa IRC[18] oder ICQ[19], als Identitätsmerkmal interpretiert werden. Gleiches gilt natürlich auch für diverse Internetforen, in denen jede Person unter einem solchen Nickname posten und mit anderen Usern kommunizieren kann. Auch elektronische Unterschriften wie die sogenannte elektronische Signatur, der noch ein Abschnitt dieser Arbeit gewidmet ist, können theoretisch als eine Dimension von technischer Identität interpretiert werden, da sie praktisch das technische Äquivalent zur echten Unterschrift einer Person sind und diese ja zur Unterzeichnung von Urkunden und Verträgen verwendet wird. Streng genommen wäre auch jede Art des Logins, zB. bei Technologien wie E-Banking oder für Internetseiten aus dem Bereich des elektronischen Handels, ein Element von technischer Identität, da das Login mittels Username und Passwort untrennbar mit einer Person verbunden ist, die mithilfe dieses Logins Transaktionen und Geschäfte tätigen könnte.

3 Die Begriffe Identitätsdiebstahl und Identitätsmissbrauch

Nachdem nun näher behandelt wurde, was eigentlich in Technik und Recht als Identität betrachtet werden kann, stellt sich die zentrale Frage, wie genau eigentlich die Begriffe Identitätsdiebstahl und Identitätsmissbrauch definiert sind. Egal, ob in den Medien, in Literatur oder auch Rechtsprechung- beide Begriffe finden häufig Verwendung. Allerdings existiert, wie auch schon beim Identitätsbegriff, keine einheitliche Definition. Ziel dieses Kapitels ist es, sowohl nach rechtlichen als auch technischen Gesichtspunkten die Begriffe Identitätsdiebstahl und Identitätsmissbrauch so gut es geht zu definieren und deren Bedeutung für diese Arbeit hervorzuheben.

3.1 Definition des Begriffs Identitätsdiebstahl

Der Begriff des Identitätsdiebstahls findet vor allem in den Medien weit häufiger Verwendung als jener des Identitätsmissbrauchs, obwohl eigentlich Identitätsmissbrauch die entsprechende Sachlage ein wenig besser treffen würde. Grund dafür ist, dass, rein rechtlich gesehen, beim Identitätsdiebstahl in den meisten Fällen kein tatsächlicher „Diebstahl“ im Sinne landläufigen Verständnisses stattfindet, da das Opfer auch nach der Durchführung des Identitätsdiebstahls im Besitz seiner Identität ist und diese weiterhin verwenden kann. Dementsprechend müssen die

18 http://www.itwissen.info/definition/lexikon/Internet-relay-chat-IRC.html (21.02.2012).
19 http://www.itwissen.info/definition/lexikon/I-seek-you-ICQ.html (21.02.2012).

Begriffe Identitätsdiebstahl und Diebstahl aus rechtlicher Sicht voneinander abgegrenzt werden, denn Diebstahl wird nach § 127 StGB folgendermaßen definiert:

„Wer eine fremde bewegliche Sache einem anderen mit dem Vorsatz wegnimmt, sich oder einen Dritten durch deren Zueignung unrechtmäßig zu bereichern, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“[20]

Es gibt allerdings bestimmte Ausnahmefälle, bei denen die Grenze zwischen diesen Begriffen etwas verschwimmt. Manche Elemente einer technischen Identität nach Kapitel 2.3 können einem Opfer durchaus im Sinne des § 127 StGB „weggenommen“ werden. So kann beispielsweise ein Angreifer, der sich Zugang zum E-Mail-Account des Opfers verschafft, einfach die Zugangsdaten ändern wodurch dem Opfer jeglicher Zugriff verwehrt wird. Das Opfer hat also praktisch seinen Account verloren, er wurde ihm vom Angreifer „weggenommen“.

Die gebräuchlichste Bezeichnung von Identitätsdiebstahl sowohl in den Medien als auch im Internet lautet „*eine missbräuchliche Nutzung personenbezogener Daten einer natürlichen Person durch Dritte*“.[21] An diesen Ansatz ist oftmals die Absicht des Täters geknüpft, sich einen betrügerischen Vermögensvorteil zu verschaffen oder den Ruf des Opfers zu schädigen.

Im Bereich des Rechts existiert keine einheitliche Definition für Identitätsdiebstahl; in den meisten europäischen Ländern werden jene Delikte mit Strafe bedroht, die auf den „Diebstahl“ der entsprechenden Daten folgen. So erfüllt beispielsweise in Österreich die missbräuchliche Nutzung der personenbezogenen Daten in vielen Fällen den Tatbestand des schweren Betrugs. § 147 StGB lautet[22]:

„(1) Wer einen Betrug begeht, indem er zur Täuschung

1. *eine falsche oder verfälschte Urkunde, ein falsches, verfälschtes oder entfremdetes unbares Zahlungsmittel, falsche oder verfälschte Daten, ein anderes solches Beweismittel oder ein unrichtiges Meßgerät benützt,*
2. *ein zur Bezeichnung der Grenze oder des Wasserstands bestimmtes Zeichen unrichtig setzt, verrückt, beseitigt oder unkenntlich macht oder*
3. *sich fälschlich für einen Beamten ausgibt, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.*

(1a) Ebenso ist zu bestrafen, wer einen Betrug mit mehr als geringem Schaden begeht, indem er

20 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (21.02.2012).
21 http://szenesprachenwiki.de/definition/identit%C3%A4tsdiebstahl/ (22.02.2012).
22 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (23.02.2012).

über die Anwendung eines verbotenen Wirkstoffs oder einer verbotenen Methode nach der Anlage der Anti-Doping-Konvention, BGBl. Nr. 451/1991, zu Zwecken des Dopings im Sport täuscht.

(2) Ebenso ist zu bestrafen, wer einen Betrug mit einem 3 000 Euro übersteigenden Schaden begeht.

(3) Wer durch die Tat einen 50 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.“

Wird vom Täter nicht der Zweck verfolgt, sich zu bereichern sondern geht es ihm darum, den Ruf des Opfers zu schädigen, so wäre er je nach Art der Rufschädigung in Österreich entweder nach

§ 111 StGB (üble Nachrede), § 115 StGB (Beleidigung) oder § 297 StGB (Verleumdung) strafbar.[23] Zusätzlich hätte das Opfer die Möglichkeit, Ersatz für den unter Umständen entstandenen Schaden nach § 1330 ABGB zivilrechtlich einzufordern.[24]

Eine andere Definition des Begriffs des Identitätsdiebstahls folgt dem Ansatz, dass nicht die missbräuchliche Verwendung der personenbezogenen Daten mit „Identitätsdiebstahl“ gleichzusetzen ist, sondern dass bereits die Aneignung dieser Daten beziehungsweise die Annahme einer bereits bestehenden Identität alleine als solcher zu bezeichnen ist.[25] Diese Definition bezieht sich also weit mehr auf das „Aneignungsmoment“; die darauf folgende, missbräuchliche Verwendung der Daten ist klar vom „Identitätsdiebstahl“ abzugrenzen, im Mittelpunkt steht vorerst die widerrechtliche Beschaffung der fremden Identität. Bei diesem Ansatz wird auch von „gestohlenen“ Daten ausgegangen, die eindeutig zur Identifizierung einer Person beitragen. Das heißt, es muss sich auch um sogenannte „Identitätsdaten“ handeln.[26] Ähnlich lautet auch die Definition im englischsprachigen Raum, wo von „identity theft“ die Rede ist:

„a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name“[27]

In den USA etwa liegt „identity theft“ nach dem „Identity Theft and Assumption Deterrence Act“ aus dem Jahre 1998 dann vor, wenn eine Person „*knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under*

23 http://www.rechteinfach.at/rechtslexikon/rufschaedigung-83.html (23.02.2012).
24 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001622 (23.02.2012).
25 http://www.boersennews.de/lexikon/begriff/identitaetsdiebstahl/562 (24.02.2012).
26 BSI, Bericht zur Lage der IT-Sicherheit in Deutschland 2011, S. 13.
27 http://en.wikipedia.org/wiki/Identity_theft (24.02.2012).

any applicable State or local law.“[28]

Allerdings ist der im Englischen gebräuchlichere Begriff für Identitätsdiebstahl „identity fraud“, der eher jenem Ansatz näher kommt, welcher Identitätsdiebstahl als missbräuchliche Nutzung der Identitätsdaten versteht:

„Identity fraud is the act of using a stolen identity to obtain goods or services by deception. This usually involves the use of stolen, forged or counterfeit documents such as a passport or driving licence. The term ‘goods or services’ typically includes bank accounts, mortgages, credit cards, retail products, an application for a job or simply dishonest claims for state benefits.“[29]

Von Prof. Dr. Georg Borges wird Identitätsdiebstahl als „*unbefugtes Sichverschaffen einer Identität“*[30] definiert. Ein Identitätsdiebstahl liegt demnach vor, „*wenn der Täter sich die Identität einer Person, also eine Menge an Daten, verschafft, durch die die betreffende Person in einem bestimmten Zusammenhang eindeutig bezeichnet wird.“*[31]

Nach einer genaueren Betrachtung dieser Definitionen des Begriffs des Identitätsdiebstahls in Recht und Technik kann man zusammenfassend von zwei grundverschiedenen Ansätzen sprechen:

- Der erste Ansatz versteht Identitätsdiebstahl als Oberbegriff für jedwede ungesetzliche und unbefugte Verwendung der gestohlenen Identitätsdaten.
- Der zweite Ansatz versteht Identitätsdiebstahl in erster Linie als die unrechtmäßige Aneignung einer fremden Identität, meint also den „Diebstahl“ der Identität selbst. Die Verwendung der gestohlenen Identität ist nach diesem Ansatz der Identitätsmissbrauch, die beiden Begriffe werden nicht, wie im ersten Ansatz, synonym verwendet.

3.2 Definition des Begriffs Identitätsmissbrauch

Eine einheitliche Definition für den Begriff des Identitätsmissbrauchs existiert, wie auch schon beim Identitätsdiebstahl, nicht. Erschwerend kommt hinzu, dass in vielen Fällen die Begriffe Identitätsdiebstahl und Identitätsmissbrauch synonym verwendet werden. Der Gebrauch des Begriff Identitätsmissbrauchs ist weit seltener, obwohl er eigentlich der missbräuchlichen Nutzung personenbezogener Daten weit besser entsprechen würde. Nach einem von vielen Ansätzen, der nicht von einer synonymen Verwendung der Begriffe ausgeht, liegt Identitätsmissbrauch bereits

28 http://www.ftc.gov/os/statutes/itada/itadact.htm#003 (01.03.2012).
29 http://en.wikipedia.org/wiki/Identity_fraud (01.03.2012).
30 Georg Borges, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 11.
31 Georg Borges, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 11.

dann vor, wenn man sich gegenüber andern unbefugt als eine andere Person ausgibt.[32] Borges definiert Identitätsmissbrauch als *„unbefugtes Agieren unter einer Identität“*.[33] Darunter fällt:[34]

- *„das Handeln gegenüber Dritten unter einer anderen als der eigenen Identität“;*
- *„das unbefugte Handeln unter einer eigenen Identität, bei der eine eigene Identität verwendet wird, die aber in dem jeweiligen Kontext nicht zugelassen wird“;*
- *„klassisches missbräuchliches Handeln unter einer fremden Identität“.*

Im Mittelpunkt dieses Ansatzes steht also das unbefugte Handeln beziehungsweise Agieren; es wird also klar zwischen den Begriffen „Identitätsdiebstahl“ und Identitätsmissbrauch differenziert. Sucht man in der Literatur nach einem signifikanten Unterschied zwischen den beiden Begriffen, dann lässt sich folgende Art der Differenzierung finden:

- Identitätsdiebstahl steht für den „Diebstahl“ der Identität, das „sich Beschaffen“ der fremden Identität oder auch das „Erschaffen“ einer fiktiven Identität, unter der nachher ein Missbrauch erfolgen soll.
- Identitätsmissbrauch meint die eigentliche Nutzung der „gestohlenen“ oder „erschaffenen“ Identität, sei es zum Zwecke der eigenen Bereicherung oder zur Diskreditierung einer natürlichen Person.

Es ergeben sich also auch in der Literatur zwei Ansätze, wie sie bereits in Kapitel 3.1 erläutert wurden.

In der Rechtsprechung ist eine einheitliche Definition des Identitätsmissbrauchs praktisch unmöglich, weil er als eine Art abstrakter Oberbegriff für viele verschiedene Tatbestände steht. Darunter fallen, wie auch schon beim Identitätsdiebstahl näher erläutert, beispielsweise der Tatbestand des schweren Betruges oder der Verleumdung. Allerdings gibt es speziell in Deutschland bereits eine beachtliche Zahl an Urteilen, die sich speziell dem Identitätsmissbrauch im Rahmen von elektronischen Handelsplattformen wie etwa ebay oder Amazon widmen. Als rechtliche Grundlage für diese Urteile dient der § 269 des deutschen StGB:

„Fälschung beweiserheblicher Daten

(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.

32 http://www.voip-office.com/voip-sicherheit/identitaetsmissbrauch (03.03.2012).
33 Georg Borges, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 9.
34 Georg Borges, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 9.

(2) Der Versuch ist strafbar.“[35]

Besonderes Aufsehen erreichte dabei ein Fall beim Amtsgericht in Euskirchen, Deutschland. Dabei hatte ein selbstständiger Kaufmann unter dem Namen einer ehemaligen Angestellten ein Konto bei dem Online-Auktionshaus ebay eingerichtet und bot dort in ihrem Namen ein Auto und eine Wohnung an. Zusätzlich hatte er unter ihrem Namen über eine Internetseite CD–Rohlinge im Wert von über 19000 Euro gekauft und auf dem Bestellformular ihre Daten angegeben. Ein Auszug des Urteils des Gerichts[36]:

„Das AG Euskirchen hat den Angeklagten gemäß §§ 269, 53 StGB wegen Fälschung beweiserheblicher Daten in 3 Fällen zu einer Gesamtgeldstrafe von 60 Tagessätzen verurteilt. Das Gericht nimmt an, dass das Einstellen eines Angebots bei eBay einem schriftlich abgefassten Vertragsangebot entspricht. Da der Angeklagte das Angebot unter falschem Namen abgegeben hat, würde bei Wahrnehmung der gespeicherten Daten der Tatbestand der Herstellung einer falschen Urkunde im Sinne von § 267 StGB vorliegen. Hinsichtlich der gespeicherten Daten, würde es sich auch um beweiserhebliche Daten handeln, die zur Täuschung im Rechtsverkehr verändert wurden. Mit den gleichen Argumenten bejaht das Gericht auch die Verfälschung beweiserheblicher Daten im Falle der Online-Bestellung.“

In Deutschland steht also das Kaufen und Verkaufen unter einer fremden Identität im Internet nach Maßgabe der zitierten Regelungen unter Strafe. Im Zusammenhang mit diesen Urteilen ist auch ganz klar die Rede von „Identitätsmissbrauch“, der Begriff ist also in der Rechtsprechung speziell in Zusammenhang mit dem Betrug bei Geschäften im Online-Handel durchaus gebräuchlich.

Wenn man miteinbezieht, wie umfangreich der Begriff der technischen Identität ist, und welche Datensätze alle als Elemente einer Identität im Internet verstanden werden können, dann sind dem Begriff des Identitätsmissbrauchs kaum Grenzen gesetzt. So könnte man beispielsweise bereits das Versenden einer betrügerischen E-Mail unter einer fremden E-Mail Adresse als Identitätsmissbrauch interpretieren; auch hier wäre eine Erfüllung des Tatbestands des Betrugs möglich. Wenn es sich dabei um eine E-Mail im Geschäftsverkehr handelt, läge nach Maßgabe des deutschen Strafrechts sogar eine Fälschung beweiserheblicher Daten vor.

Zusammenfassend zu lässt sich sagen, dass unabhängig von dem Ansatz, dem man folgt eine einheitliche oder auch eine eindeutige Definition der fraglichen Begriffe bislang fehlt. Zwar haben diese Begriffe schon lange Einzug in die Rechtsprechung und die klassische Literatur gehalten, dennoch wird deren Verständnis vorausgesetzt. Vor allem rechtlich gesehen stellt dies ein gewisses Problem dar, da Identitätsdiebstahl und Identitätsmissbrauch je nach Definition als Oberbegriffe für

35 http://dejure.org/gesetze/StGB/269.html (03.03.2012).
36 https://www.a-i3.org/content/view/1119/230/ (03.03.2012).

eine größere Anzahl an rechtlichen Tatbeständen stehen.

4 Identitätsdiebstahl und Identitätsmissbrauch mit Einsatz von Informationstechnologie

In diesem Kapitel werden grundlegende Funktionsweise, Verbreitung und Effizienz diverser auf Informationstechnologie basierender Angriffe untersucht, die dazu benutzt werden können, um an Identitätsdaten zu kommen. Dabei werden zwei Schwerpunkte gesetzt:

- Wie haben sich klassische Angriffe wie zB. Phishing, Pharming oder Spoofing in den letzten Jahren entwickelt und wie groß ist die von diesen Angriffen ausgehende Bedrohung im Hinblick auf Identitätsdiebstahl und Identitätsmissbrauch im Jahr 2012?
- Welche Angriffsmethoden sind im Jahr 2012 besonders gefährlich und welche neuen Trends sind erkennbar?

Eine Untersuchung und Bewertung der in diesem Kapitel aufgelisteten Methoden und Werkzeuge der Angreifer ist notwendig, um nach Abschluss des technischen und rechtlichen Teils der Diplomarbeit sinnvolle Lösungsvorschläge für das Problem Identitätsdiebstahl und Identitätsmissbrauch im Internet ausarbeiten zu können.

4.1 Malware, Keylogger und Crimeware Kit – Die Werkzeuge der Angreifer

Als Malware, oder auch Schadprogramm, werden Computerprogramme bezeichnet, die auf dem Computersystem eines Nutzers unerwünschte und eventuell schädliche Funktionen ausführen. In der IT-Branche dient der Begriff als Sammelbegriff für jede potentiell schädliche und feindselige Form von Software. Malware kann in mehrere verschiedene Arten unterteilt werden, wobei für diese Arbeit nur Computerviren, Trojaner, Würmer und Keylogger von Bedeutung sind:

- Computervirus[37]: Als Computervirus werden Computerprogramme bezeichnet, die sich selbst reproduzieren und von Computer zu Computer weiter übertragen können. Im Gegensatz zu anderer Malware, wie beispielsweise Würmern, benötigt ein Virus ein Wirtprogramm, um seinen Code auszuführen und in den Speicher des Rechners zu schreiben. Computerviren werden daher meist an reguläre Dateien oder Programme angehängt, über die sie sich dann mithilfe eines beliebigen Übertragungsmediums verbreiten lassen. Sobald der Nutzer die infizierte Datei ausführt, wird der Virus aktiv, wobei seine

37 http://www.itwissen.info/definition/lexikon/Virus-virus.html (06.03.2012).

Arbeitsweise je nach Typ variieren kann. In den meisten Fällen ist der Virus dazu konzipiert, andere Funktionen des Rechners lahmzulegen und sich selbst weiter auszubreiten.

- Computerwurm[38]: Ähnlich wie Computerviren sind auch Computerwürmer Programme, die sich selbst vervielfältigen und weiterverbreiten. Der wesentliche Unterschied zu Computerviren besteht darin, dass Würmer kein Wirtprogramm und keine Dateien brauchen, an die sie sich anhängen. Sie verbreiten sich meistens eigenständig entweder über das Computernetzwerk oder Wechseldatenträger, oft auch ohne Interaktion mit dem Nutzer. Der von ihnen angerichtete Schaden hängt stark von ihrem Payload, also ihrem Effekt, ab; allerdings konsumieren auch vermeintlich harmlose Würmer massiv Bandbreite für ihre Weiterverbreitung.
- Trojaner[39]: Als trojanisches Pferd, oder auch kurz Trojaner, bezeichnet man ein Computerprogramm, das als konventionelle Software getarnt ist, aber nach seiner Installation eine vor dem Nutzer verborgene Funktion ausübt. Solche Computerprogramme ähneln meistens sowohl bezüglich ihres Dateinamens als auch ihres Erscheinungsbildes einer bekannten und legitimen Software; einmal installiert und ausgeführt durch den Nutzer verrichten sie ihr Werk. Der Verbreitung von Trojanern sind dank Internet praktisch keine Grenzen gesetzt; sie können über Tauschbörsen, Datenträger, E-Mail oder sogar durch Würmer übertragen werden. Im Gegensatz zu Computerviren und Würmern infizieren Trojaner meist keine anderen Dateien und sie trachten auch nicht danach, sich zu reproduzieren. Ihr Ziel ist es, möglichst lange unentdeckt auf dem Rechner ihres Opfers zu bleiben. Die von ihnen angerichteten Schäden können je nach „Auftrag“ des Trojaners unterschiedlich hoch ausfallen. Oft ermöglichen sie Angreifern direkten Zugang zum System des Opfers, was sie auch zu einem Werkzeug für einen Identitätsdiebstahl oder Identitätsmissbrauch macht. Was Trojaner besonders beliebt und gefährlich macht, ist der Umstand, dass diese je nach Typ auch von einem Angreifer ferngesteuert und upgedated werden können. Man kann sie also, sobald der Rechner des Angriffsziels infiziert ist, je nach Bedarf anpassen.
- Keylogger[40]: Bei Keyloggern handelt es sich um Software oder Hardware, die Tastatureingaben mitprotokolliert und abspeichert. Software-Keylogger speichern sämtliche Tastatureingaben meist in einer Datei, die sie dann über Internet an den Server des Angreifers verschicken. Dabei muss es sich nicht zwingend um eine eigens entworfene

38 http://www.itwissen.info/definition/lexikon/Wurm-worm.html (06.03.2012).
39 http://www.itwissen.info/definition/lexikon/Trojaner-trojan.html (06.03.2012).
40 http://www.produktion.de/it-security-schwachstellen/ (07.03.2012).

Software handeln; der Angreifer kann sich auch beispielsweise eines Trojaners bedienen, mit dessen Hilfe er das BIOS[41] des Zielrechners umstellt, so dass dieses Tastatureingaben speichert. Hardware-Keylogger benötigen einen physischen Zugang zum Zielrechner. Sie werden zwischen Tastatur und Rechner angesteckt und speichern Tastatureingaben in einem internen Speicher. Diese Tastatureingaben können entweder über Funk an den Rechner des Angreifers übertragen werden oder der Hardware-Keylogger wird abgesteckt und seine Daten manuell ausgelesen. Für Identitätsdiebstahl und Identitätsmissbrauch werden solche Keylogger oft eingesetzt, um wichtige Logins und Kennwörter abzufangen.

Speziell in Zusammenhang mit Identitätsdiebstahl und Identitätsmissbrauch wäre eigentlich der Begriff Crimeware anstelle von Malware treffender[42]; ein Begriff für Schadsoftware, die vor allem für kommerzielle Zwecke entwickelt wurde. Malware wird im Jahr 2012 über weite Strecken zur Bereicherung der Angreifer verwendet und nichts beweist diesen Umstand besser als die vermehrte Nutzung eines verhältnismäßig neuen Werkzeugs durch die Angreifer, nämlich der Web Exploit Toolkits. Web Exploit Toolkits (kurz WET oder auch Crimeware Kits) sind, vereinfacht ausgedrückt, Baukasten-Systeme, mit deren Hilfe ein Angreifer mit verhältnismäßig niedrigem Aufwand eine größere Anzahl von Client-Rechnern mit Malware infizieren kann[43]. Zu diesem Zweck nutzt das WET Sicherheitslücken, also Exploits, in Web-Anwendungen aus[44]. Die ersten WETs wurden im Jahr 2006 bekannt, aber speziell im Zeitraum von 2010-2012 stieg deren Nutzung bei großangelegten, Malware-basierten Angriffen rasant an[45]. Ein WET ist relativ einfach, ähnlich wie ein Web Content Management System, aufgebaut: Es besteht aus einem Installationsskript, einem Login-Interface und einem Admin Panel, mit dem die notwendigen Einstellungen vorgenommen werden können. Darüber hinaus enthält jedes WET eine bestimmte Anzahl an Exploits, die vom Ersteller des Kits eingefügt wurden[46]. Ein Angriff mithilfe eines WETs gestaltet sich in der Regel wie folgt:

- Zunächst benötigt der Angreifer eine vermeintlich harmlose Webseite, die den entsprechenden Schadcode enthält und die nach Möglichkeit von einer größeren Anzahl an Clients pro Tag besucht wird. Zu diesem Zweck kann der Angreifer entweder eine bekannte und populäre Webseite mit dem Schadcode infizieren, oder er kann eine eigene Webseite

41 http://www.itwissen.info/definition/lexikon/basic-input-output-system-BIOS-Einfaches-Eingabe-Ausgabe-System.html (12.03.2012).
42 http://de.norton.com/cybercrime-crimeware (12.03.2012).
43 http://blog.zeltser.com/post/1410922437/what-are-exploit-kits (12.03.2012).
44 http://www.pcwelt.de/news/Exploit-Toolkits-Die-Evolution-der-Angriffsbaukaesten-im-Web-1444073.html (12.03.2012).
45 http://www.pcwelt.de/news/Exploit-Toolkits-Die-Evolution-der-Angriffsbaukaesten-im-Web-1444073.html (12.03.2012).
46 http://media.blackhat.com/bh-us-12/Briefings/Jones/BH_US_12_Jones_State_Web_Exploits_WP.pdf (12.03.2012).

erstellen und durch verschiedene Tricks versuchen, Besucher anzulocken. Um die Erfolgschancen zu erhöhen, kann der Angreifer die infizierte Webseite mit Methoden wie Search Engine Optimization (Suchmaschinenoptimierung) noch populärer machen[47]. Solche Methoden zielen darauf ab, die gewünschte Domain möglichst weit oben in diversen Suchmaschinenrankings, zB. bei Google, zu platzieren.

- Zweiter Schritt ist, dass der Angreifer auf dem Webserver dieser Webseite den Schadcode einschleust. Die diesbezüglich beliebteste Methode stellt aktuell die Remote File Inclusion, kurz RFI, dar, bei der fehlerhaft geschriebene Webserverscripte (meist PHP) genutzt werden, um Programmcode in den Webserver einzuschleusen und dort auszuführen[48]. Mithilfe dieser Methode schleust der Angreifer dann einen IFrame[49] ein, der auf den WET-Server des Angreifers verweist.
- Besucht nun ein Client die infizierte Webseite, tritt das Exploitskript in Aktion, welches den Client zunächst analysiert -vor allem dessen Browser-Version und Betriebssystem. Sind alle Daten über das potentielle Opfer gesammelt, so wird anhand dieser Daten der geeignete Exploit ausgewählt und vom WET-Server an den Client übertragen und auf dem Rechner des Opfers ausgeführt[50]. Im Normalfall wird von den meisten WETs der Schadcode serverseitig codiert, um eine Entdeckung zu erschweren. Zusätzlich wird in den meisten Fällen der Rechner des Opfers auf dem WET-Server vermerkt, damit der gleiche Rechner nicht mehrmals attackiert wird.
- Ist der Rechner des Opfers mit dem Exploit bzw Schadcode infiziert, so lädt dieser eine weitere Datei vom WET-Server nach, den sogenannten Loader[51]. Sobald dieser geladen und ausgeführt wurde, sorgt er dafür, dass die eigentliche Malware, in den meisten Fällen ein Trojaner, vom WET-Server geladen und dann am Rechner des Opfers ausgeführt wird.

WETs sind bei Angreifern aus 2 wesentlichen Gründen beliebt: Durch sie kann mit einem Minimum an Aufwand eine verhältnismäßig große Anzahl an Clients infiziert werden und sie liefern, gemessen an dem notwendigen Aufwand, sehr effiziente Ergebnisse. Der Cyber Security Risks Report der Firma HP DVLabs aus dem Jahr 2010 ermittelte, dass die von Angreifern eingesetzten WETs eine durchschnittliche Infektionsrate von 7,5% bis 15% erreichten[52]. Sollte also ein Angreifer erfolgreich eine Webseite infizieren, die beispielsweise 100.000 Besucher pro Monat hat, so würde er mittels WET mindestens 7500 Besucher innerhalb eines Monats infizieren. Darüber hinaus

47 http://searchengineland.com/guide/what-is-seo (12.03.2012).
48 Sicherheit in vernetzten Systemen: 16. DFN Worskhop, S. H-3.
49 http://www.itwissen.info/definition/lexikon/IFrame-inline-frame.html (12.03.2012).
50 http://privacy-pc.com/articles/the-state-of-web-exploit-toolkits-3-how-blackhole-works.html (12.03.2012).
51 http://privacy-pc.com/articles/the-state-of-web-exploit-toolkits-3-how-blackhole-works.html (12.03.2012).
52 2010 HP DVLabs , Full Year Top Cyber Security Risks Report, S. 23.

stellen WETs ein einfaches Werkzeug für technisch weniger versierte Angreifer dar, was sie nur umso gefährlicher macht. Mittels Adminpanel kann der Angreifer das WET beliebig konfigurieren. So kann er beispielsweise einstellen, welche Trojaner vom WET zur Infektion genutzt werden sollen, er kann Statistiken einsehen (wie zB. die Infektionsrate), er kann die über seine Opfer gesammelten Daten (wie Art des Browsers oder Betriebssystem) einsehen oder er kann auch gewisse IP-Adressen und Länderbereiche angeben, die von der Infektion ausgenommen werden sollen[53]. Da die Ersteller der WETs meist ausschließlich von kommerziellen Interessen geleitet werden, werden für die meisten WETs auch Sonderfunktionen gegen einen Aufpreis angeboten. Zusätzlich bringen die Ersteller meist regelmäßige Updates für ihre WETs hinaus, die mit neuen, angepassten Exploits mit einem verbesserten Interface aufwarten. Besonders wichtig sind im

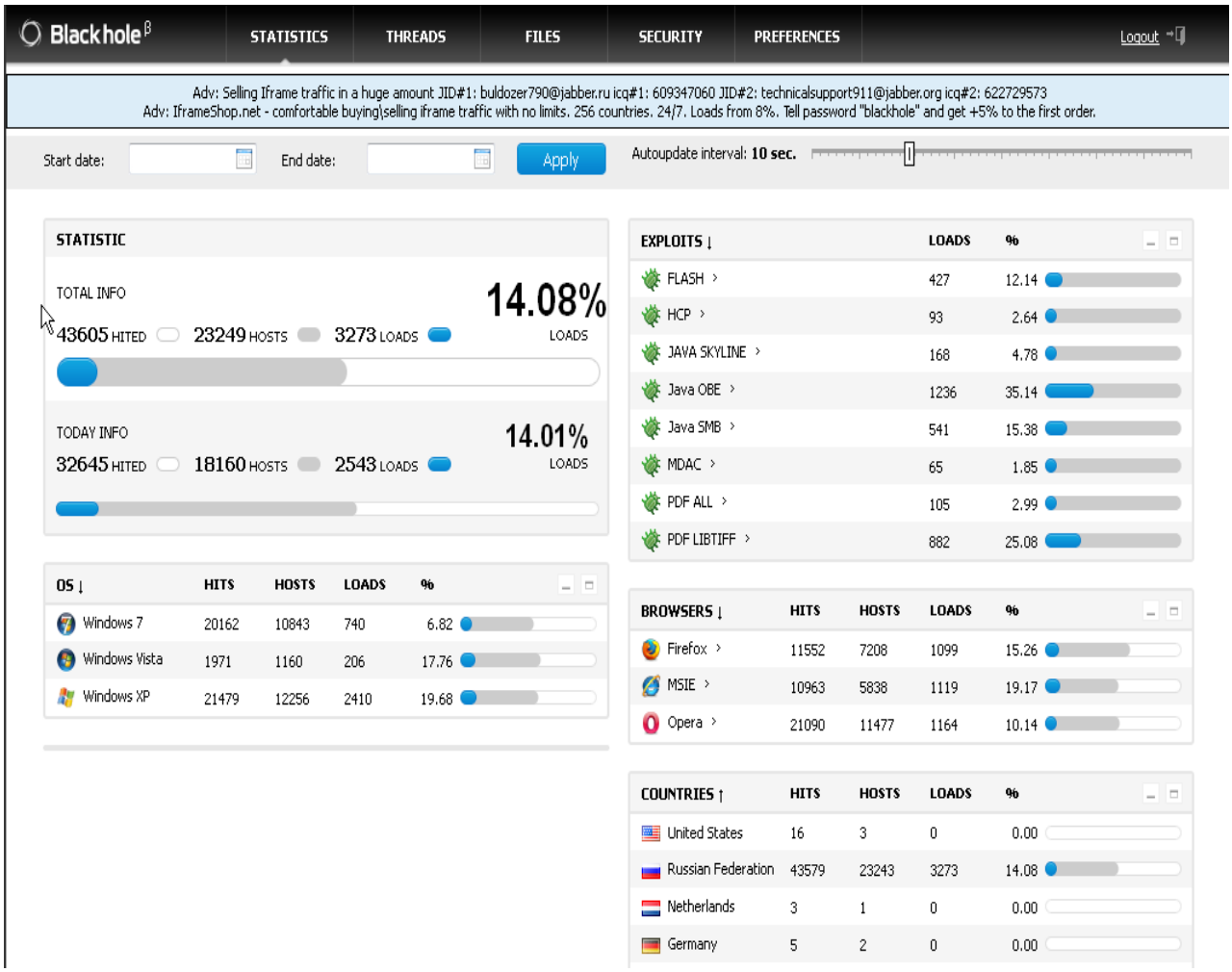

Abbildung 1: Admin Panel des WET Blackhole[54]

53 http://searchsecurity.techtarget.com/tip/Exploit-kits-evolved-How-to-defend-against-the-latest-attack-toolkits (14.03.2012).

54 http://blog.webroot.com/2011/10/ (14.03.2012).

Zusammenhang mit WETs die sogenannten Zero-Day-Exploits[55]. Dabei handelt es sich um Sicherheitslücken in Software oder Web-Anwendungen, die vom Entwickler noch nicht gefunden und somit auch noch nicht gepatcht wurden. Speziell für die Ausstattung von WETs sind solche Zero-Day-Exploits äußerst beliebt, da gegen sie logischerweise noch kein wirksamer Schutz besteht. Für solche Zero-Day-Exploits exisitiert bereits ein durchaus lukrativer Markt, da Hersteller von Malware oder WETs meist bereit sind, für die Entdeckung und Weitergabe solcher Exploits eine große Menge an Geld zu bezahlen[56].

Ein weiteres Angriffswerkzeug, das sich in den letzten 3-4 Jahren zunehmender Beliebtheit erfreute, ist das sogenannte Rootkit. Dabei handelt es sich um ein Softwaretool, mit dem Angreifer ihre Malware tarnen und vor Entdeckung durch das Opfer schützen können[57]. Rootkits werden dazu entwickelt, in das System des Opfers einzudringen und Systemfuntkionen zu manipulieren, um zB. Registrierungsschlüssel, Speichernutzung oder auch Netzwerkverbindungen von Malware zu verstecken. Im Jahr 2012 sind diesbezüglich eigentlich nur mehr Kernel-Mode Rootkits und User-Mode Rootkits von Bedeutung[58]. Kernel-Mode Rootkits dringen bis zum Betriebssystemkern eines Computersystems vor und sind in der Lage, dem Angreifer besondere Funktionen im Kontext des Kernels zur Verfügung zu stellen[59]. So kann ein solches Rootkit beispielsweise Aufrufe von Programmen abfangen, die dem Opfer Dateien oder laufende Prozesse auflisten können. User-Mode Rootkits installieren sich auf einem Rechner meist dann, wenn das Opfer mit Administratorrechten angemeldet ist. Das Rootkit kann dann Sicherheitseinstellungen manipulieren und sich Hintertüren in diversen Prozessen einbauen, wodurch zB. verwendete Netzwerkports oder Systemdienste manipuliert und getarnt werden können. User-Mode Rootkits sind deutlich einfacher aufgebaut als Kernel-Mode Rootkits und können auch entsprechend einfacher durch diverse Antivirenprogramme gefunden werden[60]. In Hinblick auf ihre Verbreitung können Rootkits als Blended-Threat Malware gesehen werden; also als Angriff, der sich aus mehreren verschiedenen Angriffsvektoren zusammensetzt[61]. Für eine erfolgreiche Infizierung eines Rechners sind normalerweise 3 Komponenten notwendig: der Dropper, der Loader und das Rootkit selbst. Der Dropper ist jene Komponente, die die Installation des Rootkits einleitet. Er benötigt für seine Aktivierung die unachtsame Mitwirkung des Opfers, zB. durch einen Klick auf ein infiziertes Bild oder auf einen bösartigen Link. Einmal aktiviert, sorgt der Dropper dafür, dass der Loader ausgeführt wird und

55 http://www.pctools.com/security-news/zero-day-vulnerability/ (14.03.2012).
56 http://derstandard.at/1373512568424/Zero-Day-Exploits-Staaten-kaufen-Sicherheitsluecken (14.03.2012).
57 http://blog.kaspersky.de/was-ist-ein-rootkit/ (14.03.2012).
58 http://www.viruslist.com/de/analysis?discuss=200883623&return=1 (14.03.2012).
59 http://www.techrepublic.com/blog/10-things/10-plus-things-you-should-know-about-rootkits/ (14.03.2012).
60 http://www.securelist.com/en/analysis/168740859/Rootkits_and_how_to_combat_them?print_mode=1 (14.03.2012).
61 http://www.zdnet.de/39199993/meister-der-tarnung-was-man-ueber-rootkits-wissen-sollte/ (14.03.2012).

entfernt sich anschließend selbst. Der Loader nutzt dann eine Schwachstelle im Rechner des Opfers, um das Rootkit zu installieren.

4.2 Man-in-the-Middle und Social Engineering – Begriffsdefinition

Bevor diverse auf Informationstechnologie basierende Angriffsvektoren näher untersucht werden, ist es noch notwendig zwei Sammelbegriffe für bestimmte Angriffsformen kurz zu definieren: Der Man-in-the-Middle-Angriff (kurz MitM) und Social Engineering Attacken. Diese beiden Begriffe werden in Medien und Literatur in Zusammenhang mit diversen Angriffsformen regelmäßig benutzt.

Im Kontext von IT-basierten Angriffsvektoren ist „Man-in-the-middle“ ein Oberbegriff für sämtliche Angriffsformen, bei denen sich ein Angreifer unbemerkt in eine Datenverbindung zwischen zwei Kommunikationspartnern einschaltet[62]. Der Angreifer sitzt dann praktisch „in der Mitte“ zwischen den beiden kommunizierenden Rechnern und kann deren Datenverkehr einsehen und gegebenenfalls auch verändern. Die Arbeitsweise des Angreifers gleicht einer virtuellen Umleitung, er fängt die Datenpakete des Senders auf ihrem Weg ab, überprüft oder manipuliert sie und leitet sie dann an den eigentlichen Empfänger weiter[63]. Angriffsformen, die noch im Rahmen dieser Arbeit untersucht werden und die sich dem „Man-in-the-middle“-Angriff zuordnen lassen, wären zB. MAC-Spoofing, ARP-Spoofing oder auch DNS-Cache-Poisoning.

Social Engineering ist eine Technik, bei der ein Angreifer durch die Täuschung des Menschen hinter dem Rechner eine von ihm gewünschte Reaktion hervorruft (wie zB. die Preisgabe sensibler Daten oder eine finanzielle Transaktion)[64]. Es handelt sich also um einen Sammelbegriff für sämtliche Angriffe, deren Ziel es ist, eine vertrauensvolle Beziehung zu dem Opfer vorzutäuschen, um dieses zu der vom Angreifer erhofften Tätigkeit zu animieren[65]. Alle Social Engineering-Angriffe haben eines gemeinsam: Sie gehen davon aus, dass der Mensch das schwächste Glied in der Kette von Sicherheitsmechanismen ist. Oft erscheint es einem Angreifer einfacher, beim Nutzer selbst den Hebel anzusetzen, anstatt dessen technische Sicherheitsmaßnahmen mit komplizierten Methoden zu umgehen. Man könnte Social Engineering im Kontext von IT auch als virtuelle Täuschung bezeichnen. Da Social Engineering-Angriffe immer auf den Menschen hinter dem Computersystem gerichtet sind, sind gängige technische Schutzmechanismen oft wirkungslos; die beste technische Sicherheitsvorkehrung versagt, wenn sie von einem Menschen freiwillig deaktiviert oder ignoriert

62 https://blog.kaspersky.de/was-ist-eine-man-in-the-middle-attacke/ (14.03.2012).
63 http://www.itwissen.info/definition/lexikon/Man-in-the-Middle-Angriff-man-in-the-middle-attack.html (14.03.2012).
64 http://www.social-engineer.org/ (14.03.2012).
65 http://www.sicherheitskultur.at/social_engineering.htm (14.03.2012).

wird. Langfristig kann nur Schulung und Sensibilisierung der Nutzer Abhilfe schaffen. Angriffsformen, die noch im Rahmen dieser Arbeit untersucht werden und die sich dem Begriff „Social Engineering“ zuordnen lassen, wären zB. Phishing oder auch Scareware.

4.3 Phishing

Phishing ist eine Umschreibung für Angriffsmethoden, deren Ziel es ist durch gefälschte E- Mails oder auch gefälschte Internetseiten dem Angriffsziel sensible Daten (wie etwa Kennwort, Kontonummer, Kreditkartennummer, richtiger Name oder ähnliches) zu entlocken[66]. Es handelt sich um ein englisches Kunstwort, zusammengesetzt aus den Wörtern fishing (Englisch für Angeln) und password (Englisch für Passwort)[67]. Das „h“ in Phishing steht für „Harvesting“, der Begriff steht also für „password harvesting fishing“.

Üblicherweise verwenden die Täter beim Phishing E–Mails und Internetseiten, die in ihrem Design den E-Mails oder Internetseiten bekannter Firmen ähneln, um das Opfer zu täuschen. Um eine möglichst große Anzahl an Opfern mit möglichst niedrigem Aufwand zu attackieren, wird von den Angreifern zunächst eine entsprechend große Zahl an E-Mail-Adressen von potentiellen Opfern gesammelt. Dafür bieten sich den Angreifern mehrere Möglichkeiten[68]:

- Der gezielte Kauf von Adressen bei entsprechenden Firmen, die von ihnen gesammelte Kundendaten weiterverkaufen.
- Der gezielte Kauf von Adressen bei Privatpersonen, die, sei es durch ihre Arbeit in der Firma oder durch Hacking oder andere Tätigkeiten, in deren Besitz gekommen sind.
- Das Durchsuchen von Internet und Datenbanken mittels eigens dafür entwickelter Programme, die automatisch E-Mail Adressen sammeln.
- Das Versenden von Ketten E-Mails.
- Erstellen von E-Mail Adressen nach dem Zufallsprinzip, indem beispielsweise der echte Name oder der Benutzername einer Person mit dem Domainnamen entsprechender Mailanbieter kombiniert wird.
- Gezielte Angriffe auf Datenbanken von Unternehmen, die lukrative Ziele für die Phisher darstellen.

Haben die Angreifer genug Adressen gesammelt, werden Spam-Mails an diese Adressen versendet,

66 http://www.itwissen.info/definition/lexikon/Phishing-phishing.html (14.03.2012).
67 http://www.computerlexikon.com/was-ist-phishing (14.03.2012).
68 http://separaum.de/informationen-zu-phishing/ (14.03.2012).

womit der eigentliche Phishing-Angriff eingeleitet wird. Dazu werden meistens dial-up-Verbindungen mit schnell wechselnden IP-Adressen oder auch fehlerhaft konfigurierte SMTP-Relay-Server, also Mail-Server, die E-Mails von einem Sender annehmen und an Dritte weiterleiten, verwendet[69].

Nach einem Bericht des deutschen BSI werden Phishing-Angriffe ohne Unterstützung durch Malware (also einfache Spam-Mails, die beispielsweise Kunden einer Bank zu einer gefälschten Webseite weiterleiten sollen) seit 2011 praktisch nicht mehr durchgeführt[70]. Die einfachste Form dieser Phishing-Mails ist häufig auch für Laien leicht zu durchschauen, was hauptsächlich an deren eher unprofessioneller Gestaltung liegt. Meistens findet sich in solchen E-Mails eine Vielzahl an Rechtschreibfehlern und auch die gefälschte Internetseite, auf die verwiesen wird, kann relativ einfach als Fake identifiziert werden; sei es, weil das Design des Original nicht wirklich professionell nachgebildet wurde oder weil beispielsweise eine komplett andere Schriftart, beziehungsweise Formatierung gewählt wurde. Darüber hinaus enthalten solche einfachen Phishing-Mails meistens keinen Link auf eine gefälschte Webseite, sondern stattdessen ein eingebettetes HTML-Formular, durch welches das Opfer seine Daten direkt in der E-Mail eintragen soll[71]. Die meisten modernen E-Mail-Clients sind zwar in der Lage, dieses Formular fehlerfrei anzuzeigen, allerdings übermitteln sie entweder die Daten nicht zum Server der Phisher, oder sie zeigen die Datenübermittlung, die von der E-Mail ausgehen soll, sofort als Betrugsversuch an und warnen somit das Opfer[72]. Bei etwas raffinierteren Phishing-Mails wird die Absenderadresse gefälscht, indem beim Standardprotokoll für das Versenden von E-Mails, dem SMTP-Protokoll, die Sendeadresse der echten Firma, die der Phisher nachzuahmen versucht, verwendet wird. Alternativ werden auch oft Absenderadressen mit leichten und nur schwer erkennbaren Typos, also gewollten Schreibfehlern, verwendet. In diesen Phishing-E-Mails sind Links zu einer gefälschten Webseite enthalten, die in ihrem Linktext zwar die echte Adresse des jeweiligen Unternehmens anzeigen, aber das durch HTML-Links oder Javascript unsichtbar gemachte Verweisziel dieser Links bringt das Opfer auf die gefälschte Website[73]. Zwar sind aktuell die meisten E-Mail-Clients bereits in der Lage, das Opfer zu warnen, falls die angezeigte Adresse und das Verweisziel voneinander abweichen, allerdings gibt es auch hier Möglichkeiten zur Umgehung dieser Sicherheitsmaßnahme. Ein Beispiel dafür wäre die Registrierung von Domains, die sich nur durch kleine Typos von der echten Internetseite unterscheiden, die bei nicht vollkommen sorgfältigem Lesen nur schwer erkennbar sind. Phishing-Angriffe dieser Art zählen zu den Social-Engineering-Angriffen, da die

69 Mertinkat, Phishing im Internet, S. 3.
70 BSI, Die Lage der IT-Sicherheit in Deutschland 2011, S. 14.
71 http://www.edv-workshop.de/nav/them/phish/phish02.htm (14.03.2012).
72 http://www.sicher-im-internet.at/schule/spam.html (14.03.2012).
73 http://www.ruhr-uni-bochum.de/nds/research/top/ipi/phishing/indexm.html (14.03.2012).

Opfer durch Täuschung dazu veranlasst werden, freiwillig ihre Daten preiszugeben. Um den psychologischen Druck auf die Opfer zu erhöhen, wird ihnen von den Angreifern in den Phishing-Mails oft ein pseudowichtiger Grund für den Klick auf den Link suggeriert. Einerseits lässt sich dadurch das Opfer in eine Stresssituation bringen, in der es über kleine Abweichungen in der Absenderadresse oder im Linktext hinweg sieht; andererseits sind Menschen eher bereit, vertrauliche Daten preiszugeben, wenn dies einem subjektiv wichtigen Zweck dient und unerlässlich ist. Beispiele könnten gefälschte Mitteilungen einer Bank oder eines elektronischen Zahlungsdienstes (wie etwa Paypal) sein, die darauf verweisen, dass deren Sicherheitssystem überarbeitet wird, wodurch eine Aktualisierung der Daten des Opfers notwendig wäre[74]. Ansonsten würde der Account des Opfers gesperrt und eine neuerliche Anmeldung wäre erforderlich. Moderne Phishing-Angriffe finden freilich ausschließlich mit Unterstützung von Malware statt[75]. Am gebräuchlichsten ist dabei die Verwendung von Trojanern, da sich diese am besten für den Diebstahl von Benutzerdaten eignen. Üblicherweise werden Trojaner als Anhang in den Phishing-Mails mitversendet und stellen für das Opfer auf den ersten Blick eine authentische und nützliche Anwendung dar[76]. Dabei kann es sich beispielsweise um eine vermeintlich harmlose Dokumentdatei oder Bilddatei handeln. Öffnet das Opfer dann diesen Anhang, so wird das Schadprogramm auf seinem Rechner installiert und läuft bei diesem im Hintergrund unbemerkt mit. Ist der Trojaner erst einmal auf dem Rechner installiert, so wird er im Rahmen eines Phishing-Angriffs meist für folgende Zwecke benutzt:

- Abfangen und Umleiten der Kommunikation zwischen dem Benutzer und der Internetpräsenz eines legitimen Unternehmens, zum Beispiel im Rahmen von E-Banking.
- Aufzeichnen von Benutzereingaben und Kennwörtern.

Für letzteren Zweck kann anstelle eines Trojaners auch beispielsweise ein Keylogger verwendet werden. Die so gesammelten Daten werden dann von den Trojanern automatisch in sogenannten Dropzones im Internet abgelegt, wo die Phisher sie bequem einsammeln können[77]. Eine weitere Angriffsmethode beim Phishing, die sich nach Zahlen der Anti Phishing Working Group seit 2012 zunehmender Beliebtheit erfreut, ist das sogenannte Shared Virtual Server Hacking[78]. Als Shared Virtual Server werden Webserver bezeichnet, die eine große Anzahl an Domains verwalten. Möchte

74 http://www.spam-info.de/2741/achtung-vor-phishing-mails-wegen-eines-angeblich-eingeschraenkten-paypal-kontos/ (17.03.2012).
75 http://www.focus.de/digital/internet/tid-15755/angriff-auf-hotmail-konten-die-tricks-der-phishing-betrueger_aid_442332.html (17.03.2012).
76 http://derstandard.at/1389857414133/Bundeskriminalamt-warnt-vor-Phishing-Betruegern-Viren-und-Trojanern (17.03.2012).
77 http://pi1.informatik.uni-mannheim.de/filepool/media/20090114-spiegel-de-cyber-verbrecher-gehen-it-forschern-in-die-falle.pdf (17.03.2012).
78 APWG, Global Phishing Survey: Trends and Domain Name Use in 1H2012, S. 8.

ein Phisher mit möglichst wenig Aufwand eine größere Anzahl an Webseiten kompromittieren, so bricht er in einen Shared Virtual Server ein, lädt eine einzelne Kopie seines Phishing-Contents auf den Webserver und ändert dann die Konfiguration des Webservers, so dass der Content des Angreifers zu jedem Hostnamen, den der Shared Virtual Server verwaltet, hinzugefügt wird[79]. Nach erfolgreichem Abschluss dieses Angriffs werden anstelle der vom Webserver verwalteten Webseiten die Phishing-Seiten angezeigt.

Die beliebtesten Ziele für Phisher sind im Normalfall Finanzdienstleister, Kreditinstitute, Banken und elektronische Zahlungsdienste. Auch elektronische Handelsplattformen (wie beispielsweise eBay oder Amazon) stellen lukrative Ziele dar. Zusätzlich wurden vor allem im Zeitraum zwischen 2010 und 2012 auch soziale Netzwerke (wie etwa Facebook) zu einem durchaus beliebten Angriffsziel für Phishing-Attacken[80]. Dies liegt vor allem daran, dass diese Netzwerke eine Fundgrube für persönliche Daten darstellen, die für die Phisher mittlerweile äußerst wertvoll sind. Solche Daten können meistens lukrativ weiterverkauft oder für einen Identitätsdiebstahl oder Identitätsmissbrauch genutzt werden. Darüber hinaus können Phisher bei Social Networks mittels gehackter oder selber erstellter Accounts ihren Spam verhältnismäßig einfach verbreiten[81]. Neben Finanzdienstleistern, E-Commerce-Anbietern und Sozialen Netzwerken sind auch Internet Service Provider und Online Spiele Ziele für Phishing und Identitätsdiebstahl, aber selbst sogenannte Filesharing-Seiten (wie etwa RapidShare). Entscheidend ist dabei auch die Größe der Unternehmen, je größer der Kundenstamm, umso mehr potentielle Opfer und umso höher die Chance auf Erfolg. Die Statistik und die Zahlen der Sicherheitsfirma Kaspersky Lab aus dem Jahr 2010 zeichnen ein eindeutiges Bild, was die beliebtesten Ziele der Phisher betrifft[82]:

Demnach betrafen mit 52,2% mehr als die Hälfte aller von Kaspersky Lab verzeichneten Phishing-Angriffe im ersten Quartal 2010 den elektronischen Zahlungsdienst PayPal. Erst mit gehörigem Abstand folgt das elektronische Auktionshaus eBay mit 13,3%. Bereits auf dem vierten Platz folgt dann das soziale Netzwerk Facebook. Der größte Anteil der Spam-Mails kommt mit 31,7% aus Asien, was vor allem daran liegt, dass eine Strafverfolgung in Ländern wie beispielsweise China äußerst schwierig ist[83]. Für die Verbreitung des Spams werden mittlerweile von den Phishern auch gehackte E-Mail-Accounts bei beliebten Anbietern wie etwa Yahoo oder Gmail benutzt, da dort inaktive Accounts lange Zeit nicht gelöscht werden und stattdessen einfach unbenutzt

79 http://storageservers.wordpress.com/2013/04/29/shared-web-hosting-servers-become-soft-target-for-mass-phishing-attacks/ (17.03.2012).
80 http://www.kaspersky.com/about/news/spam/2010/Facebook_ranks_fourth_in_the_Top_10_most_popular_phishing_targets_in_the_first_quarter_of_2010 (17.03.2012).
81 http://www.computerweekly.com/news/2240187487/FBI-warns-of-increased-spear-phishing-attacks (17.03.2012).
82 http://www.kaspersky.com/about/news/spam/2010/Facebook_ranks_fourth_in_the_Top_10_most_popular_phishing_targets_in_the_first_quarter_of_2010 (17.03.2012).
83 http://www.kaspersky.com/about/news/spam/2010/Spam_Report_May_2010 (17.03.2012).

weiterbestehen. Ein ähnliches Bild zeichnen die Zahlen der Anti Phishing Working Group, kurz

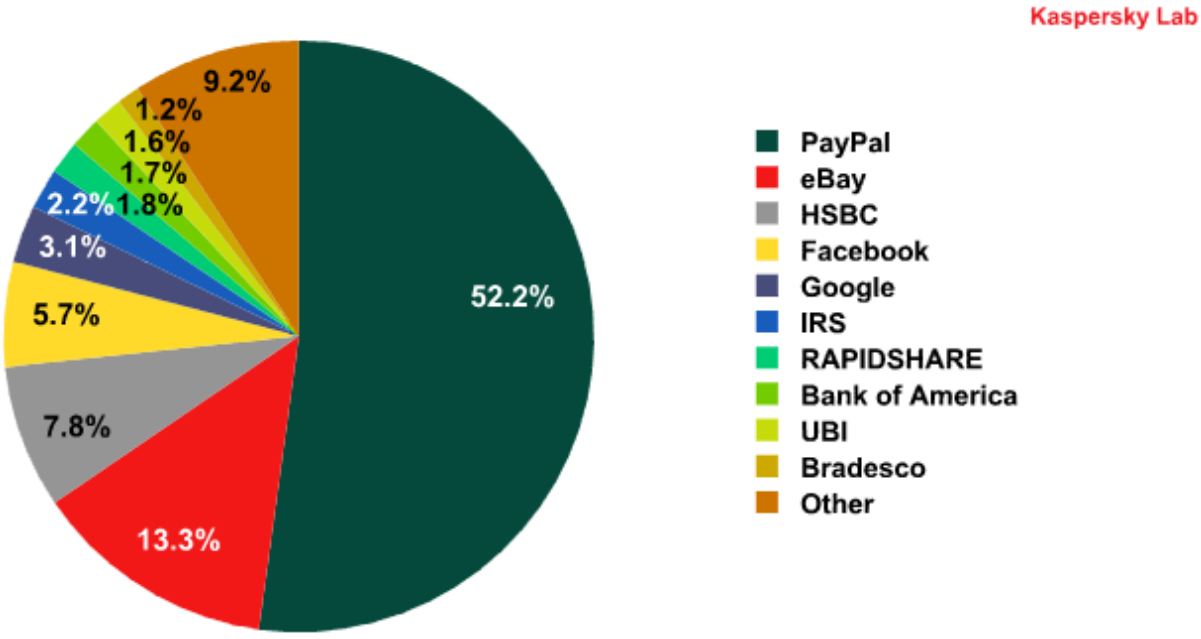

Abbildung 2: Statistik der beliebtesten Phishing Ziele von Kaspersky Lab[84]

APWG, aus dem ersten Quartal 2010[85]. 37% aller von der APWG verzeichneten Phishing-Attacken in diesem Zeitraum betrafen Payment Services wie PayPal, 35,9% betrafen den Bereich des E-Banking. Demnach waren allein 72,9% aller Phishing-Attacken ausschließlich gegen elektronische Finanzdienste gerichtet. Am meisten zugenommen gegenüber 2009 hatten Angriffe im Sektor „Other“, welcher stellvertretend für Social Networks und Online Spiele steht. Auf diesen fielen 17,9% der Phishing Attacken. Vergleicht man die Zahlen der Sicherheitsfirma Kaspersky Lab aus dem ersten Quartal 2010 mit ihren Zahlen aus dem vierten Quartal 2012, so lassen sich einige neue Trends im Hinblick auf Phishing erkennen[86]. Im vierten Quartal 2012 betrafen nur mehr 22,87% aller Phishing-Attacken elektronische Zahlungsdienste oder E-Banking, 18,44% betrafen den Bereich des elektronischen Handels. 24,46% aller Angriffe betrafen Social Networks, was gegenüber 2010 einen Anstieg von fast 19% bedeutet. Zusätzlich hatte sich eine neue Angriffsfläche gebildet, nämlich Suchmaschinen (wie beispielsweise Google). Durch eine Manipulation solcher Dienste fällt es den Phishern leichter, ihre Opfer auf gefälschte und mit Malware infizierte Webseiten umzuleiten. So betrafen 14,14% aller Phishing-Attacken Suchmaschinen. Nach dem

84 http://www.securelist.com/en/analysis/204792117/Spam_evolution_January_March_2010 (17.03.2012).
85 APWG, Phishing Activity Trends Report 1st Quarter 2010, S.7.
86 http://www.securelist.com/en/analysis/204792276 (17.03.2012).

Bericht der APWG aus dem vierten Quartal 2012 ergibt sich ein ähnliches Bild, wenngleich sich die Zahlen nicht ganz so stark geändert haben[87]. Demnach betrafen 66,5% aller Phishing Attacken immer noch die Sektoren Payment Services und E-Banking, was lediglich eine Abnahme von 6,4% bedeutet. Beachtlich ist aber, dass 27,48% aller Angriffe den Sektor „Other" betrafen, was eine Zunahme der Attacken vor allem auf Social Networks und Online Spiele bedeutet. Die meisten Phishing-Webseiten wurden mit 73,93% in den USA gefunden, die meisten Spam-Mails stammten (wie bereits 2010) aus Asien. Sowohl Kaspersky Lab als auch die APWG sehen einen neuen Trend bei Phishing von 2010 bis 2012[88]: den Fokus der Angreifer auf Identitätsdiebstahl anstelle des schnellen finanziellen Gewinns. Online Spiele und Social Networks werden als Angriffsziele zunehmend interessanter, da ein immer schneller wachsender Markt für die dort gestohlenen persönlichen Informationen und Daten im Internet existiert. In den Bereichen des E-Banking und des E-Commerce zielen Angreifer nicht mehr ausschließlich darauf ab, dem Opfer in möglichst einfacher Weise finanziellen Schaden zuzufügen, sie bemächtigen sich zunehmend seiner persönlichen Daten, die von den Banken oder den elektronischen Handelsplattformen gespeichert werden.

Die durch Phishing und den damit einhergehenden Identitätsdiebstahl verursachten Schäden sind immer noch enorm. Eine Reihe von Studien des Marktforschungsinstituts Gartner belegt, wie hoch die finanziellen Verluste durch Phishing alleine in den USA über die letzten Jahre gestiegen sind:

- Bereits 2005 verursachte Phishing in den USA einen Schaden von rund 2,5 Milliarden Dollar.[89]
- 2007 ist der Schaden auf über 3 Milliarden Dollar angestiegen; um die 3,6 Millionen Menschen meldeten einen Betrug durch Phishing.[90] Hauptgrund für diesen rasanten Anstieg wäre laut Gartner der gezielte und professionelle Einsatz von Malware bei den Phishing Attacken gewesen. Allein 32% der Opfer gaben als Ursache für den finanziellen Schaden den Diebstahl ihrer Kreditkarteninformationen an.
- Bis 2008 stieg die Anzahl der Phishing Attacken auf den Endbenutzer um 40% an. Gartner erkennt darin eine Änderung der Strategie der Phisher, man geht dazu über eine größere Masse an Phishing-Angriffen zu versenden und nimmt dafür auch einen geringeren finanziellen Gewinn pro Opfer in Kauf.[91]

In England wurde allein im Jahr 2005 von der „Association for Payment Clearing Services" ein

87 APWG, Phishing Activity Trends Report 4th Quarter 2012, S. 7.
88 http://docs.apwg.org/reports/apwg_trends_report_q2_2012.pdf (17.03.2012).
89 http://www.gartner.com/it/page.jsp?id=565125 (21.03.2012).
90 http://www.gartner.com/it/page.jsp?id=565125 (21.03.2012).
91 http://www.gartner.com/it/page.jsp?id=936913 (21.03.2012).

Schaden von 23,2 Millionen Pfund festgestellt, ein Anstieg von etwa 90% gegenüber 2004, wo der Schaden noch 12,2 Millionen Pfund betrug.[92] In Deutschland befassten sich das BKA und der IT-Branchenverband Bitkom mit den Gefahren und Schäden durch Phishing. Laut BKA verursachte Phishing im Jahr 2005 einen Schaden von etwa 10 Millionen Euro.[93] Im Jahr 2009 stieg die Anzahl der gemeldeten Phishing-Fälle um 64%, auch hier setzte der gleiche Trend wie in den USA ein. Die durchschnittliche Schadenssumme betrug nur mehr etwa 4000 Euro pro Fall, während am Beginn des Jahres 2009 vom BKA noch 10000 Euro pro Fall registriert wurden.[94] Auch in Deutschland nahm also die Masse an Phishing Attacken zu, der Schaden pro Opfer wurde aber eher geringer. Im Jahr 2010 verzeichneten das BKA und Bitkom einen Gesamtschaden von 17 Millionen Euro durch Phishing und den damit verbundenen Identitätsdiebstahl in Deutschland.[95] Die Anzahl der gemeldeten Phishing-Fälle stieg gegenüber 2009 um 71% an, die Schadenssumme verringerte sich aber auf 3500 Euro pro Fall. Hauptgrund für die immer weiter wachsende Anzahl an Phishing-Angriffen ist laut BKA das steigende technische Niveau von Schadprogrammen, die mittlerweile dazu in der Lage sind, auch anspruchsvollere Sicherungsmechanismen zu umgehen. Es wird also in IT-Know-How „investiert". In Österreich wurden im Jahr 2006 lediglich 60 Phishing-Fälle bearbeitet; allerdings geht das BMI hier von einer relativ hohen Dunkelziffer aus, da vermutlich eine Vielzahl an Phishing-Angriffen nicht angezeigt, bzw gemeldet wurde.[96] Bereits 2007 sprach das Bundeskriminalamt in Österreich von 381 gemeldeten Phishing-Fällen, der Gesamtschaden belief sich auf 1 Million Euro und auch hier wurde von einer relativ hohen Dunkelziffer ausgegangen.[97] Bei einer Enquete zum Thema Cyber-Crime und Internetsicherheit im Jahr 2011 in Klagenfurt bezifferte das BK Österreich einen Schaden von 5,7 Millionen Euro im Jahr 2010, der durch Internetbetrug verursacht wurde; also auch hier ein gewaltiger Anstieg, wobei als Grund für den Anstieg des Schadens eine sehr naive und wenig informierte Klientel genannt wurde.[98] Eine Studie des Sicherheitsdienstleisters Trusteer bestätigt, dass die Phisher seit 2008 ihre Strategie geändert haben und nun darauf setzen, eine größere Anzahl an Angriffswellen auf vielversprechende Ziele zu versenden, auch wenn dabei der Gewinn pro Opfer sinkt. Laut dieser Studie erfolgten 2009 rund 800 Angriffswellen gegen jedes Unternehmen, das ein lohnendes Ziel darstellte.[99]

92 http://www.finextra.com/news/fullstory.aspx?newsitemid=15013 (21.03.2012).
93 http://www.heise.de/security/meldung/BKA-Phishing-Faelle-haben-weiter-zugenommen-998992.html (21.03.2012).
94 http://www.heise.de/security/meldung/BKA-Phishing-Faelle-haben-weiter-zugenommen-998992.html (21.03.2012.
95 http://www.heise.de/security/meldung/BKA-und-Bitkom-17-Millionen-Euro-Schaeden-durch-Phishing-1073002.html (21.03.2012.
96 http://www.bmi.gv.at/cms/BMI_OeffentlicheSicherheit/2006/03_04/files/Phishing.pdf (21.03.2012).
97 https://www.a-i3.org/content/view/1314/214/ (21.03.2012).
98 http://futurezone.at/digitallife/5989-5-7-millionen-euro-schaden-durch-internetbetrug.php (21.03.2012).
99 http://www.trusteer.com/sites/default/files/Phishing-Statistics-Dec-2009-FIN.pdf (21.03.2012).

4.4 Cross-Site-Scripting/XSS

Durch das immer stärker ansteigende Technologieniveau im Internet bilden sich leider auch neue Angriffsvektoren, die eine Gefahr für Nutzer und Betreiber von Webanwendungen gleichermaßen darstellen. Eine der neuen Bedrohungen, die das Web 2.0 mit sich brachte, ist das sogenannte Cross-Site-Scripting. Beim Cross-Site-Scripting handelt es sich um eine Angriffsform, bei der der Angreifer Sicherheitslücken in Webanwendungen oder auf Webseiten ausnutzt, um von ihm angefertigten Script-Code zu platzieren[100]. Der Ausdruck „Cross-Site“ bezieht sich auf den Umstand, dass der Angriff zwischen den jeweiligen Aufrufen einer Website stattfindet, der Buchstabe X steht in der englischen Sprache für das Wort „cross“[101]. Es handelt sich um eine Form der „code injection“[102]: Eine verwundbare Webanwendung nimmt Daten an, die von einem Benutzer stammen, und leitet diese dann an den Browser weiter, ohne den Inhalt zu prüfen. Auf diese Weise kann der Angreifer seinen Skript-Code indirekt an den Browser des Opfers versenden und diesen auf der Seite des Clients ausführen. Der Browser des Endnutzers hat keine Möglichkeit, zu überprüfen, ob das Skript vertrauenswürdig ist oder nicht und führt dieses aus, wodurch nun das bösartige Skript Zugriff zu allen sensiblen Daten bekommt, die vom Browser im Zuge der Nutzung der betreffenden Website gespeichert wurden (wie etwa cookies). Beim Identitätsdiebstahl mit XSS-Unterstützung ist die Methode am gebräuchlichsten, bösartiges JavaScript mittels einer manipulierten URL auf einer verwundbaren Website einzuschleusen[103]. Das bösartige JavaScript erscheint dann dem Opfer in einem vertrauenswürdigen Kontext in seinem Browser. Theoretisch kann hierfür jede vom Browser interpretierbare Skriptsprache verwendet werden; am meisten verwendet wurde von den Angreifern allerdings in den Jahren 2010-2012 JavaScript aufgrund seiner starken Verbreitung und hohen Popularität[104]. Der Hauptgrund für solche XSS-Schwachstellen ist meistens eine mangelhafte Eingabe-Validierung, also das mangelhafte Filtern von Benutzereingaben im Browser.

Beim Cross-Site-Scripting lassen sich 2 Angriffsarten unterscheiden[105]:

- persistent/beständig;

- nicht-persistent/reflexiv.

100https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29 (23.03.2012).
101http://www.itwissen.info/definition/lexikon/cross-site-scripting-XSS.html (23.03.2012).
102 https://www.owasp.org/index.php/Code_Injection (23.03.2012).
103 http://weblogs.asp.net/jgalloway/archive/2011/04/28/preventing-javascript-encoding-xss-attacks-in-asp-net-mvc.aspx (23.03.2012).
104 http://www.pcwelt.de/ratgeber/Internet-Gefahr-So-funktionieren-Cross-Site-Scripting-CSRF-150841.html (23.03.2012).
105 http://www.webmasterpro.de/server/article/sicherheit-cross-site-scripting.html (23.03.2012).

Die vermutlich gefährlichere dieser 2 Varianten ist das persistente oder auch beständige Cross-Site-Scripting. Beim persistenten XSS wird der Schadcode des Angreifers permanent in die Webanwendung oder die Webseite eingebettet, vom Webserver gespeichert und bei jedem Besuch durch den Browser des Clients ausgeführt[106]. Dies erfolgt in mehreren Schritten[107]:

- Zunächst wird die Webanwendung oder die Webseite des Angriffsziels, zB. die Webpräsenz einer Bank, aufgerufen und über eine XSS-Lücke der Schadcode injiziert.
- Sobald nun ein Nutzer diese Webanwendung aufruft, wird ihm die mit dem bösartigen Skript-Code infizierte Webseite geschickt, die die Sicherheitseinstellungen seines Browsers nicht weiter verletzt.
- Einmal auf dem Rechner des Nutzer angelangt, sendet nun der XSS-Schadcode Daten an den Rechner des Angreifers, ohne dass der Nutzer eine Chance hätte, dies zu bemerken.

Hauptziel von persistentem Cross-Site-Scripting sind normalerweise Webanwendungen wie Gästebücher, Diskussionsforen oder auch Social Networks, bei denen die Eingaben der Benutzer gespeichert und im HTML-Format für andere Nutzer angezeigt werden. Ein einfaches Beispiel: Man nehme ein Online-Diskussionsforum, auch „Message Board“ genannt, bei dem keine geeignete Prüfung der Benutzereingaben erfolgt. Die Benutzereingaben werden serverseitig in einer Datenbank gespeichert. Die Nutzer sind anonym unterwegs, ihre echten Namen und ihre E-Mail-Adressen sind selbstverständlich geheim. Der Angreifer könnte sich nun einfach in diesem Forum registrieren und einen Beitrag verfassen, an den er durch <script>*schadhafter Code*</script> einen bösartigen Skript-Code anhängt, der für die anderen Nutzer nicht sichtbar ist; ihnen wird nur der Beitrag angezeigt. Jedesmal, wenn nun ein Besucher dieses Forums seinen Beitrag aufruft, wird das Skript automatisch von dessen Browser ausgeführt und erfüllt seinen Auftrag, der je nach Wunsch des Angreifers unterschiedlich ausfallen kann. In diesem Fall könnte das Skript zum Beispiel die richtigen Namen und E-Mail-Adressen der anderen Nutzer auf deren Rechner einsehen und diese Informationen an den Rechner des Angreifers weitersenden. Persistentes Cross-Site-Scripting ist vor allem deswegen so gefährlich, weil der Schadcode des Angreifers beim bloßen Betrachten durch den Nutzer bereits automatisch ausgelöst wird; es ist also keinerlei weitere Aktivität auf Nutzerseite notwendig. Des weiteren gibt es bei dieser Angriffsform fast keinen wirksamen Schutz auf der Nutzerseite.

Beim nicht-persistenten oder auch reflexiven Cross-Site-Scripting erfolgt der Angriff durch eine präparierte URL, in deren Parametern Schadcode eingefügt wurde[108].Wird diese URL durch den

106 http://www.webmasterpro.de/server/article/sicherheit-cross-site-scripting.html (24.03.2012).
107 http://excess-xss.com/ (24.03.2012).
108 http://www.webmasterpro.de/server/article/sicherheit-cross-site-scripting.html (24.03.2012).

Nutzer ausgeführt, so wird der Schadcode an den Server der Webanwendung gesendet und dort temporär bei der Generierung der Internetseite eingeschleust. Er wird allerdings nicht dauerhaft gespeichert, daher auch der Ausdruck „nicht-persistent“. Der XSS-Skript-Code wird nun vom Server im Kontext der vertrauenswürdigen Internetseite an den Browser des Nutzers gesendet, der das bösartige Skript ausführt. Es wird also die XSS-Attacke vom Server an den Nutzer reflektiert -daher auch „reflexives“ XSS. Auch hier erfolgt der Angriff in mehreren Schritten[109]:

- Der Nutzer klickt zunächst auf eine manipulierte URL und ruft über diese die gewünschte Webanwendung, zB. wieder die Webseite einer Bank, auf.
- Der Webserver der Bank schickt nun die mit dem XSS-Skript-Code infizierte Seite an den Browser des Benutzers zurück, von wo aus der Schadcode nun Daten stiehlt und an den Server des Angreifers weitersendet.

Das nicht-persistente Cross-Site-Scripting ist aktuell die am häufigsten verwendete Variante von XSS-Angriffen und wird vor allem beim Phishing eingesetzt[110]. Ein Identitätsdiebstahl durch nicht persistentes XSS hat gegenüber einer herkömmlichen Phishing-Attacke den Vorteil, dass serverseitige Schutzmaßnahmen wie etwa das SSL-Protokoll (ein Sicherheitsmechanismus der noch später in dieser Arbeit genauer untersucht wird) ausgehebelt werden, da hier der Angriff durch ein XSS-Skript im Kontext der sicheren Website erfolgt[111]. XSS-Lücken für nicht-persistentes Cross-Site-Scripting entstehen oft bei dynamischen Webseiten, wo Benutzereingaben ungefiltert durch den Server zurückgegeben werden, wo also wieder eine dynamische Webesite als Resultat generiert wird[112]. Häufig werden von Angreifern sogenannte „Fuzzer“ benutzt, um XSS-Lücken schnell und einfach zu finden. Dabei handelt es sich um Tools, die für das Testen von Software konzipiert sind[113]. Diese Fuzzer können dann systematisch in alle Felder von Formularen einer Webanwendung oder auch in alle URLs, die mit Parametern arbeiten, den Skript-Code eintragen und speichern die Ergebnisse in einem Log, wodurch der Angreifer mit verhältnismäßig wenig Aufwand XSS-Schwachstellen ausfindig machen kann[114]. Ein gutes Beispiel für reflexives XSS wäre die Kompromittierung von Suchmaschinen wie etwa Google oder auch der Suchfunktion auf diversen Webseiten: Wenn man einen Suchbegriff in Form eines Strings eingibt, dann wird üblicherweise eine Ergebnisseite erzeugt, die den jeweiligen Suchbegriff noch einmal gesondert anzeigt, meistens in der Form „Sie suchten nach *Suchbegriff*“. Eine XSS-Lücke würde nun entstehen, wenn die

109 http://excess-xss.com/ (24.03.2012).
110 http://security.stackexchange.com/questions/19373/what-is-the-danger-of-reflected-cross-site-scripting (24.03.2012).
111 http://www.computerweekly.com/tip/Cross-site-scripting-explained-How-to-prevent-XSS-attacks (24.03.2012).
112 http://www.pcwelt.de/ratgeber/XSS-kann-ueberall-lauern-Internet-Gefahr-150849.html (24.03.2012).
113 https://www.owasp.org/index.php/Fuzzing (24.03.2012).
114 Walter Kriha, Roland Schmitz, Sichere Systeme: Konzepte, Architekturen und Frameworks, S. 19.

Suchmaschine keine geeignete Maskierung für die Ergebnisseite verwendet, wenn also die Maskierung nicht nur Text sondern zB. auch JavaScript erlauben würde. Der Webanwendung kann nämlich der Suchbegriff über eine URL übergeben werden, was etwa folgendermaßen aussehen könnte[115]:

https://www.beispielsuchmaschine.com/?suche=*Suchbegriff*

Ein normales Suchergebnis würde dann etwa so aussehen:

 „Sie suchten nach“ *Suchbegriff*

Bei einer ungenügenden Maskierung könnte das Ergebnis allerdings so aussehen:

 „Sie suchten nach“ <script>*schadhaftes Skript*()</script>

Es wird also ein schadhaftes Skript durch eine präparierte URL dem Server der Webanwendung übergeben und direkt durch das Suchergebnis an den Nutzer reflektiert, dessen Browser es dann ausführt[116].

Um die von Cross-Site-Scripting ausgehende Bedrohung bis Herbst 2012 einschätzen zu können, wurden in erster Linie Zahlen und Statistiken von namhaften Sicherheitsfirmen, deren Spezialgebiet die Sicherheit für Webanwendungen und Webapplikationen ist, untersucht. Betrachtet man die Entwicklung dieser Zahlen über die letzten zwei Jahre sowie die Statistiken zum jetzigen Zeitpunkt (November 2012), so kann man nur zu dem Schluss kommen, dass die Zahl an XSS-Attacken eher zu- als abnimmt. Im Rahmen des Web Application Security Statistics Project des Web Application Security Consortium wurden 2007 und 2008 detaillierte Statistiken zu Lücken in Webanwendungen erhoben. Als Methoden dienten dafür unter anderem Black Box Tests, White Box Tests, Security Audits und automatische Scans. Nach der Statistik aus dem Jahr 2008 waren XSS-Lücken mit 43% die am stärksten verbreiteten Schwachstellen in Webapplikationen[117]. In der Statistik aus dem Jahr 2007 waren es noch 41%. White Hat Security, eine namhafte Sicherheitsfirma, die sich auf den Schutz von Webseiten spezialisiert hat, veröffentlichte zuletzt im Sommer 2012 ihren Website Security Statistics Report. Nach dessen Zahlen wiesen 55% aller untersuchten Webseiten eine XSS-Schwachstelle auf, was gleichbleibende Zahlen gegenüber dem Report aus dem Jahr 2011 und einen Anstieg von 2% gegenüber 2010 bedeutet[118]. Gemäß diesem Bericht ist XSS die größte Gefahr für Webanwendungen im Jahr 2012. Die Sicherheitsfirma Firehost, die auf die Sicherheit von Clouds spezialisiert ist, präsentierte im Rahmen ihrer Web Application Attack Statistics aus dem Jahr 2012 ähnliche Ergebnisse. 35% aller von Firehost erfassten Angriffe auf Webanwendungen im dritten

115 http://www.exploit-db.com/wp-content/themes/exploit/docs/10342.pdf (24.03.2012).
116 https://www.owasp.org/index.php/Testing_for_Cross_site_scripting (24.03.2012).
117 http://projects.webappsec.org/w/page/13246989/Web%20Application%20Security%20Statistics (24.03.2012).
118 https://www.whitehatsec.com/assets/WPstats_summer12_12th.pdf (24.03.2012).

Quartal 2012 waren XSS-Attacken, womit Cross-Site-Scripting die am stärksten verbreitete Angriffsmethode war[119]. Im vierten Quartal 2012, beginnend mit Oktober, waren es bereits 57%, was einen Anstieg von 22% innerhalb nur eines Quartals bedeutet. Alle genannten Sicherheitsfirmen sind sich einig, dass die von XSS ausgehende Gefahr im Jahr 2012 eher ansteigt, was mehrere Gründe hat: der Wunsch von Unternehmen nach möglichst billigen Lösungen für Webapplikationen, die zunehmende Verbreitung von JavaScript und der Umstand, dass eine solche

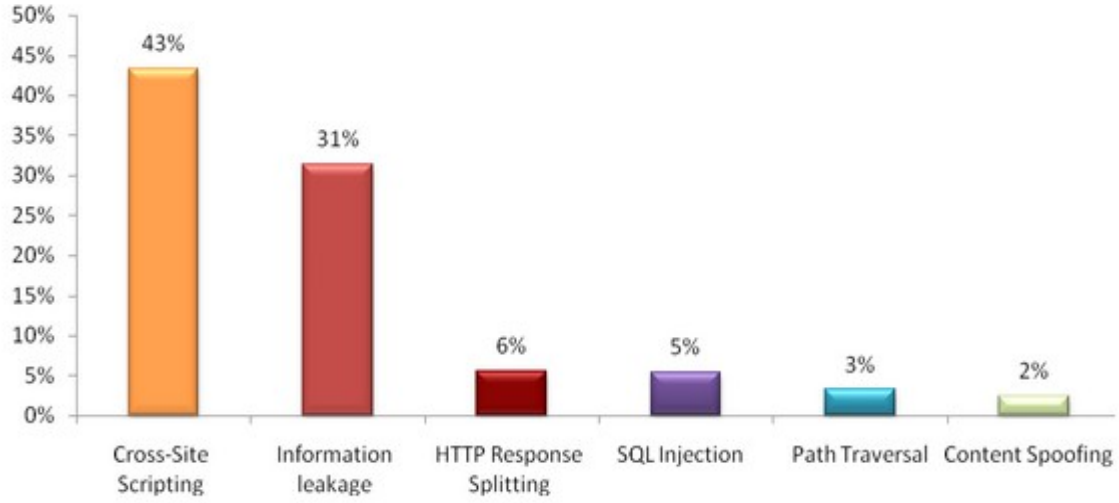

Abbildung 3: Statistik des Web Application Security Consortiums[120]

XSS-Attacke mit verhältnismäßig wenig Aufwand sehr effiziente Ergebnisse für den Angreifer

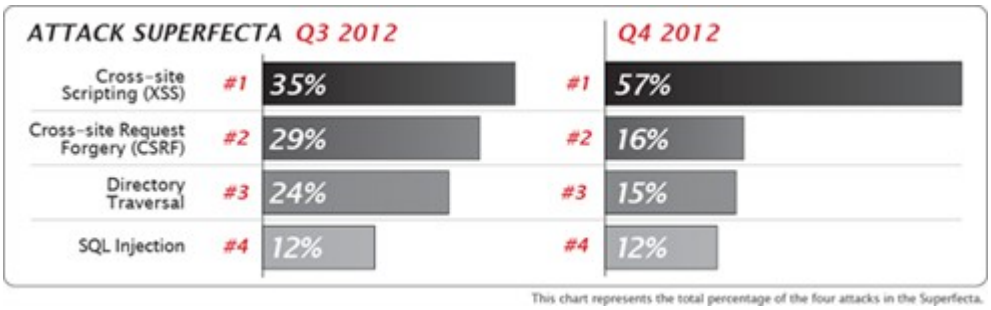

Abbildung 4: Statistik der Sicherheitsfirma Firehost[121]

119 http://www.firehost.com/company/newsroom/web-application-attack-report-fourth-quarter-2012 (24.03.2012).
120 http://projects.webappsec.org/w/page/13246989/Web%20Application%20Security%20Statistics (24.03.2012).
121 http://www.firehost.com/company/newsroom/web-application-attack-report-fourth-quarter-2012 (26.03.2012).

liefert[122]; mithilfe der bereits erwähnten Fuzzer und eines Webapplication Scanners kann jeder informationstechnisch ausreichend Versierte relativ schnell und effizient XSS-Lücken in Webanwendungen finden und eine solche Attacke ausführen. Für Identitätsdiebstahl und Identitätsmissbrauch stellen XSS-Angriffe also ein durchaus geeignetes und gefährliches Werkzeug dar.

4.5 Pharming/DNS-Cache-Poisoning

Ebenso wie bei Phishing handelt es sich auch bei Pharming um eine Methode, die auf eine betrügerische Erlangung von Daten abzielt. Der Name entstand durch eine Vermischung der beiden Begriffe „phishing“ und „farming“[123]. Der wesentliche Unterschied zum Phishing liegt darin, dass das Phishing eine Social Engineering-Attacke ist; also eine Attacke, bei der das Opfer durch Täuschung zur Preisgabe sensibler Daten gebracht wird. Pharming benötigt hingegen keinerlei Mitwirkung des Opfers. Bei Pharming ist der Angriff rein technischer Natur. Ziel ist dabei nicht das Opfer selbst, sondern die technische Infrastruktur, die die Benutzung des Internets ermöglicht. Ähnlich wie bei Phishing wird auch hier das Opfer auf eine von den Betrügern präparierte Webseite umgeleitet, allerdings durch eine Manipulation der DNS-Anfragen des Internet-Browsers des Opfers. Dabei wird die Originaladresse im Browser dergestalt verändert, dass das Opfer ohne sein Wissen und selbst bei einer korrekten Eingabe der Adresse auf die gefälschte Seite umgeleitet wird. Um dies genauer zu erläutern, ist eine kurze Beschreibung des Domain Name Systems notwendig. Eigentlich besteht jede Internetadresse aus einer Zahlenfolge, der sogenannten IP-Adresse. Zum Zwecke der Vereinfachung -da Menschen sich Begriffe einfacher merken können als Zahlenfolgen- wurde das Domain Name System erschaffen, welches es Benutzern ermöglicht, durch die Eingabe von begrifflichen Domainnamen anstelle von IP-Adressen im Browser auf die gewünschte Internetseite zu gelangen[124]. Das DNS ist zuständig für Anfragen zur Namensauflösung, man kann es sich auch wie ein elektronisches Telefonbuch vorstellen. Wenn der Benutzer den Namen einer Domain in den Browser eingibt, zum Beispiel www.testseite.at, sendet dessen Rechner eine Anfrage an einen DNS-Server, der als Antwort die zugehörige IP-Adresse liefert. Zusätzlich befindet sich auf jedem Rechner die sogenannte Hosts-Datei, eine lokale Textdatei, die eine Liste der bereits besuchten IP-Adressen enthält[125]. Diese Datei ist für die fixe Zuordnung von Domainnamen zu den

122 http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/66879-hacker-konzentrieren-sich-auf-programmiersprachenfehler/ (24.03.2012).
123 http://www.itwissen.info/definition/lexikon/Pharming-pharming.html (26.03.2012).
124 http://www.itwissen.info/definition/lexikon/domain-name-system-DNS-DNS-System.html (26.03.2012).
125 http://blog.botfrei.de/2012/01/hosts-datei-was-ist-das-oder-warum-sieht-die-sparkassenseite-so-merkwurdig-aus-windows/ (26.03.2012).

entsprechenden IP-Adressen zuständig. Bevor der Rechner des Nutzers eine Anfrage an einen DNS-Server sendet, prüft er zuerst die Hosts-Datei auf die vom Nutzer gewünschte Domain. Ist diese bereits in der Liste enthalten, so wird die Internetseite direkt nach der Namensauflösung durch die Hosts-Datei aufgerufen und es wird der DNS-Server nicht kontaktiert. Ist die Domain noch nicht in der Liste eingetragen, so wird eine Anfrage an den zuständigen DNS-Server gesendet. Die wichtigsten Komponenten des DNS sind:

- Domain-Namensraum
- Nameserver
- Resolver

Der Domain-Namensraum (auch Domain Name Space) hat eine hierarchische, baumförmige Struktur[126]. Die Spitze des Baumes wird als Wurzel oder auch root bezeichnet. Ausgehend von ihr kommen zunächst die sogenannten Top-Level-Domains, wie etwa .com, .at, .de etc. Die Top-Level-Domains spalten sich dann in die Second-Level-Domains auf, die sich dann ihrerseits in weitere

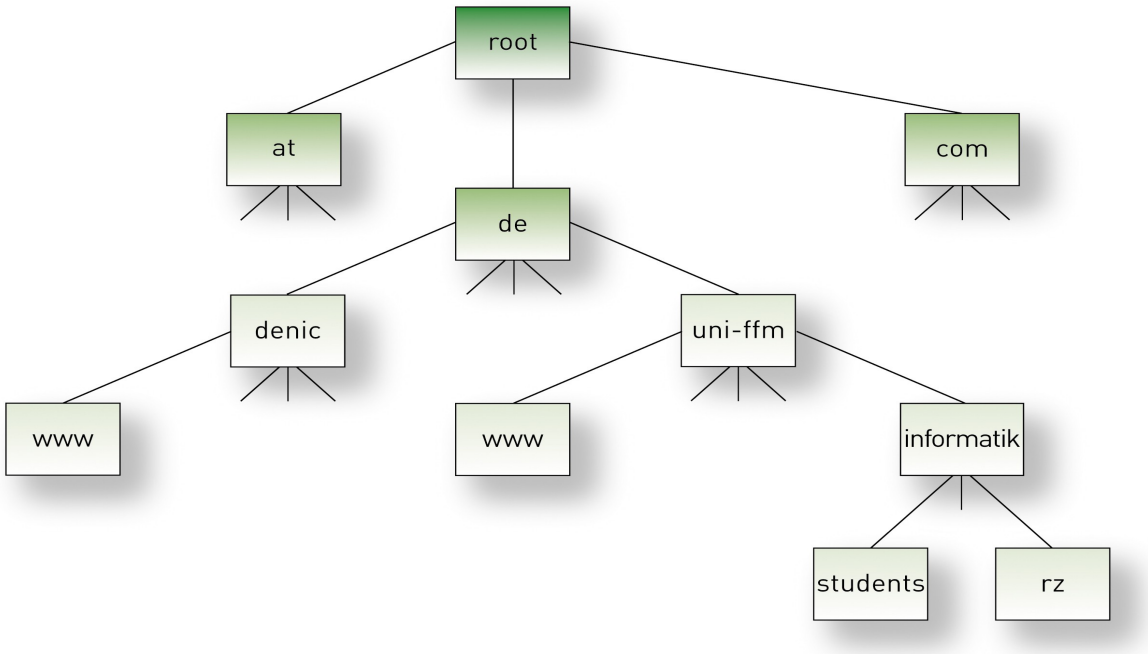

Abbildung 5: Beispielhafte Abbildung des Domain Name Space in Baumform[127]

Unterdomains aufspalten. Wichtig dabei ist, dass die jeweiligen Unterdomains der ihnen übergeordneten Domain zugeordnet sind; gemäß der obigen Abbildung wäre also zB. uni-ffm

126 http://technet.microsoft.com/en-us/library/cc958962.aspx (26.03.2012).
127 http://www.denic.de/hintergrund/nameservice/dns.html (26.03.2012).

eine .de Domain. Die zweite wichtige Komponente des DNS sind die sogenannten Nameserver; jene Server, die sich um die Namensauflösung kümmern. Jeder dieser Nameserver verwaltet jeweils eine Zone, die einem Knoten in dieser baumförmigen Struktur entspricht und alle zu diesem Knoten gehörenden Unterdomains beinhaltet[128]. Ein Nameserver ist somit für „seine“ Zone autoritativ. Außerdem „kennt“ jeder Nameserver den in dieser Baumstruktur direkt unter ihm sowie direkt über ihm befindlichen Nameserver. Die dritte Komponente des DNS sind die Resolver. Dabei handelt es sich um clientseitige Programme, die für den DNS-Teilnehmer (bzw. den Nutzer) die Anfragen zur Namensauflösung an die Nameserver senden[129]. Die Resolver senden die Anfrage zunächst immer an den DNS-Server, dem sie fix zugeordnet sind. Bei der Arbeitsweise des Resolvers unterscheidet man rekursive und iterative DNS-Anfragen. Der wesentliche Unterschied besteht darin, dass bei einer rekursiven Anfrage der Resolver die komplette Arbeit dem ihm zugeordneten Nameserver überlässt, während er sich hingegen bei einer iterativen Anfrage selber um die Auflösung der Anfrage kümmert[130]. Wenn ein Nameserver eine rekursive DNS-Anfrage bekommt, die er selber nicht auflösen kann, so kontaktiert er solange andere Nameserver, bis er dem Resolver das gewünschte Resultat liefern kann. Zur Veranschaulichung dieser Arbeitsweise ein fiktives Beispiel[131]:

- Man nehme an ein beliebiger Nutzer will die fiktive Internetseite www.testseite.at aufrufen.
- Zuerst überprüft der Resolver des Rechners, ob die IP-Adresse für diese Domain in seiner Hosts-Datei ist. Ist dies nicht der Fall, sendet er eine rekursive Anfrage an den für den Rechner des Nutzers zuständigen DNS-Server.
- Dieser DNS-Server prüft, ob er für die Zone dieser Domain autoritativ ist. Ist er nicht autoritativ, so prüft er noch seine lokale Hosts-Datei auf die gewünschte IP-Adresse. Falls auch seine Hosts-Datei die IP-Adresse nicht enthält, sendet er eine Anfrage an einen der 13 Root-Server, um die IP-Adresse der Domain herauszufinden.
- Der Root-Server erkennt, dass .at die Top-Level-Domain der gewünschten Domain ist und sendet nun die Kontaktdaten eines .at-Nameservers an den DNS-Server .
- Der DNS-Server kontaktiert diesen für die .at-Zone autoritativen Nameserver, der ihm daraufhin die Kontaktdaten eines für die testseite.at-Zone autoritativen Nameservers sendet.
- Der DNS-Server kontaktiert diesen für die testseite.at-Zone autoritativen Nameserver und erhält von diesem als Antwort die IP-Adresse für die vom Nutzer gewünschte Internetseite.

128 http://www.itwissen.info/definition/lexikon/Name-Server-name-server.html (26.03.2012).
129 http://www.itwissen.info/definition/lexikon/Resolver-resolver.html (26.03.2012).
130 http://www.elektronik-kompendium.de/sites/net/0901141.htm (26.03.2012).
131 http://technet.microsoft.com/de-de/library/cc775637%28v=ws.10%29.aspx (26.03.2012).

- Der DNS-Server sendet die IP-Adresse an den Resolver, womit die rekursive DNS-Anfrage aufgelöst wird.
- Um das DNS-Netz zu entlasten, speichern beide (sowohl der Resolver als auch der DNS-Server) die IP-Adresse für die besagte Domain in ihrer Hosts-Datei, um sie bei einer erneuten Anfrage schneller zur Verfügung zu haben.

Bei der iterativen Anfrage bekommt der Resolver als Antwort von dem entsprechenden DNS-Server einen Verweis auf den zuständigen Nameserver; das heißt, hier kümmert sich nicht der DNS-Server direkt um die Auflösung der Anfrage, sondern der Resolver „geht“ selbst von Nameserver zu Nameserver, bis er die gewünschte Antwort hat. In der Praxis sind rekursive Anfragen weit häufiger, vor allem weil viele Nameserver mit iterativen Anfragen nichts anfangen können[132]. Die Manipulation genau solcher DNS-Anfragen ist Ziel des DNS-Cache-Poisoning oder auch DNS-Spoofing. DNS- Cache-Poisoning-Angriffe zielen darauf ab, die Daten in der Hosts-Datei des Resolvers oder in der Hosts-Datei seines DNS-Servers zu verändern oder neue, falsche Daten hinzuzufügen[133]. In den meisten Fällen verändert ein erfolgreicher Angriff die Hosts-Datei von beiden. Normalerweise läuft ein solcher Angriff in folgenden Schritten ab[134]:

- Ein Nutzer möchte von seinem Rechner aus wieder die Internetseite testseite.at aufrufen.
- Der Resolver des Rechners überprüft, ob die IP-Adresse für diese Domain in seiner Hosts-Datei vorhanden ist. Nachdem er in seiner Hosts-Datei die IP-Adresse nicht findet, sendet er eine DNS-Anfrage an den entsprechenden DNS-Server.
- Was nun erfolgt, ist eine normale rekursive DNS-Anfrage; der DNS-Server prüft auch hier zuerst, ob er für die gewünschte Domain autoritativ ist und nachdem er festgestellt hat dass dem nicht so ist, durchsucht er seine lokale Hosts-Datei nach der IP. Hat er keinen Erfolg, kontaktiert er einen der 13 Root Server, der ihm daraufhin mitteilt, welcher Nameserver für .at autoritativ ist.
- Der DNS-Server kontaktiert den für .at autoritativen Nameserver, der ihm daraufhin mitteilt, welcher Nameserver für testseite,at autoritativ ist. Daraufhin kontaktiert der DNS-Server diesen Nameserver.
- Der autoritative Nameserver möchte eine Antwort an den DNS-Server senden und genau an dieser Stelle erfolgt nun die Cache-Poisoning-Attacke: Der Angreifer versucht, mit seinem DNS-Server die Kommunikation zwischen dem für den Resolver des Nutzers zuständigen DNS-Server und dem für testseite.at autoritativen Nameserver abzufangen; dies mit dem

132 http://technet.microsoft.com/de-de/library/cc775637%28v=ws.10%29.aspx (26.03.2012).
133 http://www.networkworld.com/news/tech/2008/102008-tech-update.html (26.03.2012).
134 http://blbaliyase.blogspot.com/2009/11/dns-cache-poisoning.html (27.03.2012).

Ziel, seinen DNS-Server als autoritativen Server auszugeben und dadurch dem DNS-Server gefälschte Daten als Antwort zu senden. Um dies zu erreichen, muss der Angreifer zunächst die sogenannte „Transaction-ID“[135] knacken, eine 16 Bit lange Nummer, durch welche DNS-Anfragen geschützt sind. Um sicherzustellen dass ausreichend Zeit für das Knacken der Transaction-ID vorhanden ist, steht dem Angreifer ein breites Spektrum an Methoden zur Verfügung. Im Jahr 2012 am gebräuchlichsten sind DoS-Attacken oder auch DNS-Amplification-Attacken, die mithilfe von Botnetzen ausgeführt werden. Sowohl solche DoS-Attacken als auch Botnetze werden noch in einem der folgenden Kapitel dieser Arbeit näher erläutert. Im Hinblick auf dieses Beispiel reicht es, zu erwähnen, dass eine solche DoS-Attacke einen Nameserver überlasten kann, indem eine größere Anzahl von Anfragen nahezu zeitgleich an ihn gesendet wird[136]. Der Angreifer verschafft sich also die notwendige Zeit, indem er den für testseite.at autoritativen Nameserver mit einer solchen Attacke lahmlegt.

- Nachdem der autoritative Nameserver durch die DoS-Attacke lange genug verlangsamt wurde und der Angreifer nun die ID für die DNS-Anfrage in Erfahrung gebracht hat, kann er auf die Anfrage mit einem gefälschten Datensatz antworten.
- Im letzten Schritt des Beispiels antwortet der DNS-Server des Angreifers mit einer falschen IP-Adresse zur eigentlich richtigen Domain. Der DNS-Server speichert die falsche IP-Adresse zu testseite.at in seiner Hosts-Datei und sendet die Antwort an den Resolver, der ebenfalls die falsche IP-Adresse in seine Hosts-Datei einträgt.

Die Konsequenzen dieses Angriffs: Sowohl die Hosts-Datei des Resolvers als auch jene des DNS-Servers sind nun „vergiftet“, beide speichern die falsche IP-Adresse für die Webseite testseite.at so lange, bis der Eintrag in der Hosts-Datei wieder nach einer gewissen Zeit gelöscht wird. Jeder Versuch des Nutzers, diese Webseite zu besuchen, wird ihn dank des falschen Eintrags in der Hosts-Datei seines Resolvers auf die Seite des Angreifers umleiten. Zusätzlich wird jede DNS-Anfrage nach dieser Domain von anderen Nutzern, deren Rechner dem gleichen DNS-Server zugewiesen sind, eine Antwort mit der gefälschten IP-Adresse nach sich ziehen.

Eine weitere sehr beliebte Möglichkeit des DNS-Cache-Poisoning basiert auf einer rekursiven DNS-Anfrage, die vom Angreifer selbst ausgeht. Die Rahmenbedingungen für diesen Angriff[137]:

- Der Angreifer ist selber im Besitz der Domain, nach der er beim DNS-Server anfragt.
- Der Angreifer ist im Besitz des Nameservers, der für die Auflösung der Anfrage zuständig

135 http://resources.infosecinstitute.com/dns-cache-poisoning/ (27.03.2012).
136 http://www.itwissen.info/definition/lexikon/denial-of-service-DoS-DoS-Attacke.html (27.03.2012).
137 https://cert.uni-stuttgart.de/ticker/article.php?mid=1476 (27.03.2012).

ist.

- Der Nameserver wurde so manipuliert, dass er an die Antwort für den DNS-Server noch einen gefälschten Datensatz anhängt.
- Dieser gefälschte Datensatz besteht aus dem Namen seines Angriffsziels, beispielsweise dem Domainnamen einer Bank, sowie der IP-Adresse einer gefälschten Seite im Besitz des Angreifers.

Der Angreifer sendet zunächst eine DNS-Anfrage nach seiner eigenen Domain an den für ihn zuständigen DNS-Server. Nachdem dieser die Anfrage nicht selbst auflösen kann, kontaktiert er den zuständigen Nameserver, in diesem Fall den DNS-Server des Angreifers, der ihm im Gegenzug die korrekte Antwort zusammen mit dem gefälschten Datensatz zurückschickt. Der DNS-Server übernimmt ungeprüft die Antwort und den daran angehängten Datensatz und trägt beide in seine Hosts-Datei ein. Der DNS-Server ist damit „vergiftet“; jedes Mal wenn ein Nutzer eine DNS-Anfrage mit der Webseite des Angriffsziels als Inhalt an ihn sendet, antwortet er mit der IP-Adresse der gefälschten Seite des Angreifers.

Beim DNS-Cache-Poisoning handelt es sich um eine Angriffsform, die sowohl profundes technisches Wissen als auch eine entsprechende Infrastruktur beim Angreifer voraussetzt. Speziell Verbesserungen der Sicherheitsmechanismen des DNS haben eine erfolgreiche Durchführung dieses Angriffs in den letzten Jahren massiv erschwert. Neben der Prüfung der zufällig generierten Transaction-ID führen die meisten DNS-Server noch zusätzlich bei jeder Antwort, die sie erhalten, ein sogenanntes Bailiwick Checking durch[138]. Bei diesem wird jede Antwort auf zusätzlich hinzugefügte Informationen geprüft, die sich auf eine Domain beziehen, welche sich von jener, nach der ursprünglich gefragt wurde, unterscheidet. Solche Informationen werden vom DNS-Server dann ignoriert. Auch die Transaction-ID kann nur mittels sehr aufwändiger, kryptographischer Algorithmen herausgefunden werden. Ermöglicht werden die meisten DNS-Cache-Poisoning-Angriffe durch veraltete DNS-Server, deren Software nicht mehr auf dem neuesten Stand ist, oder durch fehlerhaft konfigurierte DNS-Server[139]. Bei diesen findet in der Regel weder eine ausreichende Überprüfung der erhaltenen Antworten statt noch eine Prüfung der Authentizität des Nameservers von dem diese Antworten stammen. Eine große Sicherheitslücke des DNS wurde im Jahr 2008 von Sicherheitstechniker Dan Kaminsky entdeckt[140]. Dieser modifizierte bestehende DNS-Angriffe und kombinierte diese mit einem sogenannten Geburtstagsangriff; einem Angriff, der auf dem Geburtstagsparadoxon basiert und der durch die schiere Anzahl an Versuchen die

138 Kjell Jorgen Hole, Pharming, S. 9.
139 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g03/g03104.html (27.03.2012).
140 http://derstandard.at/1216325543381 (27.03.2012).

Erfolgswahrscheinlichkeit erhöht, sowohl die Transaction-ID als auch das Bailiwick Checking auszuhebeln[141]. Die Funktionsweise dieses DNS-Angriffs anhand eines Beispiels:

- Der Angreifer möchte eine falsche IP für die Internetseite testseite.at in einen DNS-Server einschleusen.
- Er sendet eine Anfrage nach einer inexistenten Webseite, die aber die Domain der Zielseite enthält, zb. aaa.testseite.at.
- Während der DNS-Server versucht, die Anfrage nach der inexistenten Seite aufzulösen, bombardiert der Angreifer ihn mit gefälschten Antworten, die zusätzlich eine gefälschte IP für die Domain testseite.at enthalten.
- Schlägt der Angriff fehl, wird er beliebig oft wiederholt mittels neuer Anfragen nach verschiedenen inexistenten Seiten, zb. aab.testseite.at, aac.testseite.at, aad.testseite.at. usw.

Der Sinn dahinter: Nachdem der DNS-Server für jede dieser Anfragen eine Transaction-ID verbraucht, steigt mit jeder Attacke die statistische Wahrscheinlichkeit, die richtige ID zu erraten, erheblich. Zusätzlich wird der Bailiwick Check praktisch wirkungslos, da die in den Antworten des Angreifers hinzugefügten Daten, also in diesem Beispiel die gefälschte IP zur Domain testseite.at, mit der Domain der inexistenten Seite aus der Anfrage übereinstimmen. Die gefälschten Daten jeder Antwort sind somit „in-bailiwick“ und werden vom DNS-Server ungefragt akzeptiert. Laut der Sicherheitsfirma Matasano Security würde ein Angreifer für eine solche Attacke, eine schnelle Internet-Verbindung vorausgesetzt, nur etwa 10 Sekunden benötigen[142]. Um dieser Sicherheitslücke entgegenzuwirken, wurde im Juli 2008 durch nahezu alle Hersteller von DNS-Server-Software ein Patch herausgebracht, der die sogenannte „Source Port Randomization“ einführte. Diese Methode sorgt dafür, dass die Kommunikation zwischen dem DNS-Server und einem Nameserver nicht nur durch die 16 Bit lange Transaction-ID geschützt wird, sondern auch noch durch den zufällig generierten „source port“ des DNS-Servers[143]. Der Angreifer muss nun für einen Erfolg zusätzlich zur Transaction-ID noch die 16 Bit lange, zufällige Port-Nummer erraten. Durch diese Sicherheitsmaßnahme konnte zwar die Sicherheit des DNS kurzfristig erhöht werden; Experten gehen aber davon aus, dass dies nur eine Lösung auf Zeit darstellt. Effektiv erhöht diese Methode nur die Anzahl der für einen erfolgreichen Angriff notwendigen Versuche. Außerdem hat auch die Source Port Randomization ihre Grenzen, denn Ports kleiner als 1024 sind bereits für das System

141 http://einstein.informatik.uni-oldenburg.de/rechnernetze/geburtstagsangriff.htm (27.03.2012).
142 http://www.heise.de/security/meldung/Details-zum-DNS-Sicherheitsproblem-veroeffentlicht-188905.html (27.03.2012).
143 http://www.pressebox.de/pressemitteilung/nominum-inc/Nominum-bringt-umfassendes-Sicherheitspaket-fuer-DNS-Schwachstelle/boxid/200289 (27.03.2012).

reserviert[144].

Obwohl die erfolgreiche Durchführung einer DNS-Cache-Poisoning-Attacke dem Angreifer einen relativ hohen Profit in Aussicht stellt, ist die Anzahl dieser Angriffe in den letzten Jahren deutlich zurückgegangen. Dies liegt zu einem großen Teil am Aufwand, der mit einer solchen Attacke verbunden ist. Dennoch haben Angreifer in den letzten 2-3 Jahren gezeigt, dass sie fähig sind, ihre Methoden den neuen Sicherheitsmechanismen anzupassen. Ähnlich wie beim Phishing setzen die Täter nun auch beim Pharming vermehrt auf Malware (vor allem Trojaner) um die Hosts-Datei von DNS-Servern zu vergiften. Mithilfe von Malware wird nicht mehr ein Nameserver direkt angegriffen, sondern die lokalen Hosts-Dateien oder Router und DSL-Modems von Internet Service Providern. Im November 2011 fand eine großangelegte DNS-Cache-Poisoning Attacke dieser Art in Brasilien statt[145]. Laut Zahlen der Sicherheitsfirma Kaspersky Lab sind etwa 73 Millionen Computer in Brasilien mit dem Internet verbunden[146]. Die größten ISPs des Landes haben durchschnittlich jeweils 3-4 Millionen Kunden[147]. Im Rahmen dieses Angriffs wurden zahlreiche Kunden verschiedener ISPs zum Download eines Trojaners, der als Google Defense Software getarnt war, umgeleitet, wenn sie Webseiten wie Youtube, Gmail oder Google aufrufen wollten. Die brasilianische Polizei verhaftete im Zuge der Ermittlungen mehrere Angestellte von mittelgroßen ISPs, die verdächtigt wurden, den DNS-Cache ihres Arbeitgebers manipuliert zu haben. Im Oktober 2012 wurde, ebenfalls in Brasilien, eine Attacke größeren Ausmaßes durchgeführt, die eine Sicherheitslücke in der Firmware von DSL-Modems und Routern von 6 größeren Herstellern ausnutzte[148]. Die Angreifer benutzten 2 bösartige Skripts, um Remote Access auf die jeweiligen Geräte zu erhalten. Das erste Skript war dazu konzipiert, das Internet nach verwundbaren Modems und Routern abzusuchen. Zu diesem Zweck scannte und testete es einen definierten Bereich an IP-Adressen und sobald ein Modem oder Router gefunden wurde, untersuchte das Skript das Gerät auf die Sicherheitslücke. Wurde eine solche Schwachstelle gefunden, aktivierte sich das zweite Skript, welches durch die besagte Sicherheitslücke an das Administrator Passwort des Modems gelangte und somit Zugriff auf dessen Admin Panel erhielt. Das Skript änderte dann die DNS-Einstellungen des Modems sowie dessen Passwort, um den Besitzer daran zu hindern, es später zu ändern. Mithilfe von 40 im Ausland registrierten DNS-Servern wurden DNS-Anfragen von Millionen von Nutzern umgeleitet. Allein die vier größten ISPs des Landes, Oi, Net, Telefonica und GVT, berichteten davon, dass etwa 50% ihrer Nutzer von dieser Attacke betroffen waren[149]. Offiziellen

144 http://www.heise.de/security/meldung/Reaktionen-auf-DNS-Angriffszenario-bei-deutschen-CERTS-und-Netzknoten-185376.html (27.03.2012).
145 http://net-security.org/secworld.php?id=11903 (27.03.2012).
146 http://www.ehackingnews.com/2011/11/brazil-isp-servers-under-dns-cache.html (27.03.2012).
147 http://www.securelist.com/en/blog/208193214/ (27.03.2012).
148 http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems (28.03.2012).
149 http://www.teleco.com.br/blarga.asp (28.03.2012).

Zahlen zufolge waren im März 2012 rund 4,5 Millionen Modems durch diesen Angriff kompromittiert[150]. Erleichtert werden solche Attacken in Brasilien durch die äußerst schwachen, regionalen Bestimmungen für Netzwerkgeräte. Die brasilianische Telekommunikationsbehörde, Anatel, ist für das Testen solcher Geräte zuständig und bestimmt, welche Modems von den lokalen ISPs verkauft werden dürfen. Diese Tests befassen sich ausschließlich mit der Funktionalität der Geräte und lassen meistens Aspekte der Sicherheit außer Acht, weswegen die ISPs üblicherweise ältere und billigere Modems mit verwundbarer Firmware verkaufen, um Kosten zu sparen. In vielen Fällen werden sogar Router und Modems mit einem default Passwort verkauft, das von den Angreifern mit wenig Aufwand herausgefunden werden kann. Die Nutzer sind sich solcher Gefahren oft nicht bewusst und ändern dieses default Passwort nicht. Da die meisten südamerikanischen und lateinamerikanischen Staaten ähnlich schwache regionale Regelungen aufweisen, ist es kein Zufall, dass dort die meisten DNS-Angriffe in den letzten 2 Jahren verzeichnet wurden. So wurden beispielsweise erst im Juli 2012 zwei Banken in Mexiko Opfer einer solchen Attacke, bei der die Angreifer mithilfe eines Trojaners die Hosts-Datei mehrerer Kunden der Bank veränderten, um diese auf eine gefälschte Webseite umzuleiten[151]. Der dahingehend wohl populärste Trojaner, der von 2009 bis Juli 2012 sogar das amerikanische FBI beschäftigte, war der sogenannte „DNS-Changer“. Dieser veränderte die DNS-Einstellungen des infizierten Rechners und leitete sämtlichen Internetverkehr um[152]. Zusätzlich durchsuchte er etwaige angeschlossene LAN Netzwerke auf verbundene Rechner und infizierte auch diese. Weltweit infizierte der DNS-Changer rund 4 Millionen Rechner[153]. 2012 wurden die Drahtzieher des Angriffs vom FBI im Zuge der „Operation Ghost Click“ festgenommen und ihre DNS-Server abgeschaltet[154].

All diese Fälle zeigen, dass DNS-Cache-Poisoning trotz zurückgehender Zahlen immer noch eine massive Bedrohung für die Sicherheit des Domain Name Systems darstellt. Auch wenn nur wenige Angriffe in den letzten 3-4 Jahren registriert wurden, sind aufgrund der Beschaffenheit des DNS die Opferzahlen und der Schaden meist enorm. Um Identitätsdiebstahl und Identitätsmissbrauch im Internet effizient bekämpfen zu können, sind daher auch Maßnahmen notwendig, die das DNS wirksam schützen.

150 http://www.cert.br/docs/palestras/certbr-jornada-sisp2012.pdf (28.03.2012).
151 http://www.securelist.com/en/blog/208193671/Is_it_the_end_of_the_DNSChanger_Trojan (28.03.2012).
152 http://www.dcwg.org/ (28.03.2012).
153 http://arstechnica.com/tech-policy/2011/11/how-the-most-massive-botnet-scam-ever-made-millions-for-estonian-hackers/ (28.03.2012).
154 http://www.fbi.gov/news/stories/2011/november/malware_110911 (28.03.2012).

4.6 Spoofing

Der Begriff „Spoofing“ ist englisch und bedeutet übersetzt soviel wie Manipulation oder Täuschung. Im Kontext der Informationstechnik dient Spoofing als Sammelbegriff für sämtliche Täuschungsmanöver im Internet, die darauf basieren, die Identität des Angreifers gegenüber einem Opfer durch die Manipulation technischer Erkennungsmerkmale zu verändern[155]. Der Begriff „technische Erkennungsmerkmale“ bezeichnet in diesem Zusammenhang virtuelle Eigenschaften wie IP-Adressen oder Hostnamen. Grundsätzlich lassen sich mehrere verschiedene Arten von Spoofing unterscheiden. Die wichtigsten davon sind: IP-Spoofing, ARP-Spoofing, DNS-Spoofing und MAC-Spoofing.

Bevor die verschiedenen Spoofing-Arten detailliert behandelt werden können, muss zunächst die Funktionsweise des ISO/OSI-Schichtenmodells und des darauf operierenden TCP-IP-Protokolls kurz erläutert werden. OSI steht für „Open System Interconnection“[156]; es handelt sich dabei um das derzeit im Internet vorherrschende Modell für die Kommunikation informationsverarbeitender Systeme[157]. Die grundlegende Funktionsweise: Das OSI-Schichtenmodell ermöglicht, vereinfacht ausgedrückt, die Kommunikation zwischen verschiedenen Komponenten bzw. Systemen innerhalb eines Netzwerks. Es besteht aus 7 Schichten, von denen jede bei der Übertragung von Datenpaketen spezielle Aufgaben hat, wobei die Schichten 1-4 transportorientiert und die Schichten 5-7 anwendungsorientiert sind[158]. Damit die Kommunikation, beispielsweise zwischen 2 Rechnern, reibungslos abläuft, müssen alle 7 Schichten sowohl beim Sender als auch beim Empfänger korrekt arbeiten und vordefinierte Regeln einhalten. Diese Regeln werden von einem Protokoll festgelegt[159]. Wenn nun ein Datenpaket von Rechner X an Rechner Y gesendet werden soll, durchläuft es zunächst auf Rechner X die Schichten 7 bis 1, wobei jede Schicht bestimmte Anforderungen umsetzen muss und dem Protokoll des Datenpakets Informationen hinzufügt. Das Datenpaket-Protokoll ermöglicht es den anderen Stationen bzw. Schichten, die es durchläuft, die Eigenschaften des Datenpakets festzustellen (also zB. woher es kommt, wohin es soll und Ähnliches). Auf Schicht 1 angekommen, wird das Datenpaket transportfähig gemacht und dann über ein Übertragungsmedium (wie zB. Kabel) an den Rechner Y versendet. Dort kommt es auf Schicht 1 des Rechners an und durchläuft die Schichten 1 bis 7, wobei hier Schicht für Schicht die auf Rechner X in das Datenpaket-Protokoll eingetragenen Informationen wieder von den

155 http://www.itwissen.info/definition/lexikon/Spoofing-spoofing.html (30.03.2012).
156 http://www.itwissen.info/definition/lexikon/open-systems-interconnection-OSI-Offene-Kommunikation.html (30.03.2012).
157 http://www.its05.de/computerwissen-computerhilfe/pc-netzwerk/osi-modell/osi-modell.html (30.03.2012).
158 http://www.torsten-bauer.de/referate/isoosi/ (30.03.2012).
159 http://www.netzwerke.com/OSI-Schichten-Modell.htm (30.03.2012).

entsprechenden Schichten entfernt werden. Das Datenpaket-Protokoll fungiert praktisch als Regelwerk für die einzelnen Schichten und ermöglicht damit eine reibungslose Übertragung. Die einzelnen Schichten und ihre Aufgaben, bzw ihre Funktionsweise zusammengefasst:

- Schicht 1 – Bitübertragungsschicht oder auch „Physical Layer“:

  Die Bitübertragungsschicht stellt Hilfsmittel elektrischer, mechanischer oder auch funktionaler Natur zur Verfügung, die notwendig sind, um physische Verbindungen zu aktivieren, zu deaktivieren, aufrechtzuerhalten und Bits darüber zu übertragen.[160] Sie wandelt das Datenpaket in eine technisch übertragbare Form um und kümmert sich um die Übertragung der Bits über das entsprechende Übertragungsmedium. Komponenten, die dieser Schicht zugeordnet werden können, wären beispielsweise Netzwerkkabel oder Hubs.

- Schicht 2 – Sicherungsschicht oder auch „Data Link Layer“:

  Die Sicherungsschicht ist zuständig für die zuverlässige und weitgehend fehlerfreie Übertragung der Datenpakete zwischen den Systemen, außerdem regelt sie den Zugriff auf das Übertragungsmedium[161]. Ihre Aufgaben beinhalten Fehlererkennung, Fehlerbehebung, Datenflusskontrolle und die physikalische Adressierung der Datenpakete. Des weiteren wird sie in 2 Unterschichten unterteilt: Die an Schicht 1 angrenzende MAC-Schicht und die an Schicht 3 angrenzende LLC-Schicht[162]. Die MAC-Schicht enthält die Regeln für die Nutzung des Übertragungsmediums und ist zuständig für die physikalische Adressierung. Die LLC-Schicht teilt die Datenpakete in Frames auf und kümmert sich um die Fehlererkennung sowie Fehlerbehebung. Eine Beispielkomponente von Schicht 2 wäre etwa ein Switch.

- Schicht 3 – Vermittlungsschicht oder auch „Network Layer“:

  Die Vermittlungsschicht steuert die Übertragung der Datenpakete und sorgt für die Auswahl möglichst geeigneter Verbindungswege[163]. Eine ihrer wichtigsten Aufgaben ist die Wegsuche, auf englisch auch Routing genannt. Da die Datenpakete nicht immer direkt an ihr Ziel geschickt werden können, werden sie oft von Netzwerkknoten, die auf dem Weg liegen, weitergeleitet zum nächsten Netzwerkknoten, bis sie bei ihrem Ziel ankommen[164]. Auf dieser Schicht erfolgt auch durch entsprechende Protokolle (wie zB. das IP-Protokoll) die logische

160 http://www.itwissen.info/definition/lexikon/Physikalische-Schicht-physical-layer.html (30.03.2012).
161 http://www.itwissen.info/definition/lexikon/Sicherungsschicht-DLL-data-link-layer.html (03.04.2012).
162 http://www.itwissen.info/definition/lexikon/medium-access-control-MAC-Medienzugangsverfahren.html (03.04.2012).
163 http://www.itwissen.info/definition/lexikon/Vermittlungsschicht-network-layer.html (03.04.2012).
164 http://www.itwissen.info/definition/lexikon/Routing-routing.html (03.04.2012).

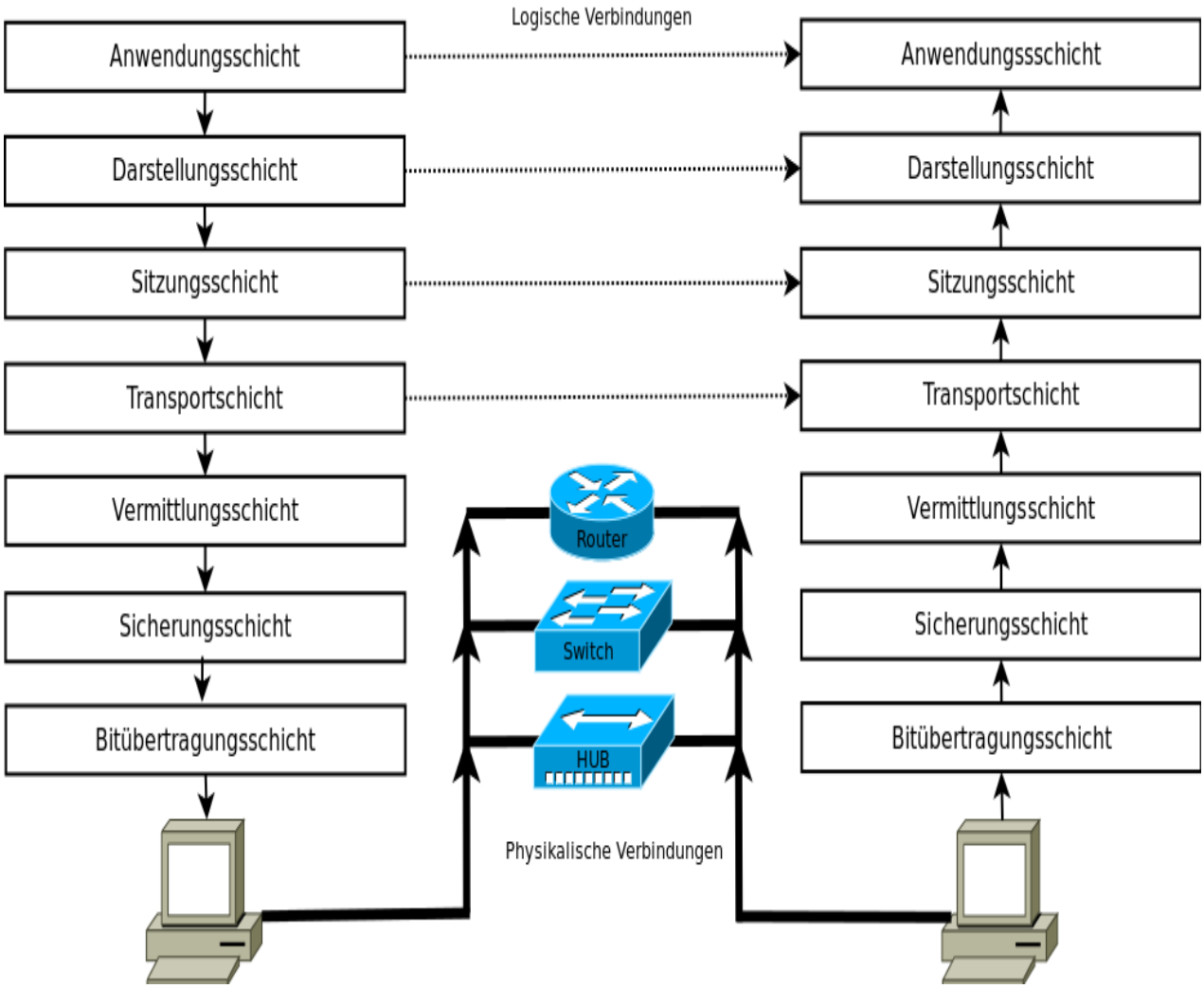

Abbildung 6: Das OSI-Modell[165]

Adressierung der Endgeräte, also der Kommunikationsendpunkte. Eine Beispielkomponente von Schicht 3 wäre zum Beispiel ein Router.

- Schicht 4 – Transportschicht oder auch „Transport Layer“:

  Die Transportschicht ist die oberste Schicht der transportorientierten Schichten und bildet die Schnittstelle zu den anwendungsorientierten Schichten 5-7. Sie kann als logische End-zu-End-Verbindung zwischen Sender und Empfänger betrachtet werden[166]. Ihre wichtigsten Aufgaben sind die Segmentierung der Daten und die Vermeidung von einem Datenstau durch Einsatz einer Flusskontrolle. Wichtige Protokolle, die auf dieser Schicht arbeiten:

165 http://wiki.ubuntu-forum.de/index.php/Baustelle:OSI-Referenzmodell (03.04.2012).
166 http://www.itwissen.info/definition/lexikon/Transportschicht-transport-layer.html (03.04.2012).

TCP, UDP, SCTP.

- Schicht 5 – Sitzungsschicht/Kommunikationsschicht oder auch „Session Layer“:

  Die Sitzungsschicht ist die unterste der anwendungsorientierten Schichten und sorgt für Aufbau, Kontrolle und Beendigung von Prozess-zu-Prozess-Verbindungen zwischen zwei Systemen[167]. Ein wichtiges Protokoll auf dieser Schicht ist das „Remote Procedure Call“, kurz RPC.

- Schicht 6 – Darstellungsschicht oder auch „Presentation Layer“:

  Die Darstellungsschicht konvertiert die Datenpakete in ein Format um, das für den Sender- oder Empfängerknoten verständlich ist[168]. Ihre Aufgaben umfassen die Kompression und Verschlüsselung der Daten. Grundsätzlich kann man sich die Darstellungsschicht auch als eine Art Dolmetscher vorstellen; sie sorgt dafür, dass Daten, die von der Anwendungsschicht des Senders gesendet werden, von der Anwendungsschicht des Empfängers gelesen werden können. Bekannte Formate und Codecs dieser Schicht: ASCII, JPEG, HTML.

- Schicht 7 – Anwendungsschicht oder auch „Application Layer“:

  Die Anwendungsschicht ist die oberste der 7 Schichten des OSI/ISO-Modells. Sie verschafft Benutzeranwendungen Zugang zum Netz[169]; man kann sie also als Schnittstelle für Nutzer und Applikationen sehen. Zu ihr gehören auch Funktionen wie etwa E-Mail, Datenübertragung, Remote-Sessions, Log-in-Prozesse, Datenbankmanagement etc. Eine Beispielkomponente für diese Schicht wäre das Gateway.

Nachdem nun das OSI-Schichtenmodell ausreichend behandelt wurde, wird das darauf operierende TCP/IP-Protokoll etwas näher erläutert. Eigentlich handelt es sich bei TCP/IP um eine Protokollfamilie, genauer gesagt um eine Kombination von „Transmission Control Protocol“ und „Internet Protocol“, welche die Vermittlungsschicht und die Transportschicht des OSI-Schichtenmodells miteinander verbindet[170]. Wie bereits bei der Erläuterung der grundlegenden Funktionsweise des OSI-Schichtenmodells erwähnt wurde, operiert das IP-Protokoll auf der Vermittlungsschicht und das TCP-Protokoll auf der Transportschicht. Derzeit ist TCP/IP das weltweite Standardprotokoll für Netzwerke -sowohl für „Local Area Networks“[171] (kurz LANs) als auch für „Wide Area Networks“[172] (kurz WANs). Die grundlegende Funktionsweise lässt sich am

167 http://www.itwissen.info/definition/lexikon/Kommunikationssteuerungsschicht-session-layer.html (03.04.2012).
168 http://www.itwissen.info/definition/lexikon/Darstellungsschicht-P-presentation-layer.html (03.04.2012).
169 http://www.itwissen.info/definition/lexikon/Anwendungsschicht-APL-application-layer.html (03.04.2012).
170 http://www.itwissen.info/definition/lexikon/transmission-control-protocol-internet-protocol-TCP-IP-TCP-IP-Protokolle.html (04.04.2012).
171 http://www.itwissen.info/definition/lexikon/local-area-network-LAN-Lokales-Netz.html (04.04.2012).
172 http://www.itwissen.info/definition/lexikon/wide-area-network-WAN-Weitverkehrsnetz.html (04.04.2012).

besten anhand des TCP/IP-Modells erklären, auch wenn dieses bereits veraltet ist und durch das OSI-Modell abgelöst wurde. Im Gegensatz zum OSI-Modell besitzt das TCP/IP-Modell nur 4 Schichten[173]:

- Die Anwendungsschicht, die im Prinzip die gleiche Funktion hat wie die Anwendungsschicht des OSI-Schichtenmodells.
- Die Transportschicht, die den Datenfluss zwischen den Kommunikationspartnern steuert und auf der das TCP-Protokoll operiert.
- Die Internet-Schicht, die sich um das Routing und die Zustellung der IP-Pakete kümmert und auf der das IP-Protokoll operiert.
- Die Netzwerkschicht, die festlegt, wie Hosts an bestimmte Netzwerke angeschlossen werden und wie dann die IP-Pakete über diese Netzwerke übertragen werden.

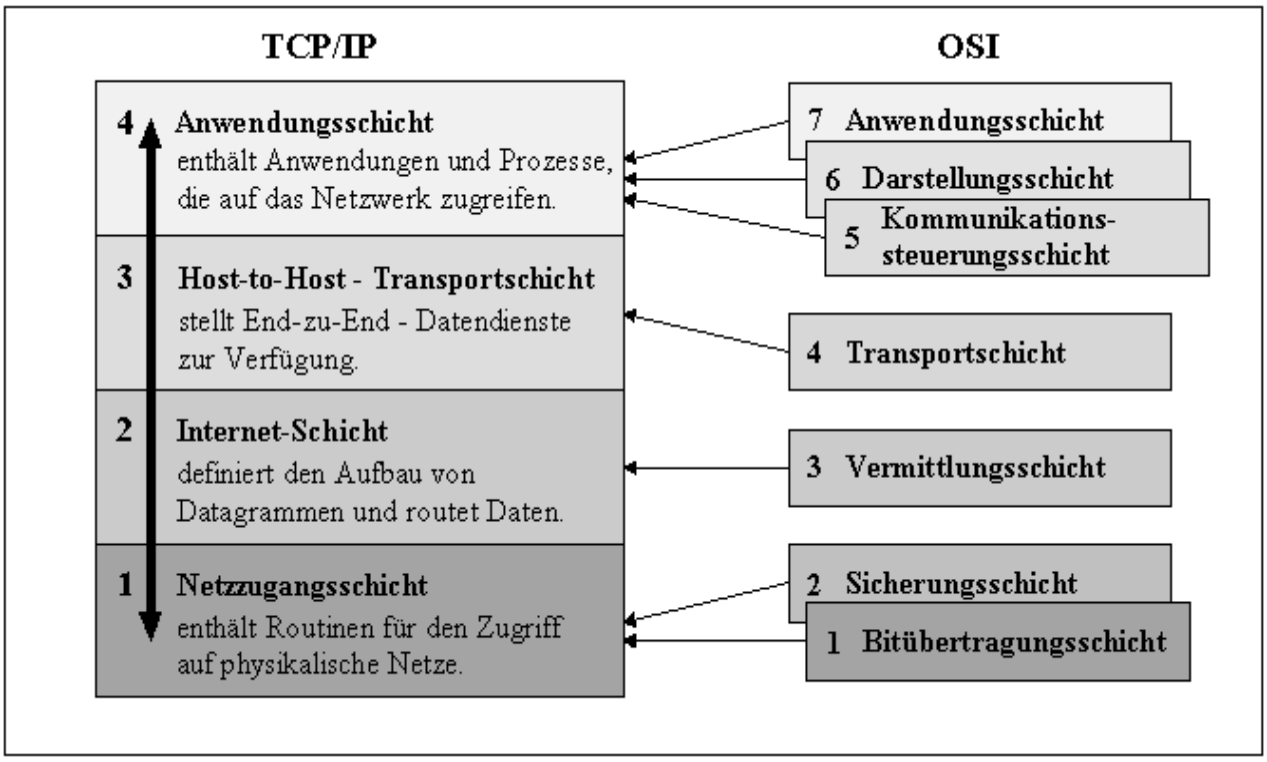

Abbildung 7:Verhältnis von TCP/IP-Modell zu OSI-Modell[174]

Im Rahmen dieses Kapitels sind nur die Transportschicht und die Internet-Schicht von Bedeutung,

173 http://www.elektronik-kompendium.de/sites/net/0606251.htm (04.04.2012).
174 http://www.ruhr-uni-bochum.de/~rothamcw/Lokale.Netze/tcpip.html (04.04.2012).

da auf diesen Schichten das TCP-Protokoll und das IP-Protokoll arbeiten und deren Funktionsweisen vor allem in Hinblick auf IP-Spoofing sehr wichtig sind. Zunächst wird das Internet-Protkoll näher behandelt. Dieses Protokoll hat 2 wichtige Aufgaben[175]:

- Datenpakete an die jeweiligen Hosts zu adressieren und deren Routing durch das Netz sicherzustellen.
- das Fragmentieren der Datenpakete.

Grundsätzlich ist IP ein verbindungsloses und unzuverlässiges Protokoll; verbindungslos, da zwischen dem Sender und Empfänger keine Ende-zu-Ende-Verbindung für die Datenübertragung hergestellt wird und unzuverlässig, da es über keine Werkzeuge zur Fehlererkennung oder Fehlerbehebung verfügt[176]. TCP/IP wurde für paketorientierte Netzwerke entwickelt. Das für IP-Pakete verwendete Format ist das sogenannte Datengramm. Ein solches IP-Datengramm besteht aus 2 Teilen[177]:

- dem sogenannten Header, der 20 Byte groß ist und der noch bis zu 40 Byte für optionale Felder hat;
- den Nutzdaten die an den Zielhost übertragen werden sollen.

Der Header enthält alle Informationen, die für die Zustellung des IP-Datengrammes notwendig sind.

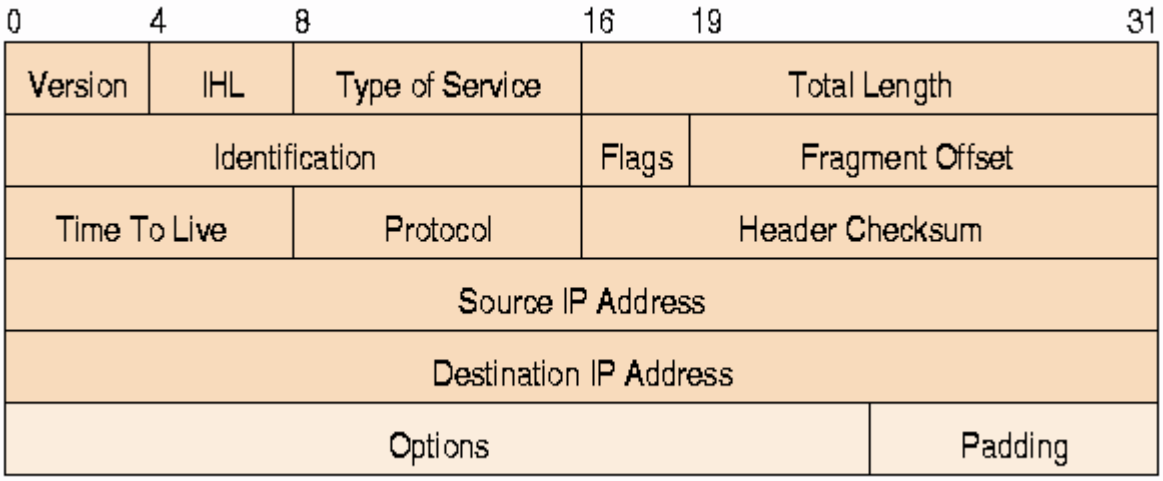

Abbildung 8: IP-Header[178]

175 http://www.elektronik-kompendium.de/sites/net/0811271.htm (04.04.2012).
176 Heiko Holtkamp, Einführung in TCP/IP, S. 17.
177 http://www.tecchannel.de/netzwerk/lan/434734/grundlagen_zu_routing_und_subnetzbildung_teil_1/index9.html (04.04.2012).
178 http://www.freesoft.org/CIE/Course/Section3/7.htm (06.04.2012).

An dieser Stelle sei erwähnt, dass sich dieser Teil der Arbeit auf IPv4 bezieht; obwohl IPv6 im Herbst 2012 bereits existiert, ist IPv4 zu diesem Zeitpunkt noch immer der über weite Strecken vorherrschende Protokollstandard im Netz[179].

Die Felder des Headers kurz erklärt[180]:

- Version: Dieses Feld gibt an, welche IP-Version genutzt wird; im konkreten Fall IPv4.
- IHL: Die „IP Header Length“ gibt Auskunft über die Länge des Protokollkopfs, da diese aufgrund der optionalen Felder variieren kann.
- Type of Service: Durch dieses Feld kann bestimmt werden, nach welchen Kriterien das Datenpaket behandelt werden soll.
- Total Length: Hier wird die Gesamtlänge des IP-Datenpakets bestimmt, also Header + Nutzdaten in Bytes.
- Identification: Üblicherweise werden IP-Datengramme in Fragmenten versendet. Alle Fragmente des gleichen Datengramms haben im Feld Identification die gleiche Identifikationsnummer eingetragen. Dadurch kann der Empfänger die ankommenden Fragmente den entsprechenden Datengrammen zuordnen. Die Identifikationsnummer wird vom Absender bestimmt.
- Flags: Dieses Feld hat eine Länge von genau 3 Bit und dient der Kontrolle der Fragmentierung eines Datengramms. Das erste Bit des Feldes ist reserviert und muss immer 0 sein, die beiden anderen werden mit DF und MF bezeichnet, was für „Don`t Fragment“ und „More Fragments“ steht. Ist das DF-Bit auf 1 gesetzt, bedeutet dies, dass das Datengramm nicht fragmentiert werden darf. Im Gegensatz dazu bedeutet ein auf 1 gesetztes MF-Bit, dass noch weitere Fragmente folgen.
- Fragment Offset: Dieses Feld ist 13 Bit breit und enthält eine Nummer, die angibt, an welcher Stelle innerhalb des IP-Datengramms ein Fragment beginnt.
- Time to Live: Gibt Auskunft über die Lebensdauer eines IP-Pakets. Bei jeder Station, also bei jedem Netzknoten, den ein IP-Paket auf seinem Weg passiert, wird der in diesem Feld eingetragene Wert um 1 verringert. Sinkt der Wert auf 0, so wird das IP-Paket verworfen. Dadurch wird verhindert, dass ein Paket unter Umständen ewig durch das Netz wandert.
- Protocol: Dieses Feld enthält die Nummer des Transportprotokolls, zu dem die im IP-Paket transportierten Nutzdaten gehören. Diese Nummer wird von der Internet Assigned Numbers

179 http://www.elektronik-kompendium.de/sites/net/1806031.htm (06.04.2012).
180 http://www.itwissen.info/definition/lexikon/IP-Header-IP-header.html (06.04.2012).

Authority definiert[181].

- Header Checksum: Dieses Feld enthält eine Prüfsumme für den Header. IP selbst ist nicht dazu in der Lage, die angehängten Nutzdaten auf Korrektheit zu überprüfen; diese Aufgabe obliegt dem TCP-Protokoll. Diese Prüfsumme muss bei jedem Netzknoten, den das IP-Paket passiert, neu verifiziert und neu berechnet werden, da sich das Time to Live Feld des Headers bei jeder Station ändert.
- Source IP Adress: Dieses Feld hat eine Größe von genau 32 Bit und enthält die IP-Adresse des Absenders des IP-Pakets[182].
- Destination IP Adress: Dieses Feld hat ebenfalls eine Größe von 32 Bit und enthält die Adresse des Zielhosts.
- Options + Padding: Dieses Feld bietet die Möglichkeit, das IP-Protokoll durch diverse Zusatzinformationen zu ergänzen. Eine genauere Erläuterung dieser Optionen ist im Rahmen dieser Arbeit nicht notwendig.

Grundsätzlich hat jeder Host und jeder Router nach IPv4 eine eindeutige, 32 Bit lange IP-Adresse, die üblicherweise dezimal in 4 Blöcken geschrieben wird[183]; dabei werden je Block 8 Bit zusammengefasst, wodurch sich für jeden Block ein Wertebereich von 0 bis 255 ergibt[184]. Eine solche IPv4-Adresse wird in 2 Teile unterteilt: Den Netzwerkteil und den Host- oder auch Rechnerteil. Der Netzwerkteil gibt Auskunft darüber, in welchem Netzwerk der jeweilige Host oder Router liegt, der Rechnerteil entspricht der konkreten Adresse des Hosts in diesem Netzwerk. Ab welchem Bit der Netzwerkteil der Adresse endet und der Rechnerteil beginnt, wird durch eine sogenannte Subnetzmaske bestimmt[185]. Da im Internet häufig Hosts aus unterschiedlichen Netzwerken miteinander kommunizieren, sind Router notwendig, um die IP-Pakete von Netzwerk zu Netzwerk weiterzuleiten. Wenn ein IP-Datenpaket versendet werden soll, werden zunächst der Netzwerkteil der Adresse des Absenders und der Netzwerkteil der Adresse des gewünschten Empfängers miteinander verglichen. Stimmen diese miteinander überein, so befindet sich der Empfänger im gleichen Netzwerk, in den meisten Fällen ist dies aber nicht der Fall. Stimmen die Netzwerkteile nicht überein, wird anhand sogenannter Routingtabellen der passende Router für die Weiterleitung des IP-Pakets bestimmt. Danach wird das Paket von Router zu Router weitergeleitet, bis es beim Zielhost ankommt. Wichtig dabei ist, dass die Adresse des Absenders und die Adresse des Empfängers vom Absender in den Header des IP-Pakets eingetragen werden und dass diese den

181 https://www.iana.org/ (06.04.2012).
182 http://www.itwissen.info/definition/lexikon/IP-Adresse-IP-address.html (06.04.2012).
183 http://www.itwissen.info/definition/lexikon/IPv4-Adresse-IPv4-address.html (06.04.2012).
184 http://www.itwissen.info/definition/lexikon/Internet-protocol-version-4-IPv4-IPv4-Protokoll.html (08.04.2012).
185 http://www.elektronik-kompendium.de/sites/net/0811271.htm (08.04.2012).

gesamten Weg über unverändert bleiben.

Das zweite wichtige Protokoll ist das auf IP aufsetzende Transmission Control Protocol, kurz TCP. TCP ist ein zuverlässiges, verbindungsorientiertes und paketvermittelndes Protokoll[186]. Innerhalb der Protokollfamilie TCP/IP hat es folgende Aufgaben[187]:

- Datensicherheit;
- Datenflusssteuerung;
- Maßnahmen gegen Datenverlust.

TCP sorgt also für einen weitgehend sicheren Transport der Daten durch ein Netzwerk. Es operiert auf Schicht 4 des OSI-Modells oder auf der Transportschicht des TCP/IP-Modells. Grundsätzlich basiert TCP auf einer End-zu-End-Verbindung zwischen 2 Hosts. Um diese Verbindung zu realisieren, werden zwei Kommunikationsendpunkte durch sogenannte „Sockets“, also Software-basierte Schnittstellen für den Austausch von Daten, bestimmt. Ein solcher Socket bzw. ein solcher Kommunikationsendpunkt wird durch die IP-Adresse und die Portnummer des jeweiligen Hosts definiert. Die Portnummer wird vom TCP-Protokoll auch dazu benutzt, die gewünschte Applikation auf dem Empfängerhost zu adressieren[188]. Die End-zu-End-Verbindung zwischen den beiden Hosts wird also durch die Socketnummern des Senders sowie des Empfängers eindeutig identifiziert. Ein kurzes Beispiel, um diese Funktionsweise zu veranschaulichen:

- Host Y bietet eine Applikation an, die von anderen Hosts genutzt werden soll. Zu diesem Zweck erstellt er einen Socket anhand seiner IP-Adresse und der Portnummer, die benutzt wird, um die Applikation zu adressieren.
- Wenn nun Host X eine Verbindung zu Y herstellen möchte, um die Applikation zu nutzen, erstellt er einen Socket anhand seiner eigenen IP-Adresse und einer dynamischen, noch nicht belegten Portnummer. Damit kann nun eine End-zu-End-Verbindung auf der Transportschicht aufgebaut werden, die durch diese beiden Sockets eindeutig identifiziert ist.

Ist eine solche Verbindung aufgebaut, besteht die Hauptaufgabe von TCP darin, den von der Applikation kommenden Datenstrom zu empfangen und diesen in sogenannte Segmente aufzuteilen. Diese Segmente werden dann mit einem TCP-Header versehen und anschließend dem Internet Protocol übergeben, das diese in Form von IP-Datengrammen, die bereits genauer erläutert wurden, versendet. Sobald diese IP-Datengramme mit den enthaltenen TCP-Daten bei einem Host

186 http://www.itwissen.info/definition/lexikon/transmission-control-protocol-TCP-TCP-Protokoll.html (08.04.2012).
187 http://www.elektronik-kompendium.de/sites/net/0812271.htm (08.04.2012).
188 http://www.itwissen.info/definition/lexikon/Socket-socket.html (08.04.2012).

angekommen sind, werden sie dort von TCP anhand ihrer Sequenznummern in die richtige Reihenfolge gebracht und danach an die adressierte Applikation übergeben[189]. Ein solches TCP-Paket besteht also aus einem Header und den zu übertragenden Daten, wobei der TCP-Header alle wichtigen Steuerinformationen für das jeweilige TCP-Paket enthält. Die Felder des TCP-Headers, kurz erklärt[190]:

- Source Port: Dieses Feld enthält die Portnummer des Senders.
- Destination Port: Dieses Feld enthält die Portnummer des Empfängers.
- Sequence Number: Die Sequenznummer wird verwendet, um die einzelnen TCP-Pakete zu identifizieren und um diese beim Empfänger wieder in der richtigen Reihenfolge zusammenzusetzen. Durch diese Nummer werden auch Duplikate verhindert, da sie sich während der Verbindung nicht wiederholen darf. Während der Datenübertragung wird die Sequenznummer vom Sender Stück für Stück erhöht.
- Acknowledgement Number: Die Acknowledgement Number oder auch Bestätigungsnummer errechnet sich aus der Sequenznummer des Senders und der Anzahl der empfangenen Bytes[191]. Mit der Bestätigungsnummer gibt der Empfänger an, welche Sequenznummer er als nächstes erwartet, er „quittiert“ sozusagen mit ihr die zu ihm gesendeten Daten.

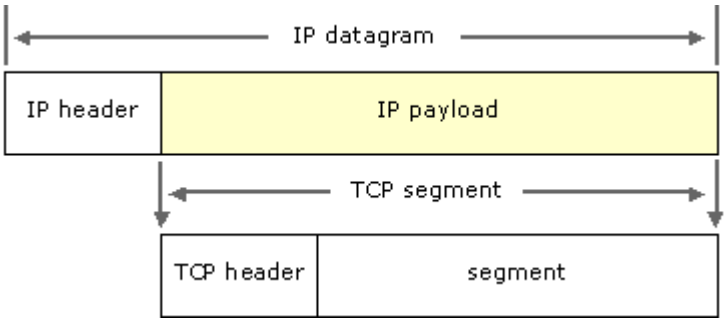

Abbildung 9: IP-Datengramm[192]

- Offset: Gibt Auskunft über die Länge des Headers.
- Reserved: Dieses Feld wird immer auf 0 gesetzt und ist für Erweiterungen des Headers reserviert.

189 Heiko Holtkamp, Einführung in TCP/IP, S. 34.
190 http://www.itwissen.info/definition/lexikon/TCP-Header-TCP-header.html (08.04.2012).
191 http://www.elektronik-kompendium.de/sites/net/0812271.htm (08.04.2012).
192 http://www.proprofs.com/mwiki/index.php/Fundamentals_Of_TCP_And_UDP (08.04.2012).

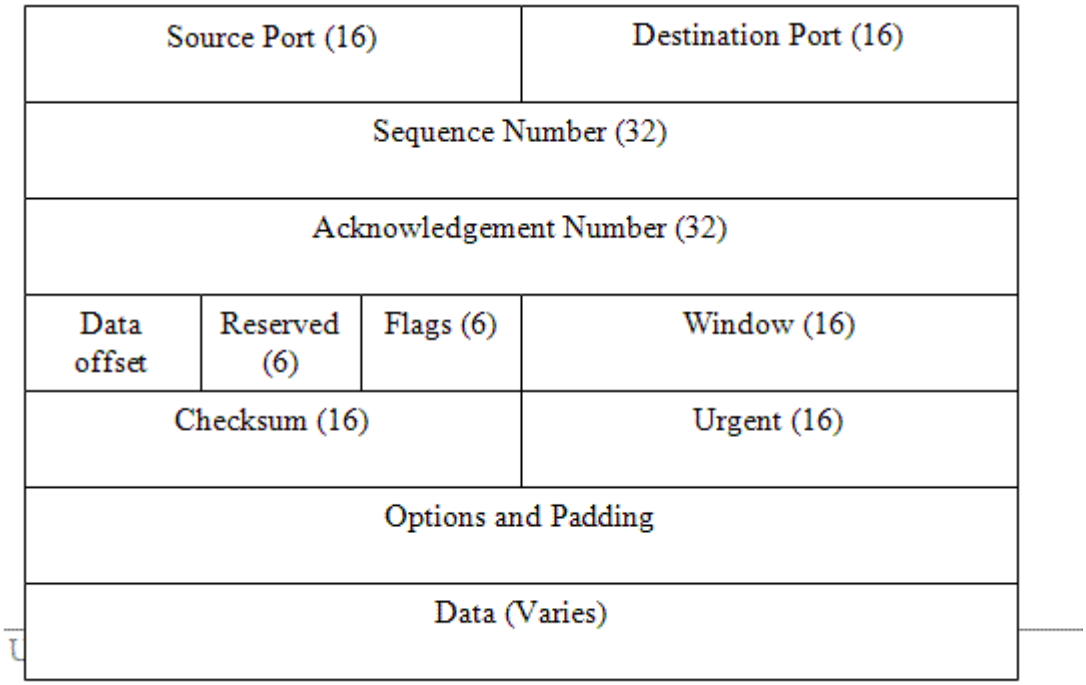

Abbildung 10: TCP-Header[193]

- Flags: Bei den Flags handelt es sich um 6 jeweils 1-Bit-große Funktionen, die zur Steuerung der Kommunikation dienen. Des Weiteren existieren für sie die beiden Zustände „gesetzt“ und „ungesetzt“. Durch das Setzen von Flags können bestimmte Aktionen im TCP-Protokoll ausgeführt werden:

  URG: Wird das URG Flag gesetzt, so bedeutet dies, dass alle Daten nach dem Header bis hin zum Urgent-Pointer-Feld sofort von der Applikation bearbeitet werden[194].

  ACK: Das Flag ACK wird gesetzt, um die Gültigkeit der Acknowledgement Number im TCP-Header zu bestätigen. Ist dieses Flag nicht gesetzt, gibt es keine Bestätigung für das TCP-Segment.

  PSH: Normalerweise werden die in einem Segment enthaltenen Daten von TCP erst eine Weile gepuffert, bis eine größere zusammengehörende Datenmenge vorhanden ist[195]. Ist das Flag PSH gesetzt, werden die im Segment befindlichen Daten sofort der jeweiligen Applikation zur Verfügung gestellt, ohne sie zu puffern.

193 http://de.wikipedia.org/wiki/Transmission_Control_Protocol (08.04.2012).
194 http://www.itwissen.info/definition/lexikon/transmission-control-protocol-TCP-TCP-Protokoll.html (08.04.2012).
195 http://www.itwissen.info/definition/lexikon/Puffer-buffer.html (08.04.2012).

RST: Das Flag RST oder auch Reset dient dazu, eine TCP-Verbindung abzubrechen oder zurückzusetzen. Dies ist vor allem im Falle eines technischen Problems notwendig.

SYN: Das SYN-Flag dient dazu, eine Verbindung zu initiieren.

FIN: Das FIN-Flag wird gesetzt, um eine Verbindung zu beenden, nachdem alle Daten erfolgreich übertragen wurden.

- Window: Dieses Feld gibt Auskunft über die maximale Anzahl an Bytes, die der Empfänger empfangen kann.
- Checksum: Die Prüfsumme dient der Kontrolle des TCP-Headers und des Datenbereichs. Dieses Feld ist vor allem für die Fehlerbehandlung von Bedeutung.
- Urgent Pointer: Dieses Feld ist nur von Bedeutung, wenn das Flag URG gesetzt ist. Der Urgent-Zeiger zusammen mit der Sequenznummer zeigt dem TCP-Protokoll, an welcher Stelle im Datenstrom sich wichtige Bytes befinden.
- Options: Dieses Feld enthält normalerweise optionale bzw. zusätzliche Informationen. Seine Aufgabe ist es, zusätzliche Funktionen zur Verfügung zu stellen, die üblicherweise nicht vorgesehen sind.
- Padding[196]: Grundsätzlich muss das Feld des TCP-Headers mit der Bezeichnung „Options“ von seiner Größe her immer ein Vielfaches von 32 Bit sein. Ist dies nicht der Fall, wird es mit 0en aufgefüllt, bis diese Bedingung erfüllt ist. Dieser Vorgang nennt sich Padding.

TCP Verbindungen werden über einen sogenannten Dreiwege-Handshake[197] realisiert. Der Verbindungsaufbau und der Verbindungsabbau erfolgen dabei in mehreren Schritten[198]:

- Möchte Host A eine Verbindung zu Host B aufbauen, so muss er diesem zuerst ein TCP-Segment senden, in dessen Header das SYN-Flag gesetzt ist. Im Header dieses Segments ist auch die Sequenznummer x enthalten, mit der A im weiteren Verlauf seine Pakete versendet.
- Ist Host B nicht für eine Verbindung bereit, sendet er ein TCP-Segment zurück, das in seinem Header ein gesetztes RST-Flag aufweist, um A mitzuteilen dass derzeit keine Verbindung möglich ist. Ist B für eine Verbindung bereit, dann sendet er ein TCP-Segment mit gesetztem SYN-Flag und gesetztem ACK-Flag zurück, um A zu bestätigen, dass er für den Empfang der Daten bereit ist. In den Header dieses Bestätigungssegments werden auch die Acknowledgement Number x+1 sowie die Sequenznummer y von Host B eingetragen.

196 http://www.itwissen.info/definition/lexikon/Padding-PL-padding-length.html (08.04.2012).
197 http://www.mentzel-web.de/net/tcp.html (08.04.2012).
198 http://www.itwissen.info/definition/lexikon/3-Wege-Handshake-3-way-handshake.html (08.04.2012).

- Nachdem Host A dieses TCP-Segment erhalten hat, sendet er seinerseits ein Bestätigungssegment mit gesetztem ACK-Flag und der Sequenznummer x+1 an Host B zurück. Außerdem wird, um die Sicherheit der Verbindung zu gewährleisten, in das Acknowledgement Number-Feld des Headers die Sequenznummer von Host B um 1 erhöht, also y+1, eingetragen.
- Damit ist eine End-zu-End-Verbindung hergestellt.
- Analog dazu erfolgt der Verbindungsabbau, nur dass hier im Header anstatt des SYN-Flags das FIN-Flag gesetzt wird.

Nachdem nun das OSI-Schichtenmodell und die Protokollfamilie TCP/IP grundlegend behandelt wurden, können nacheinander die wichtigsten Formen des Spoofing untersucht werden.

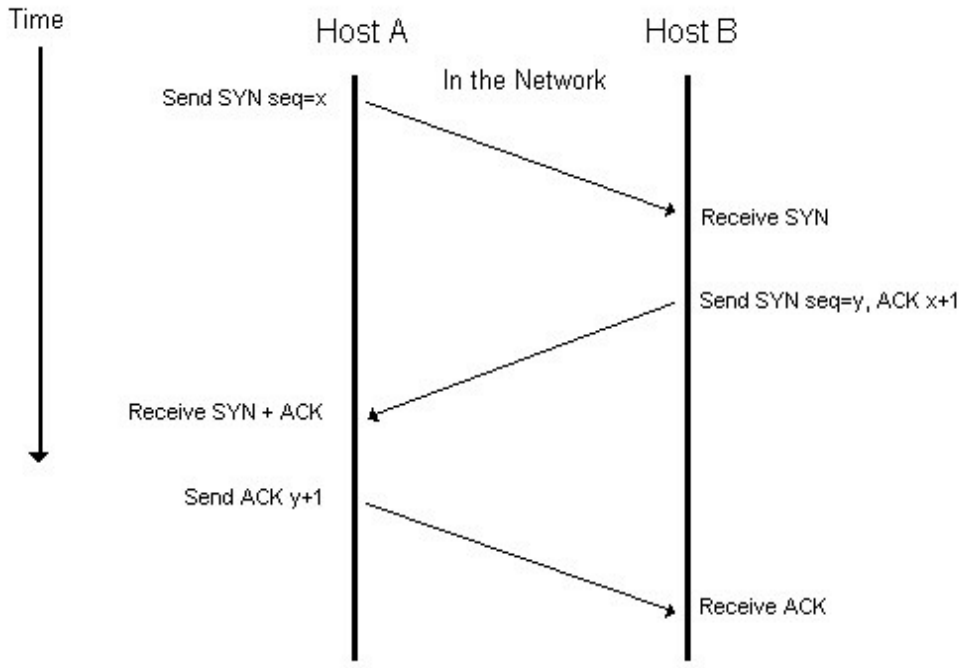

Abbildung 11: Dreiwege-Handshake[199]

4.6.1 IP-Spoofing

IP Spoofing ist eine Angriffsmethode, die darauf basiert, IP-Pakete mit einer gefälschten Absenderadresse an einen Opferrechner zu versenden[200]. Ziel ist es, die Identität des Angreifers zu verschleiern und dem Opfer die Identität eines vertrauenswürdigen Absenders vorzutäuschen. Der

199 http://www.prontosystems.org/it/tcp (17.04.2012).
200 http://www.itwissen.info/definition/lexikon/IP-Spoofing-IP-spoofing.html (17.04.2012).

Angreifer erstellt zu diesem Zweck ein eigenes IP-Paket und verändert in dessen IP-Header die Source IP Adress. Durch diese Technik ist der Angreifer dazu in der Lage, seine eigenen IP-Pakete in lokale Netzwerke einzuschleusen, ohne dass diese durch herkömmliche Sicherheitsmaßnahmen entdeckt werden können. Hauptgrund dafür ist, dass Router ihre Routing-Entscheidungen meist nur anhand der Destination IP Adress treffen und dass die von ihnen bereitgestellte Firewall eine Kommunikation mit „vertrauenswürdigen" Rechnern zulässt[201]. „Vertrauenswürdig" bedeutet in diesem Kontext, dass der Rechner, der mit einem Rechner aus dem betreffenden Netzwerk kommunizieren möchte, eine IP-Adresse aufweist, die von der Router-internen Firewall nicht geblockt wird. Solche gespooften IP-Pakete sind deswegen realisierbar, weil das IP-Protokoll keinerlei Maßnahmen besitzt, um die Felder im IP-Header vor Manipulation zu schützen oder diese zu verschlüsseln und beim Empfänger auf Korrektheit zu überprüfen[202]. IP garantiert keine Korrektheit der erhaltenen Pakete, eine Überprüfung findet nur durch TCP in Form der bereits beschriebenen Sequenznummer statt. Will also ein Angreifer IP-Pakete bei einem Opfer einschleusen, muss er zuerst die Authentifizierungsmechanismen des TCP-Protokolls aushebeln. Zwar wird IP-Spoofing allgemein als „Angriffsmethode" oder auch „Angriffstechnik" bezeichnet, allerdings stellt die Verschleierung der Quelladresse allein noch keinen Angriff dar. Vielmehr ist es die Ausgangsbasis für diverse Angriffsarten wie etwa Denial of Service-Attacken, bei denen das Spoofing dazu genutzt wird, die Identität des Angreifers zu verbergen[203]. Im Zusammenhang mit Identitätsdiebstahl und Identitätsmissbrauch ist IP-Spoofing vor allem dann eine Gefahr, wenn es dazu genutzt wird, eine bestehende TCP-Verbindung zwischen dem Angriffsziel und einem normalerweise vertrauenswürdigen Rechner zu übernehmen. Ein solcher Angriff durchläuft üblicherweise folgende Schritte[204]:

- Der Angreifer X überwacht zunächst den Datenverkehr seines Angriffsziels Y. Dafür können verschiedenen Techniken (wie etwa „Sniffing" oder „Scanning") eingesetzt werden[205].
- Sobald zu Y eine TCP-Verbindung von einem vertrauenswürdigen Rechner Z aufgebaut wird, startet X mit seinem Angriff, indem er sich in den Dreiwege-Handshake zwischen Y und Z einmischt. Es beginnt das sogenannte „TCP-Hijacking"[206].
- X muss als erstes Z lahmlegen, damit dieser nicht mehr in der Lage ist, Y zu antworten. Der Grund dafür ist, dass (obwohl sich der Angreifer als Z ausgibt) alle Antworten von Y immer

201 Tillmann Werner, Sondervorlesung „Netzsicherheit", S. 5.
202 http://www.elektronik-kompendium.de/sites/net/1412101.htm (17.04.2012).
203 http://www.symantec.com/connect/articles/ip-spoofing-introduction (17.04.2012).
204 http://users.informatik.uni-halle.de/~beckmann/Firewall/ (17.04.2012).
205 Shamid Rashid Linta, Ridgewan Khan, Todays Impact on Communication System by IP Spoofing and its Detection and Prevention, S. 30.
206 http://entwickler.de/zonen/portale/psecom,id,126,news,29378,p,0.html (17.04.2012).

noch an den richtigen Rechner Z gehen. Sobald dieser eine Antwort auf ein TCP-Paket mit gesetztem SYN-Flag erhält, das nicht von ihm stammt, beendet er die Verbindung mit einem TCP-Paket mit gesetztem RST-Flag, da er davon ausgeht dass es sich um einen Fehler handelt. Daher startet X eine SYN-Flooding-Attacke auf Z, ausgehend von einer gespooften IP-Adresse. Dabei handelt es sich um einen Angriff auf ein IT-System, bei dem massenweise TCP-Segmente mit gesetztem SYN-Flag verschickt werden, ohne im Anschluss einen vollständigen Verbindungsaufbau zu vollziehen[207]. SYN-Flooding ist eine Variante der bereits erwähnten DoS-Attacken, die eine Schwäche im TCP-Dreiwege-Handshake ausnutzt. Üblicherweise wird eine TCP-Verbindung durch ein Bestätigungssegment mit gesetzter ACK-Flag von jenem Host, der den Dreiwege-Handshake eingeleitet hat, vollständig hergestellt. Wenn nun aber dieses letzte Bestätigungssegment nicht eintrifft, wartet der andere Host noch eine Weile, bevor er die Verbindung abbricht, da ja eine Verzögerung das Segment am Eintreffen hindern könnte. Die TCP-Verbindung ist in einem halboffenen Zustand und belegt Ressourcen[208]. X sendet also eine Reihe von TCP-Segmenten mit gesetzter SYN-Flag an Z und leitet mit jedem einen Dreiwege-Handshake ein, der von X nicht durch ein Bestätigungssegment beendet wird, wodurch irgendwann Z so viele halboffenen Verbindungen hat, dass er keine weiteren TCP-Segmente mehr entgegennehmen kann.

- Nachdem Z handlungsunfähig ist, kann X nun an seiner Stelle mit Y kommunizieren. Dafür muss er die sogenannte ISN, also die „Initial Sequence Number“ von Y erraten. Die ISN ist jene Sequenznummer, die der Host, zu dem eine Verbindung durch ein SYN-Paket aufgebaut wurde, in seinem SYN+ACK-Paket zurücksendet[209]. In der Abbildung zum Dreiwege-Handshake wird sie mit y bezeichnet. Diese ist oft relativ einfach herauszufinden, da sie in den meisten Fällen von einem deterministischen Algorithmus berechnet wird. Der Algorithmus verwendet in der Regel für jede neu vergebene Sequenznummer ein fixes Inkrement, um das diese gegenüber der vorherigen erhöht wird. X kann also nun selber einige Pakete an sein Angriffsziel schicken und dadurch errechnen, welches Inkrement der Algorithmus von Y benutzt. Kennt der Angreifer das Inkrement, dann kennt er auch die zuletzt von Y verwendete Sequenznummer (jene, die er an Z in einem SYN+ACK-Paket versendet hat). X nimmt nun durch IP-Spoofing den Platz des handlungsunfähigen Z ein und sendet ein ACK-Paket mit der richtigen Sequenznummer an Y, wodurch er nun seine manipulierten Pakete versenden kann.

207 Tillmann Werner, Sondervorlesung „Netzsicherheit“, S. 9.
208 http://www.cert.org/advisories/CA-1996-21.html (17.04.2012).
209 http://www.itwissen.info/definition/lexikon/Sequenznummer-SEQ-sequence-number.html (17.04.2012).

Solche Angriffe sind, trotz der von ihnen ausgehenden Gefahr, 2012 eher eine Randerscheinung. Besorgniserregend ist eher, dass IP-Spoofing als Ausgangsbasis für viele Angriffsmethoden dient, die in jenem Teil dieser Arbeit, der sich mit 2012 massiv zunehmenden Trends befasst, noch untersucht werden. IP-Spoofing wird von Angreifern mittlerweile fast ausschließlich als Hilfsinstrument zur Ausführung von DoS-Attacken und DNS-Amplification-Attacken sowie zur Erstellung von Botnetzen genutzt[210].

4.6.2 MAC-Spoofing

Jeder Netzwerkadapter besitzt eine einzigartige physikalische Adresse, genannt „Media Access Control"-Adresse oder auch kurz MAC-Adresse. Diese Adresse dient der eindeutigen Identifizierung von Netzwerk-Hardware in einem Rechnernetz[211]. Die MAC-Adresse kann der zweiten Schicht des OSI-Modells zugeordnet werden (der Sicherungsschicht), genauer der MAC-Schicht. Die MAC-Schicht ist, wie bereits im Zuge der Beschreibung des OSI-Schichtenmodells kurz erläutert wurde, für die physikalische Adressierung zuständig. Das heißt, anhand der MAC-Adresse erfolgt die korrekte Adressierung von Netzwerkpaketen innerhalb eines WLAN- oder LAN-Netzwerks. Beim MAC-Spoofing handelt es sich um eine Angriffsmethode, bei welcher der Angreifer seine MAC-Adresse fälscht, um MAC-Filter zu umgehen, die ein WLAN- oder LAN-Netzwerk vor unbefugten Zugriffen schützen sollen[212]. Ein solcher MAC-Filter ist ein Sicherheitsmechanismus, der nur Geräten mit einer entsprechenden MAC-Adresse Zugang zu einem lokalen Netzwerk gestattet[213]; meistens in Form einer Liste im Router des Netzwerks. Nachdem die MAC-Adresse über das Betriebssystem an den Router übertragen wird, ist es relativ einfach diese durch entsprechende Software zu verändern. Unter Windows beispielsweise kann die MAC-Adresse entweder durch ein paar Handgriffe in der Systemsteuerung oder in der Registry verändert werden[214]. Auch auf anderen Betriebssystemen, wie etwa UNIX, stehen dem User einige Werkzeuge für die Änderung seiner MAC-Adresse zur Verfügung. Wenn ein Angreifer sich nun Zugang zu einem WLAN-Netzwerk verschaffen möchte, so muss er nur folgende Schritte tätigen[215]:

- Paketverkehr in diesem Netzwerk überwachen, beispielsweise durch Sniffing, um so die MAC-Adressen der zugangsberechtigten Rechner herauszufinden;

210 http://www.tu-chemnitz.de/urz/lehre/rs/rs02/gr/atatcp.htm (17.04.2012).
211 http://www.itwissen.info/definition/lexikon/MAC-Adresse-MAC-address.html (18.04.2012).
212 http://secureleaves.com/2012/11/05/layer-2-attacks-mac-address-spoofing-attacks/ (18.04.2012).
213 http://www.computerbild.de/artikel/cb-Ratgeber-Kurse-DSL-WLAN-So-sichern-Sie-Ihr-Funknetzwerk-2260871.html (18.04.2012).
214 http://www.klcconsulting.net/Change_MAC_w2k.htm (18.04.2012).
215 Joshua Wright, Detecting Wireless LAN MAC Address Spoofing, S. 2.

- MAC-Adresse ändern, um so den MAC-Filter zu umgehen.

Hat der Angreifer erst einmal Zugang zum WLAN, kann er Netzwerkpakete, die für einen anderen Rechner bestimmt sind, zu sich umleiten. Im Gegensatz zu anderen Spoofing-Varianten ist MAC-Spoofing nicht ganz so gefährlich, da diese Angriffstechnik mit starken Restriktionen für den Angreifer verbunden ist. Der Angreifer muss, um ein entsprechendes lokales Netzwerk zu attackieren, selber physisch anwesend sein. Daher ist MAC-Spoofing eher weniger für großangelegte Attacken geeignet. Einsatzgebiet für solche Angriffe sind meistens lokale Netzwerke von räumlich nahen Unternehmen oder Personen, also zB. Internetcafes, WLANs von Nachbarn in einem Wohnbau, das lokale Netzwerk in einer Firma und ähnliches.

4.6.3 ARP-Spoofing

Wie bereits erwähnt wurde, findet auf Schicht 2 des OSI-Modells die physikalische Adressierung von Netzwerkteilnehmern statt und die Hauptaufgabe von Schicht 3 ist die sichere Übertragung von Datenpaketen. Während also die Adressierung von Rechnern innerhalb eines lokalen Netzwerks anhand der MAC-Adresse erfolgt, werden Pakete über die Grenzen des Netzwerks hinaus in Form von IP-Paketen gesendet. Das „Adress Resolution Protocol“ (kurz ARP) fungiert praktisch als Dolmetscher für die Übersetzung von IP-Adressen in die jeweiligen MAC-Adressen, es bildet eine Schnittstelle zwischen der Sicherungsschicht und der Vermittlungsschicht[216]. Die wichtigste Aufgabe des ARP ist also die Abbildung von Adressen der Vermittlungsschicht auf Adressen der Sicherungsschicht[217].

Für die korrekte Zuordnung besitzt das ARP Tabellen, in denen paarweise die zusammengehörigen MAC-Adressen und IP-Adressen gespeichert werden. Die grundlegende Funktionsweise des Protokolls gestaltet sich wie folgt[218]:

- Man nehme an, ein Host X möchte Daten an einen Host Y senden. Als erstes überprüft X seine ARP-Tabelle, ob dort bereits ein Eintrag für Y vorhanden ist. Wenn ja, kann er seine Pakete direkt an die dort eingetragene MAC-Adresse versenden. Wenn nein, startet er ein ARP-Request, das an alle Hosts seines lokalen Netzwerkes gesendet wird. In diesem Request enthalten sind seine IP-Adresse, seine MAC-Adresse und die IP-Adresse des gesuchten Rechners. Als Antwort möchte er die MAC-Adresse seines Zielhosts haben.
- Die Hosts innerhalb des lokalen Netzwerks überprüfen nach Erhalt des ARP-Requests, ob sie der gesuchte Rechner sind. Ist einer von ihnen der Zielhost, so sendet er ein ARP-Reply

216 http://www.itwissen.info/definition/lexikon/address-resolution-protocol-ARP-ARP-Protokoll.html (21.04.2012).
217 Tobias Limmer, Martin Gründl, Thomas Schneider, Netzwerksicherheit – ARP-Spoofing, S. 14.
218 https://www.elektronik-kompendium.de/sites/net/0901061.htm (21.04.2012).

an die MAC-Adresse von X zurück, welches seine IP-Adresse und seine MAC-Adresse enthält. Sowohl Sender als auch Empfänger tragen dann die zusammengehörigen Adressen in ihre ARP-Tabelle ein. Falls sich der gewünschte Zielhost nicht im lokalen Netzwerk befindet, kommt das IP-Protokoll zum Zug. Host X erkennt, dass sein gewünschter Empfänger nicht innerhalb seines Netzwerks ist und leitet die Anfrage an seinen lokalen Router weiter, wobei auch der Router innerhalb eines lokalen Netzwerks eine eindeutige MAC-Adresse hat, durch die er adressiert werden kann.

- Der Router sendet nun die Anfrage von X in Form eines IP-Pakets weiter. Das ARP-Request wandert von Router zu Router, bis es schlussendlich aufgelöst werden kann. Der Vollständigkeit halber erwähnenswert wäre noch, dass die befragten Rechner, auch wenn sie nicht der Zielhost sind, trotzdem in vielen Fällen die MAC-Adresse und die IP-Adresse des Senderhosts in ihre ARP-Tabellen eintragen.

ARP-Spoofing bezeichnet die Manipulation der ARP-Tabelle bzw des ARP-Cache eines Hosts durch das Versenden gefälschter ARP-Replies[219]. ARP verfügt über keinerlei Sicherheitsmechanismen, um eine ARP-Nachricht vor Verfälschung zu schützen oder auf Korrektheit zu prüfen. Wie auch beim MAC-Spoofing muss sich der Angreifer physisch im Wirkungsbereich eines lokalen WLAN oder LAN Netzwerkes befinden. Ein Angriff mithilfe von ARP-Spoofing gestaltet sich wie folgt[220]:

- Hat der Angreifer erst einmal Zugang zu einem lokalen Netzwerk, so ist üblicherweise sein erstes Anliegen, zu erfahren, wieviele Rechner überhaupt vorhanden sind und wie ihre zugehörigen IP-Adressen lauten. Zu diesem Zweck startet er ein ARP-Request, mit welchem er nach der MAC-Adresse des Broadcasts fragt. Diese Anfrage geht an alle Hosts des Netzwerks und liefert ihm Informationen über deren IP-und MAC-Adressen in Form von ARP-Replies.
- Nachdem der Angreifer nun alle im Netzwerk vorhandenen IP-Adressen kennt, sucht er sich zwei Hosts, X und Y, als Ziele für seine Attacke aus. Sowohl X als auch Y haben in ihrem ARP-Cache einen Eintrag für den jeweils anderen mit dessen zugehöriger IP-und MAC-Adresse. Der Angreifer sendet nun an X ein unaufgefordertes ARP-Reply, auch genannt „gratuitous“ ARP-Reply[221], welches mit der IP-Adresse von Y versehen ist, aber die MAC-Adresse des Angreifers enthält. X empfängt dieses ARP-Reply und das Protokoll aktualisiert ohne weitere Überprüfung den ARP-Cache, in welchem für die IP-Adresse von Y nun die

219 Sean Whalen, An Introduction to ARP Spoofing, S. 3.
220 http://www.watchguard.com/infocenter/editorial/135324.asp (21.04.2012).
221 Tim Blazytko, Lokale und LAN-interne Angriffsszenarien auf Microsoft Windows NT 5.0-, 5.1-und 5.2-Systeme, S. 16.

MAC-Adresse des Angreifers eingetragen wird. Analog dazu sorgt der Angreifer auch dafür, dass im ARP-Cache von Y seine MAC-Adresse zur IP-Adresse von X eingetragen wird. Solche unaufgeforderten ARP-Replies sind mit relativ wenig Aufwand verbunden, sie lassen sich mit Unterstützung kostenloser Software (wie etwa Ettercap) problemlos ausführen[222].

- Wenn nun X und Y miteinander kommunizieren, läuft ihr Datenverkehr zunächst über den Rechner des Angreifers, der die Pakete, nachdem er sie überprüft oder sogar manipuliert hat, an die richtigen Rechner weiterleitet. Der Angreifer fungiert nun als eine Art Kommunikationsschnittstelle zwischen X und Y.

Die Möglichkeiten, die sich jetzt für den Angreifer bieten, um einen Identitätsdiebstahl oder Identitätsmissbrauch auszuführen, sind zahlreich. Da nun sämtlicher Datenverkehr über ihn läuft, kann er unter anderem Passwörter, E-Mails oder auch Internetverkehr und Surfgewohnheiten seiner Opfer mitschneiden. Selbst verschlüsselte Verbindungen können mithilfe gefälschter Zertifikate entschlüsselt und abgehört werden. Der Angreifer kann sein Opfer auch aus einer bestehenden Session ausloggen und diese übernehmen, oder seine Adressauflösung für Internetseiten und auch seinen Internetverkehr kontrollieren, wodurch er eine Pharming- oder Phishing-Attacke durchführen könnte. Allerdings ist, ebenso wie das MAC-Spoofing, auch das ARP-Spoofing nur begrenzt einsetzbar, da sich der Angreifer im lokalen Wirkungsbereich des jeweiligen Netzwerks befinden muss. Daher ist es für größere Angriffe eher weniger geeignet. Für vereinzelte und vor allem gezielte Angriffe stellt es allerdings sehr effiziente Ergebnisse in Aussicht. Dies liegt vor allem daran, dass gängige Betriebssysteme, trotz der Bekanntheit dieser Angriffsmethode, keine wirksamen Sicherheitsmechanismen zur Verfügung stellen. Das ARP hat, wie bereits erwähnt, keinerlei Mechanismen, um Gültigkeit und Authentizität seiner Nachrichten zu überprüfen; ARP-Nachrichten werden ungefragt akzeptiert und aktualisieren den ARP-Cache eines Rechners[223]. Lösungsansätze wie etwa statische ARP-Tabellen, sind aufgrund von Schwächen im Betriebssystem nicht praktikabel, selbst Maßnahmen wie Port Security bieten keinen wirksamen Schutz gegen ARP-Spoofing[224]. Die zunehmenden Beliebtheit von WLAN-Netzwerken sorgt zusammen mit den effizienten Ergebnissen dieser Angriffstechnik und der geringen Zahl an wirksamen Gegenmaßnahmen dafür, dass diese Form des Spoofings neben IP-Spoofing die aktuell gefährlichste im Kontext von Identitätsdiebstahl und Identitätsmissbrauch ist.

222 http://eatingsecurity.blogspot.co.at/2011/02/using-ettercap-for-arp-poisoning.html (21.04.2012).
223 http://www.erg.abdn.ac.uk/~gorry/course/inet-pages/arp.html (21.04.2012).
224 http://packetlife.net/blog/2010/may/3/port-security/ (21.04.2012).

4.7 SQL-Injection

In der heutigen Zeit werden für die Erstellung und Gestaltung von Webseiten sogenannte „Content Management Systems“ immer beliebter. Dabei handelt es sich um Systeme, mit denen Inhalte auf einer Webseite erstellt, verwaltet oder erweitert werden können[225]. Diese Inhalte werden in SQL-Datenbanken gespeichert und erst beim Webseitenzugriff durch den Nutzer in der Datenbank abgerufen und an der entsprechenden Stelle der dynamischen Webseite ausgegeben[226]. Ein Beispiel für solche Inhalte wären Webanwendungen wie Formulare für Benutzereingaben aller Art, zB. für die Authentifizierung eines Nutzers auf einer Webseite. Der Nutzer gibt in das Formular seinen Usernamen und sein Passwort ein und die Webanwendung übermittelt diese Parameter in Form einer SQL-Abfrage an die Datenbank, was zum erfolgreichen Login des Nutzers führt. Grund für die Beliebtheit von CMS ist, dass diese nur wenig Aufwand für den Inhaber der Seite darstellen, da kaum Vorkenntnisse für deren Verwendung notwendig und sie leicht zu konfigurieren sind. Auch die Administration erfordert wenig Aufwand. Zusätzlich ermöglichen sie auf einfachem Wege User-Interaktionen mit der Webseite, zB. durch Eingabeformulare oder Foren.

SQL-Injection ist eine Angriffstechnik, bei der die von einer Webanwendung an die Datenbank gesendete SQL-Abfrage durch den Angreifer manipuliert oder mit von ihm geschriebenen SQL-Befehlen ergänzt wird[227]. Ermöglicht wird diese Technik durch Sicherheitslücken in Webanwendungen, meist in Form einer mangelnden Überprüfung oder Maskierung der Benutzereingaben. Die Benutzereingaben werden von der Webanwendung als SQL-Abfrage der Datenbank übergeben, wo diese Abfrage vom SQL-Interpreter bearbeitet wird. Wenn nun diese Benutzereingabe ungeprüft und ungefiltert erfolgt, kann der Angreifer durch bestimmte Zeichen, die für den SQL-Interpreter mit Funktionen verbunden sind, die SQL-Abfrage verändern oder erweitern. Durch diese eingeschleusten SQL-Befehle kann der Angreifer die in der Datenbank befindlichen sensiblen Daten, wie beispielsweise Passwörter, ausspionieren oder auch verändern. Unter bestimmten Umständen kann ein Angreifer sogar durch SQL-Injektionen die Kontrolle über den Server erlangen. SQL-Injektionen sind ein weit verbreitetes und beliebtes Mittel für Angriffe auf dynamische Webseiten, da die meisten der von diesen Seiten verwendeten Datenbanken auf SQL basieren und ein solcher Angriff mit wenig Aufwand sehr effiziente Ergebnisse liefert[228]. Erschwerend kommt hinzu, dass den meisten Programmierern von dynamischen Webanwendungen das Wissen über dieses Sicherheitsrisiko fehlt. Das Open Web Application Security Project, kurz OWASP, bewertet in seinen Top 10 Risiken aus dem Jahr 2010 SQL-Injektionen als größte Gefahr

225 http://www.e-teaching.org/technik/distribution/cms/ (28.04.2012).
226 Justin Clarke, SQL Injection Attacks and Defense, S. 2.
227 https://www.owasp.org/index.php/SQL_Injection (28.04.2012).
228 http://www.beyondsecurity.com/about-sql-injection.html (28.04.2012).

für Webanwendungen, gleich neben Cross-Site-Scripting[229]. Bereits in Kapitel 4.4 wurden Statistiken bezüglich der größten Bedrohungen für Webseiten und Webanwendungen untersucht. Nach den dort enthaltenen Zahlen zählt SQL-Injection 2012 mit 12% zu den vier größten Bedrohungen für Webanwendungen. Diese Zahl ist gegenüber 2009 gleich geblieben. SQL-Injection ist seit 2007 eine konstant mächtige Angriffsform, die bis 2012 bereits mehrere namhafte Unternehmen in Erklärungsnot gebracht hat. Im Juni 2011 stahl eine Gruppe von Hackern namens „Lulzsec“ über eine Million an Benutzernamen und Passwörter mithilfe von SQL-Injection von den Servern des Unternehmens Sony Pictures[230]. Juli 2012 wurden durch diese Angriffsmethode 450000 Passwörter von Servern des Unternehmens Yahoo gestohlen[231]. Diese Liste ließe sich beliebig fortführen. Im Hinblick auf Identitätsdiebstahl und Identitätsmissbrauch im Internet kann SQL-Injection als eine der größten Gefahren des Jahres 2012 gesehen werden.

4.8 Cross-Site-Reference-Forgery, oder auch XSRF

Cross-Site-Reference-Forgery oder auch Cross-Site-Request-Forgery ist eine Angriffstechnik, bei der der Angreifer durch ein manipuliertes HTTP-Request ein Opfer ohne dessen Wissen dazu bringt, Aktionen im Sinne des Angreifers in einer Webanwendung auszuführen, in der das Opfer authentifiziert ist[232]. Verwundbar sind insoweit alle Webanwendungen, bei denen eine Authentifizierung des Nutzers anhand von Cookies und dem Browser erfolgt[233]. Wenn sich ein Nutzer bei einer solchen Webanwendung authentifiziert, also einloggt, speichert der Browser mittels Cookie diese Sitzung, so dass sich der Nutzer nicht unentwegt neu anmelden muss. Alles, was ein Angreifer jetzt für einen erfolgreichen XSRF-Angriff tun muss, ist eine manipulierte URL auf gut besuchten Webseiten einzuschleusen, wofür es mehrere verschiedene Techniken gibt, die allerdings hier im Detail nicht von Bedeutung sind. Eine solche manipulierte URL enthält ein bösartiges HTTP-Request, das bei einem Klick auf besagte URL dann vom Browser des Opfers ohne dessen Wissen ausgeführt wird. Der Browser übernimmt für dieses Request alle Eigenschaften des Nutzers, also gespeicherte Cookies, IP-Adresse und ähnliches[234]; er führt praktisch die vom Angreifer gewünschte Aktion im Kontext des Nutzers aus. Wenn der Nutzer beispielsweise bei einem

229 https://www.owasp.org/index.php/Top_10_2010-A1-Injection (28.04.2012).
230 http://www.zdnet.com/sony-hacked-again-in-lulzsec-breach-4010022607/ (28.04.2012).
231 http://www.computerworld.com/s/article/9229136/Yahoo_fixes_password_pilfering_bug_explains_who_s_at_risk (28.04.2012).
232 https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29 (03.05.2012).
233 Jesse Burns, Cross Site Reference Forgery, An introduction to a common web application weakness, S. 2.
234 http://projects.webappsec.org/w/page/13246919/Cross%20Site%20Request%20Forgery (03.05.2012).

Webshop authentifiziert ist, könnte er durch solche manipulierten Links dazu gebracht werden, ohne sein Wissen Artikel zu bestellen, eventuell sogar an eine andere Adresse. Die Möglichkeiten, die sich einem Angreifer durch XSRF bieten sind zahlreich. Oft ist dieser selber Nutzer der Webanwendung, die er attackieren möchte, wodurch er auch deren Linkstruktur kennt.

Wie auch XSS und SQL-Injection zählt XSRF nach den in Kapitel 4.4 präsentierten Statistiken mit 29% zu den vier größten Bedrohungen für Webanwendungen 2012. Auffällig ist allerdings, dass die Popularität dieser Angriffsform auch stark quartalsabhängig ist, was sinkende Zahlen im vierten Quartal beweisen. Als Grund dafür kommt in Betracht, dass Angreifer in diesem Quartal die einfachste und effizienteste Methode wählen, um lukrative Ziele aus dem E-Commerce Sektor gerade in der Weihnachtszeit zu attackieren. XSS ist, da effizienter und einfacher auszuführen, hierbei meist attraktiver für die Angreifer, was den Abfall von XSRF und den Anstieg von XSS im vierten Quartal 2012 erklärt. Trotzdem stellt auch XSRF eine massive Bedrohung für Webanwendungen im Hinblick auf Identitätsdiebstahl und Identitätsmissbrauch im Internet dar.

4.9 Dominierende Trends im Jahr 2012

Betrachtet man die Analysen zahlreicher Securityfirmen und IT-Sicherheitsexperten der letzten 3-4 Jahre, dann lassen sich im Hinblick auf Identitätsdiebstahl und Identitätsmissbrauch drei konstant starke Bedrohungen ausmachen, die 2012 dominieren:

- Drive-by-Downloads
- Botnetze
- DoS-Attacken/DNS-Amplification-Attacken

Als Drive-by-Download wird eine Angriffsform bezeichnet, bei der Nutzer durch den bloßen Besuch einer infizierten Webseite Malware unbeabsichtigt und unbewusst herunterladen[235]. Die Angreifer machen sich hierbei den Umstand zunutze, dass viele Webseiten mittlerweile über dynamische Funktionen verfügen, die durch clientseitige Software und Plug Ins im Browser des Nutzers (wie zB. JavaScript, Adobe Reader oder Adobe Flash) realisiert werden[236]. Ein Beispiel hierfür wären beispielsweise auf Adobe Flash basierende Werbespots, die in Webseiten eingebettet sind. Bei solchen Spots oder auch anderen dynamischen Funktionen dieser Art kommt es zu einer ständigen Übertragung von Daten zwischen Browser und Server, ohne dass der Nutzer etwas dazu

235 http://www.it.cornell.edu/security/safety/malware/driveby.cfm (06.05.2012).
236 http://www.itwissen.info/definition/lexikon/Plug-In-plug-in.html (06.05.2012).

tun müsste. Zur Durchführung eines solchen Angriffs kompromittieren die Angreifer meistens gut besuchte und populäre Webseiten, indem sie mithilfe von diversen Angriffsmethoden (wie beispielsweise SQL-Injection) Schwächen in Webanwendungen ausnützen, um ihren Schadcode auf diesen Webseiten einzuschleusen. Der Schadcode wird dann, sobald ein Nutzer die verseuchte Webseite besucht, automatisch auf dessen Rechner heruntergeladen, ohne dass dieser irgendetwas dazu beitragen muss[237]. Üblicherweise nutzt die Malware dazu Sicherheitslücken im Browser des Opfers, speziell Plug Ins oder Addons, die keinem regelmäßigen Update unterzogen wurden[238]. Wie ein solcher Angriff im Detail funktioniert, wurde bereits in Kapitel 4.1 dieser Arbeit betreffend WETs genauer ausgeführt.

Dies führt auch gleichzeitig zur zweiten wichtigen Bedrohung 2012: Botnetze. Als Bots bezeichnet man im Zusammenhang mit Cyberkriminalität Computerprogramme, die, einmal auf fremde Rechner gelangt, von einem Angreifer ferngesteuert werden können und dem Angreifer eine Reihe automatisierter Dienste zur Verfügung stellen[239]. Mithilfe von Werkzeugen wie WETs und durch Methoden wie Drive-by-Downloads kann ein Angreifer so eine Vielzahl an Rechnern mit Bots infizieren und fernsteuern. Man spricht dann bei diesen Rechnern von einem Botnetz, das von einem einzelnen Angreifer benutzt werden kann. Die Möglichkeiten, die sich einem Angreifer durch solche Botnetze bieten sind vielfältig; in der Praxis sind die Ausführung von DoS-Attacken und der Versand von Phishing-Mails die gebräuchlichsten Funktionen[240].

DoS-Attacken sind Angriffe, mit denen fremde Rechner -meistens Server, die bestimmte Webseiten oder Webanwendungen hosten- durch eine Flut von Datenanfragen über das Internet „bombardiert“ und auf diese Weise lahmgelegt werden. Im Zusammenhang mit Botnetzen ist eigentlich der Ausdruck DDos-Attacke, also Distributed Denial of Service Attacke, gebräuchlicher, da die „Bombardierung“ von mehreren ferngesteuerten Rechnern aus stattfindet[241]. Ein Beispiel für solche DDos-Attacken wäre etwa das in Kapitel 4.6.1 dieser Arbeit detailliert beschriebene SYN-Flooding, aber auch DNS-Amplification-Attacks sind 2012 durchaus beliebt gewesen. DNS-Amplification-Attacks machen sich den Umstand zunutze, dass Nameserver oft auf kurze Anfragen mit sehr langen Antwortpaketen antworten. Der Angreifer stellt daher mithilfe seines Botnetzes mehrere Anfragen, bei denen er mittels IP-Spoofing als Absenderadresse die IP-Adresse des Opfers eingibt, an Nameserver, woraufhin sämtliche Antworten der Nameserver an das Opfer zurückgeschickt

237 Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, Nagendra Modadugu, The Ghost in The Browser, Analysis of Web-based Malware, S. 5.
238 http://www.pcwelt.de/news/Secunia-Report-2010-Fehlende-Updates-sind-das-groesste-Risiko-1443404.html (06.05.2012).
239 https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/BotNetze/botnetze_node.html (06.05.2012).
240 http://www.incapsula.com/ddos/ddos-attacks/botnet-ddos.html (06.05.2012).
241 https://www.elektronik-kompendium.de/sites/net/1412091.htm (06.05.2012).

werden und dessen Rechner komplett lahmlegen[242]. Man spricht hier auch von einer Distributed-Reflected-Denial-of-Service-Attacke, oder kurz DRDoS-Attacke. Vereinfacht werden solche Angriffe durch offene Resolver, also Nameserver mit rekursiver Auflösung, im DNS[243]. Normalerweise sollte ein Resolver nur Anfragen von Clients aus der eigenen Domain entgegennehmen; es gibt allerdings, zum Ärger vieler Sicherheitsexperten, noch eine Vielzahl von Nameservern im DNS, die Anfragen beliebiger Clients entgegennehmen. Mit einem Botnetz und nur wenigen solcher offenen Resolver kann ein Angreifer ohne viel Aufwand beliebige Server attackieren. Manchmal werden solche Angriffe auch genutzt, um bestimmte Nameserver dermaßen mit Anfragen zu überfluten, dass diese lahmgelegt werden.

Die Analysen und Statistiken namhafter Sicherheitsexperten unterstreichen die von 2010 bis 2012 anhaltende Dominanz dieser Bedrohungen. Eines ist 2012 gewiss: Malware dient nicht mehr zur Profilierung ihrer Hersteller, sie wird überwiegend zu kommerziellen Zwecken eingesetzt. Hinter Malware steht eine gut organisierte und professionelle Industrie, die in erster Linie auf den Diebstahl von Daten und damit verbundene Gewinne ausgerichtet ist. Laut dem Internet Security Threat Report der Sicherheitsfirma Symantec aus dem Jahr 2011 erhöhte sich die Anzahl der auf Malware basierenden Angriffe gegenüber 2010 um 81%; mehr als 232 Millionen Identitäten wurden dadurch gestohlen[244]. 61% aller für Drive-by-Downloads verwendeten Webseiten waren „reguläre“ Webseiten, die ohne das Wissen der Betreiber mit Schadcode infiziert wurden. Wenig überraschend waren Blogs, persönliche Webseiten berühmter Personen und E-Commerce-Sites am stärksten betroffen. Besorgniserregend sei nach diesem Bericht auch ein neuer Typ von Malware: polymorphe Malware. Diese verändert konstant ihre interne Struktur, um sich vor Antivirensoftware zu verbergen. Solche Malware war für 36 Millionen Angriffe im Jahr 2011 verantwortlich. 61% aller Attacken auf Webseiten sind auf WETs zurückzuführen, die immer weiter verbreitet und einfacher zu benutzen sind. Laut dem Security Threat Report der Sicherheitsfirma Sophos aus dem Jahr 2012 werden 85% aller Malware-Typen durch Drive-by-Downloads verbreitet, 80% der infizierten Webseiten sind „reguläre“, seriöse Internetauftritte[245]. Nach diesem Bericht ist das aktuell beliebteste WET zur Ausführung von Drive-by-Downloads „Blackhole“, ein von russischen Hackern entwickeltes und sehr einfach benutzbares WET, das auf Schwachstellen speziell in Java, Adobe Flash und Adobe Reader spezialisiert ist. Die Popularität von Drive-by-Downloads führt auch dazu, dass die Hersteller bestimmter Software zunehmend gefordert werden. Laut der Sicherheitsfirma Kaspersky Lab wurden 2011 40% der Nutzer der Anwendung Adobe Reader Opfer

242 https://www.watchguard.com/infocenter/editorial/41649.asp (06.05.2012).
243 http://www.pcworld.com/article/2013109/report-open-dns-resolvers-increasingly-abused-to-amplify-ddos-attacks.html (06.05.2012).
244 Symantec, Security Threat Report 2011, S. 12-13.
245 Sophos, Security Threat Report 2012, S. 10.

von Malware-Attacken, ebenso 31,32% der Nutzer von Adobe Flash[246]. Im Jahr 2012 registrierte Kaspersky Lab 1,5 Milliarden web-basierter Attacken, das 1,7-Fache des Jahres 2011[247]. 50% aller erfolgreichen Angriffe zielten auf die Anwendung Oracle Java ab, immer noch 28% aller erfolgreichen Angriffe betrafen Adobe Reader. Die meiste Malware ist 2012 mit 25,5% in den USA beheimatet. Auf dem zweiten Platz folgt Russland mit 19,6% und an dritter Stelle China, das 2010 noch führend in dieser Statistik war.

Nicht nur Drive-by-Downloads profitieren massiv von WETs, auch Botnetze können mittlerweile durch solche Toolkits erstellt und verwaltet werden. Das 2012 auf diesem Gebiet bekannteste Toolkit ist Zeus, ein WET, mit dem Rechner schnell und einfach infiziert und so einem Botnetz hinzugefügt werden können[248]. Mittels eines übersichtlichen Control Panels ist es dem Inhaber von Zeus möglich, sein Botnetz zu kontrollieren und seine Bots sogar mit Updates zu versorgen. Eines der so erstellten Botnetze war Grum, das 120000 Rechner erfasste und für etwa 18% des globalen Spam-Aufkommens verantwortlich war, bis es Juli 2012 von einer kalifornischen Sicherheitsfirma

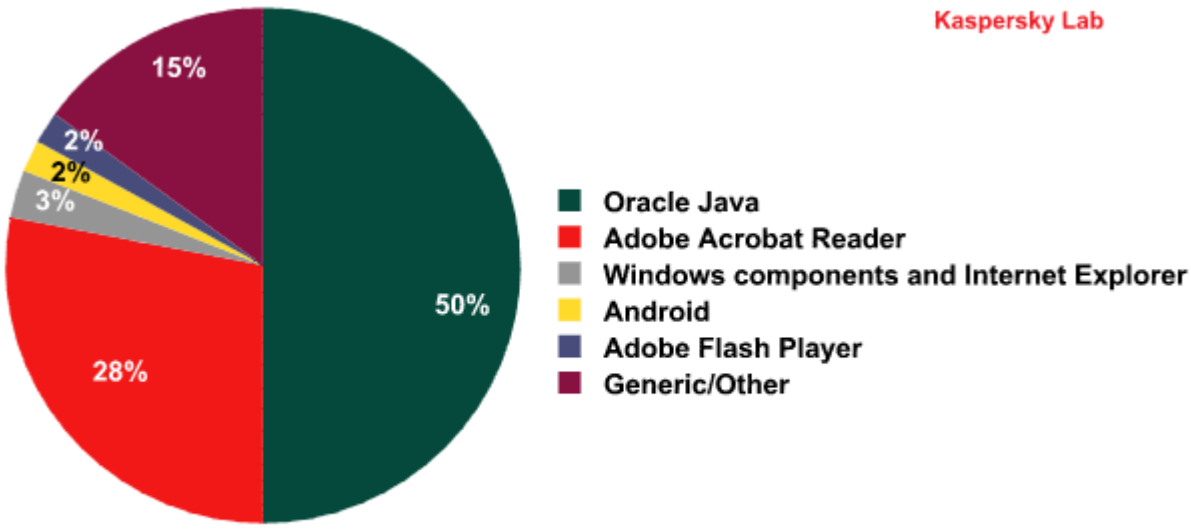

Abbildung 12: Statistik der am stärksten von Malware-Angriffen betroffenen Anwendungen[249]

abgeschaltet wurde[250]. April 2012 wurde das Botnetz Flashback entdeckt, welches aus 600000

246 Kaspersky Lab Malware Report Q1 2011, S. 20.
247http://www.kaspersky.com/about/news/virus/2012/2012_by_the_numbers_Kaspersky_Lab_now_detects_200000_new_malicious_programs_every_day (08.05.2012).
248 http://resources.infosecinstitute.com/botnets-unearthed-the-zeus-bot/ (08.05.2012).
249 http://securelist.com/analysis/kaspersky-security-bulletin/36703/kaspersky-security-bulletin-2012-the-overall-statistics-for-2012/ (08.05.2012).
250 http://www.spiegel.de/netzwelt/web/spam-botnet-grum-zerstoert-a-845232.html (08.05.2012).

Rechnern mit dem Betriebssystem Mac OS bestand[251]. Dadurch, dass die Erstellung undAdministration solcher Botnetze immer einfacher wird, steigt auch die Anzahl von DDoS-Attacken, die 2012 ausschließlich nur mehr mithilfe solcher Netzwerke ausgeführt werden. Die Sicherheitsfirma Arbot registrierte, dass 2012 die durchschnittliche Geschwindigkeit von DDoS-Angriffen gegenüber 2011 um 82% zugenommen hatte -und das bei einem um 27% größeren Volumen[252]. Nach Statistiken der Sicherheitsfirma Neustar wurde 2012 mehr als ein Fünftel aller Unternehmen in England Opfer solcher Angriffe[253]. Zahlreiche prominente Unternehmen werden mittlerweile in regelmäßigen Abständen Opfer solcher Angriffe.

2012 haben sich Trojaner gegenüber allen anderen Formen von Malware klar durchgesetzt, was Weiterentwicklung und Verbreitung betrifft. Laut dem Quarterly Report der Sicherheitsfirma PandaLabs (Zeitraum Jänner bis März 2012) sind im Schnitt 80,77% aller erfassten neuen Malware-Typen Trojaner. Des weiteren sind laut diesem Report 66,30% aller von der Firma PandaLabs verzeichneten Angriffe durch Malware auf Trojaner zurückzuführen. Der Grund für diese Dominanz liegt in der Arbeitsweise und Beschaffenheit der Trojaner. Für die Angreifer geht es vermehrt nur

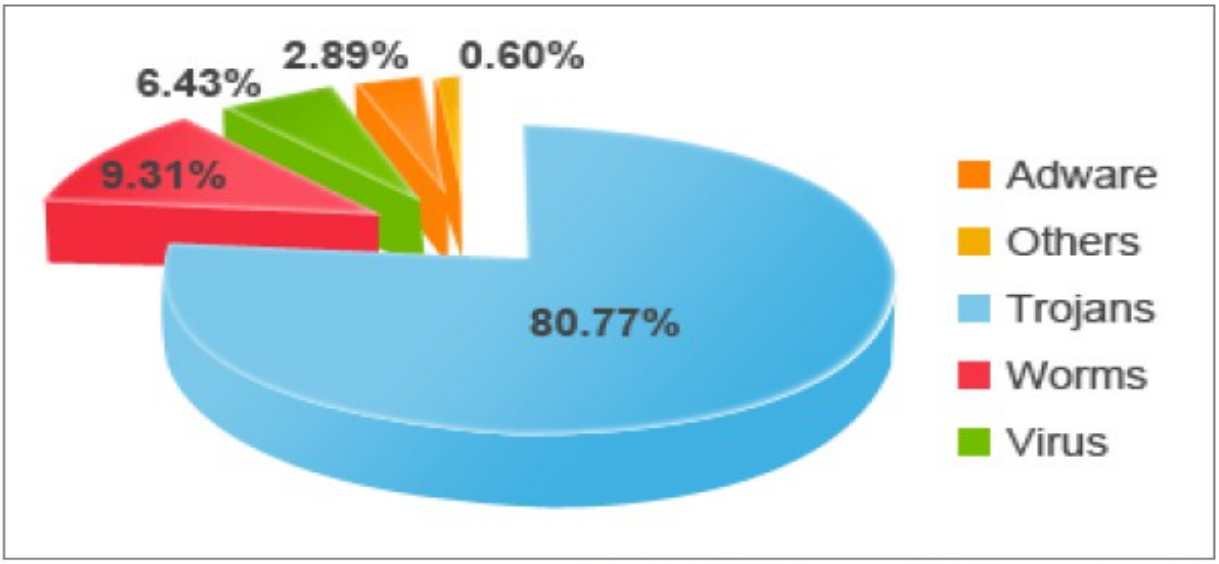

FIG.20. *NEW MALWARE STRAINS IN Q1 2012, BY TYPE.*

Abbildung 13: Malware Statistik der Firma Pandalabs von Jänner bis März[254]

251 http://www.maclife.de/panorama/netzwelt/flashback-botnet-soll-auf-600000-macs-installiert-sein (08.05.2012).
252 http://www.techweekeurope.co.uk/news/ddos-attacks-power2012-86926 (08.05.2012).
253 http://www.neustar.biz/enterprise/resources/ddos-protection/2012-ddos-attacks-report#.UmSyuBDZhdU (08.05.2012).
254 PandaLabs, Quarterly Report January-March 2012, S. 14.

mehr um den Gewinn sowie das Ausspionieren und Beschaffen von verwertbaren Identitätsdaten. Keine Malware ist für diese Aufgaben besser geeignet als Trojaner; außerdem lassen sie sich, sobald sie einmal auf ihrem Zielrechner angelangt sind, sogar durch den Angreifer updaten und mit neuen Instruktionen versehen.

Zusammenfassend lassen sich für 2012 folgende Feststellungen treffen:

- Angriffe durch Malware sind noch immer eine der größten Gefahren im Hinblick auf Identitätsdiebstahl und Identitätsmissbrauch im Internet. Dies wird sich auch in den kommenden Jahren nicht ändern, da das Entwicklungspotential auf Seiten der Angreifer noch lange nicht ausgeschöpft wurde.
- Drive-by-Downloads sind bezüglich der Verbreitung von Malware die dominierende Angriffsform. Hauptziel für die Angriffe sind mittlerweile der Browser der Nutzer inklusive seiner Addons und Webanwendungen. Java, JavaScript, Adobe Reader und Adobe Flash sind aufgrund ihrer starken Verbreitung die am stärksten betroffenen Anwendungen.
- WETs sind der Hauptgrund für die Explosion von Malware-Attacken. Durch Hilfsmittel dieser Art ist es auch technisch wenig versierten Benutzern möglich, eine große Anzahl an Rechnern zu infizieren. Für die Angreifer ist es wichtig, bei möglichst geringem Aufwand möglichst effiziente Ergebnisse zu bekommen.
- Die Motive der Angreifer sind mittlerweile ausschließlich finanzieller Natur. Gestohlene Identitäten lassen sich im Internet gut verkaufen.
- Die 3 konstant starken Bedrohungen Drive-by-Downloads, Botnetze und DDoS-Attacken sind direkt miteinander verbunden. Durch Drive-by-Downloads wird die Erstellung von Botnetzen immer leichter, während diese wiederum die Ausführung von DDoS-Attacken erleichtern.
- Viren und Würmer rücken immer mehr in den Hintergrund. Beliebteste Malware ist und bleibt der Trojaner, weil er am besten dazu konzipiert ist, die aktuellen Bedürfnisse der Angreifer zu erfüllen.

5 Rechtliche Bestimmungen zu Identitätsdiebstahl und Identitätsmissbrauch im internationalen Vergleich

In diesem Kapitel geht es primär um die Gesetzgebung zu Identitätsdiebstahl und Identitätsmissbrauch in verschiedenen Staaten. Per Mai 2012 haben bereits einige Staaten einen eigenen Straftatbestand für Identitätsdiebstahl geschaffen. Dennoch befinden sie sich, global gesehen, in der Minderheit; vor allem in der EU gibt es noch immer keine einheitliche rechtliche Regelung für Identitätsdiebstahl und Identitätsmissbrauch. In vielen europäischen Ländern, wie auch Österreich, existiert eine Reihe von Straftatbeständen (wie etwa Betrug oder Urkundenfälschung), die eine Vielzahl von Handlungen, die man dem Begriff des Identitätsmissbrauchs zuordnen könnte, unter Strafe stellen. Zusätzlich gibt es seit der Umsetzung der EU-Datenschutzrichtlinie[255] in jedem EU-Mitgliedstaat rechtliche Regelungen, die eine unerlaubte Weitergabe oder missbräuchliche Nutzung personenbezogener Daten unter Strafe stellen. Für dieses Kapitel stellt sich nun das Problem, dass ein detaillierter Vergleich sämtlicher Tatbestände, die man den Begriffen Identitätsdiebstahl und Identitätsmissbrauch in irgendeiner Weise zuordnen könnte, einen zu großen Aufwand darstellen würde. Es müssten für jedes zum Vergleich herangezogene Land dessen rechtliche Bestimmungen für Datenschutz, dessen Strafrecht, dessen Zivilrecht und gegebenenfalls auch dessen Verfassung auf sämtliche Tatbestände geprüft werden, die durch einen etwaigen Identitätsdiebstahl oder Identitätsmissbrauch berührt sein könnten. Die Kapitel 3.1 und 3.2 dieser Arbeit liefern bereits einen Ausblick auf nur einige Rechtsnormen, die mit den Begriffen des Identitätsdiebstahls und Identitätsmissbrauchs in Verbindung gebracht werden können. Daher befasst sich die Arbeit im Rahmen dieses Kapitels nur mit:

- Staaten, die bereits rechtliche Bestimmungen nur für Identitätsdiebstahl und Identitätsmissbrauch alleine besitzen;
- Österreich, der als einziger Staat gesondert behandelt wird und für den sämtliche einen Identitätsdiebstahl oder Identitätsmissbrauch betreffende Tatbestände beschrieben werden;
- einigen wenigen Staaten, die für einen Vergleich mit Österreich herangezogen werden können.

5.1 Rechtliche Bestimmungen in den USA

Die USA sind das erste Land der Welt, das gesonderte rechtliche Bestimmungen zu

255 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT (10.05.2012).

Identitätsdiebstahl und Identitätsmissbrauch entwarf und diese in Form des „Identity Theft and Assumption Deterrence Act“ im Oktober 1998 realisierte[256]. Bis zu diesem Zeitpunkt standen auch in den USA lediglich an Identitätsdiebstahl angrenzende Delikte (wie Fälschung oder Betrug) unter Strafe. Mit diesem Gesetz wurden 2 wesentliche Ziele verfolgt[257]:

- Bereits der Diebstahl bzw die Aneignung von persönlichen Informationen mit dem Ziel, diese unrechtmäßig zu benutzen, sollte unter Strafe gestellt werden.
- Der Schutz der Opfer von Identitätsdiebstahl sollte verbessert werden. Speziell immaterielle Schäden wie etwa die Herabstufung der Kreditwürdigkeit oder falsche Einträge bei diversen Jobbörsen sollten durch das Recht stärker geahndet werden.

Dabei ist der Ansatz der USA durchaus interessant: Es wurde nicht nur ein eigener Straftatbestand für Identitätsdiebstahl geschaffen, dieser ist auch mit allen anderen an einen Identitätsdiebstahl „angrenzenden“ Straftatbeständen kumulativ. Das bedeutet, dass eine Person, die Identitätsdaten an sich bringt und mit diesen einen Betrug begeht, in den USA sowohl wegen Betruges als auch wegen Identitätsdiebstahl strafbar ist. Der neue Straftatbestand stellt also nicht nur den Identitätsdiebstahl selbst unter Strafe, er erhöht dadurch auch die Strafdrohung für jegliches mit ihm einhergehende Delikt. Der für dieses Kapitel wichtige Auszug aus dem 18. Titel des United States Code[258], §1028[259] im Wortlaut:

„§1028 – Fraud and related activity in connection with identification documents, authentication features and information

(a) Whoever, in a circumstance described in subsection (c) of this section —

....

> *(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or*

....

shall be punished as provided in subsection (b) of this section.“

Sinngemäß bedeutet dies, dass durch dieses Gesetz jeder bestraft wird, der Identifikationsmittel einer anderen Person ohne rechtliche Legitimation in der Absicht überträgt, besitzt oder verwendet

256 http://www.fidis.net/interactive/wiki-on-id-related-law/wiki/United%20States%20-%20Federal%20B1.%20ID%20Theft/ (11.05.2012).
257 United States Sentencing Commission, Identity Theft – Final Report, S. 3.
258 http://www.law.cornell.edu/uscode/text (11.05.2012).
259 http://www.law.cornell.edu/uscode/text/18/1028 (11.05.2012).

durch diese Identifikationsmittel eine rechtswidrige Tat zu begehen oder zu unterstützen. Vor der Umsetzung von §1028(a)(7) war nach §1026(a)(1)-(6) nur die unberechtigte Benutzung oder Weitergabe von Identitätsdokumenten strafbar; elektronische Identitätsdaten wurden nach 18 U.S.C. §1029 behandelt[260]. Mit der Ergänzung (a)(7) versuchte der Gesetzgeber, auf die immer schnellere Entwicklung von Informationstechnologie zu reagieren; in §1028 ist nun nicht mehr nur die Rede von „identity documents", sondern von „means of identification". In 18 U.S.C. §1028(d)(7) wird genau definiert, was als „Identifikationsmittel" zu verstehen ist[261]:

„(7) the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

> *(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;*
>
> *(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;*
>
> *(C) unique electronic identification number, address, or routing code; or*
>
> *(D) telecommunication identifying information or access device (as defined in section 1029 (e));"*

Identifikationsmittel nach §1028(d)(7) wären also etwa Name, Sozialversicherungsnummer, Geburtsdatum, Führerschein, die Registrierungsnummer bei der Ausländerbehörde und ähnliche Nummern, aber auch biometrische Daten wie etwa Fingerabdrücke sowie elektronische Identifikationsnummern und Telekommunikationsidentifikationsnummern.

Telekommunikationsidentifikationsnummern werden in §1029(e)(1) und (11) näher definiert[262]:

„(e) As used in this section—

> *(1) the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)*
>
> *(11) the term "telecommunication identifying information" means electronic serial number*

260 United States Sentencing Commission, Identity Theft – Final Report, S. 2.
261 http://www.law.cornell.edu/uscode/text/18/1028 (11.05.2012).
262 http://www.law.cornell.edu/uscode/text/18/1029 (11.05.2012).

or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument.“

Erfasst werden also im Wesentlichen alle Arten von Nummern, durch die zur Telekommunikation genutzte Accounts oder ähnliche technische Infrastruktur identifiziert werden könnten.

Das Strafmaß für einen solchen Identitätsdiebstahl kann zwischen 1 und 30 Jahren Haft betragen, wobei dies von folgenden Faktoren abhängt[263]:

- Das Ausmaß des bei den Opfern angerichteten Schadens, sowohl materieller als auch immaterieller Natur;
- die Menge und Art der unrechtmäßig benutzten Identifikationsmittel;
- die Schwere des mit dem Identitätsdiebstahl einhergehenden Verbrechens.

Geschützt wird durch dieses Gesetz jede Form von Daten, die sich zur Identifizierung einer Person eignet. Es ist dabei im Hinblick auf die Strafbarkeit völlig unerheblich, ob diese Daten online erbeutet werden oder ob der Angreifer an sie durch herkömmliche Mittel, wie etwa Taschendiebstahl, Raub oder Einbruch kommt. Entscheidend ist auch, dass der eigentliche Identitätsdiebstahl, also die Übertragung, der Besitz oder der Gebrauch der Identifikationsmittel, allein noch nicht strafbar ist. Notwendig ist zusätzlich der Vorsatz, eine rechtswidrige Tat zu begehen; erst in Verbindung mit einer weiteren Straftat kann auch der Identitätsdiebstahl geahndet werden. Es ist hingegen unerheblich, ob besagte Straftat erfolgreich ist; nach 18 U.S.C. §1028(f) ist bereits der bloße Versuch strafbar, ebenso wie eine Beteiligung[264]:

„(f) Attempt and Conspiracy.— Any person who attempts or conspires to commit any offense under this section shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.“

Nach §1028(f) wird somit jeder, der einen Identitätsdiebstahl im Sinne des §1028 versucht, oder der sich an einem Identitätsdiebstahl beteiligt, mit dem gleichen Strafmaß behandelt, das auch bei einem Erfolg des Identitätsdiebstahls angemessen wäre bzw dem unmittelbaren Täter zugemessen würde.

Der Diebstahl der Daten selbst ist strafbar nach 18 U.S.C. §1030 – Fraud and related acitivity in connection with computers. Dieser stellt folgende Handlungen unter Strafe[265]:

- Unbefugten Zugang zu einem Rechner;
- unbefugte Aneignung von rechtlich geschützten Daten;

263 United States Sentencing Commission, Identity Theft – Final Report, S. 1.
264 http://www.law.cornell.edu/uscode/text/18/1028 (12.05.2012).
265 http://www.law.cornell.edu/uscode/text/18/1030 (12.05.2012).

- unbefugte Weitergabe solcher Daten an Dritte;
- Verkauf von unrechtmäßig erbeuteten und geschützten Daten.

Im September 2008 wurde §1030 durch den Identity Theft Enforcement and Restitution Act in seine derzeit gültige Form abgeändert, genauer gesagt wurde er erweitert durch §1030(a)(5)[266]:

„(a) Whoever —

(5)

> *(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;*
>
> *(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or*
>
> *(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.“*

Demnach ist also auch das bewusste Infizieren eines Rechners mit Spyware, Keyloggern oder Trojanern strafbar. Bei einem Verstoß gegen §1030 kann das Strafmaß, je nach Vergehen, 1-20 Jahre Haft betragen. Vergleichbare rechtliche Bestimmungen in Österreich wären etwa[267]:

- §118a StGB – Widerrechtlicher Zugriff auf ein Computersystem
- §119 StGB – Verletzung des Telekommunikationsgeheimnisses
- §126a StGB – Datenbeschädigung
- §126b StGB – Störung der Funktionsfähigkeit eines Computersystems
- §126c StGB – Missbrauch von Computerprogrammen oder Zugangsdaten
- §51 DSG – Datenverwendung in Gewinn- oder Schädigungsabsicht

Man könnte nach diesem Vergleich 18 U.S.C. §1030 auch zentrale Norm des amerikanischen „Computerstrafrechts“ bezeichnen.

Im Jahr 2004 wurde 18 U.S.C §1028 im Zuge des Identity Theft Penalty Enhancement Act um 18 U.S.C. §1028A, Aggravated identity theft, erweitert[268]:

„(a) Offenses.—

266 Identity Theft Enforcement and Restitution Act of 2008, S. 3.
267 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (12.05.2012).
268 Public Law 108-275, 118 STAT. 831.

(1) In general.— Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

(2) Terrorism offense.— Whoever, during and in relation to any felony violation enumerated in section 2332b (g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years.“

Wenn also jemand unbefugt Identifikationsmittel im Zuge der in §1028A(c) aufgelisteten Vergehen weitergibt, besitzt oder benutzt, dann wird seine Strafe zusätzlich zu dem für das jeweilige Vergehen drohenden Strafmaß noch um 2 Jahre erhöht, im Falle terroristischer Aktivität sogar um 5 Jahre. §1028A(c) umfasst dabei unter anderem auch Amtsmissbrauch von staatlichen Angestellten oder die Angestellten einer Bank, die ihre Stellung für einen Identitätsdiebstahl oder Identitätsmissbrauch ausnützen.

Im Mai 2006 reagierte der damalige Präsident Bush auf den immer größer werdenden Schaden, den Identitätsdiebstahl der Wirtschaft der USA zufügte, und er rief die sogenannte „President`s Identity Theft Task Force“ ins Leben[269]. Aufgabe dieser Task Force war es, eine landesweite Strategie gegen Identitätsdiebstahl zu entwickeln und diesbezüglich vor allem die Effizienz der Maßnahmen der involvierten Bundesbehörden in den Bereichen der Wachsamkeit sowie der Aufklärung, Vermeidung und Verfolgung von Identitätsdiebstahl zu erhöhen. Dabei setzte die Task Force folgende Schwerpunkte[270]:

- notwendige Änderungen an bestehenden Gesetzen, um eine möglichst effiziente strafrechtliche Verfolgung und Verurteilung der Täter zu ermöglichen;
- gezielter Einsatz von Schulungen, um sowohl staatlichen Angestellten als auch Privatpersonen zu vermitteln, wie diese persönliche Daten vor Identitätsdiebstahl schützen können;
- gezielte Zusammenarbeit mehrerer Bundesbehörden, um deren Sicherheitsmaßnahmen gegen Identitätsdiebstahl zu optimieren.

Im April 2007 präsentierte die Task Force ihren strategischen Plan mit dem Titel „Combating Identity Theft: A Strategic Plan“, welcher im wesentlichen folgende Vorschläge und Empfehlungen

269 http://www.justice.gov/archive/ittf/ (12.05.2012).
270 http://itlaw.wikia.com/wiki/President%27s_Task_Force_on_Identity_Theft (12.05.2012).

enthielt[271]:

- Um Identitätsdiebstahl zu verhindern, wäre es notwendig, sensible Daten besser zu schützen und die Personen, die diese bearbeiten und verwalten, bezüglich möglicher Angriffsvektoren zu schulen. Hierbei wäre es von enormer Wichtigkeit, den nicht notwendigen Gebrauch von SSNs im öffentlichen Sektor einzuschränken. Die sogenannte Social Security Number ist die amerikanische Sozialversicherungsnummer, sie gilt in Zusammenhang mit Identitätsdiebstahl als äußerst lohnendes Ziel, da sie in Amerika ungleich funktionsmächtiger ist als beispielsweise in Europa[272]. Mit der amerikanischen SSN können zB. bei staatlichen Behörden neue Accounts eröffnet werden; sie kann mitunter sogar für Banküberweisungen genutzt werden, weiters gilt sie als wichtigstes Identifikationsmerkmal für Steuerzwecke.Gerade deshalb wird die SSN von der Task Force als extrem schutzwürdig eingestuft und es wird empfohlen, die derzeitige Nutzung der Sozialversicherungsnummer durch staatliche Behörden genau zu überprüfen und gegebenenfalls zu überdenken. Ebenfalls geprüft werden müsse die Nutzung der SSN am privaten Sektor. Weiters wird eine gezielte Schulung von Angestellten sowohl des öffentlichen als auch des privaten Sektors auf dem Gebiet der Security und Datensicherheit vorgeschlagen. Auch eine über mehrere Jahre gehende öffentliche Kampagne mit dem Zweck, das Thema Identitätsdiebstahl der breiten Masse näher zu bringen, wird empfohlen.
- Der zweite wichtige Bereich des strategischen Plans ist es, dem Dieb, falls er an Identitätsdaten gelangt ist, die weitere Nutzung zu erschweren, um dadurch einen möglichen Identitätsdiebstahl eventuell zu verhindern. Zu diesem Zweck werden unter anderem Workshops zum Thema Authentifizierung für Angestellte empfohlen.
- Dritter Punkt des strategischen Plans ist es, die Opfer von Identitätsdiebstahl besser bei der Wiederherstellung ihres normalen Lebens zu unterstützen. Die Task Force empfiehlt landesweite Zentren, die für Opfer von Identitätsdiebstahl sämtliche wichtigen Informationen bereitstellen und die ihnen bei den nächsten Schritten beratend zur Seite stehen. Auch die Optimierung der rechtlichen Möglichkeiten, die einem Opfer zur Verfügung stehen, wird vorgeschlagen.
- Der letzte Punkt des strategischen Plans befasst sich mit einer Verschärfung der gesetzlichen Bestimmungen für Identitätsdiebstahl sowie einer effizienteren Verfolgung der Täter. Die Vorschläge der Task Force beinhalten unter anderem ein einheitliches Formular, um den Identitätsdiebstahl zu melden, einen besseren Informationsaustausch zwischen den

271 The Presidents Identity Theft Task Force, Combating Identity Theft – A Strategic Plan (12.05.2012).
272 http://www.socialsecurity.gov/ (12.05.2012).

Strafverfolgungsbehörden und dem privaten Sektor; weiters das Ziel, andere Staaten dazu zu bewegen, ebenfalls einen gesonderten Straftatbestand für Identitätsdiebstahl zu schaffen; das Ziel, andere Länder dazu zu bewegen, der Cybercrime Convention des Europarates beizutreten; das Ziel, Länder ausfindig zu machen, die aufgrund ihrer rechtlichen Bestimmungen einen besonders sicheren Aufenthaltsort für die Täter darstellen und diese auf diplomatischem Wege dazu zu bringen, ihre rechtlichen Bestimmungen anzupassen; das Sammeln statistischer Daten zum Thema Identitätsdiebstahl sowie ein gezieltes Training für Angestellte von Strafverfolgungsbehörden und Lückenschließungen bei bereits existierenden Gesetzen betreffend Identitätsdiebstahl.

Im September 2008 veröffentlichte die Task Force einen Report, der Auskunft darüber gab, welche Empfehlungen erfolgreich umgesetzt werden konnten[273]:

- In Zusammenarbeit mit dem Office of Personnel Management und der Federal Trade Commission konnte der nicht notwendige Gebrauch der SSN im öffentlichen Sektor erheblich reduziert werden. Zu diesem Zweck wurden vom OPM Richtlinien für Mitarbeiter betreffend den Umgang mit der SSN geschaffen, genannt „Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft".
- Zusätzlich wurde eine Schulung von Mitarbeitern ins Leben gerufen, die gängige Sicherheitslücken in den benutzten IT-Systemen zum Thema hatte und die den Mitarbeitern beibringen sollte, schnell auf diese zu reagieren.
- Auch das Ziel, den privaten Sektor und den Konsumenten über die Gefahren eines Identitätsdiebstahls besser zu informieren, konnte teilweise erreicht werden. Speziell die FTC war in diesem Bereich außerordentlich produktiv; von ihr wurden Empfehlungen für den privaten Sektor unter dem Namen „Protecting Personal Information: A Guide for Business" publiziert. Weiters wurden von der FTC im April und August 2008 Workshops unter dem Titel „Protecting Personal Information: Best Practices for Business" abgehalten.
- Das Ziel, eine über mehrere Jahre gehende Aufklärungskampagne zum Thema Identitätsdiebstahl ins Leben zu rufen, konnte von der FTC realisiert werden. Diese führte im Jahr 2008 eine umfassende Kampagne mit dem Namen „Deter, Detect, Defend: AvoID Theft" durch, die vor allem Konsumenten als Zielgruppe hatte und die zeigen sollte, wie diese durch relativ einfache Sicherheitsvorkehrungen Identitätsdaten besser schützen können.
- Eine bessere Schulung der Beamten der Strafverfolgungsbehörden wurde durch

273 The Presidents Identity Theft Task Force Report – 2008.

verpflichtende 7-tägige Seminare mit dem Thema Identitätsdiebstahl realisiert. Beteiligt waren unter anderem das FBI, die FTC, der U.S.Secret Service sowie der U.S.Postal Inspection Service.

- Die FTC wurde zur nationalen Anlaufstelle für Opfer von Identitätsdiebstahl. Auf ihrer Homepage befinden sich detaillierte Empfehlungen für Opfer zur Wiederherstellung ihres guten Namens sowie eine umfassende Aufklärung über deren Rechte.
- Durch den Identity Theft Enforcement and Restitution Act aus dem Jahr 2008 wurden die meisten Empfehlungen gesetzlicher Natur umgesetzt, speziell §1028, §1028A und §1030 wurden entsprechend adaptiert.
- Ein einheitliches und benutzerfreundliches Formular, durch das Opfer einen Identitätsdiebstahl schnell und unkompliziert melden können, wurde von der FTC in Form des „Identity Theft Complaint" Formulars geschaffen.
- Das Sammeln statistischer Daten zum Thema Identitätsdiebstahl wurde im November 2007 umgesetzt, im Rahmen der regelmäßig erfolgenden „Identity Theft Survey" der FTC.

Auch wenn viele der Empfehlungen der Task Force umgesetzt wurden, gibt es dennoch einige Punkte, die bisher noch nicht realisiert werden konnten[274]. Viele Länder haben noch immer keine gesonderten Straftatbestände für Identitätsdiebstahl geschaffen; Länder die aufgrund ihrer rechtlichen Lage besonders beliebte Zentren für Cyberkriminalität sind, konnten nur begrenzt zu einer Zusammenarbeit animiert werden. Speziell eine länderübergreifende Strafverfolgung gestaltet sich noch immer schwierig. Ebenfalls erfolglos blieben bisher die Bemühungen der Task Force, einen gesonderten Straftatbestand für den Diebstahl von Identitätsdaten juristischer Personen zu schaffen, womit man hauptsächlich gegen Phishing vorgehen wollte. Ein einheitliches Ausweisdokument nach dem Vorbild des neuen deutschen Personalausweises, durch welches der Gebrauch der SSN erheblich eingeschränkt werden kann, wurde zwar angedacht, aber bisher noch nicht umgesetzt. Auch nationale Standards für Datenschutz und Datensicherheit wurden noch immer nicht umgesetzt. Die Schaffung eines nationalen Zentrums für Identitätsdiebstahl wird aktuell vom Department of Justice erwogen; es ist aber fraglich, ob die dadurch entstehenden Kosten durch den vermeintlichen Nutzen gerechtfertigt werden.

Wie dringend notwendig der Einsatz dieser Task Force war, zeigen alleine die Zahlen der letzten Jahre. Laut Identity Theft Survey der FTC aus dem Jahr 2006 wurden allein im Jahr 2005 8,3 Millionen Menschen, also etwa 3,7% der amerikanischen Bevölkerung, Opfer eines Identitätsdiebstahls[275]. Von diesen Menschen wurden 3,2 Millionen Opfer eines Missbrauchs ihres

274 The Presidents Identity Theft Task Force Report – 2008.
275 FTC, 2006 Identity Theft Survey Report, S. 3.

Kreditkarten-Accounts, 3,3 Millionen wurden Opfer eines Missbrauchs sonstiger Accounts und 1,8 Millionen meldeten, dass neue Accounts unter ihrem Namen geöffnet oder persönliche Daten auf sonstige Weise vom Angreifer benutzt wurden[276]. Laut FTC waren die Schäden im Fall der Öffnung neuer Accounts weit größer als bei einem „Hijacking" bestehender Accounts des Opfers. So belief sich der durchschnittliche Schaden pro Kopf bei einer Übernahme bestehender Accounts auf etwa 500$, während bei der Öffnung neuer Accounts der Schaden pro Kopf circa 1300$ ausmachte. Im Dezember 2010 veröffentliche das Department of Justice, genauer gesagt das Bureau of Justice Statistics, einen detaillierten Bericht zu Identitätsdiebstahl über den Zeitraum von 2008 bis 2010, gestützt auf die Daten des NCVS-ITS, des National Crime Victimization Survey – Identity Theft Supplement[277]. Demnach waren zwischen 2008 und 2010 11,7 Millionen Menschen Opfer eines Identitätsdiebstahls, alleine 53% davon Opfer eines Missbrauchs ihres Kreditkartenaccounts[278]. Über die Hälfte der Opfer wusste nicht wie und wann die Täter an ihre Identitätsdaten gelangt waren; des Weiteren benötigten die Betroffenen einen längeren Zeitraum, um sämtliche durch den Identitätsdiebstahl verursachten Schäden zu beheben. Der verursachte Gesamtschaden (also der finanzielle Schaden bei den Opfern, Kosten für Aufklärung und Strafverfolgung sowie weitere Kosten) belief sich in diesem Zeitraum auf etwa 17,3 Milliarden Dollar. Im November 2011 wurde durch das Bureau of Justice Statistics ein weiterer Bericht zum Thema Identitätsdiebstahl veröffentlicht, der sich mit dem Schaden durch Identitätsdiebstahl pro Haushalt in der Zeitspanne von 2005 bis 2010 befasste. Nach diesem Bericht waren 2005 etwa 6,4 Millionen Haushalte, also 5,5% aller Haushalte in den USA, von Identitätsdiebstahl betroffen; dies bedeutet in diesem Zusammenhang, dass zumindest eine Person im Haushalt mit einem Alter von mindestens 12 Jahren Opfer mindestens einer Art von Identitätsdiebstahl war[279]. Im Jahr 2010 waren es bereits 8,6 Millionen Haushalte, was einen Anstieg von 5,5% auf 7,0% aller Haushalte in den USA bedeutet. Ein Trend, der sich in diesem Zeitraum ebenfalls abzeichnete, war, dass finanziell motivierter Identitätsdiebstahl eindeutig auf dem Vormarsch ist. Während anderweitiger Missbrauch von Identitätsdaten 2010 (anstatt 0,9% der Haushalte) nur mehr 0,6% betraf, stieg die Zahl der durch Missbrauch von Kreditkartenaccounts oder Bankaccounts zwischen 2005 und 2010 betroffenen Haushalte von 2,5% auf 3,8% an. Hilfreich bei der Sammlung von einschlägigen Daten ist das sogenannte Consumer Sentinel Network, ein Netzwerk, in dem die Meldungen von Kunden über diverse IT-Verbrechen gespeichert werden[280]. Zur Verfügung gestellt werden diese Meldungen von den jeweils zuständigen Behörden und Organisationen (wie beispielsweise die FTC, das FBI, die

276 FTC, 2006 Identity Theft Survey Report, S. 3.
277 Bureau of Justice Statistics Special Report, Victims of Identity Theft 2008.
278 Bureau of Justice Statistics Special Report, Victims of Identity Theft 2008, S. 1.
279 Bureau of Justice Statistics Crime Data Brief , Identity Theft Reported by Households 2005-2010, S. 1.
280 http://www.ftc.gov/sentinel/ (14.05.2012).

National Consumers League oder auch das Department of Defense). Ziel des CSN ist es, diese Daten den diversen Strafverfolgungsbehörden zur Verfügung zu stellen und damit sowohl auf nationaler als auch auf internationaler Ebene die Strafverfolgung bei IT-Verbrechen zu erleichtern. Nach dem Consumer Sentinel Network Data Book aus dem Jahr 2009 betrafen allein 2008 26% aller Meldungen einen Identitätsdiebstahl.[281] Etwa 28 % aller Opfer verzichteten auf eine Meldung bei der Polizei.[282]

Zusammenfassend lässt sich sagen, dass die USA einen durchaus interessanten und nicht ineffizienten Ansatz verfolgen, was Identitätsdiebstahl betrifft. Im Jahr 2006 wurden 1946 Personen wegen Identitätsdiebstahls angeklagt, 1534 wurden verurteilt.[283] Im Jahr 2007 wurden 2470 Personen angeklagt und 1943 verurteilt; das bedeutet einen Anstieg von 26,9% bei Anklagen und einen Anstieg von 26,7% bei Verurteilungen gegenüber 2006[284]. Es ist allerdings relativ schwierig einzuschätzen, ob dieser Ansatz auch in Europa den gewünschten Erfolg bringen würde, da er speziell auf die Vereinigten Staaten von Amerika zugeschnitten wurde. So verbessert beispielsweise ein zusätzlicher Anklagepunkt die Verhandlungsposition der Staatsanwaltschaft beim sogenannten „Plea Bargaining“. Dies ist Verfahren innerhalb des amerikanischen Strafprozesses, im Rahmen dessen der Angeklagte ein Geständnis abgeben kann im Austausch gegen den Verzicht der Staatsanwaltschaft auf einen oder mehrere Anklagepunkte. Andererseits existiert in Europa im Gegensatz zu den USA ein umfangreicher Datenschutzrechtsrahmen, welcher einen Diebstahl oder Missbrauch von personenbezogenen und sensiblen Daten unter Strafe stellt. Es bleibt also abzuwarten, ob das amerikanische System pro futuro Vorbildwirkung für Europa haben könnte.

5.2 Rechtliche Bestimmungen in Kanada

In Kanada können Identitätsdiebstahl und Identitätsmissbrauch, ähnlich wie in Europa, durch eine ganze Reihe von einzelnen Straftatbeständen des kanadischen Strafgesetzes, des Criminal Code, erfasst werden (zB. Betrug oder Diebstahl)[285]. Allerdings stammen die meisten dieser Straftatbestände aus einer Zeit vor der Verbreitung der Computer und vor allem des Internets. Die einzige Ausnahme bilden die etwas neueren Tatbestände für unbefugte Computernutzung (s.342.1) und Kreditkartenbetrug (s.342)[286]. Im Jahr 2004 verfasste das kanadische Department of Justice

281 Consumer Sentinel Network Data Book 2009, S. 4.
282 Consumer Sentinel Network Data Book 2009, S. 12.
283 The Presidents Identity Theft Task Force Report – 2008, S. 37.
284 The Presidents Identity Theft Task Force Report – 2008, S. 37.
285 http://laws-lois.justice.gc.ca/eng/acts/c-46/ (14.05.2012).
286 http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?lang=E&ls=s4&Parl=40&Ses=2&source=library_prb (14.05.2012).

einen Bericht, in dem erstmals empfohlen wurde, einen eigenen Straftatbestand für Identitätsdiebstahl und Identitätsmissbrauch zu schaffen ähnlich wie in den Vereinigten Staaten. In diesem Bericht wurde unter anderem angemerkt, dass zwar die meisten Formen der unbefugten Nutzung von Identitätsdaten nach dem Criminal Code strafbar wären, aber dass die unbefugte Aneignung, der Besitz, und der Handel mit diesen Daten straffrei wäre. Im Jahr 2006 startete die Canadian Internet Policy and Public Interest Clinic, kurz CIPPIC, eine Reihe von Publikationen, die sich speziell mit Identitätsdiebstahl und Identitätsmissbrauch befasste[287]. Bei CIPPIC handelt es sich um eine im Jahr 2003 an der Fakultät für Recht der Universität in Ottawa gegründete Institution, die sich mit rechtlichen Fragen und Problemen beschäftigt, die durch die Verwendung neuer Technologien entstehen. Im Rahmen dieser Publikationen wurde ebenfalls eine Anpassung des kanadischen Rechts nach amerikanischem Vorbild empfohlen[288].

Im November 2007 wurde mit dem Akt Bill C-27 ein Gesetzesentwurf gegen Identitätsdiebstahl und Identitätsmissbrauch im kanadischen Parlament, dem House of Commons, eingebracht, der aber letzten Endes nicht mehr umgesetzt wurde, bevor die Legislaturperiode im September 2008 endete[289]. Im März 2009 wurde im House of Commons der Nachfolger von Bill C-27 eingebracht, Bill S-4, schlussendlich im Oktober 2009 verabschiedet wurde[290]. Die wichtigsten Passagen des Gesetzes[291]:

„402.1 For the purposes of sections 402.2 and 403, "identity information" means any information — including biological or physiological information — of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver's licence number or password.

402.2 (1) Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

(2) Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale

287 http://www.cippic.ca/ (14.05.2012).
288 CIPPIC Working Paper Number 3 (Identity Theft Series), S. 3.
289 http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=3125690&Language=e&Mode=1&File=24#1 (14.05.2012).
290 http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=s4&source=library_prb&Parl=39&Ses=1&Language=E (14.05.2012).
291 http://laws-lois.justice.gc.ca/eng/acts/C-46/page-186.html#h-107 (14.05.2012).

another person's identity information, or has it in their possession for any of those purposes, knowing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

(3) For the purposes of subsections (1) and (2), an indictable offence referred to in either of those subsections includes an offence under any of the following sections:

- *(a) section 57 (forgery of or uttering forged passport);*
- *(b) section 58 (fraudulent use of certificate of citizenship);*
- *(c) section 130 (personating peace officer);*
- *(d) section 131 (perjury);*
- *(e) section 342 (theft, forgery, etc., of credit card);*
- *(f) section 362 (false pretence or false statement);*
- *(g) section 366 (forgery);*
- *(h) section 368 (use, trafficking or possession of forged document);*
- *(i) section 380 (fraud); and*
- *(j) section 403 (identity fraud).*

(4) An accused who is charged with an offence under subsection (1) or (2) may be tried and punished by any court having jurisdiction to try that offence in the place where the offence is alleged to have been committed or in the place where the accused is found, is arrested or is in custody. However, no proceeding in respect of the offence shall be commenced in a province without the consent of the Attorney General of that province if the offence is alleged to have been committed outside that province.

(5) Everyone who commits an offence under subsection (1) or (2)

- *(a) is guilty of an indictable offence and liable to imprisonment for a term of not more than five years; or*
- *(b) is guilty of an offence punishable on summary conviction.*

403. (1) Everyone commits an offence who fraudulently personates another person, living or dead,

- *(a) with intent to gain advantage for themselves or another person;*
- *(b) with intent to obtain any property or an interest in any property;*
- *(c) with intent to cause disadvantage to the person being personated or another person; or*

- *(d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.*

(2) For the purposes of subsection (1), personating a person includes pretending to be the person or using the person's identity information — whether by itself or in combination with identity information pertaining to any person — as if it pertains to the person using it.

(3) Everyone who commits an offence under subsection (1)

- *(a) is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years; or*
- *(b) is guilty of an offence punishable on summary conviction.*

(2) For the purposes of subsection (1), personating a person includes pretending to be the person or using the person's identity information — whether by itself or in combination with identity information pertaining to any person — as if it pertains to the person using it.

(3) Everyone who commits an offence under subsection (1)

- *(a) is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years; or*
- *(b) is guilty of an offence punishable on summary conviction.“*

S.402.1 definiert, was unter „Identitätsinformationen“ zu verstehen ist. Demnach ist eine Identitätsinformation jede Form von Information, die alleine oder zusammen mit einer anderen Information zur Identifizierung eines Individuums verwendet werden kann, wie beispielsweise etwa Kreditkartennummer, Name, Geburtsdatum oder auch DNA-Profil.

Des Weiteren unterscheidet das kanadische Gesetz zwischen s.402.2 (identity theft) und s.402.3 (identity fraud), also zwischen der unbefugten Aneignung der in s.402.1 definierten Information und deren unbefugter Benutzung.

Nach s.402.2 ist jeder strafbar, der Identitätsinformationen einer anderen Person besitzt oder sich aneignet, wenn die Umstände vernünftigerweise darauf schließen lassen, dass die Informationen zur Begehung einer Straftat dienen sollen, die auf Betrug, Täuschung oder Fälschung basiert. Ebenfalls strafbar ist jeder, der Identitätsinformationen einer anderen Person wissentlich veröffentlicht, zugänglich macht oder verkauft, in dem Wissen, dass die Informationen zur Begehung einer Straftat dienen sollen. Das Strafmaß für einen Verstoß gegen s.402.2 beträgt bis zu 5 Jahre Freiheitsstrafe.

Nach s.403.1 ist jeder strafbar, der in betrügerischer Weise vorgibt, eine andere Person zu sein, in der Absicht, sich selbst oder einem anderen einen Vorteil zu verschaffen, sich einen

Vermögensvorteil zu verschaffen, oder der Person die vorgegeben wird zu sein, oder einer anderen Person einen Nachteil zu verursachen oder sich der Verhaftung oder Strafverfolgung zu entziehen. „Vorgeben eine andere Person zu sein“ beinhaltet sowohl die Täuschung selbst als auch die unbefugte Benutzung von Identitätsinformationen dieser Person. Das Strafmaß für einen Verstoß gegen s.403.1 beträgt bis zu 10 Jahren Freiheitsstrafe.

Im kanadischen Zivilrecht, dem Civil Code of Québec, ist nach Artikel 56 eine Form von Identitätsmissbrauch strafbar[292]:

„A person who uses a name other than his or her own is liable for any resulting confusion or damage.

The holder of a name as well as his or her married or civil union spouse or close relatives may object to such use and demand redress for the damage caused.“

Demnach ist jede Person, die einen anderen Namen als ihren eigenen benutzt, für jeden hierdurch verursachten Schaden haftbar. Anspruch auf Schadenersatz haben nach Artikel 56 der Träger des Namens, dessen Ehepartner sowie dessen Kinder oder enge Verwandte.

Zusätzlich zu den gesonderten rechtlichen Bestimmungen für Identitätsdiebstahl und Identitätsmissbrauch besitzt Kanada ein bislang sehr effektives Computerstrafrecht. Neben der bereits erwähnten s.342.1, die sich mit dem Missbrauch von Computern befasst, existiert noch s.430, die sich im speziellen mit dem Abfangen, der Manipulation und auch der Zerstörung von Daten befasst[293].

Anders als die USA besitzt Kanada auch ein Datenschutzrecht, das sogenannte Canadian Privacy Law. Dieses wurde Stück für Stück erweitert[294], bis zu seiner heutigen Form[295]:

- 1983 wurde vom kanadischen Parlament der Privacy Act abgesegnet; ein Gesetz, das genau festlegt, wie staatliche Behörden mit persönlichen Informationen umzugehen haben (wie diese gesammelt werden dürfen, wie diese gespeichert werden dürfen und wie deren Sicherheit zu gewährleisten ist).
- 1985 wurde das kanadische Datenschutzgesetz durch den Access to Information Act erweitert; ein Gesetz, das Bürgern das Recht gibt, ihre von staatlichen Behörden gespeicherten Informationen einzusehen.
- 1996 wurde der Freedom of Information Act umgesetzt; ein Gesetz, das im wesentlichen

292 http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/CCQ/CCQ_A.html (20.05.2012).
293 http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/kim-crime.html (20.05.2012).
294 http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp (20.05.2012).
295 http://laws-lois.justice.gc.ca/eng/acts/P-21/ (20.05.2012).

Anpassungen des Privacy Acts und des Access to Information Acts vornahm.

- Im April 2000 wurde der Personal Information Protection and Electronic Documents Act, kurz PIPEDA, realisiert. Dieses Gesetz regelt, wie Daten von privaten Unternehmen gesammelt und gespeichert werden dürfen, aber auch wie diese geschützt werden müssen. Es handelt sich hierbei um eine Erweiterung des kanadischen Datenschutzgesetzes auf den privaten Sektor.

Zuständig für die Strafverfolgung ist die Royal Canadian Mounted Police, die nationale Polizei Kanadas[296]. Zusätzlich gibt es einige weitere Organisationen, die Meldungen über einen Identitätsdiebstahl oder Identitätsmissbrauch entgegennehmen und die aktiv bei der Strafverfolgung behilflich sind. So wurde beispielsweise von der RCMP eine web-basierte Initiative ins Leben gerufen, die sich Reporting Economic Crime On-line, kurz RECOL, nennt[297]. RECOL basiert auf einer Partnerschaft zwischen mehreren internationalen, nationalen und örtlichen Strafverfolgungsbehörden. Außerdem wird diese Partnerschaft durch private Unternehmen, die an einer Bekämpfung von Verbrechen wirtschaftlicher Art interessiert sind, unterstützt. RECOL gibt Empfehlungen, welche Strafverfolgungsbehörde bei einem Verbrechen die Ermittlungen leiten sollte; des Weiteren werden von ihr statistische Daten zu den Verbrechen und Ermittlungen gesammelt und ausgewertet. Eine weitere wichtige kanadische Organisation im Zusammenhang mit Identitätsdiebstahl und Identitätsmissbrauch nennt sich PhoneBusters, eine 1993 von der Ontario Provincial Police gegründete Organisation, die ursprünglich für Telemarketing-Betrug zuständig war[298]. Mitlerweile ist PhoneBusters auch für Betrug auf Basis von Identitätsdiebstahl zuständig, allerdings liegt der Hauptfokus auf Finanzbetrug. Weitere erwähnenswerte Institutionen, die einen wichtigen Beitrag bei der Strafverfolgung leisten, wären noch die Ontario Provincial Police[299], die über eine eigene Electronic Crime Section verfügt, sowie die Canadian Bankers Association[300], die die Strafverfolgungsbehörden und Kunden mit up-to-date Informationen über neue technische Varianten von Identitätsdiebstahl versorgt.

Trotz aller rechtlichen und organisatorischen Maßnahmen ist Identitätsdiebstahl in Kanada immer noch die am stärksten zunehmende Kriminalitätsform[301]. PhoneBusters gab bekannt, dass im Jahr 2008 über 11000 Meldungen über Identitätsdiebstahl eingingen, der Gesamtschaden belief sich auf etwa 9 Millionen Dollar[302]. Nachdem es sich hier nur um gemeldete Fälle handelt, muss davon

296 http://www.rcmp-grc.gc.ca/index-eng.htm (20.05.2012).
297 CIPPIC Working Paper Number 5(ID Theft Series), Enforcement of Identity Theft Laws, S. 1.
298 CIPPIC Working Paper Number 5(ID Theft Series), Enforcement of Identity Theft Laws, S. 2.
299 https://www.oppa.ca/ (21.05.2012).
300 http://www.cba.ca/?lang=en (21.05.2012).
301 http://www.huffingtonpost.ca/2012/09/09/identity-theft-canada_n_1868172.html (21.05.2012).
302 http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?lang=E&ls=s4&Parl=40&Ses=2&source=library_prb (21.05.2012).

ausgegangen werden, dass der tatsächliche Schaden noch höher ist. Im Jahr 2009 wurde verzeichnet, dass sich die Anzahl der Opfer fast halbiert hatte, aber der Schaden nahezu doppelt so hoch war; dies lässt darauf schließen, dass Identitätsdiebstahl zunehmend gezielter und professioneller eingesetzt wird. Das Canadian Council of Better Business Bureaus geht davon aus, dass der in Kanada insgesamt durch Identitätsdiebstahl angerichtete Schaden, also der Schaden bei Konsumenten, Unternehmen, Banken und Kreditkartenunternehmen, sich in etwa auf 2 Milliarden Dollar pro Jahr beläuft[303]. Um sich der immer schneller wachsenden Opferzahl anzunehmen, wurde am 28. Juni 2012 das Canadian Identity Theft Support Centre ins Leben gerufen[304]. Ziel dieser Institution ist es, ähnlich der FTC in den USA den Opfern von Identitätsdiebstahl jede Information und Hilfe zur Verfügung zu stellen, die notwendig sind, um das Verbrechen zu melden und um sich von dem Verbrechen wieder zu erholen. Es werden auch Maßnahmen vorgestellt, die präventiv gegen Identitätsdiebstahl wirken können.

Abschließend die wesentlichen Unterschiede zwischen den rechtlichen Rahmenbedingungen in den USA und Kanada:

- In Kanada unterscheidet das Gesetz zwischen Identitätsdiebstahl, also der unbefugten Aneignung von Identifikationsmitteln, und Identitätsmissbrauch, der unbefugten Nutzung von Identifikationsmitteln.
- Das maximale Strafmaß für Identitätsdiebstahl ist in den USA weit höher als in Kanada.
- In den USA ist auch der bloße Versuch bereits strafbar.
- Kanada verfügt in Summe über das etwas komplettere und wirkungsvollere System, was in erster Linie an einem umfangreichen Datenschutzrecht liegt, das sowohl für den öffentlichen als auch den privaten Sektor den Umgang mit personenbezogenen Daten regelt. Hierdurch ist in Summe eine weit höhere Sicherheit gegeben.

5.3 Rechtliche Bestimmungen in Australien

Im australischen Strafgesetz des Bundes, dem Criminal Code Act 1995, gibt es eine Reihe von Tatbeständen, die Identitätsdiebstahl oder Identitätsmissbrauch erfassen würden. Diebstahl, Betrug und ähnliche Delikte werden durch Part 7.2, 7.3, 7.4, 7.6 und 7.7 des Criminal Code abgedeckt[305]:

- Section 134 bestraft das Erlangen eines Besitzes oder eines finanziellen Vorteils durch

303 http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?lang=E&ls=s4&Parl=40&Ses=2&source=library_prb (21.05.2012).
304 http://idtheftsupportcentre.org/ (21.05.2012).
305 Criminal Code Act 1995 (28.05.2012).

Täuschung mit einer Freiheitsstrafe von bis zu 10 Jahren.

- Section 135 umfasst mehrere Betrugsdelikte, auch hier beträgt die maximale Freiheitsstrafe 10 Jahre.
- Section 136 und 137 sanktionieren falsche oder irreführende Informationen in Applikationen oder Dokumenten mit einer Freiheitsstrafe von 12 Monaten.
- Section 144 und 145 umfassen sämtliche Tatbestände der Fälschung, die maximale Freiheitsstrafe beträgt 10 Jahre.

Der australische Criminal Code wurde durch den Cybercrime Act 2001 um Part 10.6, 10.7 und 10.8 erweitert[306]. Die neu hinzugefügten Sections 474, 477 und 478 sanktionieren die wichtigsten Delikte mit Unterstützung von Computern, wie etwa Hacking, DoS-Attacken oder auch die Verbreitung von Malware. Part 10.8 befasst sich mit Online-Kreditkartenbetrug und Betrug bei Netbanking, wie etwa Phishing. Durch den Spam Act 2003 wurde zusätzlich noch der Versand von elektronischen Spam-Nachrichten mit australischen Links unter Strafe gestellt, als Strafmaß sind Geldstrafen bis maximal 1.1 Millionen Dollar pro Tag vorgesehen[307]. Erwähnenswert wäre auch noch der Financial Transaction Reports Act 1988, der zur Geldwäschereiprävention unter anderem das Eröffnen eines Bankkontos unter falschem Namen unter Strafe stellt und Banken dazu verpflichtet, die Identitätsdokumente einer Person bei der Kontoöffnung gründlich zu überprüfen[308].

Die australischen Bundesstaaten besitzen ausschließlich eine Gesetzgebungskompetenz in wenigen wichtigen Bereichen, wie zB. Bildung oder Justiz[309]. Daher gibt es von Bundesstaat zu Bundesstaat unterschiedliche rechtliche Regelungen zu Identitätsdiebstahl. In den meisten Bundesstaaten würde ein Identitätsdiebstahl durch ähnliche Tatbestände wie im Criminal Code Act 1995 sanktioniert werden, es gibt allerdings einige wenige Ausnahmen. Die ersten australischen Bundesstaaten, die einen gesonderten Tatbestand für Identitätsdiebstahl und Identitätsmissbrauch in ihren Gesetzen schufen, waren Queensland und Südaustralien. In Südaustralien wurde das Gesetz im Zuge des Criminal Law Consolidation Identity Theft Amendment Act 2003 um folgende Delikte erweitert[310]:

- s144 B – Vortäuschen einer falschen Identität.
- s144 C – Missbrauch von Identifikationsdaten einer lebenden oder toten natürlichen oder juristischen Person zum Zweck der Begehung einer schweren Straftat.

306 http://www.comlaw.gov.au/Details/C2004A00937 (28.05.2012).
307 http://www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf (28.05.2012).
308 http://www.austlii.edu.au/au/legis/cth/consol_act/ftra1988308/notes.html (28.05.2012).
309 http://www.australien-24.com/allgemeines/politik/ (28.05.2012).
310 http://www.legislation.sa.gov.au/LZ/V/A/2003/CRIMINAL%20LAW%20CONSOLIDATION%20%28IDENTITY%20THEFT%29%20AMENDMENT%20ACT%202003_60/2003.60.UN.PDF (28.05.2012).

- s144 D – Produktion oder Besitz von verbotenem Material.

Section 144 A definiert, was unter Identifikationsdaten nach dem Gesetz zu verstehen ist, wobei sowohl die Identifikationsdaten natürlicher als auch juristischer Personen nach dem Gesetz geschützt sind. Als Identifikationsdaten natürlicher Personen gelten unter anderem Name, Adresse, Geburtsdatum, Führerschein, der Pass, biometrische Daten, Stimmenaufzeichnungen sowie die Kreditkartennummer. Als Identifikationsdaten juristischer Personen werden der Name, ABN (Australian Business Number) sowie jedes Bankkonto, das von der juristischen Person erstellt wurde, definiert. Weiters ist nach s 144 E der Versuch nicht strafbar[311].

Queensland erweiterte im Jahr 2007 sein Strafgesetz, den Criminal Code Act 1899, um Sektion 408D, „Obtaining or dealing with identification information“[312]. Nach s 408D ist jeder strafbar, der sich Identifikationsdaten einer anderen natürlichen oder juristischen Person verschafft oder mit diesen handelt, um ein Verbrechen zu begehen oder zu ermöglichen. Nach dem Gesetz ist es auch völlig unerheblich, ob die betreffende natürliche oder juristische Person tot oder lebendig ist, ob sie wirklich existiert oder nicht oder ob sie mit der Benutzung ihrer Identifikationsdaten einverstanden ist oder nicht. Identifikationsdaten sind nach s 408D alle Arten von Information über die betreffende natürliche oder juristische Person, die entweder für sich alleine oder zusammen mit anderen Informationen benutzt werden können, um die natürliche oder juristische Person zu identifizieren. Als Strafmaß werden 3 Jahre Freiheitsstrafe vorgesehen.

Außergewöhnliche rechtliche Bestimmungen im Hinblick auf Computerkriminalität gibt es in den australischen Bundesstaaten nicht. Das australische Computerstrafrecht wird im wesentlichen durch den Cybercrime Act 2001 des Bundes definiert; ähnliche Bestimmungen wie jene im Criminal Code Act 1995 haben auch die einzelnen Bundesstaaten in ihre Gesetze übernommen. Ein umfangreiches Datenschutzrecht ist in Australien ebenso inexistent wie in den USA. Weder auf Bundesebene noch in den Gesetzen der einzelnen Bundesstaaten gibt es umfassende rechtliche Bestimmungen für den Umgang mit personenbezogenen Daten.

Durch die immer weiter zunehmende Sammlung und Verwaltung personenbezogener Daten in elektronischer Form, egal ob im privaten oder öffentlichen Sektor, sowie durch die rasante technische Entwicklung neuer Angriffsmethoden durch Betrüger sah man sich 2003 auch in Australien zu einem Umdenken betreffend Identitätsdiebstahl gezwungen. Das Australian Institute of Criminology veröffentlichte 2002 einen Report, wonach die meisten australischen Bürger nur wenig darüber wissen würden, wie sie ihre persönlichen Informationen im Internet schützen

311 http://www.legislation.sa.gov.au/LZ/V/A/2003/CRIMINAL%20LAW%20CONSOLIDATION%20%28IDENTITY%20THEFT%29%20AMENDMENT%20ACT%202003_60/2003.60.UN.PDF (28.05.2012).
312 http://www.austlii.edu.au/au/legis/qld/consol_act/cc189994/s408d.html (28.05.2012).

sollten[313]. Des Weiteren sei bereits ein Viertel aller Fälle von Betrug auf Identitätsdiebstahl zurückzuführen. Im Jahr 2003 veröffentlichte auch das Securities Industry Reasearch Centre of Asia-Pacific, kurz SIRCA, einen Report zum Thema Identitätsdiebstahl und Identitätsmissbrauch, wonach diese Art von Verbrechen die australischen Unternehmen etwa 1,1 Milliarden Dollar von 2001 bis 2002 gekostet habe[314]. Im Juli 2004 beauftragte die australische Regierung ein Expertenkomitee, das Model Criminal Law Officers Committee, mit der Ausarbeitung von Empfehlungen im Hinblick auf gesonderte rechtliche Bestimmungen für Identitätsdiebstahl und Identitätsmissbrauch auf Bundesebene. Im April 2007 veröffentlichte das MCLOC ein Diskussionspapier zum Thema „Identity Crime“[315]. In dem darauffolgenden Abschlussbericht des MCLOC (im März 2008) empfahl das Expertenkomitee auf Bundesebene drei neue Tatbestände zu schaffen, die „Identity Crime“, also Identitätsdiebstahl und Identitätsmissbrauch, abdecken sollten[316]:

- Handel mit Identifikationsinformationen;
- Besitz von Identifikationsinformationen mit dem Vorsatz, eine Straftat zu begehen oder bei der Begehung einer Straftat zu helfen;
- Besitz von Ausrüstung zur Herstellung von Identifikationsinformationen.

Das Expertenkomitee war der Ansicht, dass die bereits bestehenden Tatbestände des Criminal Code Act 1995 nicht ausreichen würden, um angemessen auf das schnelle Wachstum von Identitätsdiebstahl in Australien zu reagieren. Zusätzlich sei es notwendig, etwaige Gesetzeslücken zu schließen, um eine ordentliche Strafverfolgung zu gewährleisten.

Im Winter 2008 wurde im australischen Parlament ein Gesetzesentwurf eingebracht, der den Criminal Code Act 1995 um die vom MCLOC vorgeschlagenen neuen Tatbestände erweitern sollte; allerdings ist dieser Entwurf bis jetzt nicht umgesetzt worden[317]. Bis zum heutigen Tag gibt es in Australien keinen gesonderten Straftatbestand für Identitätsdiebstahl und Identitätsmissbrauch auf Bundesebene.

2009 wurde durch den Bundesstaat Victoria im Zuge des Crimes Amendment (Identity Crime) Act 2009 das Gesetz um die vom MCLOC empfohlenen Straftatbestände erweitert[318]. Der Gesetzesentwurf von Victoria stimmt weitgehend mit dem Bundesgesetzesentwurf überein, die

313 http://www.aic.gov.au/crime_types/economic/idfraud.aspx#aus (28.05.2012).
314 MCLOC identity crime discussion paper, S. 8.
315 MCLOC identity crime discussion paper.
316 MCLOC identity crime final report, S. 25.
317 http://www.comlaw.gov.au/Details/C2008B00274 (28.05.2012).
318http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubStatbook.nsf/f932b66241ecf1b7ca256e92000e23be/C32B10510FEF8F9ACA2575D8001ECE97/$FILE/09-22a.pdf (28.05.2012).

wichtigsten Passagen im Wortlaut[319]:

Crimes Act 1958 – Division 2AA-Identity Crime:

192A. Definitions

In this Division- identification documentation means a document or other thing that-

(a) contains or incorporates identification information; and

(b) is capable of being used by a person for the purpose of pretending to be, or passing themself off as, another person (whether living or dead, or real or fictitious); identification information means information relating to a person (whether living or dead, or real or fictitious) that is capable of being used (whether alone or in conjunction with other information) to identify, or purportedly identify, the person, being information such as-

(a) a name, address, date of birth or place of birth;

(b) information as to the person's marital status;

(c) information that identifies another person as a relative of the person;

(d) a driver licence or driver licence number;

(e) a passport or passport number;

(f) biometric data;

(g) a voice print;

(h) a credit or debit card, its number or data stored or encrypted on it;

(i) a financial account number, user name or password;

(j) a digital signature;

(k) a series of numbers or letters (or both) intended for use as a means of personal identification;

192B. Making, using or supplying identification information

319 http://www.austlii.edu.au/au/legis/vic/num_act/caca200922o2009349/ (28.05.2012).

(1) A person, who makes, uses or supplies identification information (that is not identification information that relates to that person), and-

(a) who is aware that, or aware that there is a substantial risk that, the information is identification information; and

(b) who intends to use or supply the information to commit an indictable offence, or to facilitate the commission of an indictable offence-

is guilty of an offence and liable to level 6 imprisonment (5 years maximum).

192C. Possession of identification information

(1) A person, who possesses identification information (that is not identification information that relates to the person), and-

(a) who is aware that, or aware that there is a substantial risk that, the information is identification information; and

(b) who intends to use the information to commit an indictable offence, or to facilitate the commission of an indictable offence-

is guilty of an offence and liable to imprisonment for a term not exceeding 3 years.

192D. Possession of equipment used to make etc. identification documentation

(1) A person, who possesses equipment that is capable of being used to make, use, supply or retain identification documentation, and-

(a) who intends to use, or who intends that another person will use, the equipment to make, use, supply or retain identification documentation; and

(b) who intends to use any such identification documentation to commit an indictable offence or to facilitate the commission of an indictable offence-

is guilty of an offence and liable to imprisonment for a term not exceeding 3 years.

Nach Section 192A ist unter Identifikationsinformationen jede Form von Information zu verstehen, die für sich allein oder zusammen mit anderen Informationen zur Identifikation einer Person verwendet werden kann. Darunter fallen beispielsweise biometrische Daten, Name, Adresse oder Führerschein. Section 192B bestraft das Herstellen, Lagern und Benutzen von Identifikationsinformationen -mit der Absicht, eine Straftat zu begehen oder bei der Erfüllung einer Straftat zu helfen -mit einer Freiheitsstrafe von bis zu 5 Jahren. Section 192C bestraft den Besitz von Identifikationsinformationen -mit dem Vorsatz, eine Straftat zu begehen oder bei der Erfüllung einer Straftat zu helfen -mit einer Freiheitsstrafe von bis zu 3 Jahren. Section 192D bestraft den Besitz von Ausrüstung zur Herstellung von Identifikationsinformationen -mit dem Vorsatz, diese Ausrüstung selbst zu nutzen oder Dritten zu überlassen und mit der Absicht, eine Straftat zu begehen oder bei der Erfüllung einer Straftat zu helfen, mit einer Freiheitsstrafe von bis zu 3 Jahren. Nach Section 192E ist der Versuch alleine nicht strafbar. Für die Strafverfolgung ist die Polizei desjeweiligen australischen Bundesstaates zuständig, wie etwa die Victoria Police oder die Queensland Police.

Abschließend die rechtliche Lage bezüglich Identitätsdiebstahl und Identitätsmissbrauch in Australien noch einmal kurz zusammengefasst:

- Auf Bundesebene gibt es derzeit noch keinen gesonderten Straftatbestand. Ein entsprechender Gesetzesentwurf liegt im australischen Parlament vor, wurde aber noch nicht umgesetzt.
- In Australien besitzen 3 Bundesstaaten detaillierte rechtliche Regelungen zu Identitätsdiebstahl und Identitätsmissbrauch: Queensland, Südaustralien und Victoria. Victoria hat als einziger Bundesstaat sein Gesetz an die Empfehlungen des MCLOC angepasst.
- In Australien existieren keine detaillierten rechtlichen Regelungen, die den Umgang mit personenbezogenen Daten sowohl im privaten als auch im öffentlichen Sektor regeln.
- Das Computerstrafrecht kann als durchaus umfangreich und ausreichend angesehen werden.

5.4 Rechtliche Bestimmungen in Südkorea

Südkorea besitzt aktuell keine eigenen Straftatbestände für Identitätsdiebstahl und Identitätsmissbrauch. Der Grund, warum dieser Staat trotzdem in dieser Arbeit aufgeführt wurde, ist, dass ein sehr interessanter Ansatz im Hinblick auf die zivilrechtliche Haftung bei Identitätsdiebstahl verfolgt wird. Im Zuge des Electronic Financial Transactions Act aus dem Jahr 2006 führte die südkoreanische Regierung neue Gesetze ein, nach denen nun Finanzunternehmen ihre Kunden für jeglichen virtuell entstandenen Schaden entschädigen müssen[320]. Durch dieses Gesetz wird explizit auch elektronischer Identitätsdiebstahl und ein Hacken von Kundenaccounts abgedeckt. Des Weiteren ist es völlig unerheblich, ob die Finanzunternehmen direkt für den entstandenen Schaden verantwortlich sind oder nicht[321].

Das südkoreanische Finanzministerium erachtete die neuen Gesetze als notwendig, da bereits etwa 23 Millionen Südkoreaner E-Banking aktiv nutzen würden und speziell auf diesem Sektor ein enormer Zuwachs an Betrugsfällen zu verzeichnen sei[322]. Bis 2006 hatten sich südkoreanische Banken geweigert, einen durch Identitätsdiebstahl oder Identitätsmissbrauch entstandenen Schaden bei Kunden zu ersetzen, wenn der Kunde nicht nachweisen konnte, dass die Bank für den Schaden verantwortlich war.

Der Kunde hat nach nunmehr geltender Rechtslage nur dann keinen Anspruch auf Entschädigung, wenn die Bank nachweisen kann, dass er grob unachtsam mit seinen Daten (wie etwa PIN, Kreditkartennummer oder E-Banking Passwort) umging. Das heißt: Der Kunde muss trotz der aktuellen rechtlichen Lage ein Mindestmaß an Sicherheit wahren und haftet im Ergebnis dafür.

5.5 Die Europäische Union

Bisher gibt es im Recht der Europäischen Union keine Richtlinie oder Verordnung, die direkt Identitätsdiebstahl oder Identitätsmissbrauch zum Thema hat. Es existiert aber eine Reihe von Richtlinien und Verordnungen, durch die ein Identitätsdiebstahl oder Identitätsmissbrauch sanktioniert werden könnte:

- Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr legte die Mindeststandards im Hinblick auf Datenschutz für die Mitgliedsstaaten der Europäischen Union fest[323]. Diese

320 http://www.finextra.com/news/fullstory.aspx?newsitemid=14634 (02.06.2012).
321 http://www.finextra.com/news/fullstory.aspx?newsitemid=14634 (02.06.2012).
322 https://www.bis.org/cpss/paysys/Korea.pdf (02.06.2012).
323 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT (02.06.2012).

Richtlinie wurde in allen EU-Staaten durch nationale Gesetze umgesetzt, in Österreich durch das Datenschutzgesetz 2000[324]. Dank dieser Richtlinie verfügen nahezu alle Mitgliedstaaten der EU über ein umfassendes Datenschutzgesetz, das strenge rechtliche Bestimmungen für den Umgang mit personenbezogenen Daten enthält.

- Der Rahmenbeschluss des Rates vom 28.Mai 2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit bargeldlosen Zahlungsmitteln sah unter anderem Strafsanktionen für die widerrechtliche Aneignung von Zahlungsinstrumenten, die Fälschung eines Zahlungsinstruments, die betrügerische Verwendung gestohlener oder gefälschter Zahlungsinstrumente und die unberechtigte Eingabe von Identifikationsdaten vor[325].
- Der Rahmenbeschluss 2008/841/JI des Rates vom 24.Oktober 2008 zur Bekämpfung der organisierten Kriminalität erfasst Identitätsdiebstahl und Identitätsmissbrauch, wenn diese in größerem Umfang und in organisierter Form betrieben werden[326].
- Der Rahmenbeschluss 2005/222/JI des Rates vom 24.Februar 2005 über Angriffe auf Informationssysteme erfasst den rechtswidrigen Zugriff auf Informationssysteme, rechtswidrige Systemeingriffe und den rechtswidrigen Eingriff in Daten[327]. Zusätzlich hatte dieser Rahmenbeschluss das Ziel, die grenzübergreifende Strafverfolgung bei Computerkriminalität innerhalb der EU zu erleichtern.

Neben diesen bereits existierenden Rechtsakten sind bestimmte Organisationen oder Aktionspläne hervorzuheben, für die das rasche Wachstum von Identitätsdiebstahl und Identitätsmissbrauch längst ein Thema ist:

- Im Rahmen des Single Europe Payments Area[328] (SEPA), ein Projekt im Bankwesen mit dem Ziel, einen in Europa einheitlichen Zahlungsraum für Euro-Transaktionen zu schaffen, wurde von der Kommission in Zusammenarbeit mit der EU Fraud Prevention Expert Group (FPEG)[329] ein Aktionsplan zur präventiven Betrugsbekämpfung im bargeldlosen Zahlungsverkehr (Fraud Prevention Action Plan 2004-2007) ausgearbeitet[330]. In diesem Aktionsplan wird erstmals auch Identitätsdiebstahl und Identitätsmissbrauch als massive

324 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (02.06.2012).
325 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001F0413:DE:HTML (02.06.2012).
326 http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/jl0011_de.htm (02.06.2012).
327 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:DE:NOT (02.06.2012).
328 http://ec.europa.eu/internal_market/payments/sepa/index_de.htm (02.06.2012).
329 http://ec.europa.eu/internal_market/fpeg/index_en.htm (02.06.2012).
330 http://europa.eu/legislation_summaries/fight_against_fraud/fight_against_counterfeiting/l33306_en.htm (02.06.2012).

Bedrohung für den unbaren Zahlungsverkehr in Europa gesehen. Die Mitteilung der Kommission an das Europäische Parlament enthält unter anderem folgenden Handlungsschwerpunkt[331]:

„Die Kommission wird prüfen, ob es sinnvoll wäre, für das Problem des Identitätsdiebstahls in der EU eine zentrale Anlaufstelle für Bürger und Unternehmen zu schaffen, die auch ein Register der mit der Prävention von Identitätsdiebstahl befassten Stellen führen könnte."

Inhalt dieser Mitteilung ist auch eine kurze Analyse des im Februar 2004 von der Kommission gehaltenen Workshops zum Thema Identitätsdiebstahl, wonach Identitätsdiebstahl in manchen Mitgliedstaaten der EU (etwa England oder Deutschland) das damals am schnellsten wachsende Verbrechen sei. Des Weiteren sei Identitätsdiebstahl ein sektorübergreifendes Problem, das Regierungen, Unternehmen und Bürger gleichermaßen betreffen würde und das zunehmend mit organisiertem Verbrechen verknüpft sei[332]. Im April 2008 wurde seitens der Kommission ein Report über die Implementation des Aktionsplans 2004-2007 veröffentlicht, der dem Thema Identitätsdiebstahl und Identitätsmissbrauch im elektronischen Zahlungsverkehr ein eigenes Kapitel widmete[333].

- Laut Organised Crime Threat Assessment 2007 von Europol würden zunehmend zur Authentifizierung dienende Daten und Dokumente das Ziel von organisiertem Verbrechen werden anstelle der Personen selbst[334].
- Im November 2006 wurde von der Kommission eine Konferenz zum Thema Identitätsdiebstahl und Zahlungsbetrug abgehalten[335]. Bezüglich Identitätsdiebstahls war man sich einig, dass europaweit ein besseres Verständnis des Problems notwendig sei; ebenso wäre es notwendig, gezielt statistische Daten über Identitätsdiebstahl zu sammeln, um dessen Ausmaß und Wachstum besser bewerten zu können.
- Portugal organisierte während seiner Ratspräsidentschaft im November 2007 eine Konferenz über Identitätsdiebstahl und Identitätsmissbrauch. Die Ergebnisse waren im Wesentlichen ident mit den Ergebnissen der Konferenz aus dem Jahr 2006, allerdings wurde nach der Konferenz in Portugal ein Glossar zu Identitätsdiebstahl in der EU geschaffen sowie eine analytische Studie zu Identitätssystemen durchgeführt[336].

331 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=de&numdoc=52004DC0679%20&model=guichett (02.06.2012).
332 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=de&numdoc=52004DC0679%20&model=guichett (03.06.2012).
333 http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf (03.06.2012).
334 EU Organized Crime Threat Assessment 2007, S. 17.
335 http://ec.europa.eu/internal_market/fpeg/docs/minutes_20061128.pdf (03.06.2012).
336 www.idfraudconference-pt2007.org (03.06.2012).

- Im Mai 2007 verfasste die Europäische Kommission eine Mitteilung an das Europäische Parlament mit dem Titel „Eine allgemeine Politik zur Bekämpfung der Internetkriminalität“[337]. In dieser Mitteilung wurde seitens der Kommission angesprochen, dass das größte Problem bezüglich Internetkriminalität die grenzübergreifende Strafverfolgung wäre. Häufig würde eine erfolgreiche strafrechtliche Sanktionierung eines auf der Nutzung des Internet basierenden Verbrechens von der zuständigen Gerichtsbarkeit, der Zulässigkeit elektronischer Beweismittel und den anwendbaren Rechtsvorschriften abhängen. Es müssten also entsprechende Strukturen für eine unmittelbare, grenzübergreifende operative Zusammenarbeit bei der Strafverfolgung innerhalb der EU geschaffen werden. Im Zuge dieser Mitteilung wird auch das Problem des Identitätsdiebstahls angesprochen: *„Ein besonderer Punkt, der eine gesetzliche Regelung erforderlich machen könnte, ist die in Verbindung mit Identitätsdiebstahl begangene Internetkriminalität. Allgemein wird unter Identitätsdiebstahl der Diebstahl und die Verwendung von personenbezogenen Daten zur Begehung einer anderen Straftat verstanden. In den meisten Mitgliedstaaten wird eine solche Handlung zumeist als Betrugsdelikt oder eine andere Straftat verfolgt, nicht jedoch als Identitätsdiebstahl, da Betrug als schwereres Verbrechen gilt. Identitätsdiebstahl ist in keinem Mitgliedstaat ein eigenständiger Straftatbestand. Da er sich jedoch leichter nachweisen lässt als Betrug, wäre der Zusammenarbeit der Strafverfolgungsbehörden in der EU sehr damit gedient, wenn es einen solchen Straftatbestand in allen Mitgliedstaaten gäbe“*[338]. In dieser Mitteilung wird also erstmals seitens der Kommission ein eigener Straftatbestand für Identitätsdiebstahl in der EU, zum Zweck einer Erleichterung der grenzübergreifenden Strafverfolgung, empfohlen. Eine Studie zu diesem Thema wurde zwar in dieser Mitteilung ebenfalls nahe gelegt aber bisher noch nicht umgesetzt.
- Um EU-weit die Verifizierung von Identitätsdokumenten zu erleichtern, wurde ein öffentliches Online-Register für echte Identitäts- und Reisedokumente erschaffen, das Public Register of Authentic Identity and Travel Documents Online[339]. Bei PRADO handelt es sich um „*eine mehrsprachige Website für die Verbreitung von Informationen über die Sicherheitsmerkmale echter Identitäts- und Reisedokumente an die Öffentlichkeit*“[340], also auch an private Unternehmen wie etwa Banken. Die Website wird vom Generalsekretariat des Rates der europäischen Union gehostet. Eine EU-weite Anlaufstelle für Opfer von Identitätsdiebstahl, wie sie im Aktionsplan 2004-2007 gegen den Betrug im Umgang mit

337 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:DE:PDF (03.06.2012).
338 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:DE:PDF (03.06.2012).
339 http://prado.consilium.europa.eu/DE/homeindex.html (03.06.2012).
340 http://prado.consilium.europa.eu/DE/aboutUs.html (03.06.2012).

unbaren Zahlungsmitteln gefordert wurde, wurde zwar mehrmals bereits angedacht, bisher aber noch nicht realisiert.

- Im Oktober 2007 veröffentlichte die FPEG einen Bericht zu Identitätsdiebstahl und seinen Auswirkungen auf den Finanzsektor[341]. Im Rahmen dieses Berichts wurden bereits bekannte Probleme zum Thema Identitätsdiebstahl in der Europäischen Union aufgelistet: Es gäbe keine in Europa einheitliche Definition von Identitätsdiebstahl und Identitätsmissbrauch; Identitätsdiebstahl alleine sei nicht strafbar sondern nur die darauf aufbauenden Delikte wie Betrug; es bestünden strukturelle Mängel bei der grenzübergreifenden Strafverfolgung im Rahmen von Cybercrime und eine europaweite Anlaufstelle für Opfer von Identitätsdiebstahl würde fehlen. Der Bericht kommt anschließend zu folgendem Fazit: Identitätsdiebstahl würde sich nicht nur gegen eine einzelne Person richten, sondern mehr gegen eine Art „Identitätskette“, die aus dem Rechner des Kunden, dem Internet Service Provider des Kunden und dem Finanzunternehmen bestehen würde. Aktuelle Trends hätten gezeigt, dass der Rechner des Kunden das schwächste Glied in dieser Kette wäre; dennoch müsse die Verantwortung für Identitätsdiebstahl gleichmäßig verteilt werden. Es wäre dringend anzuraten, Kunden zu „schulen“, da jede noch so effiziente Sicherheitsmaßnahme ansonsten sinnlos wäre. Des Weiteren würde das Problem Identitätsdiebstahl bereits weit über den Finanzsektor hinausgehen. Eine Zusammenarbeit zwischen den unterschiedlichen Sektoren und den öffentlichen Behörden wäre empfehlenswert. Als letzten Punkt empfiehlt die FPEG in ihrem Bericht die Hilfe für Opfer von Identitätsdiebstahl zu verbessern, da nur so eine längerfristige Steigerung des Vertrauens der Kunden in elektronische Finanzdienstleistungen erreicht werden könne.
- Im Zuge des 6. EU-Forschungsrahmenprogramms wurden die Projekte PRIME und FIDIS ins Leben gerufen. Ziel von PRIME (Privacy and Identity Management for Europe) war es einen Prototyp für ein Identitätsmanagementsystem zu entwickeln, um die Sicherheit von Kundendaten zu verbessern und Identitätsdiebstahl auf der Ebene des Computers des Kunden entgegenzuwirken[342]. Derzeit wird das Projekt unter dem Namen PrimeLife im Zuge des 7. Rahmenforschungsprogramm fortgeführt. Beim FIDIS-Netzwerk(Future of Identity in the Information Society) handelt es sich um ein Projekt, das sich (allgemein ausgedrückt) mit dem Begriff der Identität im Informationszeitalter beschäftigt[343]. Unter anderem beschäftigt sich das FIDIS-Netzwerk auch mit Identitätsdiebstahl und

341 http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf (03.06.2012).
342 https://www.prime-project.eu/ (04.06.2012).
343 http://www.fidis.net/ (04.06.2012).

Identitätsmissbrauch[344]. Unter Work Package 5.1 werden die Begriffe „identity theft“ und „identity fraud“ definiert. Unter Work Package 5.2b werden mögliche Gegenmaßnahmen für Identitätsdiebstahl und Identitätsmissbrauch aufgelistet[345]: FIDIS merkt an, dass bei der Bekämpfung von Identitätsmissbrauch weniger ein Mangel an strafrechtlichen Bestimmungen das Problem ist, sondern dass die grenzübergreifende Strafverfolgung sich in den meisten Fällen äußerst schwierig gestalten würde. Vor allem die Gesetze von Ländern außerhalb der EU würden, speziell im Hinblick auf Datenschutz, empfindliche Lücken aufweisen. Des Weiteren wäre das Recht alleine nicht in der Lage, Identitätsmissbrauch effizient zu bekämpfen, da die Täter meist über hervorragende technische Kenntnisse verfügen würden und somit einen entsprechenden Vorteil hätten, zumal die Technologie sich meist schneller entwickelt, als Gesetze angepasst werden können. Eine erfolgreiche, langfristige Bekämpfung von Identitätsmissbrauch könne nur durch eine gemeinsame Kombination aus technischen, organisatorischen, sozioökonomischen, sozialen und rechtlichen Maßnahmen erfolgen.

- Im Zuge des 7. EU-Forschungsrahmenprogramms wurden weitere Projekte wie PRISM oder SWIFT ins Leben gerufen, die sich ebenfalls mit sicheren Authentifizierungstechnologien für Online-Dienste oder mehr Sicherheit bei der Verwaltung von Identitätsdaten beschäftigen[346].
- Im November 2011 wurde vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments ein Bericht über den Vorschlag für eine Richtlinie des europäischen Parlaments über Angriffe auf Informationssysteme entworfen[347]. Unter Erwägung 7a wird Identitätsdiebstahl adressiert[348]: „*Wenn auch die Verschleierung der wahren Identität des Täters und der dem rechtmäßigen Identitätseigentümer entstandene Schaden ein wichtiges Element für die Bestimmung der Strafen innerhalb des Anwendungsbereichs dieser Richtlinie darstellen, sollte die Union doch ein horizontales Instrument entwickeln, das diese und damit zusammenhängende Straftaten in einer umfassenderen Form abdeckt, indem man sich unter anderem mit Identitätsdiebstahl, der Verbindung zum Namensrecht und Verbraucherschutz befasst.“* Es wird in diesem Bericht auch angemerkt, dass präventive Maßnahmen gegen Cyberkriminalität verbessert werden müssten und dass diesbezüglich die Bemühungen der Mitgliedstaaten gebündelt werden

344 http://www.fidis.net/resources/deliverables/forensic-implications/int-d51000/doc/4/ (04.06.2012).
345 http://www.fidis.net/resources/deliverables/forensic-implications/int-d52b000/doc/41/ (04.06.2012).
346 http://www.cordis.europa.eu/fp7/ict/security/projects_en.html#TSI (04.06.2012).
347 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/884/884601/884601de.pdf (04.06.2012).
348 http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/884/884601/884601de.pdf (04.06.2012).

sollten, da das Strafrecht alleine nicht ausreichend wäre, um den sich immer schneller verändernden Verbrechensmustern Herr zu werden.

Es gibt natürlich noch einige weitere Organisationen wie etwa ENISA[349] (European Network and Information Security Agency), die sich unter anderem auch mit Identitätsdiebstahl und Identitätsmissbrauch befassen; allerdings wurden idR keine gesonderten Berichte zu diesem Thema verfasst und nur wenige Handlungsempfehlungen gegeben. Insgesamt wurde von der EU das Budget für die Forschung im Bereich IT-Sicherheit von 750 Millionen Euro auf 1,4 Milliarden Euro für den Zeitraum von 2007-2013 angehoben.

Trotz aller Bemühungen und Empfehlungen gibt es bislang noch keinen rechtlichen Ansatzpunkt für gesonderte Straftatbestände betreffend Identitätsdiebstahl oder Identitätsmissbrauch auf EU-Ebene.

5.5.1 Österreich

Österreich hat, verglichen mit anderen EU-Mitgliedstaaten wie etwa Deutschland, England oder Frankreich, noch eher geringe Probleme mit Identitätsdiebstahl und Identitätsmissbrauch. Dennoch belegen aktuelle Zahlen des BKA, dass diese Art der Kriminalität auch in Österreich mit hoher Geschwindigkeit zunimmt. Allein im Jahr 2010 wurde in Österreich durch Internetbetrug ein Schaden von mehr als 5,7 Millionen Euro verursacht, 2,37 Millionen Euro davon entfallen allein auf Internetauktionen[350]. In diese Schadenssumme noch nicht einmal eingerechnet sind Schäden, die durch Phishing oder widerrechtliche Zugriffe auf Computersysteme entstanden sind. Außerdem würde es sich laut BKA hier nur um den gemeldeten Schaden handeln; die Dunkelziffer sei extrem hoch, wodurch ein noch weit höherer Gesamtschaden durch Internetbetrug vermutet wird. Nach der Kriminalitätsstatistik des BKA für das erste Halbjahr 2012 ist die IT-Kriminalität um mehr als 100% gestiegen. Die Zahlen im Detail[351]:

- Im ersten Halbjahr 2012 wurden im Bereich der gesamten IT-Kriminalität 4293 Delikte zur Anzeige gebracht, im Jahr 2011 waren es noch 2143 Anzeigen.
- Phishing stieg um 328% von 45 auf 193 Anzeigen.
- Hacking stieg um über 143% von 101 auf 246 Anzeigen.
- Betrug durch Missbrauch des Internets stieg von 797 auf 1606 Anzeigen.

Nach Einschätzung des BKA würden bereits etwa 80% aller Haushalte in Österreich über einen

349 http://www.enisa.europa.eu/ (04.06.2012).
350 http://futurezone.at/digitallife/5989-5-7-millionen-euro-schaden-durch-internetbetrug.php (06.06.2012).
351 http://www.bmi.gv.at/cms/BK/presse/files/KrimStat_1HJ2012.pdf (06.06.2012).

Internetanschluss verfügen, 40% aller Österreicher würden auch mit dem Handy bereits im Internet verkehren[352]. Notwendig seien laut den Experten des BKA allerdings keine zusätzlichen gesetzlichen Bestimmungen, sondern viel mehr eine umfangreiche Aufklärung der Kunden sowie präventive Maßnahmen vor allem auf technischer und sozialer Ebene. Die Täter seien zunehmend professioneller und gut organisiert; des Weiteren würden sie es mit einer relativ naiven Clientel zu tun haben, die noch dazu wenig Interesse an Fortbildung im Umgang mit technischen Hilfsmitteln habe.

In Österreich gibt es mehrere Gesetze, die Identitätsdiebstahl oder Identitätsmissbrauch erfassen können -abhängig von der Art, wie dieser begangen wurde. Wird der Identitätsdiebstahl oder Identitätsmissbrauch mit IT-Unterstützung ausgeführt, so kommen folgende Tatbestände des StGB in Frage[353]:

- § 118a – Widerrechtlicher Zugriff auf ein Computersystem[354]:

  „Wer sich in der Absicht, sich oder einem anderen Unbefugten von in einem Computersystem gespeicherten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen Zugang verschafft, indem er spezifische Sicherheitsvorkehrungen im Computersystem überwindet, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“

- § 119 – Verletzung des Telekommunikationsgeheimnisses[355]:

  „Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“

352 http://www.bka.gv.at/site/4297/default.aspx (06.06.2012).
353 Susanne Reindl-Krauskopf, Computerstrafrecht im Überblick, S. 33.
354 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).
355 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).

- § 119a – Missbräuchliches Abfangen von Daten[356]:

  „Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“

- Werden im Zuge des Identitätsdiebstahls oder Identitätsmissbrauchs geheime Daten eines Unternehmens gestohlen, um damit Gewinn zu erzielen, so ist möglicherweise auch § 123 anwendbar - „Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses“[357].

- § 126a – Datenbeschädigung[358]:

  „Wer einen anderen dadurch schädigt, daß er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“

- § 126b – Störung der Funktionsfähigkeit eines Computersystems[359]:

  „Wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt oder übermittelt, ist, wenn die Tat nicht nach § 126a mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“

- § 126c – Missbrauch von Computerprogrammen oder Zugangsdaten[360]:

  (1) Wer

  1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur

356 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).
357 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).
358 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).
359 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).
360 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).

Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder

2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen,

mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

- § 148a – Betrügerischer Datenverarbeitungsmissbrauch[361]:

  „Wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, daß er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflußt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“

- § 225a – Datenfälschung[362]:

  „Wer durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten falsche Daten mit dem Vorsatz herstellt oder echte Daten mit dem Vorsatz verfälscht, dass sie im Rechtsverkehr zum Beweis eines Rechtes, eines Rechtsverhältnisses oder einer Tatsache gebraucht werden, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.“

Wie bereits in den Kapiteln 3.1 und 3.2 erwähnt wurde, existiert keine präzise rechtliche Definition für die Begriffe Identitätsdiebstahl und Identitätsmissbrauch. Geht man im Kontext dieses Kapitels davon aus, dass es sich bei einem Identitätsdiebstahl um die unbefugte Aneignung von personenbezogenen Daten durch eine technische Angriffsmethode handelt, so wäre dies in Österreich idR nach § 118a StGB strafbar. Je nach Art des Angriffs kämen eventuell auch § 119 StGB oder § 119a StGB in Frage; wenn der Angreifer für die Aneignung der Daten Malware

361 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).

362 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).

einsetzt, so ist er wegen der diesem Einsatz vorgelagerten Handlungen zusätzlich nach § 126c StGB strafbar. Die unbefugte Nutzung der angeeigneten personenbezogenen Daten, also der eigentliche Identitätsmissbrauch, ist in den meisten Fällen nach § 108 StGB (Täuschung), oder § 146 StGB (Betrug oder schwerer Betrug) strafbar; je nach Art des Missbrauchs kommen eventuell auch § 148a, § 225a oder gegebenenfalls § 107a zum Tragen:

- § 108 – Täuschung[363]:

  „Wer einem anderen in seinen Rechten dadurch absichtlich einen Schaden zufügt, daß er ihn oder einen Dritten durch Täuschung über Tatsachen zu einer Handlung, Duldung oder Unterlassung verleitet, die den Schaden herbeiführt, ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.“

- § 146 – Betrug[364]:

  „Wer mit dem Vorsatz, durch das Verhalten des Getäuschten sich oder einen Dritten unrechtmäßig zu bereichern, jemanden durch Täuschung über Tatsachen zu einer Handlung Duldung oder Unterlassung verleitet, die diesen oder einen anderen am Vermögen schädigt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“

- § 147 – Schwerer Betrug[365]:

  „(1) Wer einen Betrug begeht, indem er zur Täuschung

  1.eine falsche oder verfälschte Urkunde, ein falsches, verfälschtes oder entfremdetes unbares Zahlungsmittel, falsche oder verfälschte Daten, ein anderes solches Beweismittel oder ein unrichtiges Meßgerät benützt,

  2.ein zur Bezeichnung der Grenze oder des Wasserstands bestimmtes Zeichen unrichtig setzt, verrückt, beseitigt oder unkenntlich macht oder

  3.sich fälschlich für einen Beamten ausgibt,

  ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

  (1a) Ebenso ist zu bestrafen, wer einen Betrug mit mehr als geringem Schaden begeht, indem er über die Anwendung eines verbotenen Wirkstoffs oder einer verbotenen Methode nach der Anlage der Anti-Doping-Konvention, BGBl. Nr. 451/1991, zu Zwecken des

363 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).
364 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).
365 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).

Dopings im Sport täuscht.

(2) Ebenso ist zu bestrafen, wer einen Betrug mit einem 3 000 Euro übersteigenden Schaden begeht.

(3) Wer durch die Tat einen 50 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.“

- § 107a – Beharrliche Verfolgung[366]:

  „(1) Wer eine Person widerrechtlich beharrlich verfolgt (Abs. 2), ist mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

  (2) Beharrlich verfolgt eine Person, wer in einer Weise, die geeignet ist, sie in ihrer Lebensführung unzumutbar zu beeinträchtigen, eine längere Zeit hindurch fortgesetzt

  1. ihre räumliche Nähe aufsucht,

  2. im Wege einer Telekommunikation oder unter Verwendung eines sonstigen Kommunikationsmittels oder über Dritte Kontakt zu ihr herstellt,

  3. unter Verwendung ihrer personenbezogenen Daten Waren oder Dienstleistungen für sie bestellt oder

  4. unter Verwendung ihrer personenbezogenen Daten Dritte veranlasst, mit ihr Kontakt aufzunehmen.“

Technische Angriffsmethoden, wie in Kapitel 4 dieser Arbeit beschrieben, würden also fast immer neben zahlreichen anderen Straftatbeständen auch jenen des schweren Betruges in Österreich erfüllen, was mit einem verhältnismäßig hohem Strafmaß verbunden wäre. Je nach Art des Identitätsmissbrauchs wären auch zahlreiche weitere Straftatbestände denkbar, wie etwa § 111 StGB (Üble Nachrede) oder § 115 StGB (Beleidigung), falls der Angreifer mit der unbefugt angeeigneten Identität Ruf und Ansehen des Identitätsinhabers schädigt. Wird der Identitätsdiebstahl oder Identitätsmissbrauch durch eine kriminelle Vereinigung verübt, so wird das Strafmaß bei einigen Tatbeständen noch einmal signifikant erhöht[367]. Selbstverständlich kann ein Identitätsdiebstahl auch ohne Unterstützung von Informationstechnologie ausgeführt werden, es wären also auch Tatbestände wie § 127 StGB (Diebstahl) oder § 142 (StGB) Raub denkbar; allerdings liegt der Fokus dieser Arbeit auf Identitätsdiebstahl und Identitätsmissbrauch im Internet, weswegen diese Möglichkeiten nicht weiter erörtert werden.

366 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).

367 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012).

Ein weiteres Gesetz, das Identitätsdiebstahl oder Identitätsmissbrauch erfassen würde, ist das österreichische Datenschutzgesetz, das DSG 2000. Dieses enthält detaillierte rechtliche Bestimmungen für den Umgang mit persönlichen Daten. Das Grundrecht auf Datenschutz wird nach § 1 DSG folgendermaßen definiert[368]:

„(1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den inArt. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK),BGBL. Nr. 210/1958 , genannten Gründen notwendig sind. Derartige Gesetze dürfen dieVerwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.“

Nach § 4 DSG handelt es sich bei personenbezogenen Daten um „*Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist“*[369]. Dieser Begriff wird also sehr allgemein definiert, was dazu führt, dass nicht nur Angaben wie Name, Adresse oder Sozialversicherungsnummer einer Person als personenbezogene Daten nach dem Gesetz erachtet werden können, sondern auch Daten wie beispielsweise Kreditkartennummern, Kontonummern oder Accountpasswörter. Unter die Verwendung von Daten fällt nach § 4 DSG *„jede Art der Handhabung von Daten, also sowohl das Verarbeiten als auch das Übermitteln von Daten“*[370]. Das Verarbeiten von Daten umfasst nach § 4 DSG das *„Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns von*

368 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012).

369 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012).

370 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012).

Daten"[371]. Die Übermittlung von Daten nach § 4 DSG ist *„die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen von Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers"*[372]. § 1 sowie § 6 und §7 DSG, welche genaue Bestimmungen für die Verwendung von Daten enthalten, bestimmen den grundlegenden Schutz personenbezogener Daten in Österreich:

Die Verarbeitung oder Übermittlung personenbezogener Daten ist nur zulässig, wenn der Betroffene dies erlaubt, es im lebenswichtigen Interesse des Betroffenen ist, oder auf Grund von Gesetzen. Bei einem Identitätsdiebstahl oder Identitätsmissbrauch im Internet handelt es sich im Regelfall zumindest um eine Verarbeitung personenbezogener Daten, womit sowohl Identitätsdiebstahl als auch Identitätsmissbrauch mangels Vorliegen eines validen Rechtfertigungsbestands zugunsten des Täters durch das österreichische DSG verboten sind. Darüber hinaus enthält das DSG in seinem 3. Abschnitt auch umfassende Anforderungen an die Auftraggeber und Dienstleister bezüglich der Datensicherheit; also betreffend Maßnahmen, die gesetzt werden müssen, um die verwalteten personenbezogenen Daten vor Missbrauch zu schützen. Erwähnenswert ist ferner, dass nach dem österreichischen DSG nicht nur die personenbezogenen Daten natürlicher Personen, sondern auch die Daten juristischer Personen unter Schutz stehen.

Zivilrechtlich gesehen stellt Identitätsmissbrauch in Österreich einen Eingriff in die Persönlichkeitsrechte eines Menschen dar. Neben dem Recht auf informationelle Selbstbestimmung wird auch der Namensschutz nach § 43 ABGB verletzt[373]:

„Wird jemandem das Recht zur Führung seines Namens bestritten oder wird er durch unbefugten Gebrauch seines Namens (Decknamens) beeinträchtigt, so kann er auf Unterlassung und bei Verschulden auf Schadenersatz klagen".

Das heißt, ein Täter kann für den unbefugten Gebrauch einer Identität nicht nur strafrechtlich belangt werden; er haftet auch zivilrechtlich für den hierdurch entstandenen Schaden.

Weitere Gesetze bezüglich Identitätsdiebstahl oder Identitätsmissbrauch sind in Österreich nur unter speziellen Umständen von Bedeutung. Wie bereits in Kapitel 2.3 erwähnt wurde, kann nicht nur die Identität eines Menschen gestohlen oder missbraucht werden, sondern auch die Identität von Unternehmen (also beispielsweise Firmennamen) oder auch die Identität von Internetdomains. In

371 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012).
372 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012).
373 http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001622 (07.06.2012).

solchen Fällen können auch das österreichische Urheberrecht oder Markenrecht zur Anwendung kommen. Zusätzlich kann im Rahmen von Internethandel auch das E-Commerce-Gesetz eine Rolle spielen; dabei geht es aber vor allem um die Frage der Haftung, die noch im einem der folgenden Kapitel etwas näher behandelt wird.

5.5.2 Deutschland

In Deutschland ist sich die Politik bereits der Probleme Identitätsdiebstahl und Identitätsmissbrauch bewusst. Im Jahr 2010 wurde auf Initiative des Bundesministerium des Innern (BMI) und im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine interdisziplinäre Studie zu Identitätsdiebstahl und Identitätsmissbrauch im Internet durchgeführt[374]. Die Studie befasst sich mit Begehungsarten dieser neuen Verbrechensform, mit geltenden rechtlichen Bestimmungen und der Bedrohung, die Identitätsdiebstahl und Identitätsmissbrauch für E-Government und E-Business darstellen. Empfohlen wird eine Reihe technischer Sicherheitsmaßnahmen sowie eine umfassende Aufklärung der Internetnutzer[375]. Die Erweiterung des deutschen Strafgesetzbuchs um einen neuen Straftatbestand wird nicht angedacht; rechtliche Adaptierungen wären nur auf EU-Ebene sinnvoll zur Erleichterung der grenzübergreifenden Strafverfolgung[376]. 2011 veröffentlichte das BSI einen Lagebericht zur IT-Sicherheit in Deutschland und widmete dabei ein ganzes Kapitel dem Thema Identitätsdiebstahl und Identitätsmissbrauch, wobei vor allem die immer professionellere Vorgehensweise der Täter als Anlass zur Sorge tituliert wird[377]:

„Identitätsdiebstahl und Identitätsmissbrauch haben sich als ein kriminelles Betätigungsfeld etabliert, das mit hoch professionellen Strukturen bearbeitet wird. Das klassische Phishing ist in den vergangenen Jahren immer weniger geworden und kaum noch feststellbar. Stattdessen nutzen die Angreifer fast ausschließlich Trojanische Pferde“.

Nach diesem Bericht haben im Jahr 2011 Fälle von Identitätsdiebstahl und Identitätsmissbrauch in Deutschland gegenüber 2009 deutlich zugenommen.

Im deutschen Strafgesetzbuch existiert derzeit noch kein eigener Straftatbestand für Identitätsdiebstahl oder Identitätsmissbrauch, es gibt aber, ähnlich wie in Österreich, eine Reihe von Tatbeständen, die anwendbar sein können. Das unbefugte Erlangen von Identitätsdaten mit

374 http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/mitMarginalspalte/06/identit%C3%A4tsdiebstahl_internet.html (08.06.2012).
375 Georg Borges, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 359.
376 Georg Borges, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 377.
377 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile (08.06.2012).

Unterstützung von IT, also der Identitätsdiebstahl, wäre im deutschen StGB potentiell strafbar nach[378]:

- § 202a – Ausspähen von Daten
- § 202b – Abfangen von Daten
- § 202c – Vorbereiten des Ausspähens und Abfangens von Daten
- § 303a – Datenveränderung

Der Identitätsmissbrauch, also die unbefugte Nutzung der Identitätsdaten, kann strafbar sein nach[379]:

- § 263 – Betrug
- § 263a – Computerbetrug
- § 267 – Urkundenfälschung
- § 269 – Fälschung beweiserheblicher Daten
- § 270 – Täuschung im Rechtsverkehr bei Datenverarbeitung
- § 132 – Amtsanmaßung
- § 132a – Missbrauch von Titeln, Berufsbezeichnungen und Abzeichen

Wird durch einen Identitätsdiebstahl oder Identitätsmissbrauch der Ruf des Identitätsinhabers geschädigt, können auch § 185 (Beleidigung), § 186 (Üble Nachrede) oder § 187 (Verleumdung) erfüllt sein[380]. Dient der Identitätsdiebstahl oder Identitätsmissbrauch dem Zwecke des Stalkings, so ist dies in Deutschland strafbar nach § 238 (Nachstellung)[381].

Ebenfalls von Bedeutung im Zusammenhang mit Identitätsdiebstahl und Identitätsmissbrauch ist, wie auch in Österreich, das Bundesdatenschutzgesetz (BDSG). Personenbezogene Daten werden in § 3 BDSG legaldefiniert als „*Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person*“[382]. Diese Definition weicht zwar leicht von jener des österreichischen DSG ab, allerdings umfasst sie ebenfalls alle Daten, die einer Person zugeordnet werden können. Nach § 4 BDSG ist „*die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat*“[383]. Das heißt, die Schutzkonzeption ist

378 http://www.gesetze-im-internet.de/stgb/index.html (08.06.2012).
379 http://www.gesetze-im-internet.de/stgb/index.html (08.06.2012).
380 http://www.gesetze-im-internet.de/stgb/index.html (08.06.2012).
381 http://www.gesetze-im-internet.de/stgb/index.html (08.06.2012).
382 http://www.gesetze-im-internet.de/bdsg_1990/__3.html (08.06.2012).
383 http://www.gesetze-im-internet.de/bdsg_1990/__4.html (08.06.2012).

dieselbe wie beim österreichischen DSG. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist also grundsätzlich nach dem BDSG verboten; nur durch Gesetze oder Zustimmung der betroffenen Person kann dieses Verbot aufgehoben werden (sogenanntes Verbot mit Erlaubnisvorbehalt). Somit ist, wie auch in Österreich, Identitätsdiebstahl oder Identitätsmissbrauch nach dem deutschen Datenschutzgesetz nicht erlaubt. Selbstverständlich existieren auch im deutschen BDSG detaillierte Bestimmungen für Behörden und Unternehmen bezüglich des Umgangs mit personenbezogenen Daten und bezüglich Mindeststandards für entsprechende Sicherheitsmaßnahmen; diese werden aber an dieser Stelle nicht weiter ausgeführt, da die sich aufgrund der Vorgaben in EU-Richtlinien praktisch kaum von jenen des österreichischen DSG unterscheiden.

Neben dem Strafrecht und dem Datenschutzrecht können auch Grundrechte bei Identitätsdiebstahl oder Identitätsmissbrauch in Deutschland zum Tragen kommen. Das unbefugte Erlangen von Daten sowie auch deren unbefugte Nutzung stellen einen Eingriff in das Allgemeine Persönlichkeitsrecht dar, genauer gesagt in das Recht auf informationelle Selbstbestimmung. Das Recht auf informationelle Selbstbestimmung wurde vom deutschen Bundesverfassungsgericht im Zuge seines Volkszählungsurteils[384] aus dem Jahr 1983 als Grundrecht anerkannt. Es handelt sich dabei um das

„*Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen“*[385]. Jedwede unbefugte Erhebung von persönlichen Daten oder deren Missbrauch stellt also auch eine Verletzung der Grundrechte dar. Weitere Grundrechte, die Identitätsdaten schützen, sind das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, welches *„dem Schutz von persönlichen Daten dient, die in informationstechnischen Systemen gespeichert oder verarbeitet werden“*[386], sowie das Telekommunikationsgeheimnis Art. 10 Abs. 1 GG[387]. Unmittelbaren Schutz gewähren diese Grundrechte in der Regel freilich nur dem Staat gegenüber.

5.5.3 Frankreich

Frankreich zählt zu den am stärksten von einschlägigen Delikten betroffenen Mitgliedstaaten der EU. Aktuellen Zahlen zufolge werden in Frankreich etwa 210.000 Menschen pro Jahr Opfer eines Identitätsdiebstahls oder Identitätsmissbrauchs; allein der Schaden auf Seiten der Opfer beträgt rund

384 http://www.servat.unibe.ch/dfr/bv065001.html# (08.06.2012).
385 http://www.servat.unibe.ch/dfr/bv065001.html# (08.06.2012).
386 http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html (09.06.2012).
387 http://www.gesetze-im-internet.de/gg/art_10.html (09.06.2012).

474 Millionen Euro jährlich[388]. Bis zum Jahr 2009 war das französische Justizministerium der Ansicht, dass neue rechtliche Bestimmungen nicht notwendig seien, da im französischen Strafrecht, dem Code pénal, Identitätsmissbrauch durch gängige Tatbestände wie etwa Betrug abgedeckt ist. Zusätzlich enthält der Code pénal Artikel 434-23, der Identitätsmissbrauch unter Strafe stellt, falls dieser zu einer Strafverfolgung gegen den eigentlichen Identitätsinhaber hätte führen können[389]. Das Strafmaß nach Art. 434-23 beträgt bis zu 5 Jahre Haft und eine Summe von 75.000 Euro Geldstrafe. 2009 wurde von der französischen Regierung ein Entwurf für eine Gesetzesänderung eingebracht, wonach das französische Strafgesetz um den Tatbestand des Identitätsmissbrauchs erweitert werden sollte (Artikel 222-16-1)[390]:

„Le fait d'utiliser, de manière réitérée, sur un réseau de communication électronique l'identité d'un tiers ou des données qui lui sont personnelles, en vue de troubler la tranquillité de cette personne ou d'autrui, est puni d'un an d'emprisonnement et de 15.000 € d'amende.

Est puni de la même peine le fait d'utiliser, sur un réseau de communication électronique, l'identité d'un tiers ou des données qui lui sont personnelles, en vue de porter atteinte à son honneur ou à sa considération."

Nach Artikel 222-16-1 ist strafbar, wer mehrmals die elektronische Identität oder personenbezogenen Daten eines anderen so gebraucht, dass dieser hierdurch gestört oder belästigt wird. Ein einmaliger Missbrauch der elektronischen Identität oder der Daten ist strafbar, wenn dies zu einer Verletzung der Ehre oder des Ansehen des Betroffenen führt. Das Strafmaß beträgt bis zu 1 Jahr Haft und 15.000 Euro Strafe. Nach diesem Entwurf würde Identitätsmissbrauch als Delikt gegen die psychische oder physische Verfassung einer Person eingestuft werden. Bis zum jetzigen Zeitpunkt wurde der Entwurf allerdings noch nicht umgesetzt. Im Februar 2010 wurde im Zuge des „Gesetzes zur Stärkung der inneren Sicherheit", auch „Loppsi 2" genannt, eine Erweiterung des Art. 434-23 um Artikel 434-23-1 angedacht, wonach Identitätsmissbrauch, der darauf abzielt, den Identitätsinhaber in Schwierigkeiten zu bringen, mit einer Freiheitsstrafe von bis zu einem Jahr zu sanktionieren ist[391]. Das Gesetz ist bereits verabschiedet, ist aber bis zum jetzigen Zeitpunkt noch nicht in Kraft getreten.

Im Jahr 2012 kam es in Frankreich zu einer Diskussion zwischen Opposition und Regierung wegen eines neuen Ansatzes bei der Bekämpfung von Identitätsdiebstahl. Am 6. März 2012 wurde von der

388 http://www.enass.fr/PDF/travaux_recherche/Identity_theft_presentation.pdf (09.06.2012).
389 http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=50A957F4368A76B876359512D1886752.tpdjo10v_3?idArticle=LEGIARTI000006418661&cidTexte=LEGITEXT000006070719&dateTexte=20120919 (09.06.2012).
390 http://www.assemblee-nationale.fr/13/projets/pl1697.asp (09.06.2012).
391http://www.senat.fr/leg/pjl09-292.html (09.06.2012).

französischen Regierung das „Gesetz zum Schutz der Identität“ verabschiedet[392]. Dieses sah die Schaffung einer zentralen biometrischen Datenbank vor, in der Fingerabdrücke und digitale Fotos von über 45 Millionen Franzosen gespeichert werden sollten. Zusätzlich hätte zur Identifizierung einer Person eine neue biometrische Identifikationskarte dienen sollen, die einen verpflichtenden Chip mit personenbezogenen Daten (wie zB. Fingerabdruck, Foto oder Größe des Besitzers) enthalten sollte. Diese biometrische Identifikationskarte hätte optional einen zweiten Chip enthalten können, der für Online-Authentifizierungen im Bereich des E-Commerce oder E-Government vorgesehen war. Die Opposition sah in diesem Gesetz einen Eingriff in die Grundrechte der Bürger, vor allem in das Recht auf Privatsphäre. Zudem wurde die Wirksamkeit des neuen Gesetzes im Hinblick auf Identitätsdiebstahl angezweifelt, da in Frankreich bisherige Erfahrungen mit biometrischen Pässen zeigten, dass diese eher unzuverlässig wären[393]. Bereits einen Tag nach der Verabschiedung des Gesetzes wurde dieses von der Opposition beim französischen Verfassungsgericht angefochten. Das Verfassungsgericht erklärte am 22. März 2012 das Gesetz aus mehreren Gründen für verfassungswidrig[394]:

- Das Gericht merkte an dass *„die Sammlung, Registrierung, Speicherung, Abfrage und Weitergabe von personenbezogenen Daten durch Vorteile für das Allgemeinwohl gerechtfertigt sein müsse, und weiters auch angemessen und verhältnismäßig umzusetzen sei“*[395]. Zwar bestünden keine Bedenken in Hinblick auf das Allgemeinwohl, aber: *„In Erwägung dessen, dass aus diesen Ausführungen folgt, dass in Anbetracht der Art der erhobenen Daten, des Ausmaßes der Verarbeitung der Daten, der technischen Ausgestaltung der Datenverarbeitung, sowie der Voraussetzungen für den Zugriff auf die Datenbank, die Bestimmungen des Artikels 5 in das Recht auf Achtung der Privatsphäre einen Eingriff vornehmen, der im Hinblick auf den verfolgten Zweck nicht als verhältnismäßig angesehen werden kann; dass die Artikel 5 und 10 des zur Prüfung vorgelegten Gesetzes daher für verfassungswidrig erklärt werden müssen;“*[396].
- Das Gericht kritisierte die Erstellung der biometrischen Datenbank, weil der Gesetzesentwurf eine Nutzung ebendieser durch die Polizei auch für andere Zwecke genehmigte.

392 http://www.assemblee-nationale.fr/13/ta/ta0883.asp (09.06.2012).
393 https://www.unwatched.org/book/export/html/6090 (09.06.2012).
394 http://www.conseil-constitutionnel.fr/conseil-constitutionnel/deutsch/entscheidungen/entscheidung-nr-2012-652-dc-vom-22-marz-2012-gesetz-zum-schutz-der-identitat.105656.html (09.06.2012).
395 http://www.conseil-constitutionnel.fr/conseil-constitutionnel/deutsch/entscheidungen/entscheidung-nr-2012-652-dc-vom-22-marz-2012-gesetz-zum-schutz-der-identitat.105656.html (09.06.2012).
396 http://www.conseil-constitutionnel.fr/conseil-constitutionnel/deutsch/entscheidungen/entscheidung-nr-2012-652-dc-vom-22-marz-2012-gesetz-zum-schutz-der-identitat.105656.html (09.06.2012).

- Aus Gründen des Datenschutzes wurde auch das Konzept der neuen biometrischen Identifikationskarte kritisiert. Eine Vermischung von amtlichem Ausweisdokument und elektronischem Authentifizierungsinstrument sei demnach nicht ausreichend durchdacht.

Nach dem Urteil des Verfassungsgerichts wurden sämtliche das Gesetz betreffenden Pläne ausgesetzt.

Neben diesen neuen Ansätzen existieren in Frankreich natürlich ähnliche rechtliche Bestimmungen zur Sanktionierung von Identitätsdiebstahl und Identitätsmissbrauch wie auch in Österreich und Deutschland. Da es hierbei aber keine signifikanten Unterschiede zur rechtlichen Lage in den beiden bereits ausführlich behandelten EU-Mitgliedstaaten gibt, wird auf eine detailliertere Auflistung an dieser Stelle verzichtet.

5.5.4 England

England ist aktuell der von einschlägigen Delikten am stärksten betroffene EU-Mitgliedstaat. Eine Studie der National Fraud Authority[397] aus dem Jahr 2010 ergab, dass etwa 1,8 Millionen Menschen jährlich in England Opfer eines Identitätsdiebstahls oder Identitätsmissbrauchs werden[398]. Der hierdurch verursachte finanzielle Schaden beläuft sich nach Zahlen der Studie auf über 2,7 Milliarden Pfund. Gegenüber 2005 bedeutet dies einen Anstieg des finanziellen Schadens um 500%; allein die Nutzung von Identitätsdaten verstorbener Personen zu kriminellen Zwecken nahm um 60% zu[399]. In England gibt es, wie in allen EU-Mitgliedstaaten, keinen eigenen Straftatbestand für Identitätsdiebstahl oder Identitätsmissbrauch; es existiert aber eine Reihe von Gesetzen, die diese Delikte erfassen würde. Die in diesem Zusammenhang wichtigen Gesetze sind:

- der Fraud Act 2006;
- der Data Protection Act 1998;
- der Computer Misuse Act 1990 und
- der Identity Cards Act 2006.

Bis zum Jahr 2006 konnte Identitätsmissbrauch nur nach dem Theft Act 1968 geahndet werden. Nach der englischen Judikatur ist Identitätsmissbrauch grundsätzlich ein Akt der Täuschung undfinanzieller Gewinn oder das Erlangen von Besitztümern durch Täuschung war nach den Bestimmungen des Theft Act strafbar[400]. Mittlerweile wurden die Bestimmungen des Theft Act

397 http://www.homeoffice.gov.uk/agencies-public-bodies/nfa/ (12.06.2012).
398 http://www.identitytheft.org.uk/faqs.asp (12.06.2012).
399 http://www.national-identity-fraud-prevention-week.co.uk/identity-theft-statistics.htm (12.06.2012).
400 http://www.legislation.gov.uk/ukpga/1968/60 (12.06.2012).

1968 bezüglich Täuschung und Betruges durch jene des Fraud Act 2006 ersetzt, da die englische Regierung nach einem Report der Law Commission zur Erkenntnis gelangte, dass aufgrund der immer schnelleren Zunahme von Betrugsdelikten mit Unterstützung von IT ein zeitgemäßeres Gesetz notwendig sei, um dieser Bedrohung Herr zu werden[401]. Das neue Gesetz sollte einen eigenen Straftatbestand für Betrug schaffen und auch neuzeitliche Angriffsmethoden wie Phishing oder Pharming erfassen[402]. Am 8. November 2006 wurde der Fraud Act 2006 beschlossen und am 15. Jänner 2007 ist er in Kraft getreten[403]. Die für diese Arbeit wichtigen Passagen im Wortlaut[404]:

„1 Fraud

(1)A person is guilty of fraud if he is in breach of any of the sections listed in subsection (2) (which provide for different ways of committing the offence).

(2)The sections are—

(a)section 2 (fraud by false representation),

(b)section 3 (fraud by failing to disclose information), and

(c)section 4 (fraud by abuse of position).

(3)A person who is guilty of fraud is liable—

(a)on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum (or to both);

(b)on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine (or to both).

2 Fraud by false representation

(1)A person is in breach of this section if he—

(a)dishonestly makes a false representation, and

(b)intends, by making the representation—

(i)to make a gain for himself or another, or

(ii)to cause loss to another or to expose another to a risk of loss.

(2)A representation is false if—

401 http://lawcommission.justice.gov.uk/docs/lc276_Fraud.pdf (12.06.2012).
402 http://www.justice.gov.uk/downloads/publications/corporate-reports/MoJ/2012/post-legislative-assessment-fraud-act-2006.pdf (12.06.2012).
403 http://www.cps.gov.uk/legal/d_to_g/fraud_act/ (12.06.2012).
404 http://www.legislation.gov.uk/ukpga/2006/35/contents (12.06.2012).

(a)it is untrue or misleading, and

(b)the person making it knows that it is, or might be, untrue or misleading.

(3)"Representation" means any representation as to fact or law, including a representation as to the state of mind of—

(a)the person making the representation, or

(b)any other person.

(4)A representation may be express or implied.

(5)For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention)."

Nach diesem Auszug aus dem Fraud Act 2006 ist jeder wegen Betruges strafbar, der vorsätzlich falsche Angaben tätigt, um sich selber oder einen anderen zu bereichern oder anderen zu schaden[405]. Als falsch gelten Angaben nach diesem Gesetz dann, wenn sie unwahr oder irreführend sind und wenn sich die Person, die diese tätigt, dieses Umstandes bewusst ist. Als Angaben zählen sowohl Tatsachen-Angaben als auch Angaben rechtlicher Natur; es spielt nach sec. 2(4) auch keine Rolle, ob diese ausdrücklicher oder stillschweigender Natur sind[406]. Nach sec. 2(5) werden auch die Eingaben in Datenverarbeitungssysteme als Angaben erfasst. Das Strafmaß beträgt nach sec. 1(3) bis zu 10 Jahre Freiheitsstrafe. Ebenfalls strafbar nach diesem Gesetz ist der intentionale Besitz und die Herstellung von Tatwerkzeugen zur Begehung von Betrug[407]:

„6 Posession etc. of articles for use in frauds

(1)A person is guilty of an offence if he has in his possession or under his control any article for use in the course of or in connection with any fraud.

(2)A person guilty of an offence under this section is liable—

(a)on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum (or to both);

(b)on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine (or to both).

7 Making or supplying articles for use in frauds

(1)A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article—

405 http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf (12.06.2012).
406 http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf (12.06.2012).
407 http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf (12.06.2012).

(a)knowing that it is designed or adapted for use in the course of or in connection with fraud, or

(b)intending it to be used to commit, or assist in the commission of, fraud.

(2)A person guilty of an offence under this section is liable—

(a)on summary conviction, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum (or to both);

(b)on conviction on indictment, to imprisonment for a term not exceeding 10 years or to a fine (or to both)".

Das Strafmaß für den Besitz solcher Tatwerkzeuge beträgt bis zu 5 Jahre Haft, für die Herstellung oder den Verkauf sogar bis zu 10 Jahre. Interessant ist in diesem Zusammenhang auch die Definition des in sec. 6 und sec. 7 verwendeten Begriffs „articles", der sinngemäß als „Tatwerkzeuge" übersetzt wurde[408]:

„8 „Article"

(1)For the purposes of—

(a)sections 6 and 7, and

(b)the provisions listed in subsection (2), so far as they relate to articles for use in the course of or in connection with fraud,

"article" includes any program or data held in electronic form."

Das bedeutet, dass als Tatwerkzeug auch Programme und Daten zu verstehen sind, womit auch Besitz, Herstellung und Vertrieb elektronischer Hilfsmittel zur Begehung eines Betruges nach diesem Gesetz verboten sind. Ein Identitätsmissbrauch würde in England also nach sec. 2 „Fraud by false representation" geahndet werden. Der Identitätsdiebstahl an sich ist zwar immer noch straffrei, aber diverse technische Angriffsmethoden zur Erlangung persönlicher Daten wären nach sec. 6 und sec. 7 strafbar, wenn sie zu einem nachfolgenden Identitätsmissbrauch führen sollen. Das zweite, im Zusammenhang mit Identitätsdiebstahl und Identitätsmissbrauch wichtige Gesetz ist der Data Protection Act 1998[409]. Hierbei handelt es sich um das englische Datenschutzgesetz, das detaillierte Regelungen und Bestimmungen für den Umgang mit personenbezogenen Daten enthält. Da es bezüglich dieses Gesetzes allerdings keine signifikanten Unterschiede zu den Pendants in Österreich und Deutschland gibt, wird auf eine nähere Ausführung an dieser Stelle verzichtet. England weist aufgrund der gemeinschaftsrechtlichen Vorgaben grundsätzlich den gleichen Schutz

408 http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf (12.06.2012).
409 http://www.legislation.gov.uk/ukpga/1998/29/contents (12.06.2012).

für personenbezogenen Daten auf, wie alle anderen EU-Mitgliedstaaten auch. Die dritte, relevante Norm, der Computer Misuse Act 1990, erfasst folgende Handlungen[410]:

- unauthorised access to computer material;
- unauthorised access with intent to commit or facilitate commission of further offences;
- unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

Dieses Gesetz sanktioniert also nach sec. 1 jede Form von unbefugtem Zugriff auf Daten eines Computers, nach sec. 2 allgemein jedweden unbefugten Zugriff auf einen Computer mit der Absicht eine Straftat zu begehen oder deren Begehen zu erleichtern und nach sec. 3 beispielsweise den Einsatz von Schadsoftware gegen ein Computersystem sowie deren Herstellung zu diesem Zweck.

Ebenfalls im Jahr 2006 wurde der Identity Cards Act umgesetzt[411]; ein Gesetz, das hauptsächlich zur Bekämpfung von Identitätsdiebstahl und Terrorismus gedacht war. Dieses sah die Einführung von landesweiten ID-Karten und Identifikationsdokumenten vor sowie eine Datenbank namens „National Identity Register", in der zur Identifizierung von Personen dienende Daten gespeichert werden sollten (wie zB. Name, Adresse, National Insurance Number, Nationalität aber auch biometrische Daten wie ein Iris Scan[412]). Die Idee dahinter war es, die in den neuen Authentifizierungsdokumenten enthaltenen Daten mit jenen in der Datenbank abzugleichen und dadurch eine landesweite, sicherere Form der Authentifizierung in England zu schaffen. Des Weiteren wurde durch dieses Gesetz ein neuer Straftatbestand geschaffen, der den Besitz falscher Identitätsdokumente sanktionierte. Im Jahr 2010 wurde der Identity Cards Act 2006 durch den Identity Documents Act 2010 ersetzt, der die Einführung der neuen Authentifizierungsdokumente und der neuen Datenbank rückgängig machte[413]. Experten hatten das mit dem Identity Cards Act 2006 verbundene Projekt mehrmals als zu kostspielig und zu wenig effizient kritisiert; zusätzlich erachtete man durch die Einführung der neuen Datenbank Grundrechte der Bürger verletzt[414]. Der neu eingeführte Straftatbestand wurde allerdings beibehalten[415]:

„4 Possession of false identity documents etc with improper intention

(1)It is an offence for a person ("P") with an improper intention to have in P's possession or under P's control—

(a)an identity document that is false and that P knows or believes to be false,

410 http://www.legislation.gov.uk/ukpga/1990/18/section/3 (12.06.2012).
411 http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf (12.06.2012).
412 http://www.legislation.gov.uk/ukpga/2006/15/contents (12.06.2012).
413 http://www.legislation.gov.uk/ukpga/2010/40/contents/enacted (12.06.2012).
414 http://news.bbc.co.uk/2/hi/uk_news/politics/8707355.stm (12.06.2012).
415 http://www.legislation.gov.uk/ukpga/2010/40/section/4/enacted (12.06.2012).

(b)an identity document that was improperly obtained and that P knows or believes to have been improperly obtained, or

(c)an identity document that relates to someone else.

(2)Each of the following is an improper intention—

(a)the intention of using the document for establishing personal information about P;

(b)the intention of allowing or inducing another to use it for establishing, ascertaining or verifying personal information about P or anyone else.“

Nach sec. 4 ist der Besitz falscher Identitätsdokumente mit einer missbräuchlichen Intention strafbar. Als falsch gilt ein Identitätsdokument dann, wenn es gefälscht ist, es unrechtmäßig erworben wurde oder einer anderen Person gehört. Eine Intention gilt dann missbräuchlich, wenn die Identitätsdokumente zu einer unrechtmäßigen Authentifizierung genutzt werden sollen oder einem dritten zu einer unrechtmäßigen Authentifizierung überlassen werden. Das Strafmaß beträgt in diesem Fall bis zu 10 Jahre Haft. Ebenfalls strafbar ist der Besitz falscher Identitätsdokumente ohne angemessenen Grund; in diesem Fall drohen bis zu 12 Monate Freiheitsstrafe[416].

5.5.5 Schweden

Schweden wurde in diese Arbeit hineingenommen, weil sich dort in den letzten Jahren ein sehr radikaler rechtlicher Ansatz bezüglich der Bekämpfung von organisierter Cyberkriminalität, also auch von Identitätsdiebstahl und Identitätsmissbrauch, herauskristallisiert hat. Laut dem Security Threat Report der Sicherheitsfirma Symantec aus dem Jahr 2007 würden sich etwa 15% aller Server, auf denen durch Hacker gestohlene Informationen und Daten gelagert werden, in Schweden befinden[417]. Organisierte Identitätsdiebe nutzen solche Server, um die erbeuteten Daten zu lagern und nachher gewinnbringend zu verkaufen. Nach diesen Zahlen würden sich nur in den USA mehr solcher Server befinden als in Schweden. Laut einer Statistik der schwedischen Kredit Rating Firma Soliditet aus dem Jahr 2009 hatte die Anzahl der wegen Identitätsdiebstahl eingefrorenen Accounts gegenüber 2006 um 79% zugenommen, wobei vor allem Menschen im Altersbereich von 20-49 Jahren betroffen waren[418]. Zahlen von Juni 2012 zeigen einen Anstieg von Identitätsdiebstahl um 42% gegenüber 2011[419]. Für den starken Anstieg nicht ganz unverantwortlich ist der Umstand, dass Schweden grundsätzlich eine „offene Gesellschaft“ ist, basierend auf dem Öffentlichkeitsprinzip.

416 http://www.legislation.gov.uk/ukpga/2010/40/section/6/enacted (12.06.2012).
417 http://www.thelocal.se/6736/20070319/ (22.06.2012).
418 http://www.thelocal.se/20794/20090720/ (22.06.2012).
419 http://scancomark.com/Management/Dramatic-growth-in-identity-theft-in-Sweden.html (22.06.2012).

Nach dem Öffentlichkeitsprinzip hat jede Person, egal ob schwedischer Staatsbürger oder nicht, das Recht, Informationen einzusehen, die sich im Besitz von öffentlichen Behörden und Ämtern befinden[420]. Darunter fallen auch in Computern gespeicherte Informationen wie Adresse, Einkommen oder Steuersatz; in bestimmten Fällen dürfen allerdings Informationen geheim gehalten werden. Um der Zunahme von organisierter Cyberkriminalität und Terrorismus entgegenzuwirken, hat Schweden durchaus umstrittene rechtliche Maßnahmen ergriffen. Im Juni 2008 verabschiedete die Regierung das sogenannte FRA - Gesetz, welches die schwedische Behörde Försvarets Radioanstalt mit dem Recht ausstattete, sämtliche elektronische Kommunikation abzuhören, die die schwedische Grenze passiert[421]. Dieses Gesetz traf auf massive Proteste. Von Datenschützern besonders kritisiert wurde der Umstand, dass diese Überwachung auch ohne Gerichtsbeschluss möglich ist; es wurde sogar ein Verfahren vor dem Europäischen Gerichtshof für Menschenrechte befürchtet[422]. Technikexperten bemängelten, dass es in der Realität kaum möglich sei, zwischen internationalem und nationalem Datenverkehr zu unterscheiden, was zu der Befürchtung führte, dass FRA auch elektronische Kommunikation innerhalb Schwedens abhören würde. Neben der politischen Opposition und Experten des Rechts und der Technik protestierten noch namhafte Unternehmen wie etwa Google oder TeliaSonera gegen das neue Gesetz, allerdings bislang erfolglos[423]. Im Sommer 2012 änderte die schwedische Regierung das Gesetz zur elektronischen Kommunikation; jenes Gesetz, das die Überwachung von Internet- und Telefonaktivität durch die Polizei regelt[424]. Nach dieser Änderung ist nun die Polizei in Schweden dazu berechtigt, den Internetverkehr oder Telefonverkehr einer Person abzuhören, noch bevor diese eines Verbrechens verdächtigt wird[425]. Besonders wichtig ist diese Änderung im Hinblick auf Identitätsdiebstahl und Identitätsmissbrauch deswegen, weil nun auch ein Verdacht auf geringere Vergehen (wie unberechtigter Zugriff auf ein Computersystem) eine polizeiliche Überwachung des Internetverkehrs rechtfertigt. Die Frage, ob diese Änderungen im Gesetz effizient gegen Identitätsdiebstahl und Identitätsmissbrauch wirken, kann zum aktuellen Zeitpunkt nicht beantwortet werden, da noch keine aussagekräftigen Zahlen vorliegen. Die rechtliche Entwicklung der letzten Jahre lässt jedenfalls darauf schließen, dass sich in Schweden die offene Gesellschaft, zumindest im Hinblick auf den Datenverkehr im Internet, zunehmend in einen Überwachungsstaat verwandelt.

420 http://www.sweden.gov.se/sb/d/2184/a/15521 (22.06.2012).
421 http://www.spiegel.de/netzwelt/web/elektronische-ueberwachung-schweden-beschliesst-web-abhoergesetz-a-560637.html (22.06.2012).
422 http://freiheitblog.wordpress.com/2008/06/19/uberwachungswahn-auf-schwedisch/ (22.06.2012).
423 http://torrentfreak.com/swedes-massively-protest-wiretap-law-080707/ (22.06.2012).
424 http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403148_text (22.06.2012).
425 http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5103862 (22.06.2012).

6 Technische Schutzmechanismen gegen Identitätsdiebstahl und Identitätsmissbrauch

Technische Schutzmechanismen dienen in erster Linie dazu, bereits den Identitätsdiebstahl selbst, also die unbefugte Aneignung von Daten, zu verhindern. Sie sind in erster Linie präventiver Natur. In Kapitel 4 wurden die gängigsten Angriffsmethoden vorgestellt, die von den Tätern benutzt werden, um an Identitätsdaten zu kommen. In diesem Kapitel sollen nun sowohl die gebräuchlichsten als auch die bislang effizientesten technischen Sicherheitsmaßnahmen kurz untersucht werden, wobei zwischen Sicherheitsmaßnahmen auf Nutzerseite (Clientseite) und Sicherheitsmaßnahmen auf Serverseite unterschieden wird.

6.1 Technische Sicherheitsmaßnahmen auf Nutzerseite

Sicherheitsmaßnahmen auf Nutzerseite dienen in erster Linie dazu, den Rechner von Privatpersonen vor Angriffen über das Internet zu schützen. Bei dieser Art von Maßnahmen ist nicht nur ihre Effizienz von Bedeutung, sondern auch der Grad an Komplexität, den sie aufweisen, da im Rahmen dieser Arbeit von einem durchschnittlichen Nutzer mit nur mäßigen technischen Kenntnissen ausgegangen wird. Ziel ist es, Maßnahmen zu erläutern, die für die breite Masse ohne tiefgehende technische Kenntnisse und ohne unverhältnismäßig hohen Aufwand realisierbar sind. Kriterien für die Bewertung von technischen Sicherheitsmaßnahmen auf Nutzerseite sind also:

- Komplexität der Sicherheitsmaßnahme und dafür nötiger Aufwand;
- Effizienz dieser Sicherheitsmaßnahme bezüglich Schutz.

6.1.1 Technische Standardsicherheitsmaßnahmen für heimische Rechner

Als Standardschutz für heimische Rechner werden von zahlreichen Experten empfohlen[426]:

- Antivirensoftware;
- Personal Firewall.

Bei Antivirensoftware handelt es sich um eine der grundlegendsten Standardsicherheitsmaßnahmen, die von nahezu allen Security–Firmen empfohlen wird. Die Bezeichnung „Antivirensoftware“ ist

426 https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/BasisschutzComputer/basisschutzComputer_node.html;jsessionid=77D0AB025DF357F4CCA5A19D8E3E8728.2_cid250 (30.06.2012).

dabei etwas irreführend, da diese nicht nur zum Schutz des heimischen Rechners vor Computerviren konzipiert ist, sondern generell zum Schutz gegen die gängigsten Arten von Malware (auch Würmer und Trojaner)[427]. Grundsätzlich dient eine Antivirensoftware dazu, Malware auf einem Rechner aufzuspüren, die infizierten Daten zu isolieren und den Nutzer durch eine entsprechende Warnmeldung zu informieren[428]. Je nach Wunsch des Nutzers können dann die betroffenen Daten gereinigt oder auch gelöscht werden. Bezüglich ihrer Arbeitsweise unterscheidet man Echtzeitscanner und manuelle Scanner. Der Echtzeitscanner ist im Hintergrund des Systems aktiv und scannt alle Dateien, Programme und den Arbeitsspeicher, unter Umständen auch den Internetverkehr[429]. Er kann je nach Präferenz des Nutzers entweder beim Lesevorgang, also beim Öffnen von Dateien, oder beim Schreibvorgang, also dem Erstellen von Dateien, seinen Scan durchführen. Die meisten Nutzer wählen die Variante des Scans beim Schreibzugriff, da hierdurch die Performance des Systems weniger beeinträchtigt wird[430]; allerdings werden so leicht von Malware befallenen Dateien übersehen, die gerade inaktiv sind. Der Echtzeitscanner stellt die gebräuchlichste Arbeitsweise von Antivirensoftware dar. Der manuelle Scanner muss vom Benutzer manuell gestartet werden und führt in diesem Fall einen Scan aller Dateien des Rechners durch[431]. Wird Malware gefunden, so wird dem Nutzer meistens die Option geboten, die infizierten Dateien zu säubern oder zu löschen. Manuelle Scanner stellen im Hinblick auf die Arbeitsweise von Antivirensoftware nicht den Standard, sondern eher eine zusätzliche Option dar. Bezüglich der Erkennung von Malware unterscheidet man reaktive und proaktive Antivirensoftware. Reaktive Antivirensoftware stellt den weitgehenden Standard für heimische Rechner dar, nahezu jede gebräuchliche Antivirensoftware arbeitet so. Bei dieser Technik werden der Antivirensoftware vom Hersteller Signaturdateien von allen aktuell bekannten Malwaretypen hinzugefügt[432]. Führt reaktive Antivirensoftware dann einen Scan durch, ist sie in der Lage, jede Malware, deren Signatur ihr bekannt ist, aufzuspüren. Der Nachteil dabei ist, dass Malware, die dem Hersteller noch nicht bekannt ist, auch nicht gefunden werden kann[433]. Proaktive Antivirensoftware benötigt keine Signaturdateien, sondern verwendet Techniken wie etwa Heuristiken oder Sandboxing. Bei heuristischen Verfahren werden die Dateien nach malwaretypischem Programmcode durchsucht, also Programmcode der für normale Dateien untypisch ist[434]. Allerdings ist es auch mit diesen Verfahren in der Praxis nur schwer möglich, unbekannte Malware zu entdecken, da von Angreifern häufig polymorphe Malware eingesetzt wird.

427 http://www.microsoft.com/security/resources/antivirus-whatis.aspx (30.06.2012).
428 http://www.bullhost.de/a/antivirensoftware.html (30.06.2012).
429 http://www.thomatechnik.de/antivirus-lexikon/begriffe/on-access-scanner.htm (30.06.2012).
430 http://www.thomatechnik.de/antivirus-lexikon/begriffe/on-access-scanner.htm (30.06.2012).
431 http://www.thomatechnik.de/antivirus-lexikon/begriffe/on-access-scanner.htm (30.06.2012).
432 http://www.computerlexikon.com/definition-virenscanner (30.06.2012).
433 http://www.computerlexikon.com/definition-virenscanner (30.06.2012).
434 http://www.computerlexikon.com/definition-virenscanner (30.06.2012).

Sandboxing ist eine Technik, bei der die Dateien oder Programme in einer gesicherten Umgebung, der sogenannten Sandbox, ausgeführt werden[435]. Weicht die Datei bei der Ausführung von dem von der Sandbox erwarteten Verhalten ab, so wird sie als potentielle Gefahr eingestuft. Die Nachteile von Sandboxing sind, dass diese Methode erstens sehr ressourcen-intensiv ist und zweitens dieEinstellungen für den Test selber vornehmen muss der Nutzer, wodurch gewisse technische Vorkenntnisse notwendig sind, um diese Methode effizient auszuführen[436]. Ein großes Problem von proaktiver Antivirensoftware ist, dass sie aufgrund ihrer sehr hohen technischen Komplexität und der sehr hohen Entwicklungskosten immer den aktuellen Malware-Trends etwas hinterherhinkt[437]. Zusätzlich erfordern einige proaktive Techniken fundiertes technisches Wissen des Nutzers, was sie zusätzlich für den privaten Gebrauch disqualifiziert. Zusammenfassend lässt sich sagen, dass bezüglich Identitätsdiebstahl und Identitätsmissbrauch im Internet Antivirensoftware lediglich als Ergänzung zu weiteren Sicherheitsmaßnahmen gesehen werden kann, aber alleine noch lange keinen wirksamen Schutz bietet. Normale, reaktive Antivirensoftware kann grundlegenden Schutz vor gängigen Typen von Malware bieten, aber gegen aktuelle Angriffsmethoden (wie etwa Drive-by-Downloads) hilft diese nicht wirklich. Darüber hinaus steht hinter Identitätsdiebstahl und Identitätsmissbrauch immer mehr eine zunehmend professionell organisierte, kriminelle Industrie, die nicht unbedeutende Ressourcen in die Entwicklung neuer Arten von Malware steckt, wodurch es für reaktive Antivirensoftware immer schwerer wird, umfassenden Schutz für heimische Systeme zu gewährleisten[438]. Trotzdem sollte Antivirensoftware, zusammen mit weiteren Sicherheitsmaßnahmen, benutzt werden.

Der zweite Bestandteil der untersuchten Standardsicherheitsmaßnahmen ist die Personal Firewall. Dabei handelt es sich um Software, die sowohl den ein-, als auch den ausgehenden Datenverkehr eines Rechners filtert[439]. Ziel dieser Sicherheitsmaßnahme ist es, den Rechner vor Angriffen von außen und innen zu schützen. Zugriffe von außen, zum Beispiel auf Programme oder Dateien, die eine Schwachstelle darstellen, können durch das selektive Blockieren des Datenverkehrs unterbunden werden, wodurch der Rechner auch vor dem Befall durch Malware geschützt werden kann. Zur Filterung des Datenverkehrs benutzt die Personal Firewall einen sogenannten Paketfilter, der den Datenverkehr anhand definierter Regeln erlaubt oder blockiert[440]. Mit diesem Paketfilter können Personal Firewalls, im Unterschied zu Netzwerk Firewalls, auch die Kommunikation von einzelnen Programmen mit dem Internet oder einem lokalen Netz blockieren. Die für die Filterung

435 http://www.computerlexikon.com/definition-virenscanner (30.06.2012).
436 http://www.itwissen.info/definition/lexikon/Sandbox.html (30.06.2012).
437 http://www.anti-malware-test.com/test-results/AntiVirus_Proactive_Protection_Test_2008 (30.06.2012).
438 http://anti-virus-rants.blogspot.co.at/2006/05/pro-active-vs-reactive-technologies.html (30.06.2012).
439 http://www.itwissen.info/definition/lexikon/Firewall-FW-firewall.html (30.06.2012).
440 http://www.itwissen.info/definition/lexikon/Paketfilter-PF-packet-filter.html (30.06.2012).

notwendigen Regeln können auf unterschiedliche Weise erstellt werden. Einige Regeln sind meistens vom Entwickler der Firewall bereits vordefiniert[441]; zusätzlich verfügen viele Personal Firewalls über einen sogenannten Lernmodus. Durch diesen können Regeln automatisch, durch Interaktion mit dem Nutzer, festgelegt werden[442]: Sobald eine Anwendung, die bisher noch nicht am Datenverkehr beteiligt war, auf das Internet zugreifen möchte, wird der Nutzer durch ein Dialogfenster gefragt, ob diese Verbindung gestattet oder blockiert werden soll. Je nach Antwort wird dann eine entsprechende Regel im Paketfilter eingetragen. Außerdem bieten die meisten Personal Firewalls dem Nutzer die Möglichkeit, manuell Regeln zu definieren und hinzuzufügen.

Der Nutzen einer Personal Firewall gegen Angriffe von außen ist durchaus umstritten. Viele Sicherheitsexperten gehen davon aus, dass Angriffe gegen Programme und Netzwerkdienste auch durch das Deaktivieren nicht benötigter Netzwerkdienste und durch regelmäßige Sicherheitsupdates vermieden werden können[443]. Zusätzlich würde eine Personal Firewall die Komplexität des Systems erhöhen und damit die Angriffsfläche vergrößern[444]. Geht es um Angriffe von innen, so kann eine Personal Firewall durchaus nützlich, sein um Backdoors zu entdecken -eine Form von Software, die oft von Trojanern auf einem Rechner installiert wird, um dem Angreifer dabei zu helfen konventionelle Zugriffssicherungen zu umgehen, sobald er auf den Rechner seines Opfers zugreift[445]. Speziell einfache Malware oder Spyware kann entlarvt werden, sobald diese nach außen kommunizieren möchte oder einen Port für den Angreifer öffnen will. Das Problem bei Angriffen dieser Art ist, dass eine Personal Firewall gegen technisch hochwertigere Malware, wie sie bereits weitgehend eingesetzt wird, machtlos ist. Neuere Malware ist in der Lage, mittels sehr einfacher Methoden eine Blockierung durch den Paketfilter zu vermeiden[446]. Meistens werden Anwendungen, die bereits als vertrauenswürdig eingestuft wurden, zur Herstellung der Verbindung mit dem Internet herangezogen. Dabei werden dann Ports benutzt, die zum Beispiel von Kommunikationsprogrammen wie Skype verwendet werden oder die für http-Anfragen des Browsers dienen[447]. Zusammenfassend lässt sich sagen, dass Personal Firewalls, obwohl vom BSI als Standardschutz für heimische Rechner empfohlen[448], einen etwas niedrigeren Schutz als Antivirensoftware und Antispyware bieten. Grund dafür sind nicht nur die bereits erwähnten Mängel bezüglich der wirksamen Abwehr modernerer Angriffe von innen und außen, sondern auch der Umstand, dass Personal Firewalls für eine effiziente Konfiguration bestimmtes technisches

441 http://www.itwissen.info/definition/lexikon/Paketfilter-PF-packet-filter.html (30.06.2012).
442 http://www.itwissen.info/definition/lexikon/Firewall-FW-firewall.html (30.06.2012).
443 https://www.bsi.bund.de/cln_174/DE/Service/FAQ/PersonalFirewall/faq_node.html (30.06.2012).
444 http://altlasten.lutz.donnerhacke.de/mitarb/lutz/usenet/Firewall.html (30.06.2012).
445 http://www.itwissen.info/definition/lexikon/Backdoor-backdoor.html (30.06.2012).
446 http://www.rrzn.uni-hannover.de/its_p_firewall.html (30.06.2012).
447 http://www.rrzn.uni-hannover.de/its_p_firewall.html (30.06.2012).
448 https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/m/m05/m05091.html (30.06.2012).

Grundwissen beim Nutzer voraussetzen. Für einen technisch nur durchschnittlich versierten Nutzer ist es oftmals schwierig zu beurteilen, ob einem Programm Zugang zum Internet gewährt werden sollte oder nicht. Jedesmal, wenn neue Software auf dem Rechner installiert wird, muss entschieden werden, ob diese mit dem Internet kommunizieren darf oder nicht. Erschwerend kommt hinzu, dass der Paketfilter sein Vorgehen in einer Logdatei protokolliert und dass speziell Angriffe von innen nur durch ein Lesen und Interpretieren dieses Logs erkannt werden können[449]. Hat der Nutzer keine entsprechenden Vorkenntnisse, kann er mit dem Inhalt des Logs nur wenig anfangen. Die Personal Firewall kann für technisch wenig versierte Nutzer auch einen gefährlichen Nebeneffekt aufweisen: Nämlich dann, wenn ein vermeintlicher Angriff von innen nur der Versuch einer normalen Software ist, ein dringend benötigtes Update zu installieren, das eventuell für die Sicherheit des Rechners von Bedeutung ist. Personal Firewalls besitzen zur Abwehr einfacher Angriffe und zum Entdecken von Backdoors durchaus einen gewissen Sinn; ob sie aber eine Pflichtmaßnahme für die Sicherheit eines heimischen Rechners sein sollte, ist fraglich.

Die hier beschriebenen Standardsicherheitsmaßnahmen sind, wie bereits erläutert wurde, zwar geeignet, einen soliden Grundschutz für einen Rechner zu gewährleisten; gegen moderne Angriffsmethoden sind sie aber nur mäßig wirkungsvoll.

6.1.2 Schutz für den heimischen Browser

Das vermutlich beliebteste Angriffsziel im Jahr 2012 ist der Browser des Nutzers[450]; also jene Software, mit welcher der Nutzer im Internet unterwegs ist[451]. Der Trend bei Webseiten geht dahin, dem Nutzer immer mehr multimediale Inhalte und entsprechende Erweiterungen zu bieten, wofür Werkzeuge wie JavaScript oder Flash notwendig sind. Auch sogenannte Plug-Ins wie der Adobe Reader gewinnen immer mehr an Beliebtheit[452]. Genau diese immer weiter wachsende Anzahl von Plug-Ins sowie die damit verbundene Vielzahl an Schnittstellen und Applikationen sorgt auch für eine signifikante Erweiterung der Angriffsfläche[453]. Um sich gegen Identitätsdiebstahl oder Identitätsmissbrauch zu schützen, sollte der Nutzer zunehmend auf die Sicherheit seines Browsers achten. Die technische Weiterentwicklung der Browser und damit auch die Verbesserung ihrer Sicherheit obliegt zwar dem Hersteller, es gibt aber einige wenige Vorsichtsmaßnahmen, die der Nutzer treffen kann:

449 http://nod32.helpmax.net/de/tools/log-dateien/ (30.06.2012).
450 http://www.itmagazine.ch/Artikel/50956/Soziale_Netzwerke_und_Browser_beliebte_Angriffsziele.html (02.07.2012).
451 http://www.itwissen.info/definition/lexikon/Browser-browser.html (02.07.2012).
452 http://www.plugins.de/was-sind-plugins/browser-plugins/ (02.07.2012).
453 http://www.browsercheck.pcwelt.de/de/dokumentation/browser-plugins-und-update-check (02.07.2012).

- die Auswahl eines sicheren Browsers;
- eine sichere Konfiguration des Browsers.

Welcher Browser der sicherste ist, kann in dieser Arbeit nur schwer beurteilt werden, da es keine einheitliche Empfehlung von Experten der IT-Sicherheit gibt. Lange Zeit galt der Browser Firefox von Mozilla als ausgesprochen sicher, da für ihn mehrere Erweiterungen, auch Add-Ons genannt, erhältlich sind, die dem Nutzer mehr Sicherheit vor beliebten Angriffsmethoden bieten. Zu erwähnen wären hierbei:

- NoScript[454]:

  Hierbei handelt es sich um eine Erweiterung für den Browser Mozilla Firefox von Giorgio Maone, die dynamische Inhalte auf Webseiten (wie etwa JavaScript, Java oder Flash) blockiert. Dem Nutzer wird anhand einer Liste die Möglichkeit geboten, vertrauenswürdige Internetseiten zu bestimmen, deren dynamische Inhalte nicht blockiert werden. NoScript bietet einen hervorragenden Schutz vor Cross Site Scripting oder Clickjacking; allerdings hat dieses Add-On wieder den Nachteil, dass es für einen nur mäßig erfahrenen Nutzer schwer zu verwalten ist. Mittlerweile existiert eine Vielzahl von Internetseiten mit dynamischen Inhalten, die bei einer Blockierung durch NoScript praktisch wertlos für den Nutzer ist. Als Beispiel wären hier Seiten mit Videostreams zu Serien oder Filmen zu nennen. Der Nutzer hätte auf Dauer das Problem, für beinahe jede besuchte Internetseite eine Entscheidung treffen zu müssen.

- Request Policy[455]:

  Request Policy ist ebenso wie NoScript ein Add-On für den Browser Mozilla Firefox und dient dazu, Zugriffe einer Webseite auf Inhalte anderer Webseiten zu blockieren. Wie auch bei NoScript hat der Nutzer die Möglichkeit, anhand einer Liste von ihm gewünschte Zugriffe zu erlauben. Request Policy bietet einen hervorragenden Schutz vor Cross Site Referrence Forgery, aber auch hier besteht wieder der Nachteil, dass für einen unerfahrenen Nutzer oft nur schwer erkennbar ist, welche Zugriffe harmlos (eventuell sogar notwendig) sind und welche nicht.

- Adblock Plus[456]:

  Adblock Plus ist ein frei konfigurierbares Add-On; es kann nach Bedarf Werbung auf Webseiten oder ebenfalls dynamische Inhalte blockieren. Diese Erweiterung ist

454 http://noscript.net/ (02.07.2012).
455 http://www.pcwelt.de/news/Firefox-Add-on-Mehr-Browser-Sicherheit-mit-Request-Policy-429308.html (02.07.2012).
456 https://adblockplus.org/de/getting_started (02.07.2012).

ausgesprochen mächtig und erlaubt es dem Nutzer auch, eigene Filter zu erstellen, entsprechend hoch ist aber auch die Komplexität.

- Better Privacy[457]:

  Webseiten mit Flash-Applikationen setzen auf dem Rechner des Nutzers Flash-Cookies, sogenannte Local Shared Objects (LSO)[458]. Dabei handelt es sich um Dateien, die benutzerspezifische Daten enthalten, die für einen späteren Wiederaufruf der Webseite oder der Webanwendung von Nutzen sind. Anders als herkömmliche Cookies verweilen LSOs dauerhaft auf dem Rechner des Nutzers. Zusätzlich können sie nicht über den Browser verwaltet werden, sondern nur über das Programm Adobe Flash, wodurch ein Löschen erschwert wird. Viele Nutzer sind sich nicht einmal der Gefahr bewusst, die durch solche LSOs entstehen kann. Mit der Erweiterung Better Privacy ist es dem Nutzer möglich, solche Flash-Cookies schnell und einfach zu löschen.

Neben den diversen Erweiterungen existiert mittlerweile für Firefox auch die Möglichkeit einer sogenannten Opt-In-Aktivierung für Plug-Ins[459]. Diese auch als Click-to-Play bekannte Funktion blockiert Inhalte aus Plug-Ins auf Webseiten, wobei auch hier dem Nutzer die Option geboten wird, gezielt gewünschte Plug-Ins zu erlauben[460]. Mit Firefox 17 soll zusätzlich eine Funktion eingebaut werden, die den Zugriff von Webseiten auf Erweiterungen des Browsers blockiert, wobei auch hier wieder anhand einer Liste die Möglichkeit geboten wird, bestimmte Zugriffe zu erlauben[461]. Allgemein bietet Firefox mit seinen Erweiterungen und Funktionen einen durchaus soliden Schutz vor einigen beliebten Angriffsmethoden. Das Prinzip in allen Fällen nennt sich Whitelist; das heißt, es ist alles verboten, was nicht vom Nutzer anhand einer manuell geführten Liste ausdrücklich erlaubt ist[462]. Das damit einhergehende Problem ist einmal mehr, dass die Wirksamkeit dieses Schutzes stark mit dem technischen Wissen des Nutzers skaliert.

Aktuell gilt, zumindest nach der Empfehlung des BSI, der Browser Google Chrome als verhältnismäßig sicher[463]. Hauptgrund dafür ist die konsequente Umsetzung von Sandbox-Technologie bei diesem Browser. Bei Google Chrome werden mehrere gleichzeitig geöffnete Tabs voneinander getrennt; das bedeutet, jeder neu geöffnete Tab ist ein in sich geschlossener Prozess,

457 http://www.golem.de/1005/74885.html (02.07.2012).
458 http://www.adobe.com/security/flashplayer/articles/lso/ (02.07.2012).
459 http://www.soeren-hentzschel.at/mozilla/firefox/2012/03/29/firefox-14-bekommt-opt-in-aktivierung-fur-plugins/ (02.07.2012).
460 https://support.mozilla.org/de/kb/warum-werden-plugins-erst-nach-einer-bestaetigung-ausgefuehrt (02.07.2012).
461 http://derstandard.at/1345164832023/Mehr-Add-on-Sicherheit-ab-Firefox-17 (02.07.2012).
462 https://www.schneier.com/blog/archives/2011/01/whitelisting_vs.html (02.07.2012).
463 https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Empfehlungen/produktkonfiguration/BSI-E-CS-001.html (02.07.2012).

der in einer gesicherten Umgebung, also einer Sandbox, abläuft[464]. Wird also eine mit Malware infizierte Webseite besucht, so wird der Malware jeglicher Zugriff auf das System oder andere Prozesse untersagt. Die Infektion bleibt innerhalb der Sandbox. Zusätzlich verwendet Google Chrome auch seine Sandbox-Technologie bei den aktuell am stärksten gefährdeten Plug-Ins Adobe Flash und Adobe PDF-Reader und besitzt eine Auto-Update-Funktion für beide, seinen integrierten Adobe Flash Player und PDF-Viewer[465]. Hierdurch wird nicht nur die Gefahr einer Infektion durch Malware gesenkt, es werden auch die beiden kritischsten Plug-Ins automatisch auf dem neuesten Stand gehalten, ohne dass der Nutzer daran denken muss. Darüber hinaus bietet Google Chrome standardmäßig Funktionen äquivalent zu NoScript von Firefox sowie ebenfalls eine Opt-In-Aktivierung für Plug-Ins[466]. Ein nicht zu unterschätzender Nachteil ist allerdings die wachsende Beliebtheit des Browsers. Nach aktuellen Zahlen ist mittlerweile Google Chrome der meistbenutzte Browser im Internet und hat damit den Internet Explorer abgelöst[467]. Da die Angreifer immer mehr aus kommerziellem Interesse heraus handeln, werden Angriffsmethoden, die den Browser als Ziel haben, zumeist für jene Browsersoftware entwickelt, bei der mit den meisten Opfern zu rechnen ist. Es muss also davon ausgegangen werden, dass der aktuell durch die Sandbox-Technologie gebotene Schutz bald umgangen werden kann.

Bezüglich der sicheren Browsereinstellungen gibt es im Internet mehrere vertrauenswürdige Seiten, die sehr verständliche Tutorien zu diesem Thema anbieten, wie etwa der Browser-Sicherheitscheck des BSI[468]. Wichtig ist dabei, unabhängig vom verwendeten Browser:

- Plug-Ins wie Java, JavaScript oder Flash standardmäßig deaktivieren und nur für vertrauenswürdige Seiten erlauben;
- die Chronik, also der vom Browser protokollierte Internetverkehr, sollte regelmäßig gelöscht werden, ebenso wie Cookies;
- Warnungen für verschlüsselte Webseiten oder als potentiell gefährlich eingestufte Webseiten immer einblenden;
- SSL-Zertifikate benutzen für die Verschlüsselung der übertragenen Daten. Zusätzlich sollten von Webseiten benutzte Zertifikate auf deren Echtheit überprüft werden;
- keine Passwörter im Passwort-Manager automatisch speichern;

464 http://blog.chromium.org/2008/10/new-approach-to-browser-security-google.html (02.07.2012).
465 http://blog.chromium.org/2008/10/new-approach-to-browser-security-google.html (02.07.2012).
466 http://www.google.at/intl/de/chrome/browser/features.html#security (02.07.2012).
467 http://www.techfieber.de/2012/05/21/web-google-chrome-meistverwendeter-browser-der-welt/ (02.07.2012).
468 https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/WegInsInternet/DerBrowser/SicherheitsCheck/sicherheitscheck_node.html (02.07.2012).

- die Einstellung des Proxy Servers von Zeit zu Zeit überprüfen;
- den Browser sowie alle verwendeten Addons und Plug-Ins immer auf dem neuesten Stand halten.

6.1.3 Fazit

Grundsätzlich muss an dieser Stelle festgehalten werden, dass die einem durchschnittlich technisch versierten Nutzer zur Verfügung stehenden Mittel zur Abwehr eines Identitätsdiebstahls im Internet begrenzt sind. Viele von Experten empfohlene Sicherheitsmaßnahmen (wie etwa Firewalls oder Verschlüsselungsprogramme) bieten gegen moderne Angriffsmethoden nur wenig Schutz. Andere, vielversprechende Ansätze (wie etwa Sandboxing-Technologie) bringen den Nachteil mit sich, dass sie für einen durchschnittlichen Internetbenutzer zu kompliziert in ihrer Ausführung sind. Dennoch gibt es einige leicht umsetzbare Maßnahmen, mit denen ein verhältnismäßig solider Schutz für heimische Rechner realisierbar ist:

- Die Untersuchung der verbreitetsten Standardsicherheitsmaßnahmen ergab, dass zumindest Antivirensoftware eingesetzt werden sollten. Die Antivirensoftware sollte nach Möglichkeit über proaktive Erkennungsverfahren verfügen, da nur so eine verhältnismäßig sichere Überwachung des Systems möglich ist. Laut Security Threat Report der Sicherheitsfirma Sophos wurden im Jahr 2011 80% aller Arten von Malware auf den Rechnern der Kunden nur durch proaktive Verfahren entdeckt[469]. Reaktive Verfahren bieten zwar eine gute Ergänzung, sind alleine aber nicht ausreichend, um Schutz vor der immer schnelleren Entwicklung neuer Malware zu bieten. Eine Empfehlung für den Einsatz einer Personal Firewall kann nach der Untersuchung in Kapitel 6.1.1 nicht gegeben werden.
- Der Browser des Nutzers wird zu einem immer beliebteren Ziel für Angreifer, ebenso wie dessen Plug-Ins und Add-Ons. Aus diesem Grund sollte nach Möglichkeit ein Browser mit Sandboxing Technologie benutzt werden, da diese den aktuell besten Schutz vor modernen Angriffen wie Drive-by-Downloads bietet. Ebenso empfiehlt es sich, einen sehr restriktiven Umgang mit Plug-Ins wie JavaScript, Java oder Adobe Flash zu pflegen und diese nur für vertrauenswürdige Seiten (nach dem Whitelist-Prinzip) zu aktivieren. Hierdurch wird auch die Gefahr für Angriffe wie Cross Site Scripting stark verringert. Sichere Einstellungen für den Browser sind, wie in Kapitel 6.1.2 erläutert wurde, auf mehreren vertrauenswürdigen Internetseiten einsehbar.

469 Sophos, Security Threat Report 2012, S. 6.

- Größtmöglicher Schutz für ein heimisches System ergibt sich dadurch, dass dessen Softwarekomponenten immer auf dem neuesten Stand gehalten werden. Von vielen Nutzern wird noch immer unterschätzt, wie wichtig es ist, vor allem in Hinblick auf neue Angriffsmethoden ein System regelmäßig mit Updates zu versorgen. Drive-by-Downloads und Web-Attack-Toolkits nutzen meistens Schwachstellen im Browser des Nutzers oder in populären Plug-Ins wie etwa Adobe Flash oder Adobe PDF-Viewer. Es ist daher dringend notwendig, sowohl den Browser als auch sämtliche Plug-Ins und Add-Ons auf dem neuesten Stand zu halten. Der Aufwand hierfür hält sich bereits in Grenzen. Browser wie Mozilla Firefox bieten eine sichere Internetseite, auf der automatisch der Browser sowie sämtliche Plug-Ins auf ihre Version überprüft werden und wo mit einem einzigen Klick sofort ein Update durchgeführt werden kann[470]. Google Chrome kümmert sich selbst um Updates für kritische Plug-Ins wie Flash, ohne dass der Nutzer daran denken muss. Doch nicht nur der Browser und dessen Plug-Ins sollten regelmäßig auf Updates überprüft werden, auch das Betriebssystem sowie sämtliche Software, der ein Zugang zum Internet gestattet wird, sollten immer auf dem neuesten Stand gehalten werden. Die Entwickler von Malware nutzen Sicherheitslücken direkt, nachdem sie bekannt wurden; im Fall von Zero-Day Sicherheitslücken sogar früher. Neue Updates dienen oft dazu, diese Lücken zu schließen und sollten daher immer so zeitig wie möglich installiert werden. Je populärer eine Softwarekomponente ist, desto größer die Gefahr für Angriffe, da hier die mittlerweile hauptsächlich finanziell motivierten Angreifer den meisten Gewinn erwarten.

6.2 Technische Sicherheitsmaßnahmen auf Serverseite

Damit sind solche Maßnahmen gemeint, die für den Schutz der Infrastruktur, auf deren Basis die Nutzer im Internet unterwegs sind, verantwortlich sind. Eine solche Infrastruktur im Sinne dieser Arbeit wären etwa das Domain Name System oder auch Netzwerke und Web-Services. In diesem Kapitel sollen auch neue Forschungstrends auf dem Gebiet der IT-Sicherheit kurz erläutert werden ebenso wie aktuelle Sicherheitsmechanismen, die sich bisher als durchaus effizient bei der Bekämpfung von Identitätsdiebstahl im Internet erwiesen haben.

6.2.1 2-Faktor-Authentifizierung

Es ist im Informationszeitalter mittlerweile üblich, auch Alltagsgeschäfte, Einkäufe oder finanzielle

470 https://www.mozilla.org/de/plugincheck/ (10.07.2012).

Transaktionen zu verschiedenen Zwecken über das Internet zu tätigen. Um das Vertrauen der Nutzer in moderne Verfahren (wie etwa Onlinebanking) zu steigern und um die Gefahr eines Identitätsdiebstahls oder Identitätsmissbrauchs im Internet zu verringern, ist es notwendig, Schutzmechanismen zu schaffen, die eine sichere Authentifizierung sowohl der Nutzer als auch der Server im Datenverkehr sicherstellen und die für eine Verschlüsselung des Datenaustausch zwischen Browser und Server sorgen können. Im Rahmen dieser Arbeit wurden diesbezüglich drei technische Schutzmechanismen näher untersucht:

- elektronische/digitale Signaturen;
- SSL/TSL;
- 2-Faktor-Authentifizierung.

Grundsätzlich kann bei einer Authentifizierung der Nachweis der Identität auf 3 Arten erbracht werden[471]:

- Nachweis durch Wissen: Die Authentisierung erfolgt durch etwas, das der Inhaber der Identität weiß. Beispiele hierfür wären Passwörter oder PINs.
- Nachweis durch Besitz: Die Authentisierung erfolgt durch etwas, das der Inhaber der Identität besitzt. Beispiele hierfür wären Chipkarten oder TAN-Listen.
- Nachweis durch körperliche Merkmale: Die Authentisierung erfolgt durch besondere körperliche Merkmale, die nur der Inhaber der Identität aufweist. Beispiele hierfür wären alle Schutzmechanismen, die auf Biometrie basieren.

Von einer 2-Faktor-Authentifizierung spricht man allgemein dann, wenn der Nachweis der Identität mit zwei dieser Verfahren kombiniert erbracht wird[472]. Ein klassisches Beispiel für 2-Faktor-Authentifizierung wäre Onlinebanking, da hier eine Transaktion nur nach folgender Authentifizierung getätigt werden kann:

- Der Nutzer muss sich mit seinem Passwort in das Onlinebankingsystem einloggen;
- Für eine Überweisung muss er eine TAN eingeben, die sich in seinem Besitz befindet.

Es handelt sich also um Nachweis durch Wissen zusammen mit Nachweis durch Besitz; ein Angreifer muss für einen Identitätsmissbrauch sowohl das Passwort als auch die TAN-Liste des Nutzers kennen. Im folgenden werden die bekanntesten Arten von elektronischer 2-Faktor-Authentifizierung untersucht:

471 http://www.itwissen.info/definition/lexikon/Authentifizierung-authentication.html (10.07.2012).
472 http://www.datenschutz-praxis.de/fachwissen/fachartikel/prufen-sie-die-moglichkeiten-der-zwei-faktor-authentifizierung/ (10.07.2012).

- Auf Hardware basierende OTP-Generatoren[473]:

  Bei Hardwaretoken handelt es sich um Hardwarekomponenten, die zur Authentifizierung von Nutzern eingesetzt werden. OTP-Generatoren sind solche Hardwaretoken und tragen zu einer sichereren Authentifizierung bei, indem sie sogenannte „One-Time-Passwords“ erzeugen[474]. Diese Token verfügen über ein Display, auf dem die OTPs angezeigt werden. Zusätzlich sind klassische Token dieser Art üblicherweise nicht mit dem Rechner des Nutzers verbunden[475]. Die Hardwaretoken können solche OTPs auf 2 verschiedene Arten generieren: zeitgesteuert oder auf Anforderung des Besitzers. Bei einer Anforderung durch den Besitzer wird durch eine bestimmte Aktion des Nutzers, beispielsweise einen Knopfdruck, ein einmal gültiges Kennwort generiert, das nur für einen Authentifizierungsversuch gültig ist[476]. Bei zeitgesteuerter Generierung erzeugt das Token selbst in bestimmten zeitlichen Abständen ein Kennwort, wobei immer das vorherige Kennwort bei Generierung eines neuen ungültig wird[477]. Im Rahmen der Authentifizierung muss dann der Nutzer zusätzlich zum normalen Login (zB. durch Benutzername und Passwort) ein vom Token generiertes OTP eingeben, damit die Anmeldung Erfolg hat[478]. Abschließend wird das OTP an einen Authentifizierungsserver übermittelt, der je nach Art der Generierung des OTP nun selbst ein OTP erzeugt und mit dem übermittelten vergleicht. Stimmen die OTPs miteinander überein, so war die Anmeldung erfolgreich. Beispiel für diese Art von OTP-Generatoren wären die weit verbreiteten SecurID-Token der Firma RSA Security[479].

- Chipkarten-/Smartcardsysteme[480]:

  Chipkarten oder auch Smartcards sind Plastikkarten, die mit integrierten Chip ausgestattet sind. Man unterscheidet Speicherchipkarten und Prozessorchipkarten. Bei Speicherchipkarten enthält der Chip einen Speicher, der nur ausgelesen oder beschrieben werden kann[481]. Bei Prozessorchipkarten, den Smartcards, verfügt der Chip über einen Mikroprozessor, mithilfe dessen kompliziertere Dienste, wie Verschlüsselungen oder Authentifizierungen möglich sind[482]. Für dieses Unterkapitel sind nur die

473 http://www.itwissen.info/definition/lexikon/one-time-password-OTP-Einmalpasswort.html (10.07.2012).
474 http://www.itwissen.info/definition/lexikon/one-time-password-OTP-Einmalpasswort.html (10.07.2012).
475 http://www.securepoint.at/produkte-ID-Control-OTP-Key.html (10.07.2012).
476 http://msdn.microsoft.com/de-de/magazine/cc507635.aspx (10.07.2012).
477 http://msdn.microsoft.com/de-de/magazine/cc507635.aspx (10.07.2012).
478 http://msdn.microsoft.com/de-de/magazine/cc507635.aspx (10.07.2012).
479 http://austria.emc.com/security/rsa-securid/rsa-securid-software-authenticators.htm (10.07.2012).
480 http://www.itwissen.info/definition/lexikon/Smartcard-smartcard.html (12.07.2012).
481 http://www.itwissen.info/definition/lexikon/Smartcard-smartcard.html (12.07.2012).
482 http://www.itwissen.info/definition/lexikon/Smartcard-smartcard.html (12.07.2012).

Prozessorchipkarten von Relevanz. Um die Chipkarte in Verbindung mit dem Rechner nutzen zu können, benötigt der Nutzer noch eine spezielle Hardware, den sogenannten Chipkartenleser (auch Terminal genannt). Nach einer Spezifikation des Zentralen Kreditausschusses (ZKA) werden Kartenlesegeräte in 4 verschiedene Sicherheitsklassen unterteilt[483]. Bei Geräten der Sicherheitsklasse 1 existiert nur eine Kontaktiereinheit für die Chipkarte ohne Tastatur sowie eine Schnittstelle zum Rechner des Nutzers (wie zB. ein USB-Anschluss)[484]. Chipkartenlesegeräte der Sicherheitsklasse 2 besitzen zusätzlich zur Kontaktiereinheit und Schnittstelle noch eine eigene Tastatur, über die die PIN der Chipkarte eingegeben werden kann[485]. Geräte der Sicherheitsklasse 3 sind grundsätzlich ausgestattet wie Geräte der Sicherheitsklasse 2, verfügen aber zusätzlich noch über ein eigenes Display, auf dem die zu signierenden Daten angezeigt werden. Darüber hinaus verfügen solche Chipkartenleser über eine eigene Firmware und sind nicht dem Rechner des Nutzers verbunden[486]. Chipkartenleser der Sicherheitsklasse 4 verfügen neben einem eigenen Display und einer eigenen Tastatur noch über ein Authentifizierungsmodul, das den Chipkartenleser eindeutig identifizieren kann[487]. Im März 2008 wurde vom ZKA ein neues Sicherheitskonzept für einen universellen Chipkartenleser entwickelt, der unter dem Markennamen „Secoder“ auf dem Markt eingeführt wurde[488]. Ziel war es, mit dem Secoder eine einheitliche Lösung für die sichere Abwicklung von Zahlungen im Internet zu bieten. Der Secoder verfügt über ein eigenes Display und eine eigene Tastatur, wodurch er zumindest einem Chipkartenleser der Sicherheitsklasse 3 entspricht[489]. Er wird über USB an den Rechner des Nutzers angeschlossen. Zusätzlich verfügen Secoder über eine integrierte Firewall, durch die Chipkarte und PIN des Nutzers vor Angriffen aus dem Internet geschützt werden sollen[490]. In der Theorie sollen damit Angriffe basierend auf Malware oder Keyloggern abgewehrt werden, da der Anwendungssoftware kein unmittelbarer Zugriff auf das Gerät erlaubt wird. Darüber hinaus unterstützt der Secoder auch die dynamische TAN-Generierung, bei welcher der Nutzer im Rahmen des Onlinebanking mit seiner Chipkarte die TAN anhand der Überweisungsdaten elektronisch erzeugt, statt sie aus einer Papierliste

-

483 http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012).
484 http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012).
485 http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012).
486 http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012).
487 http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012).
488 http://www.die-deutsche-kreditwirtschaft.de/dk/pressemitteilungen/volltext/backpid/29/article/neue-generation-von-chipkartenlesern.html?tx_ttnews[pS]=1325372400&tx_ttnews[pL]=1356994799&tx_ttnews[arc]=1&cHash=9fcdc816efa0b5fc8b6f043f428e6835 (12.07.2012).
489 http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/zulassungsverfahren/secoder.html (12.07.2012).
490 http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/zulassungsverfahren/secoder.html (12.07.2012).

zu nehmen[491]. Dadurch kann die Bank etwaige Manipulationen (wie zB. durch MitM-Angriffe) zeitig erkennen und die Verarbeitung der Transaktion stoppen. Im Juli 2009 wurde vom ZKA die Spezifikation für den Secoder 2 verabschiedet[492]. Der Secoder 2 verfügt über den gleichen Sicherheitsstandard wie der Secoder, besitzt aber einen größeren Anwendungsbereich in Hinblick auf die Signaturfunktionalitäten. So bietet er auch asymmetrische Authentisierungsverfahren auf Basis elektronischer Signaturen[493]. Dabei lautet das Konzept „what you see is what you sign"; das heißt, dem Nutzer werden genau die Daten am Display des Secoder 2 angezeigt, die signiert und übertragen werden, wodurch eine Manipulation unmöglich gemacht werden soll. Darüber hinaus unterstützt der Secoder 2 auch den Einsatz des neuen deutschen Personalausweises[494].

- Der neue Trend 2012 – Smartphones statt Hardware-Token beim Einsatz von OTPs:

  Mit 2012 wird im Rahmen von 2-Faktor-Authentifizierung auf Basis von OTPs zunehmend das Smartphone anstelle von Hardware-Token eingesetzt[495]. Gründe dafür gibt es mehrere. Der wahrscheinlich wichtigste ist, dass die meisten Nutzer bereits ihr Smartphone als Standard-Arbeitsmittel nutzen und entsprechend geübt und sicher im Umgang mit diesem Gerät sind. Da hier das eigene Mobiltelefon statt einer zusätzlichen separaten Hardware für die 2-Faktor-Authentifizierung benutzt wird, ist auch die Akzeptanz der Nutzer gegenüber dieser Variante weit größer. Technisch betrachtet ist die Funktionsweise dieses Verfahrens die gleiche wie bei Hardware-Token: Möchte der Nutzer sich anmelden, so benötigt er zusätzlich zu seinen Login-Daten noch ein OTP. Dieses OTP kann durch das Smartphone auf 2 Arten erhalten werden: Entweder durch eine App oder durch den Erhalt einer SMS. Im Falle der App wird durch eine entsprechende Software, die sich auf dem Smartphone befindet, ein OTP erzeugt[496]. Das Mobiltelefon fungiert hier also als Authentifizierungs-Token. Bei OTP durch SMS wird dem Nutzer das OTP von einem separaten Sicherheitsserver, der in einer Datenbank die Mobilfunknummer gespeichert hat, via SMS über das Mobilfunknetz gesendet. Entsprechende Verfahren werden beispielsweise durch die Firma Securepoint[497] angeboten, aber auch Unternehmen wie ECOS Technology haben im Rahmen der Fachmesse it-sa im Oktober 2012 ähnliche Produkte vorgestellt[498]. Aufgrund

491 http://www.sparkasse.de/privatkunden/konto-karte/sicherungsverfahren.html (12.07.2012).
492 http://files.messe.de/cmsdb/D/007/22434.pdf (12.07.2012).
493 http://www.die-signaturkarte.de/aktuell/Secoder_2.html (12.07.2012).
494 http://www.die-signaturkarte.de/aktuell/Secoder_2.html (12.07.2012).
495 http://www.pcwelt.de/produkte/Einmalpasswoerter-per-iPhone-OTP-Generator-58281.html (14.07.2012).
496 http://www.onelogin.com/product/strong-authentication/onelogin-otp/ (14.07.2012).
497 http://www.securepoint.de/produkte-starke-authentifizierung.html (14.07.2012).
498 https://www.info-point-security.com/security-themen/identity/item/7428-ecos-2-faktor-authentisierung-per-sms.html (14.07.2012).

der hohen Akzeptanz der Nutzer gegenüber dieser Form der Authentifizierung und der damit verbundenen Erhöhung der Sicherheit bieten seit 2012 auch bekannte Unternehmen wie Dropbox[499], Google[500] und Facebook[501] eine 2-Faktor-Authentifizierung mit Unterstützung des Mobiltelefons an.

Auch wenn 2-Faktor-Authentifizierung von vielen Sicherheitsfirmen mittlerweile empfohlen wird, weisen die hier aufgelisteten Schutzmechanismen doch gewisse Schwächen auf.

- Schwächen von Hardware-Token:

  Auf Hardware basierende OTP-Generatoren bieten grundsätzlich keinen Schutz vor MitM-Angriffen. Opfer eines solchen Angriffs wurden im März 2010 Kunden der Firma Blizzard[502]. Für das Online-Spiel World of Warcraft verkauft Blizzard sogenannte Authenticators, also Hardware-Token, die für das Einloggen in den Account des Spielers ein OTP erzeugen. Mittels eines in Echtzeit kommunizierenden Keyloggers fingen Angreifer die Login-Daten sowie das OTP der Spieler ab und sorgten dafür, dass der Spiele-Client des Nutzers abstürzt, um sich dann unverzüglich mit den abgefangenen Daten einzuloggen. Zwar sorgen Hardware-Token dafür, dass sich solche Angriffe weitaus schwieriger für den Angreifer gestalten, aber gänzlich verhindern können sie diese nicht. Ein weiteres Problem ist, dass die Sicherheit solcher Token immer mit der Sicherheit des Authentifizierungsservers skaliert, der die OTPs verifiziert. So wurde der Server der Firma RSA erst im März 2011 Opfer eines Hackerangriffs, bei dem jene Daten entwendet wurden, mit denen sich die OTPs berechnen lassen[503]. Erschwerend kommt hinzu, dass es kaum möglich ist, im Falle solcher Sicherheitslücken Sicherheitsupdates für eigenständige Hardware-Token herauszubringen. Firma und Nutzer sind gezwungen, alle Token auszutauschen.

- Schwächen von Chipkartensystemen:

  Die Sicherheit von Chipkarten skaliert sehr stark mit der Sicherheitsklasse des eingesetzten Kartenlesegeräts. Kartenleser der Sicherheitsklasse 1 bieten praktisch kaum Schutz, da die PIN des Nutzers von einfachen Keyloggern mitgelesen werden kann. Im Jahr 2007 veröffentlichten die IT-Experten Hanno Langweg und Jörg Schwenk eine Publikation, die sich mit der Sicherheit von Chipkartensystemen gegenüber herkömmlichen Malware-

499 http://stadt-bremerhaven.de/dropbox-fuehrt-2-faktor-authentifizierung-ein/ (14.07.2012).
500 http://stadt-bremerhaven.de/google-konto-und-profil-absichern/ (14.07.2012).
501 http://stadt-bremerhaven.de/facebook-doppelte-anmeldesicherheit-startet/ (14.07.2012).
502 http://www.xsized.de/2010/03/man-in-the-middle-attack-auf-blizzard-authenticator/ (14.07.2012).
503 http://www.heise.de/newsticker/meldung/RSA-Hack-koennte-Sicherheit-von-SecurID-Tokens-gefaehrden-1210245.html (14.07.2012).

Angriffen befasste[504]. Bei den Sicherheitsmaßnahmen wurde im Rahmen dieses Tests von Standardsicherheitssoftware (wie zB. gängiger reaktiver Antivirensoftware) sowie von Kartenlesegeräten der Sicherheitsklasse 2 ausgegangen. Bei den Malware-Angriffen wurden nur solche gewählt, die ein sachkundiger Angreifer ohne besondere Ausrüstung und überdurchschnittlich hohen Aufwand erstellen und die sogar ein Laie automatisiert durchführen kann. Das Ergebnis fiel vernichtend aus. Dank einfacher Angriffe auf Basis lokaler Malware waren die Studienautoren in der Lage, unter anderem Transaktionsdaten zu manipulieren oder neue Transaktionen einzufügen[505]. Kartenlesegeräte der Sicherheitsklasse 3 bieten zwar relativ hohen Schutz, sind aber mitunter auch anfällig für MitM-Angriffe, wenn unachtsame Nutzer die Überweisungsdaten am Display nicht genau kontrollieren.

- Schwächen des Smartphone:

  Alles, was zu den Schwächen von Hardware basierenden OTP-Generatoren geschrieben wurde, trifft grundsätzlich auch auf das Smartphone zu. Da es sich hierbei um einen verhältnismäßig neuen Trend handelt, liegen noch wenig Angaben und Expertisen bezüglich etwaiger Sicherheitslücken und Angriffe vor.

Ein Nachteil von allen Arten der 2-Faktor-Authentifizierung ist, dass diese einen erheblichen finanziellen Mehraufwand für Unternehmen und gegebenenfalls auch für den Nutzer bedeuten. Darüber hinaus ist ihre Implementation oftmals sehr komplex. Richtig eingesetzt, sind die in diesem Kapitel vorgestellten Authentifizierungsmechanismen aber durchaus wirksam bezüglich der Verhinderung von Identitätsdiebstahl und Identitätsmissbrauch im Internet. So urteilten etwa jene Experten, die 2009 eine Studie zu Identitätsdiebstahl und Identitätsmissbrauch im Auftrag des BSI durchführten, im Rahmen ihrer Handlungsempfehlungen, dass Chipkartensysteme auf Basis von Kartenlesegeräten der Sicherheitsklasse 3 durchaus geeignet wären, Identitätsdiebstahl beim Onlinebanking zu vermeiden[506]. Eine Gefahr würden nur Angriffe auf Basis lokaler Malware darstellen, was aber bei einer Integration von Chipkarten und Kartenlesegerät in die Gesamtapplikation vermeidbar wäre. OTPs, egal ob durch Hardware-Token oder Smartphone generiert, werden in den Handlungsempfehlungen dieser Studie als gutes Mittel angesehen, um sichere sitzungsbasierte Authentifizierungen zu gewährleisten. Vor allem der Zugang zu Servern und Serverapplikationen müsse durch OTP-Verfahren oder Chipkartensysteme gesichert werden, da hier ein erfolgreicher Angriff fatale Konsequenzen hätte. Auch Sicherheitsfirmen wie ECOS[507] oder

504 Hanno Langweg, Jörg Schwenk, Schutz von FinTS/HBCI-Clients gegenüber Malware.
505 Hanno Langweg, Jörg Schwenk, Schutz von FinTS/HBCI-Clients gegenüber Malware.
506 Georg Borges, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 360.
507 http://www.ecos.de/notfallarbeitsplaetze.html (14.07.2012).

Symantec[508] haben ihr Angebot erweitert und bieten vor allem für die Authentifizierung innerhalb von Unternehmen entsprechende Hardware an.

6.2.2 Die elektronische Signatur und PKI

Bevor auf die Funktionsweise von elektronischen Signaturen und SSL genauer eingegangen werden kann, ist es notwendig, kurz zu erläutern wie solche Verschlüsselungsverfahren funktionieren. Verschlüsselungstechniken dienen, vereinfacht ausgedrückt, dazu, Daten während der Übertragung unlesbar zu machen. Die Daten werden mithilfe von mathematischen Verfahren durch einen sogenannten Schlüssel so abgeändert, dass sie für potentielle Angreifer nicht mehr lesbar sind[509]. Beim Empfänger angekommen, werden die so verschlüsselten Daten wieder mithilfe mathematischer Verfahren durch einen Schlüssel entschlüsselt, also wieder in eine lesbare Form gebracht[510]. Man unterscheidet allgemein zwischen symmetrischer und asymmetrischer Verschlüsselung. Bei der symmetrischen Verschlüsselung wird für das Verschlüsseln und das Entschlüsseln der gleiche Schlüssel verwendet.

Bei der asymmetrischen Verschlüsselung wird ein Schlüsselpaar, ein öffentlicher und ein privater Schlüssel, generiert. Der öffentliche Schlüssel dient dazu, Daten für den Inhaber des privaten Schlüssels zu verschlüsseln. Der private Schlüssel ermöglicht es seinem Inhaber, alle auf diese Weise verschlüsselten Daten zu entschlüsseln[511]. Der private Schlüssel ist dabei nur im Besitz des Anwenders, während der öffentliche Schlüssel allgemein zugänglich ist oder vom Anwender an den Kommunikationspartner gesendet wird.

Die Begriffe elektronische Signatur und digitale Signatur müssen klar voneinander abgegrenzt werden; während es sich bei der elektronischen Signatur um einen rein rechtlichen Begriff handelt, ist die digitale Signatur ein technischer Begriff und meint ein kryptographisches Verfahren. Ziel der elektronischen Signatur ist es, eine eindeutige und sichere Identifizierung eines Kommunikationspartners beim Datenverkehr im Internet zu gewährleisten[512]. Die allgemeine (technische) Definition der elektronischen Signatur lautet[513]:

„Die elektronische (oder digitale) Signatur bietet die Möglichkeit, elektronische Daten mit einer

508 http://www.symantec.com/business/support/index?page=content&id=HOWTO42048 (14.07.2012).
509 https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Sicherheitsmechanismen/sicherPKI/pki_node.html (20.07.2012).
510 http://www.itwissen.info/definition/lexikon/Sicherheitsinfrastruktur-PKI-public-key-infrastructure.html (20.07.2012).
511 http://www.dartmouth.edu/~deploypki/overview.html (20.07.2012).
512 http://www.digitales.oesterreich.gv.at/site/5567/default.aspx (20.07.2012).
513 http://www.a-sit.at/de/signatur/ (20.07.2012).

"Unterschrift" zu versehen. Damit kann nachgeprüft werden, ob die elektronischen Informationen tatsächlich vom Signator stammen und ob sie im Originalzustand - also unverändert - sind. Weiters können Signaturen zur Identifikation (z.B. beim Online-Banking) verwendet werden. Diese Merkmale sind beim Empfänger elektronisch signierter Daten überprüfbar und dadurch wird das Vertrauen in elektronische Kommunikation wesentlich gesteigert."

Die rechtlichen Rahmenbedingungen und Vorgaben für elektronische Signaturen enthält die europäische Signaturrichtlinie.[514] Die rechtliche Definition der elektronischen Signatur nach der EU-Signaturrichtlinie Artikel 2 Z 1[515]:

„Im Sinne dieser Richtlinie bezeichnet der Ausdruck

1. "elektronische Signatur" Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen;"

Sowohl die europäische Signaturrichtlinie als auch die jeweiligen Signaturgesetze der Mitgliedstaaten gehen bezüglich der elektronischen Signatur von einem technologieneutralen Ansatz aus[516]. Das bedeutet, auf welche Weise diese elektronische Signatur technisch umgesetzt wird, ist nicht weiter relevant. In den Signaturgesetzen der Mitgliedstaaten wird auch geregelt, dass elektronische Signaturen nicht im geschäftlichen Verkehr diskriminiert werden dürfen und von Behörden sowie Gerichten anerkannt werden müssen; der eigenhändigen Unterschrift sind sie aber nur ebenbürtig, wenn sie den gesetzlich definierten Mindeststandards entsprechen[517]. Die technische Umsetzung der elektronischen Signatur erfolgt aktuell durch die digitale Signatur und das digitale Zertifikat[518]. Ein digitales Zertifikat entspricht einem digitalen Ausweis; genauer gesagt, ist es ein Datensatz, der durch kryptografische Verfahren auf seine Integrität und Authentizität geprüft werden kann[519]. Ist beispielsweise der Führerschein eine Referenz für den Identitätsnachweis in der realen Welt, so kann man sich digitale Zertifikate als Referenz für den Identitätsnachweis im Internet vorstellen. Ein solches digitales Zertifikat enthält allgemeine Informationen über den Zertifikatinhaber sowie dessen öffentlichen Schlüssel. Ausgestellt werden digitale Zertifikate von Zertifizierungsstellen (certificate authorities, oder kurz CA). CA haben auch die Aufgabe, vor dem Verkauf der Zertifikate den Interessenten genau zu überprüfen und tragen die volle Verantwortung für die Integrität der von ihnen ausgestellten Zertifikate[520]. Üblicherweise werden digitale

514 http://europa.eu/legislation_summaries/information_society/other_policies/l24118_de.htm (20.07.2012).
515 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=de (20.07.2012).
516 http://www.digitales.oesterreich.gv.at/site/5567/default.aspx (20.07.2012).
517 http://www.internet4jurists.at/intern25.htm (20.07.2012).
518 http://www.itwissen.info/definition/lexikon/Digitale-Signatur-DSig-digital-signature.html (20.07.2012).
519 http://www.itwissen.info/definition/lexikon/Zertifikat-certificate.html (20.07.2012).
520 http://www.itwissen.info/definition/lexikon/Zertifizierungsstelle-CA-certification-authority.html (20.07.2012).

Zertifikate von der ausstellenden CA im Internet veröffentlicht, meistens in einem sogenannten Verzeichnisdienst oder auch directory service, damit jeder Nutzer die Echtheit der Zertifikate überprüfen kann. Bei der Ausstellung eines digitalen Zertifikats erhält der Käufer einen einmaligen privaten Schlüssel, den er immer geheim halten muss. Im folgenden werden nun die Begriffe digitales Zertifikat und SSL-Zertifikat synonym verwendet. Die digitale Signatur baut grundsätzlich auf dem digitalen Zertifikat auf. Sie ist nichts anderes als eine Art virtuelle Unterschrift auf einem elektronischen Dokument oder einer elektronischen Nachricht*, „die aus einem kryptografischen Code besteht, der aus dem Dokument oder der Nachricht und dem digitalen Zertifikat berechnet wird*."[521] Sie arbeitet auf Basis einer asymmetrischen Verschlüsselung. Ihre Funktionsweise, grundlegend erklärt[522]:

- Sollen Daten elektronisch signiert werden, so wird aus diesen Daten zunächst ein Hashwert berechnet.
- Der Absender der Daten verschlüsselt den gebildeten Hashwert mit dem privaten Schlüssel seines digitalen Zertifikats.
- Die signierten Daten werden zusammen mit dem öffentlichen Schlüssel an den Empfänger geschickt.
- Nach dem Empfang der Daten wird die digitale Signatur geprüft. Dabei wird zunächst der Hashwert der empfangenen Daten erneut gebildet.
- Mittels des öffentlichen Schlüssels wird die digitale Signatur entschlüsselt, wobei das Ergebnis dieses Vorgangs der bei der Signaturerzeugung generierte Hashwert ist.
- Die beiden Hashwerte werden miteinander abgeglichen. Stimmen sie überein, so ist dies eine Bestätigung dafür, dass die Daten „unterwegs" nicht verändert wurden.
- Als letzter Schritt wird das digitale Zertifikat des Absenders geprüft, indem es mit dem Zertifikat im Verzeichnisdienst der entsprechenden CA abgeglichen wird.

Moderne Signaturverfahren auf Basis digitaler Zertifikate und digitaler Signaturen sorgen also dafür, dass dank des privaten Schlüssels Daten bei der Übertragung nicht verändert werden können und dass nur der Besitzer des privaten Schlüssels und niemand sonst diese signieren kann. Wer den privaten Schlüssel nicht besitzt, kann Daten weder mit einer entsprechenden digitalen Signatur versehen, noch diese verändern, ohne dass die digitale Signatur dadurch ungültig wird. Dank des öffentlichen Schlüssels, der frei zugänglich ist, können solche Signaturen auch mit verhältnismäßig geringem Aufwand geprüft werden. Die gesamte technische Infrastruktur, innerhalb derer digitale

521 http://www.cryptoshop.com/index.php (20.07.2012).
522 http://www.kryptowissen.de/asymmetrische-verschluesselung.html (20.07.2012).

Zertifikate und digitale Signaturen erstellt, eingesetzt und überprüft werden, wird als Public-Key-Infrastruktur bezeichnet[523]. In Österreich gibt es bereits eine Reihe von Anwendungen, basierend auf elektronischen Signaturen, die mithilfe der sogenannten Bürgerkarte benutzt werden können. Bei der Bürgerkarte handelt es sich um eine Chipkarte, die mit einer digitalen Signatur und einem digitalen Zertifikat versehen ist[524]. Eindeutige Identifikation des Besitzers der Karte wird durch eine Personenbindung erreicht, im Zuge derer eine Stammzahl als weiteres Identitätsmerkmal mit dem digitalen Zertifikat kombiniert wird[525]. Der eindeutige Identitätsnachweis ergibt sich also durch Zertifikat und Stammzahl, wobei die Stammzahl von einer Stammzahlenregisterbehörde verwaltet wird. Seitens der österreichischen Bundesregierung wird ein Bürgerportal angeboten, das umfangreiche Informationen zum Thema Bürgerkarte bietet[526]. Eine solche Bürgerkarte kann für den zukünftigen Besitzer auf Wunsch neu angefertigt werden; es ist aber auch möglich, bestehende Chipkarten wie beispielsweise eine e-card oder auch eine Bankomatkarte auf die Funtkionalität einer Bürgerkarte zu erweitern. Die technische Umsetzung der Bürgerkarte erfolgt durch eine Bürgerkartenumgebung (BKU) und ein Chipkartenlesegerät[527]. Bei der BKU handelt es sich um ein Softwarepaket für den heimischen Rechner, das die Verwaltung und Benutzung der Bürgerkarte ermöglicht[528]. Mittlerweile ist es auch möglich, anhand der sogenannten Handy-Signatur das Mobiltelefon anstelle der Bürgerkarte zu nutzen, wobei hier TANs für den Einsatz der elektronischen Signatur verwendet werden[529]. Sowohl für das Handy als auch den heimischen Rechner ist es möglich, eine Online-BKU anstelle der lokalen Software zu nutzen, bei der über JAVA die benötigten Funktionen als Applet im Browser ausgeführt werden[530]. Die zur Verfügung stehenden Anwendungen sind in Österreich zahlreich. So können beispielsweise Amtswege im Rahmen von E-Government durch die Bürgerkarte erledigt werden, PDF-Dateien oder E-Mails können signiert werden und sogar Onlinebanking kann bei Banken mit der Bürgerkarte ausgeführt werden sofern das Verfahren seitens des Finanzinstituts unterstützt wird. Eine detaillierte Liste aller zur Verfügung stehenden Anwendungen ist im Bürgerportal einsehbar[531].

Leider sind auch elektronische Signaturen, die im Rahmen einer PKI eingesetzt werden, anfällig für Angriffe. Die österreichische Bürgerkarte wies in der Vergangenheit mehrmals beträchtliche Sicherheitslücken auf, zuletzt im April 2012[532]. Ein Student der FH Oberösterreich in Hagenberg

523 http://www.itwissen.info/definition/lexikon/Public-Key-Verfahren-public-key-method.html (20.07.2012).
524 http://www.digitales.oesterreich.gv.at/site/5268/default.aspx (20.07.2012).
525 http://www.digitales.oesterreich.gv.at/site/5567/default.aspx#a5 (20.07.2012).
526 http://www.buergerkarte.at/index.de.php (20.07.2012).
527 http://www.digitales.oesterreich.gv.at/site/5621/default.aspx (20.07.2012).
528 http://www.digitales.oesterreich.gv.at/site/5621/default.aspx (20.07.2012).
529 http://www.buergerkarte.at/wie-funktioniert.de.php (22.07.2012).
530 https://www.handy-signatur.at/mobile/info_bk.html (22.07.2012).
531 https://www.help.gv.at/aof/sigliste-flow (22.07.2012).
532 http://derstandard.at/1334795565969/Security-Forum-Sicherheitsluecke-bei-Buergerkarte (22.07.2012).

fand eine Sicherheitslücke, nach der es einem Angreifer möglich gewesen wäre, Nutzer über ein

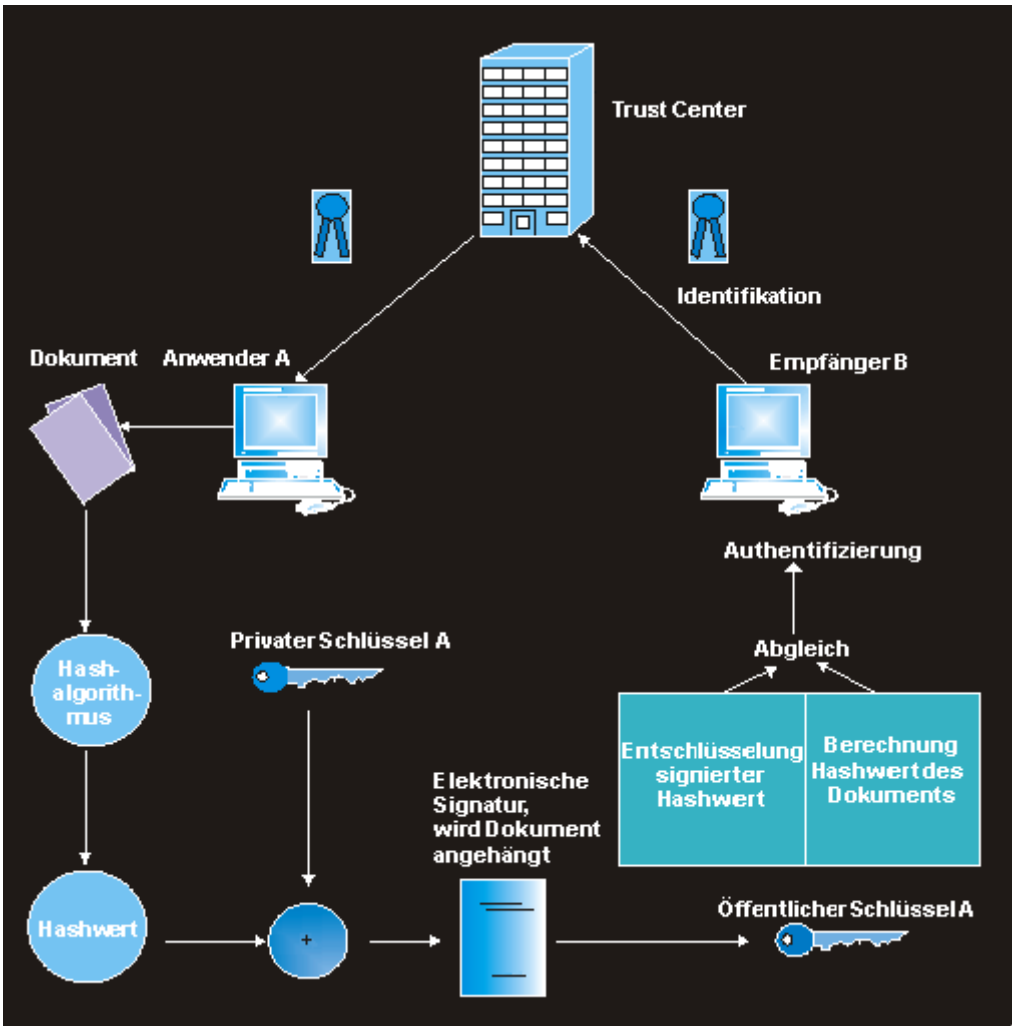

Abbildung 14: Funktionsweise der elektronischen Signatur[533]

manipuliertes JAVA-Applet auf eine gefälschte Webseite umzuleiten. Durch ein iFrame gelang es ihm, die erfolgreiche Authentifizierung des Besitzers der Bürgerkarte abzufangen und alle Funktionen der Bürgerkarte mit der Identität des Besitzers zu nutzen[534]. Auch Bürgerkarten sind somit kein garantierter Schutz gegen Identitätsdiebstahl. Darüber hinaus zeigt eine Statistik aus dem Jahr 2011, dass die Akzeptanz der Nutzer gegenüber der Bürgerkarte noch relativ niedrig ist[535]. Die tatsächliche Nutzung der Bürgerkarte liegt demnach unter 10%, wobei vor allem die zu

533 http://www.itwissen.info/definition/lexikon/Digitale-Signatur-DSig-digital-signature.html (22.07.2012).
534 http://ettisan.wordpress.com/2012/02/29/implementation-of-an-universal-forgery-on-the-austrian-burgerkarte/ (22.07.2012).
535 Statistik Austria, IKT-Einsatz in Haushalten, S. 26.

komplizierte technische Umgebung und Vertrauensmängel als Hauptgründe angegeben werden[536]. Trotzdem bietet die Bürgerkarte durch eine 2-Faktor-Authentifizierung vor allem gegen konventionelle Angriffsmethoden einen ausgezeichneten Schutz -vorausgesetzt, sie wird in Verbindung mit der BKU und dem Kartenlesegerät eingesetzt:

- Um die Bürgerkarte im Onlinebanking einzusetzen, sind sowohl der Besitz der Chipkarte als auch ihr PIN als Zugangscode notwendig. Somit ist jeglicher auf konventionellem Phishing basierende Angriff praktisch unmöglich, da der Angreifer, selbst wenn er in den Besitz des PIN gelangt, zusätzlich noch die Chipkarte selbst brauchen würde, um eine Transaktion durchzuführen[537]. Dazu kommt, dass die Transaktionsvorgänge elektronisch signiert werden und dass das hierdurch entstehende Signaturergebnis nicht wiederverwendbar oder reproduzierbar ist, was einen Missbrauch durch die Angreifer ausschließt.
- Einfache Malware, die dazu konzipiert ist, unbemerkt auf dem Rechner des Nutzers Daten und Passwörter zu sammeln, ist ebenfalls wirkungslos, da auch hier ohne einen Besitz der Chipkarte kein Missbrauch möglich ist.
- Pharming-Attacken können praktisch aus den gleichen Gründen verhindert werden.

6.2.3 SSL

Public-Key-Infrastrukturen bilden weiters die Basis für den Einsatz von SSL. SSL steht für Secure Socket Layer und bezeichnet ein Sicherheitsprotokoll, das für eine Verschlüsselung des Datenverkehrs zwischen Browser und Server sorgt[538]. Im OSI-Schichtenmodell liegt SSL zwischen der Anwendungsschicht und der Transportschicht. Das SSL-Protokoll soll die Sicherheit einer Verbindung durch das Erfüllen von 3 Kriterien gewährleisten[539]:

- Die Daten werden bei der Übertragung verschlüsselt, wodurch sie nur von den Kommunikationspartnern gelesen werden können.
- Es wird durch ein SSL-Zertifikat für eine sichere elektronische Authentifizierung des Servers gesorgt.
- Durch sogenannte Message Authentication Codes–Algorithmen wird sichergestellt, dass die Daten unverändert beim Empfänger ankommen und nicht manipuliert wurden[540].

536 http://futurezone.at/digitallife/10633-oesterreicher-vertrauen-buergerkarte-nicht.php (22.07.2012).
537 http://www.bmi.gv.at/cms/BMI_OeffentlicheSicherheit/2007/03_04/files/IT_Sicherheit.pdf (22.07.2012).
538 http://www.itwissen.info/definition/lexikon/secure-socket-layer-SSL-SSL-Protokoll.html (28.07.2012).
539 http://www.elektronik-kompendium.de/sites/net/0902281.htm (28.07.2012).
540 http://www.itwissen.info/definition/lexikon/message-authentication-code-MAC-MAC-Code.html (28.07.2012).

Erkennen kann man SSL-gesicherte Webseiten an in der URL befindlichen Kürzel https (HyperText Transfer Protocol Secure). Der Aufbau einer durch SSL gesicherten Verbindung kann entweder durch den Nutzer oder durch den Server erfolgen[541]:

- Der Nutzer kann eine gesicherte Verbindung initiieren, indem er in der URL der gewünschten Webseite https statt http eingibt. Optional können solche Verbindungen auch von Browser-Add-Ons automatisch ausgelöst werden.
- Serverseitige SSL-Verbindungen sind bei besonders heiklen Diensten wie etwa Netbanking der Standard.

Für den Aufbau der Verbindung sorgt ein Teilprotokoll von SSL, das sogenannte SSL Handshake Protocol, welches die zu verwendenden kryptographischen Verfahren auswählt, für eine sichere Authentifizierung des Servers sorgt und den Sitzungsschlüssel für die Verschlüsselung berechnet. Erwähnenswert hierbei ist, dass die Verschlüsselung während des Verbindungsaufbaus asymmetrischer Natur ist. Der Verbindungsaufbau gestaltet sich wie folgt[542]:

- Der Browser fordert das SSL-Zertifikat des Servers zu dessen Authentifizierung an. Außerdem sendet er in dieser Anfrage eine Liste aller Verschlüsselungsverfahren mit, die er unterstützt.
- Der Server sendet dem Browser eine Antwort, die das ausgewählte Verschlüsselungsverfahren und sein SSL-Zertifikat zusammen mit dem öffentlichen Schlüssel enthält.
- Der Browser prüft das SSL-Zertifikat auf dessen Echtheit, indem er es mit dem Zertifikat im Verzeichnisdienst der entsprechenden CA abgleicht. Ist das Zertifikat falsch oder abgelaufen, so erhält der Nutzer eine Warnmeldung. Ist das Zertifikat echt, so war die Authentifizierung des Servers erfolgreich und der Browser generiert einen Sitzungsschlüssel für ein symmetrisches Verschlüsselungsverfahren. Diesen Sitzungsschlüssel verschlüsselt der Browser mit dem öffentlichen Schlüssel des Servers und sendet diesen an den Server.
- Der Server entschlüsselt die Nachricht mit seinem privaten Schlüssel und kennt nun den Sitzungsschlüssel.

Damit ist der Verbindungsaufbau abgeschlossen, es folgt der Datenaustausch zwischen Browser und Server im Rahmen einer symmetrischen Verschlüsselung durch den Sitzungsschlüssel. Dabei erfolgen Übertragung und Verschlüsselung der Daten durch ein weiteres Teilprotokoll von SSL, das sogenannte Record Protokoll. Dieses teilt die zu versendenden Daten in Blöcke (SSL-Records) auf,

541 http://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/de_DE/HTML/user277.htm (28.07.2012).
542 http://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/de_DE/HTML/user277.htm (28.07.2012).

verschlüsselt sie mit dem Sitzungsschlüssel und sichert jedes der Datenpakete mit einem angehängten MAC gegen Manipulation[543].

Die letzte Version von SSL ist aktuell SSL 3.0; seit dieser Version wird das Protokoll unter dem Namen TLS weiterentwickelt, was für Transport Layer Security steht. Die Funktionsweise von TLS ist aber über weite Strecken mit jener von SSL identisch, weswegen TLS 1.0 auch als SSL 3.1 bezeichnet werden kann[544]. Die meisten Internetseiten unterstützen beides, also sowohl SSL 3.0 als auch TLS 1.0, wobei SSL 2.0 wegen mangelnder Sicherheit kaum mehr unterstützt wird. Im Rahmen dieser Arbeit werden die Begriffe SSL und TLS daher synonym verwendet. SSL bietet im Kampf gegen Identitätsdiebstahl und Identitätsmissbrauch folgende Vorteile:

- eine sichere Authentifizierung des Servers anhand von SSL-Zertifikaten sowie eine sichere Verbindung zwischen Browser und Server;
- durch sogenannte SSL-Clientzertifikate wäre es theoretisch auch für den Server möglich, im Rahmen einer bilateralen Authentifizierung während des Handshakes den Browser eines Nutzers zu identifizieren und gegebenenfalls wiederzuerkennen[545]. Dies würde vor allem Identitätsmissbrauch bei online-Versandhäusern(wie etwa Amazon) erschweren. Die meisten Unternehmen haben aber diese Art der Nutzer-Authentifizierung noch nicht umgesetzt, da es vor allem im Hinblick auf den Datenschutz noch ungeklärte Fragen gibt.
- SSL benötigt praktisch keine besonderen technischen Vorkenntnisse des Nutzers, da die Authentifizierung und der Datenaustausch komplett automatisch erfolgen. Der Nutzer kann anhand bestimmter visueller Zeichen(zB. das Symbol eines Vorhängeschlosses in der URL der besuchten Webseite) erkennen, dass es sich um eine sichere Verbindung handelt. Er muss lediglich SSL 3.0/TLS 1.0 in seinen Browsereinstellungen aktivieren[546].

Selbstverständlich hat SSL/TLS auch einige signifikante Nachteile:

- Public-Key-Infrastrukturen, die für eine sichere Authentifizierung von Webseiten auf Basis von SSL-Zertifikaten notwendig sind, sind sowohl bei Nutzern als auch Unternehmen nicht besonders beliebt. Grund dafür ist, dass die technische Umsetzung einer solchen PKI meist sehr komplex ist und entsprechend hohe Kosten verursacht.
- SSL/TLS war und ist ein beliebtes Ziel für MitM-Angriffe[547]. Im Jahr 2009 wurde von Moxie Marlinspike im Rahmen der Sicherheitskonferenz „Black Hat“ ein neuer MitM-

543 https://www.cryptoheaven.com/Security/Presentation/SSL-protocol.htm (28.07.2012).
544 http://www.itwissen.info/definition/lexikon/transport-layer-security-TLS-TLS-Protokoll.html (28.07.2012).
545 http://pilif.github.com/2008/05/why-is-nobody-using-ssl-client-certificates/ (28.07.2012).
546 http://www.bev.gv.at/portal/page?_pageid=696,1682731&_dad=portal&_schema=PORTAL (28.07.2012).
547 http://www.ceilers-news.de/serendipity/207-Man-in-the-Middle-Angriffe-auf-HTTPS.html (28.07.2012).

Angriff vorgestellt, der sich eines eigens für den Angriff entwickelten Proxys namens „SSLStrip“ bedient[548]. Dieser Angriff macht sich den Umstand zunutze, dass eine sichere HTTPS-Verbindung in vielen Fällen nicht durch den Nutzer initiiert wird, sondern dass eine solche Verbindung zumeist durch einen Klick auf entsprechende Links erfolgt, zB. auf Login-Buttons einer Webseite. Der Proxy SSLStrip durchsucht Webseiten nach eingebetteten https-Links und ersetzt diese durch durch http-Anfragen, die mit der Ziel-URL identisch sind[549]. Sobald der Nutzer auf einen solchen Link klickt, wird dies vom Proxy erkannt und dieser startet selbst eine SSL-Verbindung zum vom Opfer aufgerufenen Server. Der Proxy kommuniziert nun, wann immer es notwendig ist, verschlüsselt mit dem Server und sendet bei Bedarf Daten des Servers unverschlüsselt an den Nutzer weiter. Dieser MitM-Angriff zielt also nicht darauf, eine SSL-Verbindung zu knacken; er verhindert den Aufbau einer solchen Verbindung zwischen Nutzer und Server. Da es für den Nutzer nie zu einer gesicherten Verbindung kommt, gibt der Browser auch keine entsprechende Warnmeldung aus. Der Nutzer selbst könnte zwar den Angriff durch einen genauen Blick auf die URL in seinem Browser erkennen, in den meisten Fällen jedoch fällt dies nicht weiter auf, zumal SSLStrip sogar das Symbol des Vorhängeschlosses im Browser des Nutzers fälschen kann. Der Proxy selbst kann in ein LAN durch Angriffe wie ARP-Spoofing eingeschleust werden, gegen heimische Rechner könnte der Angreifer SSLStrip mittels DNS-Cache-Poisoning einsetzen.

- Neben SSL selbst und dem Nutzer sind auch die CA sowie die digitalen Zertifikate anfällig für Angriffe. In der jüngeren Vergangenheit wurden CA wiederholt Opfer von Hackingangriffen, bei denen Zertifikate für bereits existierende Webseiten erbeutet wurden[550]. Dazu war es lange Zeit auch möglich, digitale Zertifikate zu fälschen und für Phishing-Angriffe einzusetzen[551].

Auch wenn SSL allein keinen kompletten Schutz vor Identitätsdiebstahl und Identitätsmissbrauch im Internet bietet, so kann diese Technologie doch eine sinnvolle Grundlage zu dessen Bekämpfung sein. Die vom BSI in Auftrag gegebene Studie zu Identitätsdiebstahl und Identitätsmissbrauch im Internet führt in ihren Handlungsempfehlungen für technische Sicherheitsmaßnahmen SSL zur Authentifizierung von Servern und Nutzern im Internet auf[552]. Um Angriffe durch Tools wie zB.

548 http://www.heise.de/newsticker/meldung/Black-Hat-Neue-Angriffsmethoden-auf-SSL-vorgestellt-198285.html (28.07.2012).
549 http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf (28.07.2012).
550 http://www.heise.de/security/meldung/SSL-GAU-zwingt-Browser-Hersteller-zu-Updates-1212986.html (30.07.2012).
551 http://www.ceilers-news.de/serendipity/284-SSL-Der-naechste-Nagel-im-Sarg.html (30.07.2012).
552 Georg Borges, Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 363.

SSLStrip weniger effizient zu machen, wird empfohlen, ungesicherte Verbindungen durch klare visuelle Merkmale(wie etwa eine rot unterlegte Adressleiste im Browser) anzuzeigen. Auch Sicherheitsfirmen wie Symantec empfehlen für Unternehmen den umfassenden Einsatz von SSL[553].

6.2.4 Schutz für den Browser – Reputationsbasierte Schutzmechanismen

Im Jahr 2012 ist nach wie vor der Browser eines der beliebtesten Ziele für Angreifer[554]. Um Identitätsdiebstahl und Identitätsmissbrauch im Internet zu unterbinden, ist es notwendig, neue Schutzmechanismen für den Browser zu entwickeln. Im Rahmen dieser Arbeit wurden 3 neue Trends auf dem Gebiet der IT-Sicherheit, die vor allem für den Browser konzipiert wurden, untersucht:

- Browser-Sandboxing;
- Reputationsbasierte Schutzmechanismen im Browser;
- HSTS.

Browser-Sandboxing wurde bereits in Kapitel 6.1.2 näher beschrieben. Hier ist nur noch hinzuzufügen, dass Sandboxing-Technologie dieser Art, also voll in den Browser integriertes Sandboxing, zukünftig in jedem modernen Browser vorhanden sein sollte, da hierdurch sehr hoher Schutz erreicht werden kann. Gegenüber konventioneller Sandboxing-Software, die in Kapitel 6.1.1 näher beschrieben wurde, hat Browser-Sandboxing den Vorteil, dass der Nutzer praktisch nicht mit diesem Schutzmechanismus interagieren muss und somit keine besonderen technischen Kenntnisse notwendig sind.

Reputationsbasierte Technologien zum Schutz vor Malware wurden erstmals im September 2009 von der Sicherheitsfirma Symantec eingesetzt[555]. Diese Technologie stützt sich auf große Mengen von gesammelten Daten, die aus verschiedenen Quellen gewonnen werden; darunter beispielsweise anonymisierte Daten von Symantec-Kunden, anonymisierte Daten von Software-Entwicklern sowie anonymisierte Daten von anderen Unternehmen. Alle diese Daten fließen in eine sogenannte „Reputation Engine“, die für jede Datei, die überprüft werden soll, ein Reputationsprofil erstellt, welches sich aus den Attributen der Datei(wie etwa Alter, digitale Signatur oder Verbreitung) ergibt[556]. Dieses Reputationsprofil ist dann für alle Symantec-Kunden frei zugänglich. Wird also eine Datei aufgrund ihrer Reputation als Datei mit Schadpotential eingestuft, wird sie blockiert.

553 Symantec Internet Security Threat Report, S. 44.
554 http://www.itmagazine.ch/Artikel/50956/Soziale_Netzwerke_und_Browser_beliebte_Angriffsziele.html (04.08.2012).
555 http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20090915_01 (04.08.2012).
556 http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20090915_01 (04.08.2012).

Erwähnenswert hierbei ist, dass reputationsbasierter Schutz vor Malware keinesfalls einen Ersatz für reaktive und proaktive Malware-Erkennung ist, sondern eine Ergänzung zu diesen Verfahren darstellt und somit den Schutz für den Nutzer noch einmal erhöhen soll. Dieser Schutz wurde vermehrt auch in Browser integriert, um diese vor gefährlichen Webseiten zu warnen und um den Schutz der Browser vor Angriffen durch Malware zu erweitern. Reputationsbasierte Schutzmechanismen im Browser können grundsätzlich auf 2 verschiedene Arten arbeiten. Man unterscheidet:

- adressbasierte Reputation[557]:

  Auf Basis von Browser-Rückmeldungen und Erfahrungen anderer Nutzer werden URLs entsprechende Reputationswerte zugeordnet und bekannte Angriffs-URLs werden in eine Blacklist eingetragen, die von einer zentralen Stelle verwaltet wird. Besucht ein Nutzer eine Webseite, so wird im Hintergrund vom Browser diese Blacklist geladen. Ist die angesteuerte URL in diese Blacklist eingetragen, so wird der Nutzer vom Browser durch eine entsprechende Meldung gewarnt, bevor die Seite geöffnet wird.

- inhaltsbasierte Reputation[558]:

  Inhaltsbasierte Reputation funktioniert nach dem gleichen Blacklisting-Prinzip wie adressbasierte Reputation; hier werden nicht der URL, sondern den heruntergeladenen Inhalten auf Webseiten Reputationswerte zugeordnet. Wird beim Besuch einer Webseite vom Browser ein Inhalt heruntergeladen, der sich auf der Blacklist befindet, wird dieser Inhalt vom blockiert und nicht über den Browser ausgeführt.

Diese beiden Schutzmechanismen können auch zusammenarbeiten und so eine Art 2-Schichten-Schutz für den Rechner bilden. Wenn der Nutzer eine Webseite besucht, wird zunächst die URL auf ihre Reputation überprüft und danach, falls die URL nicht in der Blacklist enthalten ist, ergänzend noch die Inhalte[559]. Erwähnenswert ist ferner dass Reputationswerte nicht zwingend nach dem Blacklist-Prinzip verwaltet werden müssen, sondern dass auch eine Anwendung des Whitelist-Prinzips möglich ist[560]. Dabei werden URLs bzw Inhalte, die als unbedenklich eingestuft wurden, in eine zentrale Whitelist eingetragen. Der Browser lädt diese Whitelist bei Besuch einer URL und ist die Internetadresse oder der konkrete Inhalt enthalten, so wird ein Zugriff gestattet. Des Weiteren

557 Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 16.
558 Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 16.
559 Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 16.
560 Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 17.

können lokale und zentrale Blacklists und Whitelists eingesetzt werden[561]. Die lokalen Listen liegen im Browser vor und speichern all jene URLs und Inhalte, die bereits geladen wurden, je nach Typ entweder in lokalen Blacklists oder Whitelists. Lokale Listen dienen dazu, den Kommunikationsaufwand für den Browser zu reduzieren, da dieser ansonsten bei jeder besuchten Webseite die zentralen Listen laden müsste[562]. So werden die zentralen Listen nur geladen, wenn die URLs oder Inhalte nicht in den lokalen Listen des Browsers vorliegen. Für den Einsatz von reputationsbasierten Schutzmechanismen im Browser wurden von Microsoft und Google zwei verschiedene Technologien entwickelt:

- SmartScreen-Filter von Microsoft[563]:

  Beim SmartScreen-Filter von Microsoft arbeiten ein adressbasiertes Reputationssystem und ein inhaltsbasiertes Reputationssystem zusammen. Das adressbasierte Reputationssystem verwendet lokale und zentrale Blacklists sowie lokale Whitelists, um den Kommunikationsaufwand für den Browser zu reduzieren. Ohne die lokalen Whitelists müsste der Browser bei jeder URL, die sich nicht in den lokalen Blacklists befindet, die zentralen Blacklists kontaktieren. Eine Aktualisierung der Blacklists erfolgt beim Start des Browsers und in Zeitintervallen von unter 60 Minuten. Das inhaltsbasierte Reputationssystem, auch Application Reputation genannt, arbeitet auf Basis von lokalen und zentralen Black- und Whitelists. Der Smartscreen-Filter erlaubt übrigens eine teilweise Blockierung von Webseiten. In diesem Fall werden nur jene Inhalte einer Webseite blockiert bzw nicht angezeigt, die auf den Blacklists stehen.

- Safe Browsing von Google[564]:

  Safe Browsing von Google arbeitete bis Februar 2012 nur auf Basis eines adressbasierten Reputationssystems. Dieses verwendet lokale Black- und Whitelists und zentrale Blacklists. Eine Aktualisierung der lokalen Blacklist erfolgt circa alle 30 Minuten. Per Februar 2012 wurde mit Google Chrome 17 auch ein inhaltsbasiertes Reputationssystem hinzugefügt.

Im März 2012 wurde eine Studie vom Fraunhofer SIT veröffentlicht, in deren Rahmen untersucht wurde, wie gut reputationsbasierte Schutzmechanismen in Browsern gegen Malware-Angriffe wirken. Herangezogen wurden für die Untersuchung folgende Browser[565]:

561 Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 17.
562 Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 17.
563 http://windows.microsoft.com/de-at/windows7/smartscreen-filter-frequently-asked-questions-ie9 (04.08.2012).
564 http://www.google.com/transparencyreport/safebrowsing/?hl=de (04.08.2012).
565 Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 19.

- Google Chrome 14;
- Mozilla Firefox 6;
- Microsoft Internet Explorer 8;
- Microsoft Internet Explorer 9;
- Apple Safari 5.

Alle Browser bis auf Microsoft Internet Explorer verwenden Safe Browsing als Technologie. Freilich wurde nur die 32-Bit Version dieser Browser getestet. Es wurde auch bei den Rahmenbedingungen der Studie angemerkt, dass mit Google Chrome 17 vermutlich bessere Leistungsfähigkeit(wegen Implementierung eines inhaltsbasierten Reputationssystems) gegeben wäre; diese Version kam aber für den Test zu spät. Die Rahmenbedingungen der Untersuchung lauteten wie folgt[566]:

- Die aufgelisteten Browser wurden unter gleichen Bedingungen mit denselben Angriffen konfrontiert. Es wurden jeweils mit Malware infizierte Webseiten gesammelt und diese dann mit den Browsern angesteuert.
- Gemessen wurde nur die Effizienz der in den Browser integrierten, reputationsbasierten Schutzmechanismen gegen Angriffe durch Malware-URLs; weitere Schutzmechanismen der Browser wurden nicht untersucht.
- Die Versionen der Browser wurden über den gesamten Messungszeitraum nicht geändert.
- Die Untersuchung wurde als Black-Box-Analyse ausgeführt; es wurden nur die Ein- und Ausgaben der Browser bewertet, interne Vorgänge dagegen nicht berücksichtigt.
- Die Browser wurden mehrmals mit der gleichen Malware-URL angegriffen, um die für Aktualisierungen der Blacklists benötigte Zeit zu überprüfen.
- Alle Browser wurden in ihrer Standardkonfiguration und ohne Erweiterungen eingesetzt, da diese Bedingungen nach Ansicht der Tester dem durchschnittlichen technischen Wissen der Nutzer/innen entsprechen würde.

Das Ergebnis der Untersuchung war ernüchternd[567]:

- Wie bereits betont, wurde nur das adressbasierte Reputationssystem getestet. Mit 34,9% konnte Internet Explorer 9 gerade einmal ein Drittel der Malware-URLs als solche

566 Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 19-21.
567 Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 24-33.

erkennen. Zweiter wurde Internet Explorer 8 mit 34,1% und dritter wurde Chrome mit 11,1%. Firefox(8,2%) und Safari(9,2%) schafften es nicht einmal, 10% der Malware-URLs zu erkennen.

- Die Application Reputation des SmartScreen-Filters konnte nur 7,3% der Malware identifizieren, wobei 3,1% dieser Malware auch durch das adressbasierte Reputationssystem erkannt werden konnte. Effizient aufgedeckt wurden also dadurch zusätzlich lediglich 4,2%.
- Bei der Aktivierung beider Reputationssysteme kam Internet Explorer 9 auf einen Anteil von 39,1%.

Internet Explorer ist zwar im Hinblick auf reputationsbasierte Schutzmechanismen die beste Software, allerdings kann von dieser Studie nicht auf die Gesamtsicherheit der Browser geschlossen werden. Man hält am Ende der Studie fest, dass reputationsbasierte Schutzmechanismen für Browser maximal als Ergänzung zu weiterem Schutz vor Malware gesehen werden können[568]. Als solche Ergänzung sind sie aber durchaus sinnvoll. Eine ähnliche Untersuchung war von der Sicherheitsfirma NSS Labs im September 2012 durchgeführt worden, diesmal mit aktuelleren Browser-Versionen[569]:

- Microsoft Internet Explorer 10;
- Google Chrome 21;
- Mozilla Firefox 15;
- Apple Safari 5.

Erwähnenswert dabei ist, dass zwar Chrome bei diesem Test über ein inhaltsbasiertes Reputationssystem verfügt, das in Version 17 hinzugefügt wurde; Firefox und Safari allerdings, die auch Safe Browsing verwenden, nicht. Die Rahmenbedingungen für die Untersuchung waren ähnlich wie bei der Studie des Fraunhofer SIT: Über einen Zeitraum von 20 Tagen wurden mit den Browsern zuvor gesammelte Malware-URLs angesteuert und es wurde gemessen, wie viele dieser Aufrufe blockiert wurden. Das Ergebnis der Untersuchung wich stark von jenem der Fraunhofer SIT-Studie ab[570]:

- Nur durch das adressbasierte Reputationssystem allein konnte Internet Explorer 88,5% aller Malware-URLs blocken. Chrome mit 4,5%, Firefox mit 4,3% und Safari mit 4,2% waren von diesem Wert weit entfernt.

568Fraunhofer SIT, Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern , S. 32.
569 NSS Labs , Browser Security Comparative Analysis, S. 2.
570 NSS Labs, Browser Security Comparative Analysis, S. 5-7.

- Durch Application Reputation konnte Internet Explorer zusätzlich 10,6% an Malware-URLs blocken, die nicht durch das adressbasierte Reputationssystem erkannt wurden. Chrome 21 konnte durch das neue inhaltsbasierte Reputationssystem zusätzlich 65,8% aller Malware URLs erkennen. Insgesamt kommt Internet Explorer somit auf 99,1% und Chrome auf 70,4%.

Die Zeit, die für das Updaten der lokalen und zentralen Blacklists benötigt wird, ist bei beiden Untersuchungen moderat. Der Umstand, dass bei der Studie von NSS Labs deutlich bessere Ergebnisse erzielt wurden, zeigt, dass reputationsbasierte Schutzmechanismen noch viel Entwicklungspotential besitzen. Sie skalieren vor allem mit der Geschwindigkeit und Häufigkeit, mit der die lokalen und zentralen Blacklists upgedated werden. Technisch gesehen stellen somit reputationsbasierte Schutzmechanismen im Browser eine gute erste Verteidigungslinie dar, die ergänzend zu anderen Schutzmechanismen wirkt. Vor allem der Umstand, dass der Nutzer selbst nichts tun muss für diesen Schutz(außer auf die Warnmeldungen zu reagieren), sorgt dafür dass auch technisch wenig versierte Nutzer profitieren. Rechtlich stellen reputationsbasierte Schutzmechanismen aber durchaus ein Problem dar. So kritisierte etwa der kanadische Sicherheitsexperte Nadim Kobeissi, dass durch den SmartScreen-Filter der Firma Microsoft Persönlichkeitsrechte und die Privatsphäre von Menschen verletzt werden[571]. Soll eine Software aus dem Internet installiert werden, so prüft der SmartScreen-Filter den Installer und sendet Daten an Microsoft[572]. Unter diesen Daten befinden sich unter anderem der eindeutige Hash-Wert, der Name der Datei, falls vorhanden eine digitale Signatur sowie die IP-Adresse des Rechners des Nutzers. Microsoft weiß somit von jeder Applikation, die ein Nutzer im Internet installiert und kann diese auch dem Nutzer eindeutig zuordnen. Auch bei Safe Browsing werden Daten an den Anbieter übertragen(zB. welche Webseiten der Nutzer besucht hat oder diverse Kennwörter)[573]. Sowohl bezüglich Datenschutz als auch betreffend Identitätsdiebstahl und Identitätsmissbrauch eröffnen reputationsbasierte Schutzmechanismen neue Probleme:

- Der Nutzer erfährt nichts von den Datenübertragungsvorgängen und hat auch kein Wissen darüber, wie diese Daten gespeichert und ausgewertet werden.
- Bekommt ein Angreifer Zugang zu diesen Daten, wäre hierdurch erst recht die Gefahr eines Identitätsdiebstahls gegeben.
- Die Daten könnten theoretisch während der Übertragung von Dritten abgefangen werden.

Auch wenn reputationsbasierte Schutzmechanismen also durchaus ihren Nutzen bei der

571 http://log.nadim.cc/?p=78 (04.08.2012).
572 http://log.nadim.cc/?p=78 (04.08.2012).
573 http://wiki.vorratsdatenspeicherung.de/images/Googlesafebrowsing-deaktivierung.pdf (20.08.2012).

Bekämpfung von Identitätsdiebstahl und Identitätsmissbrauch im Internet haben, bleibt hier abzuwarten, ob die genannten Probleme in absehbarer Zeit behoben werden.

6.2.5 Schutz für den Browser – HSTS

Bei HSTS(HTTP Strict Transport Security) handelt es sich um einen Mechanismus, der entwickelt wurde, um das in Kapitel 5.2.3 beschriebene SSL-Stripping zu verhindern. Die Entwicklung dieses Protokolls begann im Jahr 2009, direkt nach Bekanntwerden des MitM-Angriffs auf Basis von SSL-Strip. Mit Oktober 2012 wurde HSTS als Standard akzeptiert[574]. HSTS wird dadurch aktiviert, dass der Server einer durch HTTPS geschützten Webseite dem Browser des Nutzers einen speziellen HTTP-Response Header als Antwort sendet. Dieser Header ist folgendermaßen aufgebaut[575]:

```
Strict-Transport-Security: max-age=Gültigkeitsdauer;
includeSubDomains
```

Erhält der Browser vom Server diesen Header, so wandelt er von nun an automatisch alle HTTP-Anfragen auf diese Seite in HTTPS-Anfragen um. Das Feld max-age im Header enthält die Gültigkeitsdauer und gibt mit dieser an, wie lange der Browser HTTP-Anfragen auf den Server in HTTPS-Anfragen umwandelt. Die Gültigkeitsdauer wird in Sekunden angegeben und läuft ab jenem Zeitpunkt, zu dem der Browser zum letzten Mal auf die Webseite zugegriffen hat; es empfiehlt sich also, diese möglichst hoch anzusetzen. Das Feld includeSubDomains ist optional; bei Aktivierung werden auch alle Subdomains des Servers mit HSTS geschützt[576]. Neben dem Schutz vor SSL-Stripping bietet HSTS noch einen weiteren Schutz: Sollte das SSL-Serverzertifikat vom Browser als nicht vertrauenswürdig eingestuft werden, sorgt HSTS dafür, dass die Verbindung zum Server automatisch unterbrochen wird -anders als bei normalen SSL-Verbindungen, wo der Nutzer sich über die Warnung mit einem Klick hinwegsetzen kann[577]. Im November 2012 wurde von der Münchner Sicherheitsfirma SecureNet eine Studie veröffentlicht, die Aufschluss über die Verbreitung von HSTS geben sollte. Die Rahmenbedingungen der Studie waren folgende[578]:

- Durch ein Skript sollten Webseiten auf das Vorhandensein eines HSTS-Headers geprüft werden.
- Bei Seiten, die einen HSTS-Header hatten, wurden die Felder max-age und includeSubDomains geprüft.

574 https://www.owasp.org/index.php/HTTP_Strict_Transport_Security (20.08.2012).
575 https://www.owasp.org/index.php/HTTP_Strict_Transport_Security (20.08.2012).
576 https://www.owasp.org/index.php/HTTP_Strict_Transport_Security (20.08.2012).
577 https://hacks.mozilla.org/2010/08/firefox-4-http-strict-transport-security-force-https/ (20.08.2012).
578 SecureNet, Aktuelle Verbreitung von HTTP Strict Transport Security, S. 3.

- Überprüft wurde 1 Million der weltweit meistbesuchten Webseiten, die darin enthaltenen de-Domains und die Login-Seiten deutscher Onlinebanking-Seiten.
- Webseiten, die über keinen HTTPS-Schutz verfügen oder deren Zertifikat fehlerhaft ist, wurden bei der Auswertung nicht berücksichtigt.

Die Bewertung fiel verheerend aus[579]:

- Nur 10% der untersuchten Webseiten verfügen über HTTPS-Schutz. Von diesen 100.000 Seiten besitzen gerade einmal 410 den HSTS-Header. Von diesen 410 Webseiten hatten gerade einmal 222 den Wert von max-age auf den von der Studie empfohlenen Wert von 31.536.000, also Gültigkeitsdauer 1 Jahr, gesetzt. 100 Seiten definierten hier einen Wert, der kleiner als der empfohlene Mindestwert von 30 Tagen ist. Das bedeutet, von diesen 10% bieten gerade einmal 0,4% Schutz durch HSTS, wobei hiervon nur 0,25% wirklich effizient geschützt sind.
- Die Zahl der de-Domains belief sich auf 39.270, von denen 6.209 über Schutz durch HTTPS verfügten. Lediglich 12 Webseiten implementierten Schutz durch HSTS, wobei lediglich 5 davon den empfohlenen Mindestwert von 30 Tagen im Feld max-age gesetzt hatten. Von diesen 5 Webseiten hatten nur 3 das Feld includeSubDomains aktiviert. Dies bedeutet also, dass von den 6.209 meistbesuchten deutschen Webseiten mit HTTPS-Schutz gerade einmal 0,2% durch HSTS effizient geschützt sind.
- Von den 424 deutschen Onlinebanking-Seiten, die alle durch HTTPS geschützt waren, verfügten lediglich 7 Seiten über Schutz durch HSTS. Das Feld includeSubDomains war bei keiner dieser 7 Seiten gesetzt; nur 1 Seite hatte das Feld max-age richtig gesetzt. Das bedeutet, von lediglich 7 Seiten war nur eine einzige effizient durch HSTS bewehrt.

In ihrem Fazit merkten die Autoren der Studie kritisch an, dass es komplett unverständlich sei, warum eine nun bereits 3 Jahre alte Angriffsmethode wie SSL-Stripping trotz eines wirksamen Schutzmechanismus für SSL-Verbindungen noch immer eine massive Bedrohung für die überwiegende Mehrheit der meistbesuchten Webseiten der Welt darstelle[580]. Neben der geringen Verbreitung von HSTS ist auch ein zu niedrig gesetzter Wert im Feld max-age des Headers ein gravierendes Problem: Es könnte bei einer zu geringen Gültigkeitsdauer der Schutz, der bei einem vorherigen Besuch der Webseite aktiviert wurde, wieder abgelaufen sein. In diesem Fall wäre die Gefahr eines SSL-Stripping gegeben, da dieses ein Neusetzen des Headers verhindern würde[581].

579 SecureNet, Aktuelle Verbreitung von HTTP Strict Transport Security, S. 5-7.
580 SecureNet, Aktuelle Verbreitung von HTTP Strict Transport Security, S. 7.
581 http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Whitepaper.pdf (20.08.2012).

Eine andere Gefahr würde ein MitM-Angriff darstellen, der beim ersten Besuch des Nutzers auf der durch HSTS geschützten Webseite erfolgt. Der Browser weiß bei einem ersten Besuch noch nicht, ob er eine verschlüsselte oder unverschlüsselte Verbindung nutzen soll und steuert oftmals die HTTP-Version der Seite an. Gelingt es einem Angreifer, sich hier zwischen Browser und Server zu schalten, könnte der Angreifer den Aufbau einer durch HSTS gesicherten Verbindung im Keim ersticken[582]. Allerdings haben moderne Browser hier bereits sehr gute Schutzmechanismen, um solche MitM-Angriffe zu unterbinden. Von aktuellen Versionen der Browser Firefox und Chrome werden sogenannte HSTS-Listen geführt, in denen Webseiten enthalten sind, die Schutz durch HSTS anbieten[583]. Wird eine solche Webseite erstmals besucht, so erwarten die Browser automatisch einen HSTS-Header und lassen nur verschlüsselte Verbindungen zu. Hinzu kommt, dass nur solche Webseiten in den Listen enthalten sind, deren Wert im Feld max-age mindestens 18 Wochen beträgt. Grundsätzlich sorgt HSTS für einen sehr guten Schutz von SSL-Verbindungen; es ist empfehlenswert, den Anwendungsbereich dieses Protokolls zu erweitern. Aktuell sind normale SSL-Verbindungen immer noch anfällig für SSL-Stripping. Daher empfiehlt es sich, jede durch SSL gesicherte Webseite zusätzlich mit HSTS zu bewehren.

6.2.6 Sicherheit im Online-Banking – mTAN und eTAN+

Bei TANs(Transaktionsnummern) handelt es sich um Einmalpasswörter, mit denen im Online-Banking Transaktionen authentifiziert werden[584]. Durch Login-Daten oder PIN zusammen mit den TANs wird eine 2-Faktor-Authentifizierung umgesetzt. Konventionelle TAN-Verfahren haben das Problem, dass sie anfällig gegenüber MitM-Angriffen oder Phishing-Attacken auf Basis von Malware sind. Seit 2007 werden allerdings durch das mTAN- und eTAN+-Verfahren höhere Sicherheitsstandards im Bereich des Online-Banking gesetzt[585].

Beim eTAN+-Verfahren werden TANs durch ein Hardware-Token erstellt[586]. Das Token generiert dabei die TANs unter Einbeziehung bestimmter Daten(wie algorithmischer Schlüssel oder Uhrzeit) und anhand transaktionsabhängiger Daten(wie etwa der Kontonummer des Empfängers). Für die Eingabe der transaktionsabhängigen Daten verfügt das Token meist über eine Zifferntastatur, aber auch eine Übertragung der Daten zwischen PC und Token ist möglich. Dadurch, dass die TAN auch

582 http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Whitepaper.pdf (20.08.2012).
583 http://www.soeren-hentzschel.at/mozilla/firefox/2012/11/08/hsts-liste-schutzt-firefox-ab-version-17-vor-man-in-the-middle-attacken/ (20.08.2012).
584 https://netbanking.sparkasse.at/hilfe/sicherheit/TAN (22.08.2012).
585 https://www.it-sicherheit.de/ratgeber/it_sicherheitstipps/online_dienste_sicher_nutzen/online_banking/ (22.08.2012).
586 http://www.girokonto.info/ratgeber/etan-und-etan-plus/ (22.08.2012).

anhand der Eingabe der Empfängerkontonummer generiert wird und dass diese TAN sich nur auf diese eine Transaktion bezieht und nur für diese gültig ist, wird ein sehr hoher Schutz im Rahmen von Online-Banking garantiert[587]. Bislang ist noch kein Angriff bekannt, der, eine korrekte Ausführung des Verfahrens vorausgesetzt, die eTAN+-Prozeduren aushebeln konnte.

Ebenfalls erhöhte Sicherheit beim Online-Banking bot über diese Zeit das mTAN-Verfahren. Bei diesem Verfahren werden die TANs von der Bank per SMS an den Nutzer versendet[588]. Meldet sich der Nutzer beim Online-Banking an und veranlasst er eine Transaktion, so werden die Transaktionsdaten zunächst an die Bank gesendet. Die Bank sendet dann eine SMS an den Nutzer zurück, welche die zufällig generierte TAN und noch einmal die Transaktionsdaten, wie etwa Kontonummer des Empfängers und Betrag, enthält[589]. Der Nutzer hat durch diese SMS noch einmal die Möglichkeit, die Transaktionsdaten auf deren Korrektheit zu prüfen. Anschließend wird die Transaktion durch Eingabe der TAN authentifiziert. Bei diesem Verfahren wird durch das Mobiltelefon eine relativ sichere 2-Faktor-Authentifizierung gewährleistet. Dadurch, dass das Handy nicht direkt mit dem Rechner des Nutzers verbunden ist und dadurch, dass die Bank dem Kunden neben der TAN noch einmal die transaktionsspezifischen Daten schickt, wird im Normalfall erhöhte Sicherheit gewährleistet. Zusätzlich bezieht sich die TAN, wie auch beim eTAN+-Verfahren, nur auf eine einzige Transaktion und verliert danach ihre Gültigkeit. Beim mTAN-Verfahren ist lediglich zu bedenken, dass der Schutz sehr stark mit der Sicherheit des Mobiltelefons skaliert. Der Trend im Jahr 2012 geht dahin, dass Smartphones über eigene Betriebssysteme, eigenen Internetzugang und über immer mehr Funktionen verfügen. Dies erhöht die Wahrscheinlichkeit, dass das Smartphone Ziel von Malware-Angriffen wird. Darüber hinaus wird das eigene Smartphone immer öfter mit dem heimischen Rechner synchronisiert, was ebenfalls eine Vergrößerung der Angriffsfläche zur Folge hat. Bislang sind erfolgreiche Angriffe auf dieses Verfahren, dessen korrekte Ausführung vorausgesetzt, rar. Allerdings nehmen mit Herbst 2012 Berichte zu, nach denen das mTAN-Verfahren zunehmend unsicherer wird, hauptsächlich wegen speziell für Smartphones konzipierter Trojaner[590].

6.2.7 Sicherheit des DNS – DNSSEC

DNS-Cache-Poisoning stellt immer noch eine der größten Bedrohungen für das DNS dar. Der bereits in Kapitel 3.3.3 erläuterte Angriff von Kaminsky hat die Grenzen der herkömmlichen

587 http://www.girokonto.info/ratgeber/etan-und-etan-plus/ (22.08.2012).
588 http://blog.botfrei.de/2011/10/onlinebanking-das-mobile-tan-verfahren/ (22.08.2012).
589 http://blog.botfrei.de/2011/10/onlinebanking-das-mobile-tan-verfahren/ (22.08.2012).
590 http://www.berlin.de/polizei/presse-fahndung/archiv/377949/index.html (22.08.2012).

Sicherheitsmechanismen des DNS aufgezeigt. Die Domain Name System Security Extensions(kurz DNSSEC) bilden einen neuen Ansatz bezüglich der sicheren Authentifizierung von DNS-Nameservern. Bei DNSSEC handelt es sich um Sicherheitserweiterungen des DNS, mit denen die Authentizität und Integrität der Daten bei DNS-Transaktionen gewährleistet werden sollen[591]. Technisch realisiert wird dies durch eine PKI wie bei den elektronischen Signaturen. DNSSEC signiert DNS-Transaktionen mit einer digitalen Signatur, die zusammen mit den anderen Daten versendet wird. Diese digitale Signatur wird im Rahmen einer asymmetrischen Verschlüsselung durch einen privaten Schlüssel signiert und kann vom Empfänger durch einen öffentlichen Schlüssel entschlüsselt werden[592]. Dieses Schlüsselpaar nennt man auch Zonenschlüssel, da es für jede Zone des DNS, also von der Root-Domain über die Top Level Domain bis hin zur Domain, ein einzigartiges Schlüsselpaar gibt. Um den Kommunikationsaufwand zu verringern, wird eine sogenannte Chain of Trust gebildet. Dies bedeutet, dass im DNS-Baum hoch gelegene Zonen immer alle öffentlichen Schlüssel der ihnen unterstehenden Zonen besitzen, also zb die Root-Zone den öffentlichen Schlüssel der .de-Zone und diese wiederum den öffentlichen Schlüssel aller .de-Domains. Durch diese Chain of Trust brauchen die Resolver der DNS-Nameserver nur den öffentlichen Schlüssel der obersten Zone zu kennen, um die digitale Signatur einer DNS-Transaktion zu entschlüsseln[593]. Die restliche Funktionsweise gestaltet sich ähnlich wie jene der bereits in Kapitel 5.2.2 beschriebenen PKI. DNS-Transaktionen werden mit einer digitalen Signatur versehen, die mittels des privaten Zonenschlüssels vom Master-Server der jeweiligen Zone verschlüsselt wird[594]. Der DNS-Client kann dann mittels des öffentlich zugänglichen Zonenschlüssels die Signatur entschlüsseln und so sicherstellen, dass die Daten nicht verändert wurden und auch wirklich von dem gewünschten DNS-Server stammen. Mittlerweile wird DNSSEC bereits umfassend eingesetzt. Im Mai 2010 wurde DNSSEC auf allen Rootservern eingeführt[595], mit Dezember 2010 für .net und .com[596], mit Mai 2011 für die TLD .de[597] und mit Februar 2012 wurde es für die TLD .at umgesetzt[598]. Dies bedeutet allerdings lediglich, dass eine Authentifizierung durch DNSSEC technisch möglich ist; nicht, dass bereits jeder Endnutzer und jede Domain diese Möglichkeit nutzen. Laut einer Statistik der Internet Corporation for Assigned

591 http://www.itwissen.info/definition/lexikon/DNSSEC-domain-name-system-security-extension.html (24.08.2012).
592 http://www.itwissen.info/definition/lexikon/DNSSEC-domain-name-system-security-extension.html (24.08.2012).
593 http://www.verisigninc.com/de_DE/why-verisign/innovation-initiatives/dnssec/how-dnssec-works/index.xhtml (24.08.2012).
594 http://www.verisigninc.com/de_DE/why-verisign/innovation-initiatives/dnssec/how-dnssec-works/index.xhtml (24.08.2012).
595 http://www.heise.de/newsticker/meldung/DNSSEC-in-der-DNS-Rootzone-gestartet-1039401.html (24.08.2012).
596 http://www.heise.de/newsticker/meldung/Rascher-Start-von-DNSSEC-bei-net-und-com-1128745.html (24.08.2012).
597 http://www.denic.de/domains/dnssec.html (24.08.2012).
598 http://www.nic.at/service/technische_informationen/dnssec/ (24.08.2012).

Names and Numbers (ICANN) von November 2012 haben von 316 Top Level Domains aktuell 105, also etwa ein Drittel, DNSSEC-Signaturen[599]. 96 dieser TLDs haben ihren Schlüssel in der Rootzone hinterlegt. Obwohl also DNSSEC bereits seit einiger Zeit angeboten wird, wird es vermutlich noch eine Weile dauern, bis es bei allen Domains und beim Endnutzer angekommen ist. Selbstverständlich hat DNSSEC auch gewisse Schwächen[600]:

- Denial-of-Service-Angriffe können durch DNSSEC nicht verhindert werden.
- DNSSEC schützt zwar vor DNS-Cache-Poisoning, aber es kann nicht verhindern, dass ein Angreifer einen Nameserver übernimmt und diesen kompromittiert.
- Ähnlich wie bei allen PKIs stellt sich hier das Problem, dass die notwendige technische Infrastruktur zur Erstellung, Verifizierung und Verwaltung der Schlüssel sehr aufwändig ist.
- Wie auch bei anderen PKIs besteht die Möglichkeit, dass die für die Verwaltung und Erstellung der entsprechenden Schlüssel zuständigen Stellen selbst das Ziel von Angriffen werden.

Vor allem für Domains aus den Bereichen des Online-Banking oder Online-Versandhandhandels kann der gezielte Einsatz von DNSSEC durchaus sinnvoll sein, da gerade hier der Einsatz eines aufwändigen Angriffs wie DNS-Cache-Poisoning sehr effiziente Ergebnisse erzielen kann.

7 – Zusammenfassung

Die im Rahmen dieser Arbeit durchgeführte Recherche hat ergeben, dass das Problem Identitätsdiebstahl nur durch einen interdisziplinären Ansatz effizient bekämpft werden kann. Strafrechtliche Bestimmungen alleine sind, wie bereits das Beispiel USA sehr gut zeigt, nicht ausreichend, um die Zunahme von Identitätsdiebstahl und Identitätsmissbrauch langfristig einzudämmen, zumal sie erst dann ihre hauptsächliche Wirkung entfalten, wenn der Schaden bereits eingetreten ist. Schutzmechanismen gegen Identitätsdiebstahl sollten auf 3 Ebenen gesetzt werden, und zwar auf:

- technischer Ebene;
- rechtlicher Ebene;
- sozialer Ebene.

599 http://stats.research.icann.org/dns/tld_report/ (24.08.2012).
600 http://www.dvmag.de/dnssec/ (24.08.2012).

Dadurch, dass hinter Identitätsdiebstahl und Identitätsmissbrauch eine zunehmend organisierte und finanziell motivierte, kriminelle Industrie steht, ist es für Sicherheitsfirmen und Forscher äußerst schwierig, probate Gegenmittel zu präsentieren. Dennoch gibt es, wie in den letzten Kapiteln näher beschrieben, einige Schutzmechanismen, die, richtig eingesetzt dazu beitragen, das Risiko eines Identitätsdiebstahls oder Identitätsmissbrauchs im Internet zu verringern:

- 2-Faktor-Authentifizierung auf Basis von Hardware-Token oder Chipkartensystemen sollte vor allem für die Authentifizierung technischer Mitarbeiter von Unternehmen zur Anmeldung in Netzwerken oder bei wichtigen Diensten genützt werden. Da die hierfür notwendige Hardware meist teuer und die entsprechende Verwaltung relativ aufwändig ist, sollte vor allem der Zugang zu kritischen technischen Diensten innerhalb von Unternehmen auf diese Weise gesichert sein, da hier entsprechendes Fachwissen und eine entsprechende finanzielle Infrastruktur vorausgesetzt werden kann.
- 2-Faktor-Authentifizierung durch das Mobiltelefon sollte für den privaten Nutzer zur Anmeldung bei kritischen Seiten, die Identitätsdaten enthalten(zB. Social Networks) angeboten werden. Unternehmen wie Google oder Facebook sind diesbezüglich bereits auf einem guten Weg.
- Die elektronische Signatur kann, richtig eingesetzt, dabei helfen, konventionelle Angriffe wie Phishing oder Pharming zu verhindern. Leider ergibt sich bei der österreichischen Bürgerkarte das Problem, dass die Akzeptanz der Bevölkerung noch sehr niedrig ist.
- SSL-Zertifikate sollten im Internet flächendeckend für kritische Webseiten sowohl zur Authentifizierung von Servern als auch von Nutzern eingesetzt werden. Als kritische Webseiten gelten hierbei alle Seiten, bei denen durch Identitätsdiebstahl oder Identitätsmissbrauch ein Schaden verursacht werden könnte; besonders gefährdet sind Seiten aus den Bereichen des Online-Banking und Internethandels. Es sollte zusätzlich HSTS genutzt werden, um MitM-Angriffe zu unterbinden.
- Im Bereich des Online-Banking sollten ausschließlich sichere Verfahren wie eTAN+ oder mTAN verwendet werden; vor allem bei mTAN muss genau beobachtet werden, welche neuen Möglichkeiten sich für Angreifer durch die ständige Weiterentwicklung von Smartphones bieten.

Ferner sollten folgende Schwerpunkte gesetzt werden:

- DNSSEC sollte vor allem für besonders gefährdete Domains(wie etwa aus dem Bereich des Online-Banking) verpflichtend eingesetzt werden.

- Chipkartenlesegeräte einer geringeren Sicherheitsklasse als 3 bieten nur wenig Schutz und sollten daher nicht für entsprechende Authentifizierung angeboten werden.
- Bei Antivirensoftware sollten vor allem proaktive Verfahren, die auf Basis von Verhaltensanalysen oder Sandboxing arbeiten, stärker forciert werden, da reaktive Verfahren allein mit der rasanten Entwicklung neuer Malware nicht mehr mithalten können.
- Reputationsbasierte Schutzmechanismen stellen eine gute erste Verteidigungslinie für den Browser und das Betriebssystem dar; hier muss aber in Zukunft genau beobachtet und kontrolliert werden, welche Daten über den Nutzer gespeichert und verwaltet werden.
- Für den Browser sollten Sandboxing-Technologien wie jene von Google Chrome als Standard eingesetzt werden, da hier eine Reihe gefährlicher Angriffe unterbunden werden kann.
- Potentiell mächtige PlugIns wie JavaScript oder Flash sollten im Browser nach dem Whitelisting-Prinzip verwaltet werden. Dies bedeutet, dass diese nur für ausgewählte Webseiten aktiviert sind.

Wie bereits in den Kapiteln 5.5.1 und 5.5.2 erläutert wurde, ist jede technische Angriffsmethode, die für einen Identitätsdiebstahl oder Identitätsmissbrauch im Internet eingesetzt wird, nach dem Strafrecht der EU-Mitgliedstaaten sanktionierbar. Darüber hinaus erfüllt Identitätsmissbrauch in nahezu jedem EU-Mitgliedstaat den Straftatbestand des (schweren) Betruges. Rein rechtlich gesehen sind somit die meisten Sachverhalte tatbestandlich abgedeckt, wodurch sich die Frage stellt, ob ein gesonderter Straftatbestand für Identitätsdiebstahl und Identitätsmissbrauch (ähnlich wie in den USA in Kanada oder in Australien) überhaupt notwendig ist. Diese Frage lässt sich selbst nach der Untersuchung der strafrechtlichen Regelungen vieler Länder nur schwer beantworten. Grundsätzlich sind strafrechtliche Regelungen in erster Linie nicht präventiver Natur wie etwa technische Sicherheitsmaßnahmen. Sie greifen dann, wenn der Identitätsdiebstahl oder Identitätsmissbrauch bereits erfolgt ist und stellen somit das letzte Mittel zur Bekämpfung dieses Problems dar. Die in Kapitel 5.5 betrachteten Berichte der EU sehen in einem EU-weiten, einheitlichen Straftatbestand nur einen einzigen Vorteil: die Erleichterung einer grenzübergreifenden Strafverfolgung bei Identitätsdiebstahl innerhalb der EU. Ansonsten ergäbe sich, gemessen an den bereits existierenden gesetzlichen Regelungen der EU-Mitgliedstaaten, kein zusätzlicher Vorteil. Damit dieser Vorteil real zum Tragen käme, müsste ein solcher Straftatbestand durch eine entsprechende EU-Regelung geschaffen werden; ein gesetzlicher Alleingang einzelner EU-Mitgliedstaaten hätte nur wenig Sinn. Der Ansatz der USA zielt darauf ab, den Identitätsdiebstahl selbst durch einen zusätzlichen Straftatbestand stärker zu sanktionieren, um dem

besonderen Schädigungspotential(gemeint ist hierbei die psychosoziale Belastung des Opfers) dieses Vergehens Tribut zu zollen. Dabei handelt es sich allerdings um einen speziell auf das Rechtssystem der Vereinigten Staaten zugeschnittenen Ansatz, der dementsprechend von anderen Ländern nicht ohne Weiteres übernommen werden kann. Das Beispiel USA zeigt auch sehr gut, dass entsprechende strafrechtliche Bestimmungen alleine nur mäßig erfolgreich sind, wenn es keine klaren gesetzlichen Regelungen zum Umgang mit persönlichen Daten gibt. Von allen in dieser Arbeit untersuchten Ländern war keines schwerer von Identitätsdiebstahl und Identitätsmissbrauch betroffen als die USA. Nach dem in Kapitel 5.1 behandelten Bericht der Federal Trade Commission liegt dies unter anderem daran, dass es speziell in den USA für Angreifer extrem einfach ist, mit verhältnismäßig wenig Aufwand an personenbezogene Daten zu kommen. Um also rechtlich gegen Identitätsdiebstahl und Identitätsmissbrauch vorzugehen, ist mehr notwendig als nur strafrechtliche Regelungen allein. Empfehlenswert sind:

- ein wirklich umfassendes Datenschutzgesetz oder ähnliche rechtliche Bestimmungen, die detaillierte Regelungen für den Umgang mit persönlichen Daten enthalten -sowohl für private Unternehmen als auch staatliche Behörden;
- strafrechtliche Bestimmungen, welche technische Angriffsmethoden unter Strafe stellen.
- strafrechtliche Bestimmungen die Identitätsdiebstahl oder Identitätsmissbrauch mit Schädigungsabsicht sanktionieren.

Die Untersuchung diverser Rechtsvorschriften in Kapitel 5 hat ergeben, dass der bestmögliche rechtliche Schutz gegen Identitätsdiebstahl und Identitätsmissbrauch in jenen Staaten geboten wird, die über die hier vorgeschlagenen rechtlichen Bestimmungen verfügen. Staaten wie die USA, die immer noch kein umfassendes Datenschutzgesetz besitzen, oder Staaten wie Großbritannien, die lange Zeit nicht einmal einen eigenen Straftatbestand für Betrug hatten, hatten entsprechend mehr Probleme mit Identitätsdiebstahl und Identitätsmissbrauch. Dagegen kann der durch das Recht gebotene Schutz vor diesem Problem in Kanada und in diversen EU-Mitgliedstaaten wie Österreich oder Deutschland als verhältnismäßig gut angesehen werden. Hier sind weniger die rechtlichen Bestimmungen das Problem als vielmehr die Naivität und Sorglosigkeit der Opfer. Es wäre zu erwägen, rechtliche Sorgfaltspflichten für den Verkehr von Privatpersonen im Internet zu schaffen. Es gibt zwar bereits diverse Quellen, die verständliche Best-Practice-Guidelines für den Internetverkehr enthalten, aber durch das Recht könnte hier eine gewisse Gebotswirkung erzielt werden. Speziell für Online-Banking oder Internethandel wäre eine rechtlich verpflichtende Aufklärung empfehlenswert, die über informative E-Mails oder Warnhinweise auf der Webseite oder beim Login hinausgehen. Dies ist allerdings relativ schwierig zu realisieren. In Zukunft muss vor allem untersucht werden, ob das Strafrecht im Hinblick auf Identitätsdiebstahl oder

Identitätsmissbrauch bei sozialen Netzwerken adaptiert werden muss. Identitätsdiebstahl und Identitätsmissbrauch ohne finanziellen Schaden ist aktuell nach dem Strafrecht aller EU-Mitgliedstaaten nicht gerichtlich strafbar. Werden bei sozialen Netzwerken Daten (wie etwa der Name einer Person) für falsche Accounts benutzt, so kann dies zwar einen Verstoß gegen das Datenschutzrecht darstellen oder zivilrechtlich verfolgbar sein; es wird freilich in den meisten Fällen, falls keine Straftat vorliegt, durch soziale Netzwerke wie Facebook einem entsprechenden Ansuchen bezüglich einer Preisgabe der Daten des Täters nicht nachgekommen. Diese Form des Identitätsmissbrauchs kann dem Ansehen und dem Ruf des Opfers mitunter beträchtlichen Schaden zufügen, auch Stalking wird auf diese Weise erleichtert. Hier muss untersucht werden, ob eine Ausweitung des Strafrechts auf diese Form des Identitätsdiebstahls und Identitätsmissbrauchs sinnvoll wäre. In Zukunft wird es auch immer wichtiger, die virtuelle Identität einer Person zu schützen. Accounts bei diversen Webseiten, die mit dem Nutzer in Verbindung gebracht werden können, Accounts in Online-Diskussionsforen, „Nicknames“ in Gästebüchern oder Accounts bei Videoportalen wie Youtube können als eine Art virtuelle Identität betrachtet werden. Da sie aber nicht durch das Persönlichkeitsrecht geschützt werden, kann auch hier Identitätsdiebstahl praktisch ungestraft erfolgen. Das Strafrecht hat freilich das Problem, dass es nur schwer mit der Geschwindigkeit der technischen Entwicklung mithalten kann. Daher sollte es auch als letztes Glied in der Kette zur Bekämpfung von Identitätsdiebstahl und Identitätsmissbrauch gesehen werden.

Zuletzt ist eine Bekämpfung des Problems mit sozialen Maßnahmen empfehlenswert. „*The human factor is truly security`s weakest link.*“[601]. Mit diesen Worten erklärt Kevin Mitnick in seinem Buch „The Art of Deception“(„Die Kunst der Täuschung“) kurz und knapp, wer das schwächste Glied in der Kette der IT-Sicherheit ist. Die technisch hochwertigsten Schutzmechanismen sind wirkungslos, wenn der am Computer sitzende Mensch auf einfache Täuschungen hineinfällt. Speziell die in Kapitel 4 näher untersuchten Social Engineering-Angriffe können nicht nur durch technische Schutzmechanismen gestoppt werden, da sie auf den Menschen hinter dem Rechner abzielen. Neben technischen und rechtlichen Maßnahmen sind also auch soziale Vorbeugungsmaßnahmen notwendig, um drohenden Identitätsdiebstahl oder Identitätsmissbrauch zu verhindern oder um zumindest den Schaden gering zu halten. Als solche soziale Vorbeugungsmaßnahmen sind alle Maßnahmen zu verstehen, die der Information und Aufklärung sowohl der Nutzer als auch der technischen Fachkräfte oder Bediensteten der Justiz dienen. Beim Nutzer muss sichergestellt werden, dass dieser über gängige Angriffsmethoden im Internet, die Identitätsdiebstahl oder Identitätsmissbrauch zur Folge haben können, informiert wird. Diese Information muss dabei auf einem Weg bereitgestellt werden, durch den gewährleistet werden kann, dass der Nutzer die

601 Kevin Mitnick – The Art of Deception, Seite 16

Information auch sicher erhält und versteht. Diverse Informationsseiten im Internet(wie beispielsweise jene des deutschen BSI) sind zwar hilfreich, aber es kann nicht gesichert werden, dass jeder Nutzer diese Informationen auch liest. Wichtig ist hier eventuell doch eine klare Rechtsvorschrift, um die Anbieter in kritischen Bereichen(wie Online-Banking oder Internethandel) dazu zu verpflichten, Nutzer/innen entsprechend aufzuklären. Speziell im Online-Banking und im Internethandel versuchen Anbieter ihren Kunden eine immer einfachere und bequemere Bedienbarkeit der notwendigen Infrastruktur zu bieten, wodurch der Kunde, oft mit nur sehr geringem technischen Wissen, sehr viel Verantwortung besitzt. Es besteht also Handlungsbedarf im Hinblick auf die Informationspflicht der Anbieter von potentiell gefährdeten Diensten. Darunter fallen nicht nur die Anbieter von Online-Banking, sondern auch die Hersteller von diversen IT-Produkten(wie etwa Chipkartenlesegeräten oder Antivirensoftware). Es sollte unbedingt größte Anstrengung unternommen werden, um zu erreichen, dass Nutzer/innen grundlegende Gefahren des Internets kennen und dass sie zumindest die heimische technische Umgebung konfigurieren und verwalten können. Auch Bedienstete privater Unternehmen und staatlicher Behörden, die persönliche Daten verwalten, müssen erheblich stärker aufgeklärt werden. Dafür wären professionelle Schulungen und Workshops gut geeignet. Bei Schulungen muss auf folgende Kriterien geachtet werden:

- Das Niveau der Schulung muss dem Wissensstand und der Position des Bediensteten im Unternehmen angemessen sein. Technische Fachkräfte benötigen weit spezifischere Informationen als andere Mitarbeiter.
- Schulungen müssen in zeitlich regelmäßigen Abständen erfolgen, damit sichergestellt werden kann, dass die Mitarbeiter/innen auf einem verhältnismäßig aktuellen Wissensstand sind.

Auch Mitarbeiter der Justiz, wie Richter und Staatsanwälte, oder Mitarbeiter der für IT-Kriminalität zuständigen Strafverfolgungsbehörden sollten an solchen Schulungen teilnehmen. Richter und Staatsanwälte benötigen zwar nicht zwingend profundes technisches Wissen; speziell die Fähigkeit dabei, technische Beweismittel(wie etwa E-Mails oder Logfiles) richtig einzuschätzen, ist von großer Wichtigkeit. Speziell bei Haftungsfragen sollten zuständige Richter/innen grundlegendes Wissen über die eingesetzten Technologien und Angriffsmethoden verfügen. Als unverzichtbar anzusehen sind nach den Ergebnissen dieser Arbeit zentrale Anlaufstellen für die Opfer von Identitätsdiebstahl und Identitätsmissbrauch. Die Webseite der Federal Trade Commission in den USA und die in England gebotene Webseite für Opfer von Identitätsdiebstahl sind in diesem Zusammenhang als vorbildlich zu nennen. Obwohl der in Kapitel 5.5 behandelte Bericht der FPEG eine zentrale Anlaufstelle für die Opfer von Identitätsdiebstahl und Identitätsmissbrauch in Europa

vorschlägt, ist dieser Plan bislang noch nicht umgesetzt worden. Eine solche Anlaufstelle wäre aber aus zwei Gründen notwendig:

- Opfer von Identitätsdiebstahl sind meistens mit der Einschätzung des eingehenden Schadens überfordert und tendieren dazu, diesen nicht einmal zu melden. Darüber hinaus wissen rechtlich nur durchschnittlich versierte Opfer meistens nicht, welche juristischen Schritte zu tätigen sind und ob sie selbst oder Dritte für den entstandenen Schaden haften. Eine zentrale Anlaufstelle im Internet, auf der sämtliche Informationen vorhanden sind, wie bei Identitätsdiebstahl vorzugehen ist, wäre hier enorm hilfreich. Es wäre einfach eine verständliche Anleitung zu bieten, wie und bei wem das Opfer Anzeige erstatten kann, welche Schritte im Hinblick auf den Vorfall sonst zu tätigen sind und was getan werden sollte, um etwaige Folgeschäden zu verhindern.
- Eine solche Anlaufstelle könnte auch, ähnlich wie die FTC in den USA, gleichzeitig wichtige Informationen zur Prävention von Identitätsdiebstahl bereitstellen.

8 Abbildungsverzeichnis

9 Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik: Bericht zur Lage der IT-Sicherheit in Deutschland 2011, S. 13. Abgerufen am 23.02.2012 von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph: Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 11, Springer-Verlag Berlin Heidelberg, 2011

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph:

Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 11, Springer-Verlag Berlin Heidelberg, 2011

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph:

Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 9, Springer-Verlag Berlin Heidelberg, 2011

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph:

Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 9, Springer-Verlag Berlin Heidelberg, 2011

Jason Jones: State of Web Exploit Kits. Abgerufen am 12.03.2012 von:

http://media.blackhat.com/bh-us 12/Briefings/Jones/BH_US_12_Jones_State_Web_Exploits_WP.pdf

Paulsen, Christian: Sicherheit in vernetzten Systemen: 16. DFN Workshop, S. H-3, Books on Demand Verlag Norderstedt, 2009

HP DVLabs: 2010 Full Year Top Cyber Security Risks Report, S. 23. Abgerufen am 12.03.2012 von:

http://dvlabs.tippingpoint.com/img/FullYear2010%20Risk%20Report.pdf

Mertinkat, Moritz: Von Postbank bis PayPal – Phishing im Internet, S. 3, Universität Freiburg

Bundesamt für Sicherheit in der Informationstechnik: Bericht zur Lage der IT-Sicherheit in Deutschland 2011, S. 14. Abgerufen am 23.02.2012 von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

Anti-Phishing Working Group: Global Phishing Survey: Trends and Domain Name Use in 1H2012, S. 8, Oktober 2012. Abgerufen am 17.03.2012 von:

http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2012.pdf

Anti-Phishing Working Group: Phishing Activity Trends Report 1st Quarter 2010, S. 7, Jänner bis März 2010. Abgerufen am 17.03.2012 von :

http://docs.apwg.org/reports/apwg_report_Q1_2010.pdf

Anti-Phishing Working Group: Phishing Activity Trends Report 4th Quarter 2012, S. 7, Oktober bis Dezember 2012. Abgerufen am 20.12.2012 von :

http://docs.apwg.org/reports/apwg_trends_report_Q4_2012.pdf

Anti-Phishing Working Group: Phishing Activity Trends Report 2nd Quarter 2012, April bis Juni 2012. Abgerufen am 07.09.2012 von:

http://docs.apwg.org/reports/apwg_trends_report_q2_2012.pdf

Kriha, Walter; Schmitz, Roland: Sichere Systeme: Konzepte, Architekturen und Frameworks, S. 19, Springer-Verlag Berlin Heidelberg, 2009

Global Evolution Security: Cross-Site-Scripting: Dokumentation, Analyse & Techniken. Abgerufen am 24.03.2012 von :

http://www.exploit-db.com/wp-content/themes/exploit/docs/10342.pdf

White Hat Security: White Hat Security Website Statistics Report, 2012. Abgerufen am 24.03.2012 von :

https://www.whitehatsec.com/assets/WPstats_summer12_12th.pdf

Jorgen Hole, Kjell: Pharming, S. 9, Universität von Bergen, 2012. Abgerufen am 28.03.2012 von:

http://www.kjhole.com/WebSec/PDF/Pharming.pdf

Holtkamp, Heiko: Einführung in TCP/IP, S. 17, Universität Bielefeld, 2002. Abgerufen am 04.04.2012 von :

http://www.rvs.uni-bielefeld.de/~heiko/tcpip/tcpip.pdf

Holtkamp, Heiko: Einführung in TCP/IP, S. 34, Universität Bielefeld, 2002. Abgerufen am 08.04.2012 von :

http://www.rvs.uni-bielefeld.de/~heiko/tcpip/tcpip.pdf

Werner, Tillmann; Reusch, Edwin: Sondervorlesung „Netz-Sicherheit“: Botnetze - eine technische Einführung, S. 5, Universität Bonn, Juni 2006. Abgerufen am 17.04.2012 von:

http://net.cs.uni-bonn.de/fileadmin/events/Special/BSI/2006-06-29_Sondervorlesung_Netzsicherheit_publication.pdf

Rashid Linta, Shamid; Khan, Ridgewan: Todays Impact on Communication System by IP Spoofing and its Detection and Prevention, S. 30, Grin Verlag.

Werner, Tillmann; Reusch, Edwin: Sondervorlesung „Netz-Sicherheit“: Botnetze - eine technische Einführung, S. 9, Universität Bonn, Juni 2006. Abgerufen am 17.04.2012 von:

http://net.cs.uni-bonn.de/fileadmin/events/Special/BSI/2006-06-29_Sondervorlesung_Netzsicherheit_publication.pdf

Wright, Joshua: Detecting Wireless LAN MAC Address Spoofing, S. 2, Jänner 2003. Abgerufen am 18.04.2012 von:

http://www.rootsecure.net/content/downloads/pdf/wlan_macspooof_detection.pdf

Limmer, Tobias; Gründl, Martin; Schneider, Thomas: Netzwerksicherheit – ARP-Spoofing, S. 14, Dezember 2007. Abgerufen am 21.04.2012 von :

http://www.ccs-labs.org/~dressler/teaching/netzwerksicherheit-ws0708/uebung07.pdf

Whalen, Sean: An Introduction to ARP Spoofing, S. 3, April 2001. Abgerufen am 21.04.2012 von :

http://rootsecure.net/content/downloads/pdf/arp_spoofing_intro.pdf

Blazytko, Tim: Lokale und LAN-interne Angriffsszenarien auf Microsoft Windows NT 5.0-, 5.1- und 5.2-Systeme, S. 16, Juni 2008. Abgerufen am 21.04.2012 von:

http://ia700508.us.archive.org/21/items/Lokale-UndLan-interneAngriffsszenarienAufMicrosoftWindowsNt5.0-5.1-/Lokale_und_LAN-interne_Angriffe_auf_Windows_NT_5-Systeme.pdf

Clarke, Justin: SQL Injection Attacks and Defense, S. 2, Elsevier Verlag USA, 2012

Burns, Jesse: Cross Site Reference Forgery: An introduction to a common web application weakness, S. 2, 2005. Abgerufen am 03.05.2012 von :

http://dl.packetstormsecurity.net/papers/web/XSRF_Paper.pdf

Provos, Niels; McNamee, Dean; Mavrommatis, Panayiotis; Wang, Ke; Modadugu, Nagendra: The Ghost in The Browser: Analysis of Web-based Malware, S. 5. Abgerufen am 06.05.2012 von : https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/provos/provos.pdf

Symantec: Internet Security Threat Report 2011, S. 12-13. Abgerufen am 06.05.2012 von: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Sophos: Security Threat Report 2012, S. 10. Abgerufen am 06.05.2012 von: http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

Kaspersky Lab: Malware Report Q1 2011, S. 20, Mai 2011. Abgerufen am 08.05.2012 von : http://www.kaspersky.com/downloads/pdf/kaspersky_lab_q1_malware_2011_report.pdf

PandaLabs: Quarterly Report January-March 2012, S. 14. Abgerufen am 08.05.2012 von: http://press.pandasecurity.com/wp-content/uploads/2012/05/Quarterly-Report-PandaLabs-January-March-2012.pdf

United States Sentencing Commission: Identity Theft – Final Report, S. 3, Dezember 1999. Abgerufen am 11.05.2012 von: http://www.ussc.gov/sites/default/files/pdf/research-and-publications/working-group-reports/intellectual-property-and-tech/19991215-identity-theft/identexs.pdf

United States Sentencing Commission: Identity Theft – Final Report, S. 2, Dezember 1999. Abgerufen am 11.05.2012 von: http://www.ussc.gov/sites/default/files/pdf/research-and-publications/working-group-reports/intellectual-property-and-tech/19991215-identity-theft/identexs.pdf

United States Sentencing Commission: Identity Theft – Final Report, S. 1, Dezember 1999. Abgerufen am 11.05.2012 von: http://www.ussc.gov/sites/default/files/pdf/research-and-publications/working-group-reports/intellectual-property-and-tech/19991215-identity-theft/identexs.pdf

Kongress der vereinigten Staaten: Identity Theft Enforcement and Restitution Act of 2008. Abgerufen am 12.05.2012 von : http://www.gpo.gov/fdsys/pkg/BILLS-110hr5938enr/pdf/BILLS-110hr5938enr.pdf

Kongress der vereinigten Staaten: Public Law 108-275, 118 STAT. 831, 15.06.2004. Abgerufen am 12.05.2012 von:

http://www.gpo.gov/fdsys/pkg/PLAW-108publ275/pdf/PLAW-108publ275.pdf

The Presidents Identity Theft Task Force: Combating Identity Theft: A Strategic Plan, April 2007. Abgerufen am 12.05.2012 von:

http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/downloadabledocuments/combating_identity_theft_a_strategic_plan.pdf

The Presidents Identity Theft Task Force: Task Force Report, September 2008. Abgerufen am 12.05.2012 von:

http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf

The Presidents Identity Theft Task Force: Task Force Report, September 2008. Abgerufen am 14.05.2012 von:

http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf

Federal Trade Commission, Synovate: 2006 Identity Theft Survey Report, S. 3, November 2007. Abgerufen am 14.05.2012 von:

http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf

Federal Trade Commission, Synovate: 2006 Identity Theft Survey Report, S. 3, November 2007. Abgerufen am 14.05.2012 von:

http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate/synovatereport.pdf

U.S. Department of Justice – Office of Justice Programs: Bureau of Justice Statistics Special Report: Victims of Identity Theft, 2008. Abgerufen am 14.05.2012 von:

http://www.bjs.gov/content/pub/pdf/vit08.pdf

U.S. Department of Justice – Office of Justice Programs: Bureau of Justice Statistics Special Report: Victims of Identity Theft, 2008, S. 1. Abgerufen am 14.05.2012 von:

http://www.bjs.gov/content/pub/pdf/vit08.pdf

U.S. Department of Justice – Office of Justice Programs: Bureau of Justice Statistics Crime Data Brief: Identity Theft Reported by Households, 2005-2010, S. 1, November 2011. Abgerufen am 14.05.2012 von:

http://www.bjs.gov/content/pub/pdf/itrh0510.pdf

Federal Trade Commission: Consumer Sentinel Network Data Book for January – December 2009, Februar 2010, S. 4. Abgerufen am 14.05.2012 von:

http://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2009/sentinel-cy2009.pdf

Federal Trade Commission: Consumer Sentinel Network Data Book for January – December 2009, Februar 2010, S. 12. Abgerufen am 14.05.2012 von:

http://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2009/sentinel-cy2009.pdf

The Presidents Identity Theft Task Force: Task Force Report, September 2008, S. 37. Abgerufen am 14.05.2012 von:

http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf

The Presidents Identity Theft Task Force: Task Force Report, September 2008, S. 37. Abgerufen am 14.05.2012 von:

http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf

Canadian Internet Policy and Public Interest Clinic: CIPPIC Working Paper No. 3 (ID Theft Series): Legislative Approaches to Identity Theft, März 2007, S. 3. Abgerufen am 20.05.2012 von:

https://www.cippic.ca/sites/default/files/IDT_No.3-Legislation.pdf

Canadian Internet Policy and Public Interest Clinic: CIPPIC Working Paper No. 5 (ID Theft Series): Enforcement of Identity Theft Laws, Juli 2007, S. 1. Abgerufen am 21.05.2012 von:

https://www.cippic.ca/sites/default/files/LawEnforcement.pdf

Canadian Internet Policy and Public Interest Clinic: CIPPIC Working Paper No. 5 (ID Theft Series): Enforcement of Identity Theft Laws, Juli 2007, S. 2. Abgerufen am 21.05.2012 von:

https://www.cippic.ca/sites/default/files/LawEnforcement.pdf

Australian Government ComLaw: Criminal Code Act 1995. Abgerufen am 28.05.2012 von:

http://www.comlaw.gov.au/Details/C2012C00451

Australian Government, National Office for the Information Economy, Australian Communications Authority: Spam Act 2003. Abgerufen am 28.05.2012 von:

http://www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf

The Parlament of South Australia: Criminal Law Consolidation (Identity Theft) Amendment Act 2003, Dezember 2003. Abgerufen am 28.05.2012 von:

http://www.legislation.sa.gov.au/LZ/V/A/2003/CRIMINAL%20LAW%20CONSOLIDATION%20%28IDENTITY%20THEFT%29%20AMENDMENT%20ACT%202003_60/2003.60.UN.PDF

The Parlament of South Australia: Criminal Law Consolidation (Identity Theft) Amendment Act 2003, Dezember 2003. Abgerufen am 28.05.2012 von:

http://www.legislation.sa.gov.au/LZ/V/A/2003/CRIMINAL%20LAW%20CONSOLIDATION%20%28IDENTITY%20THEFT%29%20AMENDMENT%20ACT%202003_60/2003.60.UN.PDF

Model Criminal Law Officers Committee of the Standing Committee of Attorneys-General: Identity Crime Discussion Paper: Chapter 3, April 2007, S. 8. Abgerufen am 28.05.2012 von:

http://www.sclj.gov.au/agdbasev7wr/sclj/documents/pdf/mcloc_mcc_chapter_3_identity_crime_discussion_paper_pdf.pdf

Model Criminal Law Officers Committee of the Standing Committee of Attorneys-General: Identity Crime Discussion Paper: Chapter 3, April 2007. Abgerufen am 28.05.2012 von:

http://www.sclj.gov.au/agdbasev7wr/sclj/documents/pdf/mcloc_mcc_chapter_3_identity_crime_discussion_paper_pdf.pdf

Model Criminal Law Officers Committee of the Standing Committee of Attorneys-General: Identity Crime Final Report, März 2008, S. 25. Abgerufen am 28.05.2012 von:

http://www.sclj.gov.au/agdbasev7wr/sclj/documents/pdf/identity_crime_final_report_march_2008.pdf

The Parlament of Victoria, Australia: Crimes Amendment (Identity Crime) Act 2009, Juni 2009. Abgerufen am 28.05.2012 von:

http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubStatbook.nsf/f932b66241ecf1b7ca256e92000e23be/C32B10510FEF8F9ACA2575D8001ECE97/$FILE/09-22a.pdf

Executive Meeting of East Asia-Pacific Central Banks: Payment Systems in EMEAP Economies: Payment Systems in Korea, Juli 2002. Abgerufen am 02.06.2012 von:

https://www.bis.org/cpss/paysys/Korea.pdf

Commission of the European Communities: Commission Staff Working Document: Report on Fraud regarding non cash means of payments in the EU: the implementation of the 2004-2007 EU action plan, April 2008. Abgerufen am 03.06.2012 von:

http://ec.europa.eu/internal_market/payments/docs/fraud/implementation_report_en.pdf

Europol: OCTA – EU Organized Crime Threat Assessment 2007, Juni 2007, S. 17. Abgerufen am 03.06.2012 von:

https://www.europol.europa.eu/sites/default/files/publications/octa2007.pdf

European Commission, Internal Market and Services DG: 11th Meeting of the Fraud Prevention Expert Group 28.November 2006, Dezember 2006. Abgerufen am 03.06.2012 von:

http://ec.europa.eu/internal_market/fpeg/docs/minutes_20061128.pdf

Kommission der europäischen Gemeinschaften: Mitteilung der Kommission an das europäische Parlament, den Rat und den Ausschuss der Regionen – Eine allgemeine Politik zur Bekämpfung der Internetkriminalität, Mai 2007. Abgerufen am 03.06.2012 von:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:DE:PDF

Kommission der europäischen Gemeinschaften: Mitteilung der Kommission an das europäische Parlament, den Rat und den Ausschuss der Regionen – Eine allgemeine Politik zur Bekämpfung der Internetkriminalität, Mai 2007. Abgerufen am 03.06.2012 von:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:DE:PDF

European Commission, Internal Market and Services DG: Fraud Prevention Expert Group – Report on Identity Theft/Fraud, Oktober 2007. Abgerufen am 03.06.2012 von:

http://ec.europa.eu/internal_market/fpeg/docs/id-theft-report_en.pdf

Europäisches Parlament, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres: Entwurf einer legislativen Entschliessung des europäischen Parlaments zu dem Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, November 2011. Abgerufen am 04.06.2012 von:

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/884/884601/884601de.pdf

Europäisches Parlament, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres: Entwurf einer legislativen Entschliessung des europäischen Parlaments zu dem Vorschlag für eine Richtlinie des europäischen Parlaments und des Rates über Angriffe auf Informationssysteme und zur Aufhebung des Rahmenbeschlusses 2005/222/JI des Rates, November 2011. Abgerufen am 04.06.2012 von:

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/884/884601/884601de.pdf

Reindl-Krauskopf, Susanne: Computerstrafrecht im Überblick, 2., überarbeitete Auflage, S. 33, Facultas Verlag 2009

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph:

Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 359, Springer-Verlag Berlin Heidelberg, 2011

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph:

Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 377, Springer-Verlag Berlin Heidelberg, 2011

Bundesamt für Sicherheit in der Informationstechnik: Bericht zur Lage der IT-Sicherheit in Deutschland 2011. Abgerufen am 08.06.2012 von:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011_nbf.pdf?__blob=publicationFile

Cointre, Ludovic; Leroy, Fabienne; Pycke, Anthony; Rauline, Pascale: Identity Theft – A Potential Market?, 2010. Abgerufen am 09.06.2012 von:

http://www.enass.fr/PDF/travaux_recherche/Identity_theft_presentation.pdf

The Law Commission, LAW COM No 276, United Kingdom: Fraud – Report on a reference under section 3(1)(e) of the Law Commissions Act 1965, Juli 2002. Abgerufen am 12.06.2012 von:

http://lawcommission.justice.gov.uk/docs/lc276_Fraud.pdf

Ministry of Justice, United Kingdom: Post-legislative assessment of the Fraud Act 2006, Memorandum to the Justice Select Committee, Juni 2012. Abgerufen am 12.06.2012 von:

http://www.justice.gov.uk/downloads/publications/corporate-reports/MoJ/2012/post-legislative-assessment-fraud-act-2006.pdf

Parlament des vereinigten Königreichs: Fraud Act 2006, Chapter 35, November 2006. Abgerufen am 12.06.2012 von:

http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf

Parlament des vereinigten Königreichs: Fraud Act 2006, Chapter 35, November 2006. Abgerufen am 12.06.2012 von:

http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf

Parlament des vereinigten Königreichs: Fraud Act 2006, Chapter 35, November 2006. Abgerufen am 12.06.2012 von:

http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf

Parlament des vereinigten Königreichs: Fraud Act 2006, Chapter 35, November 2006. Abgerufen am 12.06.2012 von:

http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf

Parlament des vereinigten Königreichs: Identity Cards Act 2006, Chapter 15, März 2006. Abgerufen am 12.06.2012 von:

http://www.legislation.gov.uk/ukpga/2006/15/pdfs/ukpga_20060015_en.pdf

Sophos: Security Threat Report 2012, S. 6. Abgerufen am 02.07.2012 von:

http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf

Langweg, Hanno; Schwenk, Jörg: Schutz von FinTS/HBCI-Clients gegenüber Malware, Juni 2007. Abgerufen am 14.07.2012 von:

http://www.hanno-langweg.de/hanno/research/dach07p.pdf

Langweg, Hanno; Schwenk, Jörg: Schutz von FinTS/HBCI-Clients gegenüber Malware, Juni 2007. Abgerufen am 14.07.2012 von:

http://www.hanno-langweg.de/hanno/research/dach07p.pdf

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph: Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 360, Springer-Verlag Berlin Heidelberg, 2011

Statistik Austria: IKT-Einsatz in Haushalten 2012, S. 26. Abgerufen am 22.07.2012 von:http://www.statistik.at/web_de/dynamic/services/publikationen/17/publdetail?id=17&listid=17&detail=559

Borges, Georg; Schwenk, Jörg; Stuckenberg, Carl-Friedrich; Wegener, Christoph: Identitätsdiebstahl und Identitätsmissbrauch im Internet, S. 363, Springer-Verlag Berlin Heidelberg, 2011

Symantec: Internet Security Threat Report 2011, S. 44. Abgerufen am 04.08.2012 von:

http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 16. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 16. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 16. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 17. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 17. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 17. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 19. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 19-21. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 24-33. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

Fraunhofer-Institut für sichere Informationstechnik: SIT Technical Reports - Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern, März 2012, S. 32. Abgerufen am 04.08.2012 von:

https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf

NSS Labs: Browser Security Comparative Analysis, 2012, S. 2. Abgerufen am 04.08.2012 von:

https://www.nsslabs.com/reports/browser-security-comparative-analysis-report-socially-engineered-malware

NSS Labs: Browser Security Comparative Analysis, 2012, S. 5-7. Abgerufen am 04.08.2012 von:

https://www.nsslabs.com/reports/browser-security-comparative-analysis-report-socially-engineered-malware

SecureNet: Web Application Security Untersuchung - Aktuelle Verbreitung von HTTP Strict Transport Security (HSTS), November 2012, S. 3. Abgerufen am 20.08.2012 von:

http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Verbreitung.pdf

SecureNet: Web Application Security Untersuchung - Aktuelle Verbreitung von HTTP Strict Transport Security (HSTS), November 2012, S. 5-7. Abgerufen am 20.08.2012 von:

http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Verbreitung.pdf

SecureNet: Web Application Security Untersuchung - Aktuelle Verbreitung von HTTP Strict Transport Security (HSTS), November 2012, S. 7. Abgerufen am 20.08.2012 von:

http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Verbreitung.pdf

SecureNet: Whitepaper – HTTP Strict Transport Security (HSTS), November 2012. Abgerufen am 20.08.2012 von:

http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Whitepaper.pdf

SecureNet: Whitepaper – HTTP Strict Transport Security (HSTS), November 2012. Abgerufen am 20.08.2012 von:

http://www.securenet.de/fileadmin/papers/HTTP_Strict_Transport_Security_HSTS_Whitepaper.pdf

Mitnick, Kevin: The Art of Deception, S. 16, Wiley Verlag, 2002

10 Online-Quellen

http://derstandard.at/1291455064176/70-Prozent-der-EU-Haushalte-haben-Zugang-zum-Internet (11.01.2012)

http://www.statistik.at/web_de/statistiken/informationsgesellschaft/ikt-einsatz_in_haushalten/index.html (17.01.2012)

http://ods3.schule.de/aseminar/entwicklung/identkrise.htm (23.01.2012)

http://www.praxisphilosophie.de/mead.htm (30.01.2012)

http://www.uni-muenster.de/Leibniz/seite2.html (30.01.2012)

https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326 (08.02.2012)

http://www.gesetze-im-internet.de/beurkg/__40.html (08.02. 2012)

http://dejure.org/gesetze/GwG/3.html (08.02.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827 (09.02.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827 (09.02.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827 (09.02.2012)

http://www.gesetze-im-internet.de/markeng/__14.html (10.02.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10004827 (10.02.2012)

http://www.domainrecht-aktuell.de/domainrecht_einleitung.htm (10.02.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (14.02.2012)

http://www.gesetze-im-internet.de/bdsg_1990/__3.html (18.02.2012)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT (18.02.2012)

http://www.itwissen.info/definition/lexikon/Internet-relay-chat-IRC.html (21.02.2012)

http://www.itwissen.info/definition/lexikon/I-seek-you-ICQ.html (21.02.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=Bundesnormen&Gesetzesnummer=10002296 (21.02.2012)

http://szenesprachenwiki.de/definition/identit%C3%A4tsdiebstahl/ (22.02.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=Bundesnormen&Gesetzesnummer=10002296 (23.02.2012)

http://www.rechteinfach.at/rechtslexikon/rufschaedigung-83.html (23.02.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=Bundesnormen&Gesetzesnummer=10001622 (23.02.2012)

http://www.boersennews.de/lexikon/begriff/identitaetsdiebstahl/562 (24.02.2012)

http://en.wikipedia.org/wiki/Identity_theft (24.02.2012)

http://www.ftc.gov/os/statutes/itada/itadact.htm#003 (01.03.2012)

http://en.wikipedia.org/wiki/Identity_fraud (01.03.2012)

http://www.voip-office.com/voip-sicherheit/identitaetsmissbrauch (03.03.2012)

http://dejure.org/gesetze/StGB/269.html (03.03.2012)

https://www.a-i3.org/content/view/1119/230/ (03.03.2012)

http://www.itwissen.info/definition/lexikon/Virus-virus.html (06.03.2012)

http://www.itwissen.info/definition/lexikon/Wurm-worm.html (06.03.2012)

http://www.itwissen.info/definition/lexikon/Trojaner-trojan.html (06.03.2012)

http://www.produktion.de/it-security-schwachstellen/ (07.03.2012)

http://www.itwissen.info/definition/lexikon/basic-input-output-system-BIOS-Einfaches-Eingabe-Ausgabe-System.html (12.03.2012)

http://de.norton.com/cybercrime-crimeware (12.03.2012)

http://blog.zeltser.com/post/1410922437/what-are-exploit-kits (12.03.2012)

http://www.pcwelt.de/news/Exploit-Toolkits-Die-Evolution-der-Angriffsbaukaesten-im-Web-1444073.html (12.03.2012)

http://www.pcwelt.de/news/Exploit-Toolkits-Die-Evolution-der-Angriffsbaukaesten-im-Web-1444073.html (12.03.2012)

http://searchengineland.com/guide/what-is-seo (12.03.2012)

http://www.itwissen.info/definition/lexikon/IFrame-inline-frame.html (12.03.2012)

http://privacy-pc.com/articles/the-state-of-web-exploit-toolkits-3-how-blackhole-works.html (12.03.2012)

http://privacy-pc.com/articles/the-state-of-web-exploit-toolkits-3-how-blackhole-works.html (12.03.2012)

http://searchsecurity.techtarget.com/tip/Exploit-kits-evolved-How-to-defend-against-the-latest-attack-toolkits (14.03.2012)

http://blog.webroot.com/2011/10/ (14.03.2012)

http://www.pctools.com/security-news/zero-day-vulnerability/ (14.03.2012)

http://derstandard.at/1373512568424/Zero-Day-Exploits-Staaten-kaufen-Sicherheitsluecken (14.03.2012)

http://blog.kaspersky.de/was-ist-ein-rootkit/ (14.03.2012)

http://www.viruslist.com/de/analysis?discuss=200883623&return=1 (14.03.2012)

http://www.techrepublic.com/blog/10-things/10-plus-things-you-should-know-about-rootkits/ (14.03.2012)

http://www.securelist.com/en/analysis/168740859/Rootkits_and_how_to_combat_them?print_mode=1 (14.03.2012)

http://www.zdnet.de/39199993/meister-der-tarnung-was-man-ueber-rootkits-wissen-sollte/ (14.03.2012)

https://blog.kaspersky.de/was-ist-eine-man-in-the-middle-attacke/ (14.03.2012)

http://www.itwissen.info/definition/lexikon/Man-in-the-Middle-Angriff-man-in-the-middle-attack.html (14.03.2012)

http://www.social-engineer.org/ (14.03.2012)

http://www.sicherheitskultur.at/social_engineering.htm (14.03.2012)

http://www.itwissen.info/definition/lexikon/Phishing-phishing.html (14.03.2012)

http://www.computerlexikon.com/was-ist-phishing (14.03.2012)

http://separaum.de/informationen-zu-phishing/ (14.03.2012)

http://www.edv-workshop.de/nav/them/phish/phish02.htm (14.03.2012)

http://www.sicher-im-internet.at/schule/spam.html (14.03.2012)

http://www.ruhr-uni-bochum.de/nds/research/top/ipi/phishing/indexm.html (14.03.2012)

http://www.spam-info.de/2741/achtung-vor-phishing-mails-wegen-eines-angeblich-eingeschraenkten-paypal-kontos/ (17.03.2012)

http://www.focus.de/digital/internet/tid-15755/angriff-auf-hotmail-konten-die-tricks-der-phishing-betrueger_aid_442332.html (17.03.2012)

http://derstandard.at/1389857414133/Bundeskriminalamt-warnt-vor-Phishing-Betruegern-Viren-und-Trojanern (17.03.2012)

http://pi1.informatik.uni-mannheim.de/filepool/media/20090114-spiegel-de-cyber-verbrecher-gehen-it-forschern-in-die-falle.pdf (17.03.2012)

http://storageservers.wordpress.com/2013/04/29/shared-web-hosting-servers-become-soft-target-for-mass-phishing-attacks/ (17.03.2012)

http://www.kaspersky.com/about/news/spam/2010/Facebook_ranks_fourth_in_the_Top_10_most_popular_phishing_targets_in_the_first_quarter_of_2010 (17.03.2012)

http://www.computerweekly.com/news/2240187487/FBI-warns-of-increased-spear-phishing-attacks (17.03.2012)

http://www.kaspersky.com/about/news/spam/2010/Facebook_ranks_fourth_in_the_Top_10_most_popular_phishing_targets_in_the_first_quarter_of_2010 (17.03.2012)

http://www.kaspersky.com/about/news/spam/2010/Spam_Report_May_2010 (17.03.2012)

http://www.securelist.com/en/analysis/204792117/Spam_evolution_January_March_2010 (17.03.2012)

http://www.securelist.com/en/analysis/204792276 (17.03.2012)

http://www.gartner.com/it/page.jsp?id=565125 (21.03.2012)

http://www.gartner.com/it/page.jsp?id=565125 (21.03.2012)

http://www.gartner.com/it/page.jsp?id=936913 (21.03.2012)

http://www.finextra.com/news/fullstory.aspx?newsitemid=15013 (21.03.2012)

http://www.heise.de/security/meldung/BKA-Phishing-Faelle-haben-weiter-zugenommen-998992.html (21.03.2012

http://www.heise.de/security/meldung/BKA-Phishing-Faelle-haben-weiter-zugenommen-998992.html (21.03.2012

http://www.heise.de/security/meldung/BKA-und-Bitkom-17-Millionen-Euro-Schaeden-durch-Phishing-1073002.html (21.03.2012)

http://www.bmi.gv.at/cms/BMI_OeffentlicheSicherheit/2006/03_04/files/Phishing.pdf (21.03.2012)

https://www.a-i3.org/content/view/1314/214/ (21.03.2012)

http://futurezone.at/digitallife/5989-5-7-millionen-euro-schaden-durch-internetbetrug.php (21.03.2012)

http://www.trusteer.com/sites/default/files/Phishing-Statistics-Dec-2009-FIN.pdf (21.03.2012)

https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29 (23.03.2012)

http://www.itwissen.info/definition/lexikon/cross-site-scripting-XSS.html (23.03.2012)

https://www.owasp.org/index.php/Code_Injection (23.03.2012)

http://weblogs.asp.net/jgalloway/archive/2011/04/28/preventing-javascript-encoding-xss-attacks-in-asp-net-mvc.aspx (23.03.2012)

http://www.pcwelt.de/ratgeber/Internet-Gefahr-So-funktionieren-Cross-Site-Scripting-CSRF-150841.html (23.03.2012)

http://www.webmasterpro.de/server/article/sicherheit-cross-site-scripting.html (23.03.2012)

http://www.webmasterpro.de/server/article/sicherheit-cross-site-scripting.html (24.03.2012)

http://excess-xss.com/ (24.03.2012)

http://www.webmasterpro.de/server/article/sicherheit-cross-site-scripting.html (24.03.2012)

http://excess-xss.com/ (24.03.2012)

http://security.stackexchange.com/questions/19373/what-is-the-danger-of-reflected-cross-site-scripting (24.03.2012)

http://www.computerweekly.com/tip/Cross-site-scripting-explained-How-to-prevent-XSS-attacks (24.03.2012)

http://www.pcwelt.de/ratgeber/XSS-kann-ueberall-lauern-Internet-Gefahr-150849.html (24.03.2012)

https://www.owasp.org/index.php/Fuzzing (24.03.2012)

https://www.owasp.org/index.php/Testing_for_Cross_site_scripting (24.03.2012)

http://projects.webappsec.org/w/page/13246989/Web%20Application%20Security%20Statistics (24.03.2012)

http://www.firehost.com/company/newsroom/web-application-attack-report-fourth-quarter-2012 (24.03.2012)

http://projects.webappsec.org/w/page/13246989/Web%20Application%20Security%20Statistics (24.03.2012)

http://www.firehost.com/company/newsroom/web-application-attack-report-fourth-quarter-2012 (26.03.2012)

http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/66879-hacker-konzentrieren-sich-auf-programmiersprachenfehler/ (24.03.2012)

http://www.itwissen.info/definition/lexikon/Pharming-pharming.html (26.03.2012)

http://www.itwissen.info/definition/lexikon/domain-name-system-DNS-DNS-System.html (26.03.2012)

http://blog.botfrei.de/2012/01/hosts-datei-was-ist-das-oder-warum-sieht-die-sparkassenseite-so-merkwurdig-aus-windows/ (26.03.2012)

http://technet.microsoft.com/en-us/library/cc958962.aspx (26.03.2012)

http://www.denic.de/hintergrund/nameservice/dns.html (26.03.2012)

http://www.itwissen.info/definition/lexikon/Name-Server-name-server.html (26.03.2012)

http://www.itwissen.info/definition/lexikon/Resolver-resolver.html (26.03.2012)

http://www.elektronik-kompendium.de/sites/net/0901141.htm (26.03.2012)

http://technet.microsoft.com/de-de/library/cc775637%28v=ws.10%29.aspx (26.03.2012)

http://technet.microsoft.com/de-de/library/cc775637%28v=ws.10%29.aspx (26.03.2012)

http://www.networkworld.com/news/tech/2008/102008-tech-update.html (26.03.2012)

http://blbaliyase.blogspot.com/2009/11/dns-cache-poisoning.html (27.03.2012)

http://resources.infosecinstitute.com/dns-cache-poisoning/ (27.03.2012)

http://www.itwissen.info/definition/lexikon/denial-of-service-DoS-DoS-Attacke.html (27.03.2012)

https://cert.uni-stuttgart.de/ticker/article.php?mid=1476 (27.03.2012)

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g03/g03104.html (27.03.2012)

http://derstandard.at/1216325543381 (27.03.2012)

http://einstein.informatik.uni-oldenburg.de/rechnernetze/geburtstagsangriff.htm (27.03.2012)

http://www.heise.de/security/meldung/Details-zum-DNS-Sicherheitsproblem-veroeffentlicht-188905.html (27.03.2012)

http://www.pressebox.de/pressemitteilung/nominum-inc/Nominum-bringt-umfassendes-Sicherheitspaket-fuer- DNS-Schwachstelle/boxid/200289 (27.03.2012)

http://www.heise.de/security/meldung/Reaktionen-auf-DNS-Angriffszenario-bei-deutschen-CERTS-und-Netzknoten-185376.html (27.03.2012)

http://net-security.org/secworld.php?id=11903 (27.03.2012)

http://www.ehackingnews.com/2011/11/brazil-isp-servers-under-dns-cache.html (27.03.2012)

http://www.securelist.com/en/blog/208193214/ (27.03.2012)

http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems (28.03.2012)

http://www.teleco.com.br/blarga.asp (28.03.2012)

http://www.securelist.com/en/blog/208193671/Is_it_the_end_of_the_DNSChanger_Trojan (28.03.2012)

http://www.dcwg.org/ (28.03.2012)

http://www.cert.br/docs/palestras/certbr-jornada-sisp2012.pdf (28.03.2012)

http://arstechnica.com/tech-policy/2011/11/how-the-most-massive-botnet-scam-ever-made-millions-for-estonian- hackers/ (28.03.2012)

http://www.fbi.gov/news/stories/2011/november/malware_110911 (28.03.2012)

http://www.itwissen.info/definition/lexikon/Spoofing-spoofing.html (30.03.2012)

http://www.itwissen.info/definition/lexikon/open-systems-interconnection-OSI-Offene-Kommunikation.html (30.03.2012)

http://www.its05.de/computerwissen-computerhilfe/pc-netzwerk/osi-modell/osi-modell.html (30.03.2012)

http://www.torsten-bauer.de/referate/isoosi/ (30.03.2012)

http://www.netzwerke.com/OSI-Schichten-Modell.htm (30.03.2012)

http://www.itwissen.info/definition/lexikon/Physikalische-Schicht-physical-layer.html (30.03.2012)

http://www.itwissen.info/definition/lexikon/Sicherungsschicht-DLL-data-link-layer.html (03.04.2012)

http://www.itwissen.info/definition/lexikon/medium-access-control-MAC-Medienzugangsverfahren.html (03.04.2012)

http://www.itwissen.info/definition/lexikon/Vermittlungsschicht-network-layer.html (03.04.2012)

http://www.itwissen.info/definition/lexikon/Routing-routing.html (03.04.2012)

http://wiki.ubuntu-forum.de/index.php/Baustelle:OSI-Referenzmodell (03.04.2012)

http://www.itwissen.info/definition/lexikon/Transportschicht-transport-layer.html (03.04.2012)

http://www.itwissen.info/definition/lexikon/Kommunikationssteuerungsschicht-session-layer.html (03.04.2012)

http://www.itwissen.info/definition/lexikon/Darstellungsschicht-P-presentation-layer.html (03.04.2012)

http://www.itwissen.info/definition/lexikon/Anwendungsschicht-APL-application-layer.html (03.04.2012)

http://www.itwissen.info/definition/lexikon/transmission-control-protocol-internet-protocol-TCP-IP-TCP-IP-Protokolle.html (04.04.2012)

http://www.itwissen.info/definition/lexikon/local-area-network-LAN-Lokales-Netz.html (04.04.2012)

http://www.itwissen.info/definition/lexikon/wide-area-network-WAN-Weitverkehrsnetz.html (04.04.2012)

http://www.elektronik-kompendium.de/sites/net/0606251.htm (04.04.2012)

http://www.ruhr-uni-bochum.de/~rothamcw/Lokale.Netze/tcpip.html (04.04.2012)

http://www.elektronik-kompendium.de/sites/net/0811271.htm (04.04.2012)

http://www.tecchannel.de/netzwerk/lan/434734/grundlagen_zu_routing_und_subnetzbildung_teil_1/index9.html (04.04.2012)

http://www.freesoft.org/CIE/Course/Section3/7.htm (06.04.2012)

http://www.elektronik-kompendium.de/sites/net/1806031.htm (06.04.2012)

http://www.itwissen.info/definition/lexikon/IP-Header-IP-header.html (06.04.2012)

https://www.iana.org/ (06.04.2012)

http://www.itwissen.info/definition/lexikon/IP-Adresse-IP-address.html (06.04.2012)

http://www.itwissen.info/definition/lexikon/IPv4-Adresse-IPv4-address.html (06.04.2012)

http://www.itwissen.info/definition/lexikon/Internet-protocol-version-4-IPv4-IPv4-Protokoll.html (08.04.2012)

http://www.elektronik-kompendium.de/sites/net/0811271.htm (08.04.2012)

http://www.itwissen.info/definition/lexikon/transmission-control-protocol-TCP-TCP-Protokoll.html (08.04.2012)

http://www.elektronik-kompendium.de/sites/net/0812271.htm (08.04.2012)

http://www.itwissen.info/definition/lexikon/Socket-socket.html (08.04.2012)

http://www.itwissen.info/definition/lexikon/TCP-Header-TCP-header.html (08.04.2012)

http://www.elektronik-kompendium.de/sites/net/0812271.htm (08.04.2012)

http://www.proprofs.com/mwiki/index.php/Fundamentals_Of_TCP_And_UDP (08.04.2012)

http://de.wikipedia.org/wiki/Transmission_Control_Protocol (08.04.2012)

http://www.itwissen.info/definition/lexikon/transmission-control-protocol-TCP-TCP-Protokoll.html (08.04.2012)

http://www.itwissen.info/definition/lexikon/Puffer-buffer.html (08.04.2012)

http://www.itwissen.info/definition/lexikon/Padding-PL-padding-length.html (08.04.2012)

http://www.mentzel-web.de/net/tcp.html (08.04.2012)

http://www.itwissen.info/definition/lexikon/3-Wege-Handshake-3-way-handshake.html (08.04.2012)

http://www.prontosystems.org/it/tcp (17.04.2012)

http://www.itwissen.info/definition/lexikon/IP-Spoofing-IP-spoofing.html (17.04.2012)

http://www.elektronik-kompendium.de/sites/net/1412101.htm (17.04.2012)

http://www.symantec.com/connect/articles/ip-spoofing-introduction (17.04.2012)

http://users.informatik.uni-halle.de/~beckmann/Firewall/ (17.04.2012)

http://entwickler.de/zonen/portale/psecom,id,126,news,29378,p,0.html (17.04.2012)

http://www.cert.org/advisories/CA-1996-21.html (17.04.2012)

http://www.itwissen.info/definition/lexikon/Sequenznummer-SEQ-sequence-number.html (17.04.2012)

http://www.tu-chemnitz.de/urz/lehre/rs/rs02/gr/atatcp.htm (17.04.2012)

http://www.itwissen.info/definition/lexikon/MAC-Adresse-MAC-address.html (18.04.2012)

http://secureleaves.com/2012/11/05/layer-2-attacks-mac-address-spoofing-attacks/ (18.04.2012)

http://www.computerbild.de/artikel/cb-Ratgeber-Kurse-DSL-WLAN-So-sichern-Sie-Ihr-Funknetzwerk-2260871.html (18.04.2012)

http://www.klcconsulting.net/Change_MAC_w2k.htm (18.04.2012)

http://www.itwissen.info/definition/lexikon/address-resolution-protocol-ARP-ARP-Protokoll.html (21.04.2012)

https://www.elektronik-kompendium.de/sites/net/0901061.htm (21.04.2012)

http://www.watchguard.com/infocenter/editorial/135324.asp (21.04.2012)

http://eatingsecurity.blogspot.co.at/2011/02/using-ettercap-for-arp-poisoning.html (21.04.2012)

http://www.erg.abdn.ac.uk/~gorry/course/inet-pages/arp.html (21.04.2012)

http://packetlife.net/blog/2010/may/3/port-security/ (21.04.2012)

http://www.e-teaching.org/technik/distribution/cms/ (28.04.2012)

https://www.owasp.org/index.php/SQL_Injection (28.04.2012)

http://www.beyondsecurity.com/about-sql-injection.html (28.04.2012)

https://www.owasp.org/index.php/Top_10_2010-A1-Injection (28.04.2012)

http://www.zdnet.com/sony-hacked-again-in-lulzsec-breach-4010022607/ (28.04.2012)

http://www.computerworld.com/s/article/9229136/Yahoo_fixes_password_pilfering_bug_explains_who_s_at_risk (28.04.2012)

https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29 (03.05.2012)

http://projects.webappsec.org/w/page/13246919/Cross%20Site%20Request%20Forgery (03.05.2012)

http://www.it.cornell.edu/security/safety/malware/driveby.cfm (06.05.2012)

http://www.itwissen.info/definition/lexikon/Plug-In-plug-in.html (06.05.2012)

http://www.pcwelt.de/news/Secunia-Report-2010-Fehlende-Updates-sind-das-groesste-Risiko-1443404.html (06.05.2012)

https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/BotNetze/botnetze_node.html (06.05.2012)

http://www.incapsula.com/ddos/ddos-attacks/botnet-ddos.html (06.05.2012)

https://www.elektronik-kompendium.de/sites/net/1412091.htm (06.05.2012)

https://www.watchguard.com/infocenter/editorial/41649.asp (06.05.2012)

http://www.pcworld.com/article/2013109/report-open-dns-resolvers-increasingly-abused-to-amplify-ddos-attacks.html (06.05.2012)

http://www.kaspersky.com/about/news/virus/2012/2012_by_the_numbers_Kaspersky_Lab_now_detects_200000_new_malicious_programs_every_day (08.05.2012)

http://resources.infosecinstitute.com/botnets-unearthed-the-zeus-bot/ (08.05.2012)

http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012 (08.05.2012)

http://www.spiegel.de/netzwelt/web/spam-botnet-grum-zerstoert-a-845232.html (08.05.2012)

http://www.maclife.de/panorama/netzwelt/flashback-botnet-soll-auf-600000-macs-installiert-sein (08.05.2012)

http://www.techweekeurope.co.uk/news/ddos-attacks-power2012-86926 (08.05.2012)

http://www.neustar.biz/enterprise/resources/ddos-protection/2012-ddos-attacks-report#.UmSyuBDZhdU (08.05.2012)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT (10.05.2012)

http://www.fidis.net/interactive/wiki-on-id-related-law/wiki/United%20States%20-%20Federal%20B1.%20ID%20Theft/ (11.05.2012)

http://www.law.cornell.edu/uscode/text (11.05.2012)

http://www.law.cornell.edu/uscode/text/18/1028 (11.05.2012)

http://www.law.cornell.edu/uscode/text/18/1028 (11.05.2012)

http://www.law.cornell.edu/uscode/text/18/1029 (11.05.2012)

http://www.law.cornell.edu/uscode/text/18/1028 (12.05.2012)

http://www.law.cornell.edu/uscode/text/18/1030 (12.05.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (12.05.2012)

http://www.justice.gov/archive/ittf/ (12.05.2012)

http://itlaw.wikia.com/wiki/President%27s_Task_Force_on_Identity_Theft (12.05.2012)

http://www.socialsecurity.gov/ (12.05.2012)

http://www.ftc.gov/sentinel/ (14.05.2012)

http://laws-lois.justice.gc.ca/eng/acts/c-46/ (14.05.2012)

http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?lang=E&ls=s4&Parl=40&Ses=2&source=library_prb (14.05.2012)

http://www.cippic.ca/ (14.05.2012)

http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=3125690&Language=e&Mode=1&File=24#1 (14.05.2012)

http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=s4&source=library_prb&Parl=39&Ses=1&Language=E (14.05.2012)

http://laws-lois.justice.gc.ca/eng/acts/C-46/page-186.html#h-107 (14.05.2012)

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/CCQ/CCQ_A.html (20.05.2012)

http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/kim-crime.html (20.05.2012)

http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp (20.05.2012)

http://laws-lois.justice.gc.ca/eng/acts/P-21/ (20.05.2012)

http://www.rcmp-grc.gc.ca/index-eng.htm (20.05.2012)

https://www.oppa.ca/ (21.05.2012)

http://www.cba.ca/?lang=en (21.05.2012)

http://www.huffingtonpost.ca/2012/09/09/identity-theft-canada_n_1868172.html (21.05.2012)

http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?lang=E&ls=s4&Parl=40&Ses=2&source=library_prb (21.05.2012)

http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?lang=E&ls=s4&Parl=40&Ses=2&source=library_prb (21.05.2012)

http://idtheftsupportcentre.org/ (21.05.2012)

http://www.comlaw.gov.au/Details/C2004A00937 (28.05.2012)

http://www.austlii.edu.au/au/legis/cth/consol_act/ftra1988308/notes.html (28.05.2012)

http://www.australien-24.com/allgemeines/politik/ (28.05.2012)

http://www.austlii.edu.au/au/legis/qld/consol_act/cc189994/s408d.html (28.05.2012)

http://www.aic.gov.au/crime_types/economic/idfraud.aspx#aus (28.05.2012)

http://www.comlaw.gov.au/Details/C2008B00274 (28.05.2012)

http://www.austlii.edu.au/au/legis/vic/num_act/caca200922o2009349/ (28.05.2012)

http://www.finextra.com/news/fullstory.aspx?newsitemid=14634 (02.06.2012)

http://www.finextra.com/news/fullstory.aspx?newsitemid=14634 (02.06.2012)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT (02.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (02.06.2012)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001F0413:DE:HTML (02.06.2012)

http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/jl0011_de.htm (02.06.2012)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:DE:NOT (02.06.2012)

http://ec.europa.eu/internal_market/payments/sepa/index_de.htm (02.06.2012)

http://ec.europa.eu/internal_market/fpeg/index_en.htm (02.06.2012)

http://europa.eu/legislation_summaries/fight_against_fraud/fight_against_counterfeiting/l33306_en.htm (02.06.2012)

http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=de&numdoc=52004DC0679%20&model=guichett (02.06.2012)

http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=de&numdoc=52004DC0679%20&model=guichett (03.06.2012)

www.idfraudconference-pt2007.org (03.06.2012)

http://prado.consilium.europa.eu/DE/homeindex.html (03.06.2012)

http://prado.consilium.europa.eu/DE/aboutUs.html (03.06.2012)

https://www.prime-project.eu/ (04.06.2012)

http://www.fidis.net/ (04.06.2012)

http://www.fidis.net/resources/deliverables/forensic-implications/int-d51000/doc/4/ (04.06.2012)

http://www.fidis.net/resources/deliverables/forensic-implications/int-d52b000/doc/41/ (04.06.2012)

http://www.cordis.europa.eu/fp7/ict/security/projects_en.html#TSI (04.06.2012)

http://www.enisa.europa.eu/ (04.06.2012)

http://futurezone.at/digitallife/5989-5-7-millionen-euro-schaden-durch-internetbetrug.php (06.06.2012)

http://www.bmi.gv.at/cms/BK/presse/files/KrimStat_1HJ2012.pdf (06.06.2012)

http://www.bka.gv.at/site/4297/default.aspx (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=Bundesnormen&Gesetzesnummer=10002296 (06.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=bundesnormen&Gesetzesnummer=10001597 (07.06.2012)

http://www.ris.bka.gv.at/GeltendeFassung.wxe?
Abfrage=Bundesnormen&Gesetzesnummer=10001622 (07.06.2012)

http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/mitMarginalspalte/06/identit
%C3%A4tsdiebstahl_internet.html (08.06.2012)

http://www.gesetze-im-internet.de/stgb/index.html (08.06.2012)

http://www.gesetze-im-internet.de/stgb/index.html (08.06.2012)

http://www.gesetze-im-internet.de/stgb/index.html (08.06.2012)

http://www.gesetze-im-internet.de/stgb/index.html (08.06.2012)

http://www.gesetze-im-internet.de/bdsg_1990/__3.html (08.06.2012)

http://www.gesetze-im-internet.de/bdsg_1990/__4.html (08.06.2012)

http://www.servat.unibe.ch/dfr/bv065001.html# (08.06.2012)

http://www.servat.unibe.ch/dfr/bv065001.html# (08.06.2012)

http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html
(09.06.2012)

http://www.gesetze-im-internet.de/gg/art_10.html (09.06.2012)

http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=50A957F4368A76B876359512D18
86752.tpdjo10v_3?
idArticle=LEGIARTI000006418661&cidTexte=LEGITEXT000006070719&dateTexte=20120919
(09.06.2012)

http://www.assemblee-nationale.fr/13/projets/pl1697.asp (09.06.2012)

http://www.senat.fr/leg/pjl09-292.html (09.06.2012)

http://www.assemblee-nationale.fr/13/ta/ta0883.asp (09.06.2012)

https://www.unwatched.org/book/export/html/6090 (09.06.2012)

http://www.conseil-constitutionnel.fr/conseil-constitutionnel/deutsch/entscheidungen/entscheidung-nr-2012-652-dc-vom-22-marz-2012-gesetz-zum-schutz-der-identitat.105656.html (09.06.2012)

http://www.conseil-constitutionnel.fr/conseil-constitutionnel/deutsch/entscheidungen/entscheidung-nr-2012-652-dc-vom-22-marz-2012-gesetz-zum-schutz-der-identitat.105656.html (09.06.2012)

http://www.conseil-constitutionnel.fr/conseil-constitutionnel/deutsch/entscheidungen/entscheidung-nr-2012-652-dc-vom-22-marz-2012-gesetz-zum-schutz-der-identitat.105656.html (09.06.2012)

http://www.homeoffice.gov.uk/agencies-public-bodies/nfa/ (12.06.2012)

http://www.identitytheft.org.uk/faqs.asp (12.06.2012)

http://www.national-identity-fraud-prevention-week.co.uk/identity-theft-statistics.htm (12.06.2012)

http://www.legislation.gov.uk/ukpga/1968/60 (12.06.2012)

http://www.cps.gov.uk/legal/d_to_g/fraud_act/ (12.06.2012)

http://www.legislation.gov.uk/ukpga/2006/35/contents (12.06.2012)

http://www.legislation.gov.uk/ukpga/1998/29/contents (12.06.2012)

http://www.legislation.gov.uk/ukpga/1990/18/section/3 (12.06.2012)

http://www.legislation.gov.uk/ukpga/2006/15/contents (12.06.2012)

http://www.legislation.gov.uk/ukpga/2010/40/contents/enacted (12.06.2012)

http://news.bbc.co.uk/2/hi/uk_news/politics/8707355.stm (12.06.2012)

http://www.legislation.gov.uk/ukpga/2010/40/section/4/enacted (12.06.2012)

http://www.legislation.gov.uk/ukpga/2010/40/section/6/enacted (12.06.2012)

http://www.thelocal.se/6736/20070319/ (22.06.2012)

http://www.thelocal.se/20794/20090720/ (22.06.2012)

http://scancomark.com/Management/Dramatic-growth-in-identity-theft-in-Sweden.html (22.06.2012)

http://www.sweden.gov.se/sb/d/2184/a/15521 (22.06.2012)

http://www.spiegel.de/netzwelt/web/elektronische-ueberwachung-schweden-beschliesst-web-abhoergesetz-a-560637.html (22.06.2012)

http://freiheitblog.wordpress.com/2008/06/19/uberwachungswahn-auf-schwedisch/ (22.06.2012)

http://torrentfreak.com/swedes-massively-protest-wiretap-law-080707/ (22.06.2012)

http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403148_text (22.06.2012)

http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5103862 (22.06.2012)

https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/BasisschutzComputer/basisschutzComputer_node.html;jsessionid=77D0AB025DF357F4CCA5A19D8E3E8728.2_cid250 (30.06.2012)

http://www.microsoft.com/security/resources/antivirus-whatis.aspx (30.06.2012)

http://www.bullhost.de/a/antivirensoftware.html (30.06.2012)

http://www.thomatechnik.de/antivirus-lexikon/begriffe/on-access-scanner.htm (30.06.2012)

http://www.thomatechnik.de/antivirus-lexikon/begriffe/on-access-scanner.htm (30.06.2012)

http://www.thomatechnik.de/antivirus-lexikon/begriffe/on-access-scanner.htm (30.06.2012)

http://www.computerlexikon.com/definition-virenscanner (30.06.2012)

http://www.computerlexikon.com/definition-virenscanner (30.06.2012)

http://www.computerlexikon.com/definition-virenscanner (30.06.2012)

http://www.computerlexikon.com/definition-virenscanner (30.06.2012)

http://www.itwissen.info/definition/lexikon/Sandbox.html (30.06.2012)

http://www.anti-malware-test.com/test-results/AntiVirus_Proactive_Protection_Test_2008 (30.06.2012)

http://anti-virus-rants.blogspot.co.at/2006/05/pro-active-vs-reactive-technologies.html (30.06.2012)

http://www.itwissen.info/definition/lexikon/Firewall-FW-firewall.html (30.06.2012)

http://www.itwissen.info/definition/lexikon/Paketfilter-PF-packet-filter.html (30.06.2012)

http://www.itwissen.info/definition/lexikon/Paketfilter-PF-packet-filter.html (30.06.2012)

http://www.itwissen.info/definition/lexikon/Firewall-FW-firewall.html (30.06.2012)

https://www.bsi.bund.de/cln_174/DE/Service/FAQ/PersonalFirewall/faq_node.html (30.06.2012)

http://altlasten.lutz.donnerhacke.de/mitarb/lutz/usenet/Firewall.html (30.06.2012)

http://www.itwissen.info/definition/lexikon/Backdoor-backdoor.html (30.06.2012)

http://www.rrzn.uni-hannover.de/its_p_firewall.html (30.06.2012)

http://www.rrzn.uni-hannover.de/its_p_firewall.html (30.06.2012)

https://www.bsi.bund.de/cln_174/ContentBSI/grundschutz/kataloge/m/m05/m05091.html (30.06.2012)

http://nod32.helpmax.net/de/tools/log-dateien/ (30.06.2012)

http://www.itmagazine.ch/Artikel/50956/Soziale_Netzwerke_und_Browser_beliebte_Angriffsziele.html (02.07.2012)

http://www.itwissen.info/definition/lexikon/Browser-browser.html (02.07.2012)

http://www.plugins.de/was-sind-plugins/browser-plugins/ (02.07.2012)

http://www.browsercheck.pcwelt.de/de/dokumentation/browser-plugins-und-update-check (02.07.2012)

http://noscript.net/ (02.07.2012)

http://www.pcwelt.de/news/Firefox-Add-on-Mehr-Browser-Sicherheit-mit-Request-Policy-429308.html (02.07.2012)

https://adblockplus.org/de/getting_started (02.07.2012)

http://www.golem.de/1005/74885.html (02.07.2012)

http://www.adobe.com/security/flashplayer/articles/lso/ (02.07.2012)

http://www.soeren-hentzschel.at/mozilla/firefox/2012/03/29/firefox-14-bekommt-opt-in-aktivierung-fur-plugins/ (02.07.2012)

https://support.mozilla.org/de/kb/warum-werden-plugins-erst-nach-einer-bestaetigung-ausgefuehrt (02.07.2012)

http://derstandard.at/1345164832023/Mehr-Add-on-Sicherheit-ab-Firefox-17 (02.07.2012)

https://www.schneier.com/blog/archives/2011/01/whitelisting_vs.html (02.07.2012)

https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Empfehlungen/produktkonfiguration/BSI-E-CS-001.html (02.07.2012)

http://blog.chromium.org/2008/10/new-approach-to-browser-security-google.html (02.07.2012)

http://blog.chromium.org/2008/10/new-approach-to-browser-security-google.html (02.07.2012)

http://www.google.at/intl/de/chrome/browser/features.html#security (02.07.2012)

http://www.techfieber.de/2012/05/21/web-google-chrome-meistverwendeter-browser-der-welt/ (02.07.2012)

https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/WegInsInternet/DerBrowser/SicherheitsCheck/sicherheitscheck_node.html (02.07.2012)

https://www.mozilla.org/de/plugincheck/ (10.07.2012)

http://www.itwissen.info/definition/lexikon/Authentifizierung-authentication.html (10.07.2012)

http://www.datenschutz-praxis.de/fachwissen/fachartikel/prufen-sie-die-moglichkeiten-der-zwei-faktor-authentifizierung/ (10.07.2012)

http://www.itwissen.info/definition/lexikon/one-time-password-OTP-Einmalpasswort.html (10.07.2012)

http://www.itwissen.info/definition/lexikon/one-time-password-OTP-Einmalpasswort.html (10.07.2012)

http://www.securepoint.at/produkte-ID-Control-OTP-Key.html (10.07.2012)

http://msdn.microsoft.com/de-de/magazine/cc507635.aspx (10.07.2012)

http://msdn.microsoft.com/de-de/magazine/cc507635.aspx (10.07.2012)

http://msdn.microsoft.com/de-de/magazine/cc507635.aspx (10.07.2012)

http://austria.emc.com/security/rsa-securid/rsa-securid-software-authenticators.htm (10.07.2012)

http://www.itwissen.info/definition/lexikon/Smartcard-smartcard.html (12.07.2012)

http://www.itwissen.info/definition/lexikon/Smartcard-smartcard.html (12.07.2012)

http://www.itwissen.info/definition/lexikon/Smartcard-smartcard.html (12.07.2012)

http://www.die-deutsche-kreditwirtschaft.de/dk/pressemitteilungen/volltext/backpid/29/article/neue-generation-von-chipkartenlesern.html?tx_ttnews[pS]=1325372400&tx_ttnews[pL]=1356994799&tx_ttnews[arc]=1&cHash=9fcdc816efa0b5fc8b6f043f428e6835 (12.07.2012)

http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/zulassungsverfahren/secoder.html (12.07.2012)

http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/zulassungsverfahren/secoder.html (12.07.2012)

http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012)

http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012).....141

http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012)

http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012)

http://www.geldkarte-shop.de/templates/default/images/chipkartenleser_uebersicht.pdf (12.07.2012)

http://www.sparkasse.de/privatkunden/konto-karte/sicherungsverfahren.html (12.07.2012)

http://files.messe.de/cmsdb/D/007/22434.pdf (12.07.2012)

http://www.die-signaturkarte.de/aktuell/Secoder_2.html (12.07.2012)

http://www.die-signaturkarte.de/aktuell/Secoder_2.html (12.07.2012)

http://www.pcwelt.de/produkte/Einmalpasswoerter-per-iPhone-OTP-Generator-58281.html (14.07.2012)

http://www.onelogin.com/product/strong-authentication/onelogin-otp/ (14.07.2012)

http://www.securepoint.de/produkte-starke-authentifizierung.html (14.07.2012)

https://www.info-point-security.com/security-themen/identity/item/7428-ecos-2-faktor-authentisierung-per-sms.html (14.07.2012)

http://stadt-bremerhaven.de/dropbox-fuehrt-2-faktor-authentifizierung-ein/ (14.07.2012)

http://stadt-bremerhaven.de/google-konto-und-profil-absichern/ (14.07.2012)

http://stadt-bremerhaven.de/facebook-doppelte-anmeldesicherheit-startet/ (14.07.2012)

http://www.xsized.de/2010/03/man-in-the-middle-attack-auf-blizzard-authenticator/ (14.07.2012)

http://www.heise.de/newsticker/meldung/RSA-Hack-koennte-Sicherheit-von-SecurID-Tokens-gefaehrden-1210245.html (14.07.2012)

http://www.ecos.de/notfallarbeitsplaetze.html (14.07.2012)

http://www.symantec.com/business/support/index?page=content&id=HOWTO42048 (14.07.2012)

https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/Sicherheitsmechanismen/sicherPKI/pki_node.html (20.07.2012)

http://www.itwissen.info/definition/lexikon/Sicherheitsinfrastruktur-PKI-public-key-infrastructure.html (20.07.2012)

http://www.dartmouth.edu/~deploypki/overview.html (20.07.2012)

http://www.digitales.oesterreich.gv.at/site/5567/default.aspx (20.07.2012)

http://www.a-sit.at/de/signatur/ (20.07.2012)

http://europa.eu/legislation_summaries/information_society/other_policies/l24118_de.htm (20.07.2012)

http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=31999L0093&model=guichett&lg=de (20.07.2012)

http://www.digitales.oesterreich.gv.at/site/5567/default.aspx (20.07.2012)

http://www.internet4jurists.at/intern25.htm (20.07.2012)

http://www.itwissen.info/definition/lexikon/Digitale-Signatur-DSig-digital-signature.html (20.07.2012)

http://www.itwissen.info/definition/lexikon/Zertifikat-certificate.html (20.07.2012)

http://www.itwissen.info/definition/lexikon/Zertifizierungsstelle-CA-certification-authority.html (20.07.2012)

http://www.cryptoshop.com/index.php (20.07.2012)

http://www.kryptowissen.de/asymmetrische-verschluesselung.html (20.07.2012)

http://www.itwissen.info/definition/lexikon/Public-Key-Verfahren-public-key-method.html (20.07.2012)

http://www.digitales.oesterreich.gv.at/site/5268/default.aspx (20.07.2012)

http://www.digitales.oesterreich.gv.at/site/5567/default.aspx#a5 (20.07.2012)

http://www.buergerkarte.at/index.de.php (20.07.2012)

http://www.digitales.oesterreich.gv.at/site/5621/default.aspx (20.07.2012)

http://www.digitales.oesterreich.gv.at/site/5621/default.aspx (20.07.2012)

http://www.buergerkarte.at/wie-funktioniert.de.php (22.07.2012)

https://www.handy-signatur.at/mobile/info_bk.html (22.07.2012)

https://www.help.gv.at/aof/sigliste-flow (22.07.2012)

http://derstandard.at/1334795565969/Security-Forum-Sicherheitsluecke-bei-Buergerkarte (22.07.2012)

http://www.itwissen.info/definition/lexikon/Digitale-Signatur-DSig-digital-signature.html (22.07.2012)

http://ettisan.wordpress.com/2012/02/29/implementation-of-an-universal-forgery-on-the-austrian-burgerkarte/ (22.07.2012)

http://futurezone.at/digitallife/10633-oesterreicher-vertrauen-buergerkarte-nicht.php (22.07.2012)

http://www.bmi.gv.at/cms/BMI_OeffentlicheSicherheit/2007/03_04/files/IT_Sicherheit.pdf (22.07.2012)

http://www.itwissen.info/definition/lexikon/secure-socket-layer-SSL-SSL-Protokoll.html (28.07.2012)

http://www.elektronik-kompendium.de/sites/net/0902281.htm (28.07.2012)

http://www.itwissen.info/definition/lexikon/message-authentication-code-MAC-MAC-Code.html (28.07.2012)

http://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/de_DE/HTML/user277.htm (28.07.2012)

http://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/de_DE/HTML/user277.htm (28.07.2012)

https://www.cryptoheaven.com/Security/Presentation/SSL-protocol.htm (28.07.2012)

http://www.itwissen.info/definition/lexikon/transport-layer-security-TLS-TLS-Protokoll.html (28.07.2012)

http://pilif.github.com/2008/05/why-is-nobody-using-ssl-client-certificates/ (28.07.2012)

http://www.bev.gv.at/portal/page?_pageid=696,1682731&_dad=portal&_schema=PORTAL (28.07.2012)

http://www.ceilers-news.de/serendipity/207-Man-in-the-Middle-Angriffe-auf-HTTPS.html (28.07.2012)

http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf (28.07.2012)

http://www.heise.de/newsticker/meldung/Black-Hat-Neue-Angriffsmethoden-auf-SSL-vorgestellt-198285.html (28.07.2012)

http://www.heise.de/security/meldung/SSL-GAU-zwingt-Browser-Hersteller-zu-Updates-1212986.html (30.07.2012)

http://www.ceilers-news.de/serendipity/284-SSL-Der-naechste-Nagel-im-Sarg.html (30.07.2012)

http://www.itmagazine.ch/Artikel/50956/Soziale_Netzwerke_und_Browser_beliebte_Angriffsziele.html (04.08.2012)

http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20090915_01 (04.08.2012)

http://www.symantec.com/de/de/about/news/release/article.jsp?prid=20090915_01 (04.08.2012)

http://windows.microsoft.com/de-at/windows7/smartscreen-filter-frequently-asked-questions-ie9 (04.08.2012)

http://www.google.com/transparencyreport/safebrowsing/?hl=de (04.08.2012)

http://wiki.vorratsdatenspeicherung.de/images/Googlesafebrowsing-deaktivierung.pdf (20.08.2012)

http://log.nadim.cc/?p=78 (04.08.2012)

http://log.nadim.cc/?p=78 (04.08.2012)

https://www.owasp.org/index.php/HTTP_Strict_Transport_Security (20.08.2012)

https://www.owasp.org/index.php/HTTP_Strict_Transport_Security (20.08.2012)

https://www.owasp.org/index.php/HTTP_Strict_Transport_Security (20.08.2012)

https://hacks.mozilla.org/2010/08/firefox-4-http-strict-transport-security-force-https/ (20.08.2012)

http://www.soeren-hentzschel.at/mozilla/firefox/2012/11/08/hsts-liste-schutzt-firefox-ab-version-17-vor-man-in-the-middle-attacken/ (20.08.2012)

https://netbanking.sparkasse.at/hilfe/sicherheit/TAN (22.08.2012)

https://www.it-sicherheit.de/ratgeber/it_sicherheitstipps/online_dienste_sicher_nutzen/online_banking/ (22.08.2012)

http://www.girokonto.info/ratgeber/etan-und-etan-plus/ (22.08.2012)

http://www.girokonto.info/ratgeber/etan-und-etan-plus/ (22.08.2012)

http://blog.botfrei.de/2011/10/onlinebanking-das-mobile-tan-verfahren/ (22.08.2012)

http://blog.botfrei.de/2011/10/onlinebanking-das-mobile-tan-verfahren/ (22.08.2012)

http://www.berlin.de/polizei/presse-fahndung/archiv/377949/index.html (22.08.2012)

http://www.itwissen.info/definition/lexikon/DNSSEC-domain-name-system-security-extension.html (24.08.2012)

http://www.itwissen.info/definition/lexikon/DNSSEC-domain-name-system-security-extension.html (24.08.2012)

http://www.verisigninc.com/de_DE/why-verisign/innovation-initiatives/dnssec/how-dnssec-works/index.xhtml (24.08.2012)

http://www.verisigninc.com/de_DE/why-verisign/innovation-initiatives/dnssec/how-dnssec-works/index.xhtml (24.08.2012)

http://www.heise.de/newsticker/meldung/DNSSEC-in-der-DNS-Rootzone-gestartet-1039401.html (24.08.2012)

http://www.heise.de/newsticker/meldung/Rascher-Start-von-DNSSEC-bei-net-und-com-1128745.html (24.08.2012)

http://www.denic.de/domains/dnssec.html (24.08.2012)

http://www.nic.at/service/technische_informationen/dnssec/ (24.08.2012)

http://stats.research.icann.org/dns/tld_report/ (24.08.2012)

http://www.dvmag.de/dnssec/ (24.08.2012)