

Diplomarbeit

**Gefahren durch nicht-gerichtete
Angriffe im Internet**

Universität-GH Paderborn
Fachbereich Wirtschaftswissenschaften
Fachgebiet Wirtschaftsinformatik
Prof. Dr. L. Suhl

Arne Sendke
Oberwöhrener Str. 1
31655 Stadthagen

MatrikelNr.: 3370411

22. Dezember 2000

EIDESSTATTLICHE ERKLÄRUNG

Hiermit erkläre ich an Eides Statt, dass ich die vorliegende Arbeit selbständig und ohne unerlaubte fremde Hilfe angefertigt, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und die den benutzten Quellen und Hilfsmittel wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Arne Sendke, Stadthagen

22. Dezember 2000

Zusammenfassung

Diese Diplomarbeit thematisiert nicht-gerichtete Angriffe im Internet und die dadurch für den normalen Nutzer entstehenden Gefahren. Dazu werden zuerst rechtliche sowie technische Grundlagen erläutert, um so auch den Lesern einen Einstieg zu ermöglichen, die in diesem Gebiet nur wenige Vorkenntnisse haben. Anschließend werden bekannte Angriffsmittel, wie z.B. Viren und Trojaner, Angriffsziele, wie z.B. das Sammeln von Daten und Mischformen, wie z.B. WebSpoofing, in ihren Anwendungen und Techniken erläutert, mit dem Ziel den Leser einerseits ausführlich zu informieren und ihm so die Möglichkeit zu geben, diese Gefahren für sich einzuschätzen und andererseits ihn auch zu sensibilisieren, so dass Angriffe frühzeitig erkannt werden können. Das Kapitel Gegenmaßnahmen führt dann bekannte Verteidigungsmöglichkeiten auf, die dem Leser helfen, sich grundsätzlich zu schützen. Abschließend erfolgt ein kurzes Resümee. In dem letzten Kapitel werden sehr detaillierte technische Aspekte behandelt.

Inhaltsverzeichnis

Tabellenverzeichnis **vi**

Abbildungsverzeichnis **vi**

I Einleitung **1**

1 Charakterisierung der aktuellen Situation **2**

II Rechtliche Situation **4**

2 Gesetzgebung in Deutschland **5**

2.1 Strafgesetzbuch 5

2.2 Bundesdatenschutzgesetz 5

2.2.1 Informelle Selbstbestimmung 6

2.2.2 Inhalt des Bundesdatenschutzgesetz 6

2.3 Weiterführende Rechtsvorschriften 7

2.3.1 Telekommunikationsgesetz 7

2.3.2 Teledienstgesetz 7

2.3.3 Teledienstschutzgesetz 8

2.3.4 Sonstige Gesetze und Verordnungen 8

3 Europäische Regelungen **9**

4 Außereuropäische Regelungen **10**

4.1 US-Amerika 10

III Relevante Basistechnologien **12**

5 Protokolle **12**

6 Datenübertragung im Internet **12**

7 Aufbau des World Wide Web **14**

7.1 Uniform Resource Locator 15

7.2 Hypertext Markup Language 15

7.2.1 Aufbau 16

7.2.2 Ausgewählte Elemente 16

7.3 Hypertext Transfer Protocol 16

<i>INHALTSVERZEICHNIS</i>	ii
7.3.1 Cookie	17
8 Das Domain Name System	18
9 EMail	20
IV Angriffsarten	21
10 Begriffliche Abgrenzung	21
11 Angriff auf Vertraulichkeit: Datenspuren	22
11.1 Einleitung	22
11.2 Datensammeln: passive Methoden	25
11.2.1 Dynamische Elemente	25
11.2.2 Cookie	26
11.2.3 WebBug	27
11.2.4 Beispiel: DoubleClick	28
11.2.5 Weitere Marketinggesellschaften	30
11.3 Datensammeln: aktive Methoden	30
11.3.1 Globally Unique Identifier	31
11.3.2 Metadaten in Microsoft Office 97 Dokumenten	32
11.3.3 Eingesetzte Programme	33
11.3.4 TRUSTe	34
11.4 Bewußte Informationsweitergabe	34
11.4.1 EMail	35
11.4.2 Homepage	35
11.4.3 Usenet	35
12 Angriff auf Vertraulichkeit: Spoofing	36
12.1 Domain Name System Spoofing	36
12.1.1 Domain Name Lookup	37
12.1.2 Wirkung eines DNS Spoofings	37
12.1.3 Cache Pollution	39
12.1.4 Query-ID guess	39
12.2 WebSpoofing	41
12.2.1 Einleitung	41
12.2.2 URL Rewriting	41
12.2.3 Vortäuschen einer Seite	43
13 Schadhafte Programme	43
13.1 Einleitung	43
13.2 klassische Viren	45
13.2.1 Definition	45

13.2.2	Einteilung	46
13.2.3	Schäden	47
13.2.4	Beispiele	48
13.2.5	Infizierung	49
13.3	Würmer	51
13.4	Hoax	51
13.4.1	Arten	52
13.4.2	Schaden	53
13.5	Trojaner	53
13.5.1	Beispiele von Trojanern	53
13.6	Fehlerhafte Programme	55
13.6.1	Beispiele	55
13.7	Gefährliche Programme	56
13.7.1	Hintertürprogramme	56
13.7.2	Überwachungsprogramme	57
13.7.3	Aktive Elemente	58
14	Sozialer Angriff	59
V	Gegenmaßnahmen	60
15	Verhaltensregeln	60
15.1	Allgemeine Verhaltensmaßnahmen	60
15.1.1	Schutz persönlicher Daten	61
15.1.2	Vorsichtiges Surfen	61
15.1.3	Umsichtiges Mailen	62
15.1.4	Infizierungen vermeiden	62
15.1.5	Datensicherung	63
15.2	Veränderte Einstellungen	64
15.2.1	Internet-Browser	64
15.2.2	Microsoft Office	66
15.2.3	Windows-Explorer	67
16	Programme	67
16.1	Clientseitige Programme	67
16.1.1	Cookie finder	68
16.1.2	Viren und Trojaner	68
16.1.3	Schadhafte Programme entdecken	68
16.1.4	Schadhafte Programme entfernen	70
16.1.5	Viewer	71
16.1.6	Abwehrmaßnahmen gegen GUID	71
16.1.7	Metadaten	71
16.1.8	Firewalls	72

16.2	Serverseitige Programme	73
16.2.1	Anonymizer	73
16.2.2	Kryptographische Verfahren	74
16.2.3	Zufällige Query-IDs	76
16.2.4	Domain Namen überprüfen	76
16.2.5	EMail	77
VI	Abschließende Betrachtung	79
VII	Anhang	83
A	Grundlage verwendeter Protokolle	83
A.1	Das OSI-Referenzmodell	83
A.2	Aufbau des IPv4 Headers	84
A.3	Aufbau des TCP Headers	86
A.4	Funktion des TCP/IP Protokolls	87
A.5	Aufbau der HTTP Header	88
A.5.1	HTTP Request Header	88
A.5.2	HTTP Response Header	90
B	Grundlage der Adressierung	91
B.1	IP Adressen	91
B.2	Ressourcen Records	92
B.3	TCP Adressen	93
C	Grundlage der Verschlüsselung	93
C.1	Sichere Verschlüsselung	94
C.2	Symmetrische Verfahren	95
C.2.1	Funktion	95
C.2.2	Data Encryption Standard	95
C.2.3	Sicherheit	96
C.3	Asymmetrische Verfahren	96
C.3.1	Funktion	96
C.3.2	Beispiel: RSA Kryptosystem	97
C.3.3	Sicherheit	98
C.4	Symmetrische vs. Asymmetrische Verfahren	98
D	Erstellte Programme	99
E	Verzeichniss der Abkürzungen	101

<i>INHALTSVERZEICHNIS</i>	v
Literaturverzeichnis	104
Index	111

Tabellenverzeichnis

1	Zusammenarbeitende Internetseiten mit Onlineagenturen . . .	30
2	Abwehr durch Verhaltensmaßnahmen	60
3	Abwehr durch veränderte Einstellungen	64
4	Abwehr durch Client-Programme	68
5	Abwehr durch Serverseitige Programme	73
6	well known ports	93

Abbildungsverzeichnis

1	Transfer eines FTP-Datenpaketes	13
2	Protokoll Kapselung	14
3	DNS Spoofing	38
4	Verschlüsselung zwischen zwei Servern	75
5	IP Head	84
6	TCP Head	86
7	IP-Adreßklassen	92
8	Aufbau der Resource Records	93
9	Eine Runde der DES Verschlüsselung	95

Teil I

Einleitung

Diese Diplomarbeit verfolgt das Ziel, die für den Nutzer des Internets real vorhandenen Gefahren zu beschreiben, sowie mögliche Gegenmaßnahmen auszuarbeiten und diese auch für den Laien nachvollziehbar zu präsentieren. Die möglichen Angriffe im Internet lassen sich generell in zwei Kategorien unterteilen:

- **Gerichtete Angriffsformen:** Bei dieser Variante kennt der Angreifer das Opfer, bzw. hat ein Ziel, wie z.B. ein bestimmtes Programm oder eine Domäne anzugreifen.
- **Nicht-gerichtete Angriffsformen:** Hierbei kennt der Angreifer das Ziel nicht, bzw. nur sehr ungenau, z.B. Viren, die freigesetzt werden oder mit schadhafte Skripten versehene Internetseiten, die jeden Besucher angreifen.

Generell beschränken sich die aufgeführten Betrachtungen auf nicht-gerichtete Angriffe. Folgende Gründe sind dafür heranzuziehen.

Die gerichteten Angriffe sind in den meisten Fällen sehr komplex und zeitaufwendig, da die Art der Ausführung stark von den Sicherheitslücken der beim Ziel verwendeten Soft- und Hardware abhängt. Bereits eine neuere Version desselben Programmes erlaubt in vielen Fällen nicht den gleichen Angriff. Daraus ergibt sich, dass eine Beschreibung der gerichteten Angriffe zu oberflächlich wäre, bzw. hier nicht angebracht, da nur in den seltensten Fällen ein normaler Nutzer Ziel eines solchen Angriffes werden dürfte. Viel eher werden Firmen und Institutionen Gegenstand solcher Angriffsformen.

Die Angriffe der zweiten Kategorie lassen sich, wie nachfolgend noch ausführlich gezeigt wird, in den meisten Fällen automatisieren, mit den Auswirkungen, dass die Ausführung längst nicht so zeitaufwendig ist und gegen viele Ziele gleichzeitig gerichtet sein kann. Aufgrund der Automatisierbarkeit der meisten nicht-gerichteten Angriffe wird der normale Nutzer des Internets Ziel dieser Angriffsform.

Die für das Verständnis notwendigen technischen Grundlagen sind, soweit sinnvoll, in einem eigenen Kapitel erläutert. Dabei wurde versucht, eine allen verständliche Ausdrucksform zu finden, um die Arbeit nicht von vornherein auf einen kleinen Kreis „Eingeweihter“ zu beschränken. Da die Ausführung der Angriffe einem stetigen Wandel unterworfen ist, wird im Anhang ein detaillierter Blick auf technische Grundlagen gegeben, um auch neue Angriffe

erkennen zu können.

Aus zwei Gründen werden die Angriffe und Abwehrmaßnahmen in den meisten Fällen auf Windows 95 oder 98 bezogen. Der erste Grund ergibt sich aus der Verbreitung. Die Betriebssysteme von Microsoft werden von den meisten Nutzern des Internets eingesetzt. Der zweite Grund liegt in dem Aufbau des Betriebssystems begründet. Während vergleichbare Systeme in ihrem Aufbau bereits grundlegende Sicherheitsmechanismen beinhalten, wie z.B. eine zwingend notwendige Anmeldung und daraus ableitend eine nicht oder nur sehr schwer umgehbare Dateisicherung, fehlen den Windows 9x Varianten diese Möglichkeiten grundsätzlich.

1 Charakterisierung der aktuellen Situation

Die derzeitige Situation im Internet präsentiert sich ungefähr wie folgt:

- Das Internet wächst derzeit exponentiell. Zwischen den Jahren 1981 und 2000 stieg die Anzahl der im Internet vertretenen Hosts von 213 auf ungefähr 93 Millionen¹. Ähnliches Wachstum läßt sich auch bei Programmen verfolgen, so waren für das Betriebssystem Microsoft Windows 3.11 noch zehn Disketten ausreichend, während MS-Windows 2000 ungefähr 800 MByte auf der Festplatte benötigt. Dieses rasche Wachstum führt dazu, dass genutzte Protokolle und Software durch ständig notwendige Erweiterungen und Anpassungen immer undurchsichtiger werden und als Folge davon die Komplexität der Systeme und deren Interaktionen überlinear zunehmen.
- Es werden immer mehr Betriebssysteme und Programme verkauft, deren Benutzerfreundlichkeit trotz steigender Komplexität ständig zunimmt und die so immer mehr Grundeinstellungen für den Nutzer automatisch vornehmen. Dieser muß nichts wissen oder lesen, nur noch einen Button drücken und er ist „Online“. Zudem hat eine Umfrage unter 2.117 Personen ergeben, daß zwar 86 % einen besseren Datenschutz fordern, aber nur 10 % davon z.B. ihren Internet-Browser so konfiguriert hatten, daß dieser Cookies ablehnt. [HeiseDA00]
- Die natürliche Informationsasymmetrie zwischen Hersteller von Software und deren Käufer verstärkt sich durch Programme, die selbst wenn der Nutzer sich informieren möchte, wenig oder keine Informationen über sich oder das Thema preisgeben. So hat eine stichprobenartige Suche in der Hilfe der Programme Internet Explorer und Netscape Navigator bei folgender, zufällig gewählter Suchliste: Angriff, Datenschutz,

¹<http://www.isc.org/ds/host-count-history.html>

Gefahren, Schutz, TCP, Trojaner, IP, Viren, nur zu einem Treffer geführt. Bei dem Begriff Schutz hat der Internet Explorer eine produkt-eigene Technik erläutert, den sogenannten Microsoft Authenticode.

- Mit jedem neuen Programm wird in der Werbung die erhöhte Sicherheit zu seinem Vorgänger oder Konkurrenzprodukten angepriesen und so der Eindruck auf Seiten des Nutzers erhärtet, dass jetzt nichts mehr passieren kann. Kommt es doch zu einem erfolgreichen Angriff, wird auf Fehler des Nutzers verwiesen oder von einem Intelligenztest für Computerbediener gesprochen.²
- In den meisten Fällen werden Computer mit Microsoft Windows für einen Zugang zum Internet genutzt. Diese Homogenität auf Betriebssystemebene vereinfacht eine automatisierte Ausnutzung von gefundenen Sicherheitslücken.
- Vorhandene Sicherheitsmechanismen in den Programmen werden bei der Installation schlecht konfiguriert oder überhaupt nicht aktiviert. Die Ursache der meisten erfolgreichen Angriffe liegt, wie später noch gezeigt, in einer falschen Konfiguration der vorhandenen Sicherheitsmechanismen.

Aus den geschilderten Charakteristika ergibt sich ein hohes Gefahrenpotential für die meisten Internetnutzer. Die Anzahl der Angriffe steigt, während immer mehr Nutzer ohne Vorkenntnisse ins Internet gelangen und die dort vorhandenen Gefahren in keiner Weise einschätzen können. Diese Diplomarbeit hat den Anspruch, dem normalen Nutzer des Internets einen Überblick der derzeit gebräuchlichen nicht-gerichteten Angriffe zu geben und vor allem Möglichkeiten, sich zu schützen, aufzuzeigen.

Damit der Leser legale und illegale Tätigkeiten unterscheiden und somit Angriffe als solche überhaupt erkennen kann, folgt ein kurzer Überblick der derzeitigen rechtlichen Situation. Anschließend werden genutzte Technologien erläutert, so dass auch Leser ohne technische Vorbildung in der Lage sind, die aufgeführten Angriffe und Verteidigungsmaßnahmen zu verstehen und gegebenenfalls technisch neue Angriffe zu erkennen.

²Zitat nach Bill Gates nach dem Angriff des Skript Virus I LOVE YOU [HeiseB00]

Teil II

Rechtliche Situation

Wann immer eine neue Situation entstand, wurde zuerst versucht, die vorhandenen rechtlichen Möglichkeiten auf diese zu übertragen. Erst als sich diese Vorgehensweise als ungeeignet erwies, wurden neue Gesetze verfaßt. In den Anfängen des Internets wurden beispielsweise Hacker häufig wegen Hausfriedensbruch angeklagt. [Anon99, S. 759]

Eines der grundlegenden Probleme im Internet ist die Frage, welche Rechtsprechung herangezogen werden soll. Jeder hat die Möglichkeit, im Internet Handlungen zu tätigen, die in einem anderen Land spürbar werden und dort verboten sind. Sollen in diesem Fall die Gesetze des Täter- oder des Opferlandes angenommen werden? Ist es dem Täter überhaupt zumutbar, alle Gesetze der erreichbaren Länder zu kennen oder bedeutet die Tat aus einem nahezu rechtsfreien Raum, dass sie nicht geahndet werden kann? Solange es keine übernationale, von allen Ländern akzeptierte rechtliche Grundlage gibt, ist dieses Problem nicht zu überwinden.

Eines der zahlreichen anderen Probleme ergibt sich aus den neuen technischen Möglichkeiten des Internets, den Links. Hier stellt sich die Frage: Sind Linksetzer für die verlinkten Inhalte haftbar? Dazu gibt es verschiedenste Ansichten. Am 29. März berichtete der Spiegel Online über die Empörung in der Boulevard Presse, vor allem der Zeitung Bild, über einen Link auf der Homepage des Frauenministeriums, der zu einer sogenannten Sex-Site führen sollte.³ [SpiegelFS00] Wie sieht der Fall aus, wenn z.B. jemand auf seiner Homepage einen Link zu einer Seite gesetzt hat, auf der eine Bauanleitung für Bomben und gleichzeitig Prämien für die Ermordung bestimmter Personen aufgeführt sind. Außerdem gibt es noch markenrechtliche Bedenken, so fordert der Rechtsanwalt von Gravenreuth, dass vor dem Setzen von Links kostenpflichtige Markennamenrecherchen durchgeführt werden.

Neben diesen geschilderten Schwierigkeiten gibt es noch unzählige andere ungelöste Probleme, deren Tragweite aufgrund sich ändernder Technik noch nicht absehbar ist. Im weiteren Verlauf werden die vorhandenen rechtlichen Mittel in Deutschland, der EU und der USA erläutert.

³Diese Behauptung ist inkorrekt, da sechs Klicks notwendig waren, um die besagte Seite zu erreichen.

2 Gesetzgebung in Deutschland

In Deutschland gibt es zwei herausragende Rechtsvorschriften, die viele möglichen Rechtsstreitfälle im Internet abdecken. Diese sind das *Strafgesetzbuch* (StGB) und das *Bundesdatenschutzgesetz* (BDSG).

2.1 Strafgesetzbuch

“Schadhafte“ Handlungen, die Daten und Computeranlagen betreffen, sind im *Strafgesetzbuch* (StGB) unter den folgenden Paragraphen aufgeführt:

§ 202a *Ausspähen von Daten*

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

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch oder magnetisch unmittelbar gespeichert sind oder übermittelt werden.

§ 303a *Datenveränderung*

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

(2) Der Versuch ist strafbar.

§ 303b *Computersabotage*

Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er

(1) eine Tat nach § 303a Abs. 1 begeht oder

(2) eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

2.2 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) wurde am 20. Dezember 1990 verabschiedet. Es hat den Zweck, den Einzelnen vor Beeinträchtigungen in seinem Persönlichkeitsrecht durch den Umgang mit seinen personenbezogenen Daten zu schützen. [Bundes95, S. 7] Eingeführt wurde das Gesetz in Reaktion auf das sogenannte Volkszählungsurteil⁴ vom 15.12.1983. In diesem hat das

⁴Aufgrund einer anstehenden Volkszählung wurde das sogenannte Volkszählungsgesetz erlassen, in dem die Erhebung detaillierter personenbezogener Daten erlaubt wurde. Dagegen wurde vor dem Bundesverfassungsgericht erfolgreich geklagt. <http://www.datenschutz.berlin.de/gesetze/sonstige/volksz.htm>

Bundesverfassungsgericht aus den Art. 1 und 2 des Grundgesetzes den Begriff der *informellen Selbstbestimmung* abgeleitet.

2.2.1 Informelle Selbstbestimmung

Aufgrund der weltweiten Einmaligkeit dieses Urteiles und der Wichtigkeit bezüglich datenschutzrechtlicher Bestimmungen wird nachfolgend das Urteil und vor allem die zentrale Begründung des Gerichts wiedergegeben. [Bundes95, S. 82]

- Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über persönliche Daten zu bestimmen.
- Einschränkungen dieses Rechts auf informelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen, gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

Zur Begründung schreibt das Bundesverfassungsgericht: “ *Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.* “ [Bundes95, S. 8]

2.2.2 Inhalt des Bundesdatenschutzgesetz

Mit obigem Schutzanspruch stellt das BDSG allgemeine datenschutzrechtliche Grundregeln auf. Insbesondere werden folgende Rechte der Betroffenen geregelt:

§ 19 *Recht auf Auskunft*

§ 20 *Recht auf Berichtigung, Sperrung oder Löschung*

§ 21 *Recht auf Anrufung des Bundesbeauftragten für den Datenschutz*

Weiter bestimmt das Gesetz in dem § 43 die Strafvorschriften. In diesen heißt es, wer unbefugt von diesem Gesetz geschützte, personenbezogene Daten, die nicht offenkundig sind, speichert, verändert, übermittelt, bereithält oder beschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft. [Bundes95, S. 79]

2.3 Weiterführende Rechtsvorschriften

Zusätzlich können noch weitere Rechtsvorschriften auf das Internet bezogen werden. Einige herausragende werden nachfolgend auszugsweise beschrieben.

2.3.1 Telekommunikationsgesetz

Im August 1996 trat das *Telekommunikationsgesetz* (TKG) in Kraft, um die rechtlichen Rahmenbedingungen für einen Wettbewerb im Telekommunikationsmarkt zu schaffen. Daneben enthält das Gesetz Regelungen zur Sicherstellung des Datenschutzes und des Fernmeldegeheimnisses.

In § 3 des TKG werden im Abs. 2 durch den Ausdruck „Betreiben von Übertragungswegen“ auch die Provider in den Einflußbereich des Gesetzes einbezogen. In § 85 erstreckt sich der Anwendungsbereich des Fernmeldegeheimnisses auf den Inhalt einer Telekommunikation und die Tatsache ob jemand an einem Telekommunikationsvorgang beteiligt war. Die notwendigen, datenschutzrechtlichen Maßnahmen für diese Unternehmen werden in § 89 des TKG beschrieben. Insbesondere bestimmt dieser Paragraph, welche Daten gespeichert bzw. nicht gespeichert werden dürfen. Ein Verstoß kann nach § 94 mit Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe bestraft werden.

2.3.2 Teledienstgesetz

Für die Anbieter zur Nutzung des Internets ist vor allem die Frage der Haftung für die angebotenen Inhalte besonders wichtig. Hier sagt der § 5 des Teledienstgesetzes (TDG) im Absatz 2 und 3, dass Zugangsdienste für angebotene, fremde Inhalte nur dann haftbar gemacht werden können, wenn sie davon Kenntnis haben und die Sperrung technisch möglich und zumutbar ist.

2.3.3 Teledienstdatenschutzgesetz

Die Vorschriften des Teledienstdatenschutzgesetzes (TDDSG) sind zum Schutz personenbezogener Daten von Telediensten. So bestimmt zum Beispiel der § 3 (Grundsätze für die Verarbeitung personenbezogener Daten), dass personenbezogene Daten nur zur Durchführung von Telediensten erhoben oder verarbeitet werden dürfen, wenn ein Gesetz oder der Nutzer dies explizit erlauben (Abs. 1). Dabei gilt es, so wenige Daten wie möglich zu erheben oder zu nutzen (Abs. 3). Weiterhin ist der Nutzer vor der Erhebung über Art, Umfang, Ort und Zweck der Erhebung und Nutzung seiner Daten zu unterrichten. Weitere relevante Paragraphen dieses Gesetzes sind:

§ 4 *Datenschutzrechtliche Pflichten des Diensteanbieters*

Dem Nutzer muß die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym ermöglicht werden, soweit dies technisch möglich und zumutbar ist. (Abs. 4) Nutzungsprofile sind nur bei der Verwendung von Pseudonymen zulässig und dürfen in keinem Fall mit Daten über den Träger des Pseudonyms zusammengeführt werden.

§ 5 *Bestandsdaten*

Der Diensteanbieter darf personenbezogene Daten eines Nutzers erheben, verarbeiten und nutzen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses erforderlich sind (Bestandsdaten). Eine Nutzung dieser Daten für Beratung, Werbung oder Marktforschung ist nur mit ausdrücklicher Einwilligung der Nutzer zulässig.

2.3.4 Sonstige Gesetze und Verordnungen

Neben den hier vorgestellten Verordnungen, gibt es in Deutschland eine Reihe weiterer Gesetze, die in der einen oder anderen Weise den Datenschutz behandeln. Da sich diese nach den Vorschriften in dem BDSG richten, werden sie nachfolgend nur ansatzweise vorgestellt.

- *Telekommunikationsdienstunternehmen-Datenschutzverordnung*
Diese Verordnung vom 12. Juli 1996 regelt den Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten.
- *Telekommunikations-Kundenschutzverordnung*
In dieser Verordnung vom 11. Dezember 1997 werden die Rechte und Pflichten der Anbieter und Kunden von Telekommunikationsdienstleistungen geregelt.

- *Postdienstunternehmen-Datenschutzverordnung*

Diese Verordnung regelt den Schutz personenbezogener Daten der am Postverkehr Beteiligten.

Für bestimmte Fälle im Umgang mit Daten sind Ausnahmeregelungen getroffen worden. Diese werden in einzelnen Gesetzen genauer umrissen. Eine Liste dieser Gesetze und Verordnungen läßt sich auf den Internetseiten des Bundesbeauftragten für Datenschutz einsehen.⁵

3 Europäische Regelungen

Zum StGB vergleichbare Bestimmungen wurden vom Europäischen Parlament nicht getroffen, aber mit der Richtlinie 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten wurde der Datenschutz europaweit geregelt, um mögliche Nachteile für den zwischenstaatlichen Handel zu vermeiden.⁶ Da auch hier viele Bestimmungen dem BDSG ähneln, werden diese nicht gesondert behandelt. Die hier aufgelisteten Absätze verdienen besondere Beachtung und haben zum Teil international für erhebliche Schwierigkeiten gesorgt.

In dem Abschnitt III, Artikel 8, Abs. 1 wird die Verarbeitung personenbezogener Daten, aus denen rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben unter sagt, außer die Betroffenen stimmen ausdrücklich zu.

Der Abschnitt IV regelt die Übermittlung personenbezogener Daten in Drittländer, insbesondere in solche, die über kein „angemessenes“ Schutzniveau⁷ der Daten verfügen. Im Klartext bedeutete diese Bestimmung, dass z.B. keine Daten an Länder wie die USA übermittelt werden dürfen, da ein allgemeingültiger Datenschutz nicht gesetzlich geregelt ist.

Da diese Vorschrift den Handel zwischen den USA und den europäischen Ländern erschweren könnte, wurde seit ca. zwei Jahren zwischen der EU und dem U.S. Department of Commerce verhandelt, um für die personenbezogenen Daten der europäischen Bürger ein angemessenes Schutzniveau erreichen zu können. Das eigentliche Problem dieser Verhandlung ist, dass in den USA der nationale Konsens eine zentrale Datenschutzbehörde nicht zuläßt, da

⁵<http://www.bfd.bund.de/information/gesetz.html>

⁶<http://www.datenschutz-berlin.de/infomat/heft24/dde.htm>

⁷Dieser Begriff ist näher bestimmt in Absatz 2 anhand vorhandener Sicherheitsmaßnahmen, Rechtsnormen, usw. .

dieser kein Vertrauen entgegengebracht werden würde.⁸ Im Zuge dieser Verhandlung wurde das sogenannte „*Sichere-Hafen-Prinzip*“ formuliert, in dem zu bestimmten Unternehmen, die sich freiwillig Datenschutzbestimmungen auferlegen, der Datentransfer erlaubt ist.⁹

4 Außereuropäische Regelungen

Im Vergleich zu Europa fällt sofort auf, dass ein genereller Datenschutz keine Selbstverständlichkeit ist. Nur in acht weiteren Ländern gibt es Datenschutzbehörden, z.B. Australien, Israel, Kanada, Taiwan.¹⁰ Insofern kann man ohne weiteres sagen, dass Europa bezogen auf Datenschutz eine führende Rolle einnimmt.

4.1 US-Amerika

Datenschutzrechtlich gibt es in den USA, bis auf wenige Ausnahmen, keinerlei Regelungen. Vorhandene Ausnahmen betreffen echte Sonderfälle und sind mühsam vor Gericht erstritten worden, wie z.B. das Recht einer Person, den Aufdruck seines Gesichtes auf die Etiketten von Flaschen zu untersagen, oder, dass Videotheken nicht die Titel der geliehenen Filme personenbezogen verkaufen dürfen. Es ist beispielsweise üblich, dass Supermärkte die Information, wer was gekauft hat, an andere Unternehmen weitergeben, z.B. Namenslisten von Zigarettenkäufern an Krankenkassen. In einem anderen Fall werden aktuelle Positionen von Mobiltelefonbesitzern an große Konzerne verkauft, so dass diese dem Besitzer eines Mobiltelefons eine SMS über besonders günstige Angebote schicken, wenn er in die Nähe einer ihrer Filialen kommt.

Computereinbrüche und Sabotage wurden in den Vereinigten Staaten bis 1986 als Hausfriedensbruch betrachtet. Dies änderte sich, als der *Computer Fraud and Abuse Act* verabschiedet wurde.¹¹ In diesem werden bestimmte Handlungen, wie Einbruch, Störung des Ablaufes oder Beschädigungen von Computersystemen, die als „Federal-Interest-Computer“ bezeichnet sind, mit einer Strafe bis 20 Jahre Gefängnis oder einer Geldstrafe geahndet. Unter diesen Begriff fallen alle Computer, die für das Finanzinstitut oder die Regierung vorgesehen oder solche die über Staatsgrenzen hinweg zusammengeschlossen

⁸Eine Umfrage von 1996 unter erwachsenen Amerikanern ergab, dass 74 % der Befragten davon überzeugt sind, dass die Regierung regelmäßig an Verschwörungen beteiligt ist. [Rötzer00]

⁹http://europa.eu.int/comm/internal_market/en/media/dataprot/news/shprinciples.pdf

¹⁰<http://www.datenschutz-berlin.de/sonstige/behoerde/internat.htm>

¹¹<http://www4.law.cornell.edu/uscode/18/1030.html>

sind, also alle am Internet angeschlossenen Computer. [Anon99, S. 761] Die meisten Staaten der USA haben dieses Gesetz übernommen.

Teil III

Relevante Basistechnologien

Bevor auf die verschiedenen Angriffe und Gegenmaßnahmen eingegangen wird, besteht die Notwendigkeit, bestimmte grundlegende Begriffe und Technologien zu erläutern, um so eine gleiche Wissensbasis annehmen zu können. Zur Erleichterung des Verständnisses wird in diesem Abschnitt nur eine kurze, oberflächliche Betrachtung der wichtigsten Sachverhalte vorgenommen. Eine weiterführende Darstellung erfolgt im Anhang.

5 Protokolle

Zum Verständnis von Netzprotokollen ist es wichtig, zwischen einer *Nachricht* als solche und einem *Paket* zu unterscheiden. Mit Nachricht ist allgemein eine vollständige Dateneinheit einer beliebigen Art, die von einem Prozeß zu einem Ort gesendet wird, gemeint. Eine Zahlungsanweisung im Internet stellt dabei beispielsweise genauso eine Nachricht dar, wie eine EMail. Ein Paket ist ein einzelner Datenblock, der im Netz zwischen zwei Orten übertragen wird. Eine Nachricht wird beim Transport über das Internet falls sie zu groß ist, in verschiedene Pakete zerlegt, die jedes für sich zum Zielort gelangen und dort wieder zu einer Nachricht zusammengesetzt werden. [Smith98, S. 26f]

Protokolle sind notwendig, um Pakete korrekt transportieren und an dem Zielort richtig zusammensetzen zu können. Sie regeln den Austausch von Nachrichten zwischen Kommunikationspartnern und machen diesen somit erst möglich. Beim Telefonieren wird beispielsweise ein solches, sehr komplexes Protokoll genutzt. Neben der technischen Seite gibt es eine soziale Protokollebene mit einer geregelten Verbindungsanfrage, -annahme, -kollision, einem Header, in diesem Fall die Begrüßung mit Höflichkeitsfloskeln, und der eigentlichen Nachricht. Dazu kommen Umgangsformen wie z.B. den Anderen ausreden lassen und so etwas Fundamentales, wie die genutzte Sprache. [Santifaller93, S. 20]

6 Datenübertragung im Internet

Die im Internet eingesetzten Protokolle wurden ab 1968 entwickelt. Sie werden in sogenannten *Request for Comments* (RFC) beschrieben und lassen sich in vier Schichten, den sogenannten TCP/IP Protokollschichten einteilen. [Fuhrberg98, S. 9] Wird ein Datenpaket verschickt, so wird dieses von einer Protokollschicht zur nächsten übergeben, bewegt sich also sozusagen

nach unten, wird dann übertragen und wandert am Ziel wieder durch alle Protokollschichten nach oben. Jede Protokollebene kommuniziert dabei mit der gleichen Ebene auf der anderen Seite unter Rückgriff auf die unteren Schichten. Die beiden derzeit gebräuchlichsten Protokolle TCP und IP und ihre Header sind im Anhang genauer erläutert.

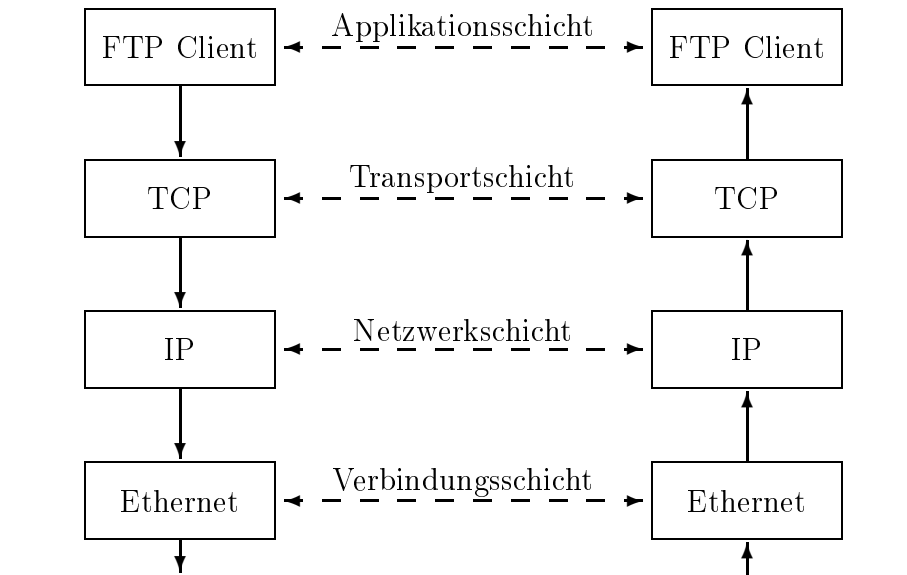


Abbildung 1: Transfer eines FTP-Datenpaketes

1. **Verbindungsschicht:** Diese beinhaltet die Treiber des Betriebssystems und die der korrespondierenden Netzwerkkarte. Sie stellt die Schnittstelle zur Hardware dar. [StevensI94, S. 2] Ein Beispiel für diese Schicht ist das weit verbreitete Ethernet-Protokoll. [Fuhrberg98, S. 9]
2. **Internet- oder Netzwerkschicht:** Hier wird die Bewegung der Datenpakete im Internet geregelt. Verwendete Protokolle in dieser Schicht sind beispielsweise das *Internet Protocol* (IP) und das *Internet Control Message Protocol* (ICMP). [StevensI94, S. 2]
3. **Transportschicht:** In dieser Schicht wird ein Datenfluß zwischen zwei Computern ermöglicht. Das *Transmission Control Protocol* (TCP) und das *User Datagram Protocol* (UDP) gehören zu dieser Schicht. [StevensI94, S. 2]
4. **Anwendungsschicht:** Diese behandelt die Details einer beteiligten Applikation, wie z.B. Telnet, FTP oder das *Domain Name System*. [StevensI94, S. 2]

Bei der geschilderten Kommunikation zwischen zwei Partnern wird das Datenpaket, wie erläutert, durch die einzelnen Protokollschichten bewegt, wobei jede ihren eigenen Datenkopf (Header) anfügt, um mit der jeweiligen anderen Schicht Daten austauschen zu können. So wird ein Datenpaket auf dem Weg zum Zielrechner immer größer. Überschreitet es dabei eine bestimmte, eingestellte Größe, so wird es auf der entsprechenden Ebene einfach in zwei oder mehr Pakete zerlegt, die dann einzeln übertragen werden. Folgendes Bild soll die Kapselung verdeutlichen: [Hartmann, Punkt 2]

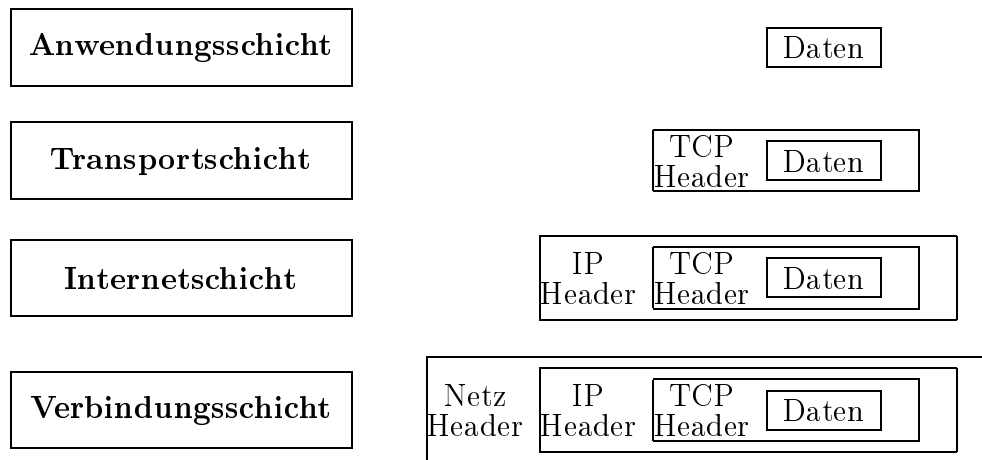


Abbildung 2: Protokoll Kapselung

7 Aufbau des World Wide Web

Das World Wide Web entstand aus einer von Tim Berners-Lee gegründeten Initiative, mit dem Ziel das Internet für einen Informationsaustausch zwischen Wissenschaftlern zu nutzen. Ziel dieser Initiative war es, Dokumente online zur Verfügung zu stellen und solche Konzepte, wie Hypertextfunktionalität und dadurch Verweise auf andere Dokumente zu ermöglichen. [Münz98, tbad.htm]

Das World Wide Web (WWW) basiert heute auf vier grundlegenden Konzepten: [HTML97, S. xii]

1. Mit Hilfe der sogenannten **Uniform Resource Locator (URL)** werden Dateien, wie z.B. Bilder oder Texte (allgemein als Ressourcen bezeichnet) adressiert.
2. Die **Hypertext Markup Language (HTML)** ist die Sprache, in der WWW Dokumente geschrieben sind.

3. Das **Hypertext Transfer Protocol (HTTP)** wird genutzt, um Hypertext Dokumente über das Internet zu senden.
4. Durch das sogenannte **server-side resource processing** erhält ein Nutzer die Möglichkeit mit Ressourcen auf dem Server zu interagieren.

7.1 Uniform Resource Locator

Dieser stellt das gebräuchliche Adressformat im Internet dar und spezifiziert einen Ort und wie darauf zugegriffen wird. Entsprechend besteht eine URL, wie z.B. **http://www.beispiel.de/shareware/index.html** aus mehreren Teilen. [HTML97, S. 341ff]

- An erster Stelle steht das genutzte Protokoll, mit dem die Anfrage an den Server gestellt und auch gleichzeitig das erwartete Format der Antwort spezifiziert wird. In diesem Beispiel ist dies HTTP. Andere mögliche Protokolle sind ftp, https, telnet oder wais. [HTML97, S. 349]
- Danach folgt mit `www.beispiel.de` der Name der Internet Domain und somit der Ort des Zielservers. Dieser Name wird mit Hilfe des Domain Name Systems (DNS) in eine IP-Adresse umgewandelt, die nötig ist, um Datenpakete über das Internet verschicken zu können. An dieser Stelle kann auch direkt die IP Adresse mit `http://207.201.156.106` angegeben werden.
- Optional kann die Port Nummer des genutzten Protokolles angegeben werden, z.B. `http://www.beispiel.de:80`. Wird kein Port angegeben, so gilt die Grundeinstellung abhängig von dem gewählten Protokoll (siehe *well known ports*).
- Der Verweis auf die Ressource befindet sich am Ende der URL. In dem Beispiel ist dies `/shareware/index.htm`. Hier wird auf die Datei `index.htm` in dem Verzeichniss `shareware` verwiesen. Folgt keine genaue Angabe der Ressource, so wird automatisch die im Webservers eingestellte Datei angeboten.

7.2 Hypertext Markup Language

Die *Hypertext Markup Language* (HTML) hat die Aufgabe, die logischen Bestandteile eines Dokuments (Layout) zu beschreiben. Dazu enthält sie Befehle zum Markieren und Darstellen typischer Elemente eines Dokumentes. [Münz98, `tbae.htm`] Der Vorteil von HTML Dateien ist ihre hohe Portabilität. So kann eine HTML Datei mit Hilfe eines Internet-Browser auf praktisch jeder beliebigen Plattform dargestellt bzw. mit jedem dort vorhanden Editor geöffnet und bearbeitet werden.

7.2.1 Aufbau

Eine HTML Datei besteht grundsätzlich aus zwei Teilen: [Münz98, tcab.htm]

- **Header:** Dieser enthält Angaben zu Titel, Autor, Inhalt u.a., im Folgenden als Metadaten bezeichnet.
- **Body:** Dieser enthält den eigentlichen, angezeigten Text und Bilder.

Diese Abschnitte werden mit Befehlen eingeleitet und beendet. Dazu kommt eine Einleitung am Anfang der Datei, damit der Internet-Browser diese als HTML Datei erkennt. Die dazu notwendige Befehlsstruktur ist:

```
<html>
  <head> WIRKUNGSBEREICH </head>
  <body> WIRKUNGSBEREICH </body>
</html>
```

7.2.2 Ausgewählte Elemente

In dem weiteren Text dieser Ausarbeitung wird wiederholt ein Bezug zu bestimmten HTML-spezifischen Befehlen, sogenannten *Tags*, hergestellt. Tags werden durch spitze Klammern markiert. Fast alle HTML Befehle haben ein Start- und ein Endtag, die den Wirkungsbereich umschließen. [Münz98, tcaa.htm]

Verwendete Befehle sind:

- **IMG Tag**, Syntax: ``
Der Internet-Browser lädt automatisch das Bild `Name` aus dem Verzeichnis `Quelle`.
- **A HREF Tag**, Syntax: `Text`
Durch Anklicken von `Text` wird der Nutzer zu dem `Ziel` gebracht.

7.3 Hypertext Transfer Protocol

Das *Hypertext Transfer Protocol* (HTTP) unterstützt den Datenaustausch mit Mechanismen, wie z.B. die Bereitstellungen von Informationen über den Status einer Verbindung (erfolgreich oder nicht) oder die Art der versendeten Daten und deren Methoden. [HTML97, S. 369] Es ist ein Protokoll der Anwendungsschicht mit dem Daten zwischen einem HTTP-Server (Web Server) und einem HTTP-Client (Internet-Browser) übertragen werden können. [Fuhrberg98, S. 33]

Das HTTP ist in der Version 1.0 als zustandsloses Client/Server Protokoll aufgebaut¹², da bei dem Beenden einer Verbindung von dem Server keine Daten über diese im Speicher gehalten werden. Dieses konstruktionsbedingte Merkmal ist notwendig, da eine Verbindung im Netz zu jedem beliebigen Zeitpunkt, z.B. aufgrund einer Handlung des Nutzers oder eines Programmfehlers, zusammenbrechen kann und nicht wieder neu aufgebaut wird. [RFC1945, 1.3]

Eine HTTP Sitzung erfolgt in vier Schritten:

1. **Verbindungsaufbau:** Das Clientprogramm, typischerweise ein Internet-Browser, öffnet eine Verbindung, indem es einen Webserver kontaktiert.
2. **Request:** Der Client sendet eine Nachricht an den Server, die einen HTTP Header beinhaltet, in dem die Parameter dieser Verbindung festgelegt sind, z.B. die zu nutzende Methode oder welche Dokumententypen akzeptiert werden.
3. **Response:** Der Server antwortet auf die Anfrage des Clients.
4. **Verbindungsabbau:** Der Server beendet die Sitzung ohne danach irgendwelche Informationen über die Sitzung im Speicher zu halten.

Dieses Sitzungsmodell wird für jede Transaktion angewandt. Wenn z.B. auf einer Internetseite mehrere Bilder dargestellt werden, so wird jedes einzelne Bild mit dem obigen Verfahren geladen.

Der genaue Aufbau eines HTTP Headers wird im Anhang erläutert.

7.3.1 Cookie

Ein Cookie¹³ wird per Set-Cookie Befehl in einem HTTP Header übertragen und besteht aus einer einfachen Zeichenfolge, die dauerhaft von dem Internet-Browser desjenigen, der das Cookie erhält, gespeichert wird. [Whalen, 1.1] Diese Zeichenfolge beinhaltet gemäß der Spezifikation von Netscape [Netscape] folgende Variablen:

- **Name** - Name des Cookies
- **expires** - spezifiziert, ab wann der Cookie vom Internet-Browser nicht länger gespeichert oder abgegeben wird

¹²In der Version 1.1 kann in dem Request angegeben werden, dass eine Verbindung solange geöffnet ist, bis diese explizit beendet wird. [HTTP00, S. 4]

¹³engl. cookie: Keks, Plätzchen

- **domain** - muss z.B. im Format beispiel.de vorliegen und beschreibt, an wen das Cookie abgegeben wird. Dies geschieht nur dann, wenn die gespeicherte Domain mit der aktuellen übereinstimmt.
- **path** - wird benutzt, um einen Bereich der Domain benennen zu können, in der das Cookie aktiv ist. Der mögliche Eintrag „\“ erlaubt uneingeschränkten Zugriff innerhalb dieser Domain.
- **secure** - wenn ein Cookie so markiert ist, dann wird es nur über sichere Kanäle, also verschlüsselt, übertragen.

Von Netscape werden Cookies in die Datei cookie.txt gespeichert. Der Internet Explorer dagegen hinterlegt sie in dem Ordner \windows\cookies.

8 Das Domain Name System

Im Internet hat jeder Computer, um Datenpakete überhaupt erhalten zu können, eine eindeutige Adresse, an die Daten zugestellt werden. Diese sogenannte *Medium Access Control* (MAC) Adresse ist fest in der Netzwerkkarte eines Computers verankert. Damit werden Datenpakete auf der untersten Protokollschicht zugeordnet. Das darüber liegende Internet Protokoll (IP) verfügt mit den sogenannten *IP-Adressen* über einen eigenen Adressraum. Diese stellen eine übergeordnete Adressierung dar und werden immer auf die Hardwareadresse abgebildet. Die IP-Adresse ergibt sich aus dem Netz, in dem sich der Computer gerade befindet und ist ebenso weltweit eindeutig. Sie besteht generell aus zwölf¹⁴ Zahlen angeordnet in Vierergruppen, durch einen Punkt getrennt, z.B. 207.201.156.106. Da sich Menschen Namen im Vergleich zu Zahlen besser merken können, wurde das Domain Name System (DNS) geschaffen, mit dem Ziel sogenannte Domain Namen, wie z.B. www.beispiel.de, in die benötigten IP Adressen umzuwandeln. Dieser Vorgang wird *domain name lookup* genannt und findet im Internet für jeden auf Domain Namen basierenden Zugriff statt.

Für die Umwandlung sind sogenannte Domain Name Server zuständig. Bei einer Anfrage geben diese die zugehörige Adresse bekannt. Ermöglicht wird dies durch eine Datenbank auf diesen Servern, in der die IP Adressen und Domainnamen aller Hosts eines Netzes eingetragen sind. Bei einer Anfrage überprüft der Server in seiner Datenbank den Namen. Ist diese Suche erfolgreich, schickt er die Adresse an den Client zurück. Bei Mißerfolg, d. h. wenn er nicht den richtigen Eintrag hat, übergibt er die Anfrage an den übergeordneten Server. Dieser Prozeß setzt sich solange von Name Server zu Name Server

¹⁴Führende Nullen in den einzelnen Segmenten, wie im Beispiel 127.0.0.1, werden nicht ausgeschrieben.

fort, bis die IP-Adresse gefunden wurde, oder der Name Server der Top-Level Domain meldet, dass der gesuchte Name nicht existiert. [HeiseF97, S. 347]

Die über die Erde verteilten DNS Server sind untereinander verbunden, damit eine Anfrage an den zuständigen Server weitergegeben werden kann, falls der aktuelle Server die Antwort nicht kennt. Um die Effizienz zu steigern speichern alle Name Server die IP-Adressen schon einmal erfragter Domains in einem lokalen Cache, damit bei wiederholten Anfragen nach dem gleichen Ziel, die Frage sofort beantwortet werden kann. [Lauer98, S. 73f]

Es gibt verschiedene Arten von Name Servern: [HeiseF97, S. 351]

- Ein **Primary-Server** ist der Hauptserver einer Domain. Er kann jede, diese Domain betreffende Frage beantworten.
- Der **Secondary-Server** liefert wie der Hauptserver verbindliche Antworten und lädt seinen Datenbestand, der bei Bedarf aktualisiert wird, vom Primary-Server.

Der einen Computer beschreibende Name im Internet setzt sich aus dem Rechnernamen gefolgt von einem Punkt und dem Domainnamen zusammen. Dieser kann aus verschiedenen Teilen bestehen, die durch Punkte getrennt sind. [Fuhrberg98, S. 27] So bezeichnet `www.beispiel.de` den allgemeinen Web Server der Domain `beispiel.de`, während `gustav.uni-paderborn.de` den Rechner `gustav` der Domain `uni-paderborn.de` adressiert.

Da bei einigen Millionen im Internet erreichbaren Computern eine Orientierung oder Zuordnung nur sehr schwer möglich ist, hat sich zur Erleichterung eine hierarchische Namensstruktur durchgesetzt. Die oberste Ebene wird *top level domain* genannt. Von diesen gibt es über hundert, ein paar der wichtigsten Namen zeigt die folgende Tabelle: [Lauer98, S. 74]

<i>Name</i>	<i>Zuordnung</i>
.arpa	Reverse Lookup
.com	kommerzielle Organisationen
.de	Länderkürzel für Deutschland
.gov	US-Behörden
.mil	US-Militär
.net	Netzwerk-Betreiber

Neben der Funktion, zu jedem Rechnernamen die zugehörige Internet-Adresse zu liefern (domain name lookup), besitzt das DNS noch die Aufgabe, auch die umgekehrte Auflösung, d.h. die Abbildung von Adressen auf Rechnernamen, zu ermöglichen (*reverse dns lookup*). Hierzu wird die Top-Level Domain `arpa`

genutzt. [Fuhrberg98, S. 28]

Die Daten, die in Verbindung mit Domain Namen stehen, sind in *Resource Records* (RR) gespeichert. Diese RR's enthalten die eigentlichen Informationen für den Domain Name Server sowie eine Lebenszeit, genannt (*time to live*), nach deren Ablauf der Eintrag gelöscht wird. Eine genauere Betrachtung der RR erfolgt im Anhang.

9 EMail

Der EMail Dienst des Internets ist bezüglich seines Aufbaus relativ einfach. Eine Nachricht wird in Form eines Textpaketes anhand seines Headers von einem Computer zu einem anderen gesendet. Für jedes Zeichen der Nachricht stehen sieben Bit zur Verfügung, so dass nur die Standardzeichen des *ASCII* Codes übertragen werden können, also keine Sonderzeichen wie z.B. Ä, Ü, Ö usw. Um Sonderzeichen und andere Inhalte, wie Programme oder Bilder verschicken zu können, wurde das sogenannte UUencoding und dann das neuere *Multipurpose Internet Mail Extensions* (MIME) Verfahren entwickelt, die besondere Zeichen auf die vorhandenen sieben Bit abbilden. [Smith98, S. 86, S. 211]

Soll eine EMail im Internet verschickt werden, baut der MailClient des Senders eine Verbindung zu seinem MailProvider auf und übergibt diesem die Mail mittels des *Simple Mail Transfer Protocols* (SMTP). Der Provider verschickt die Mail weiter an die passende Domain, gemäß der im Header angegebenen Adresse. Dort bleibt sie gespeichert, bis sie mittels des *Post Office Protocols Version 3* (POP3) heruntergeladen wird. [Lauer98, S. 205] Eine Adresse besteht aus einem Nutzernamen und einem Domainnamen, getrennt durch ein @. Beispielsweise adressiert test@beispiel.de den Nutzer test in der Domain beispiel.de. Eine vollständige Beschreibung von SMTP läßt sich im *Request for comments* (RFC) 821 nachlesen. [RFC821] Unter anderem unterstützt dieses Protokoll folgende Befehle:

- **HELLO**: baut eine Verbindung zu dem MailServer auf.
- **MAIL FROM**:bereitet die Mail vor.
- **RCPT TO**: bezeichnet den Empfänger.
- **DATA**: gibt den Mail Inhalt an.
- **QUIT**: beendet die Sitzung.

Teil IV

Angriffsarten

Im Internet sieht sich ein Nutzer den vielfältigsten Angriffsformen ausgesetzt. Auf der Seite der Gegner befinden sich unterschiedlichste Personengruppen, wie z.B. jugendliche Hacker, die einfach Spaß an der Zerstörung haben, profitmäßig vorgehende Betrüger, große Firmen, die möglichst viel über potentielle Kunden erfahren möchten und weitere. Gemein ist allen Angreifern, dass sie in den meisten Fällen im Vergleich zu normalen Nutzern über sehr viel mehr Basiswissen und technisches Know-how verfügen. Unterstützung findet der Nutzer wiederum bei Organisationen und einzelnen Personen, die versuchen, ihm möglichst durchdachte und sichere Konzepte umgesetzt in bestimmte Programme zu verkaufen oder kostenlos zur Verfügung zu stellen. Aufgrund der ständig währenden Angriffe und Abwehrmaßnahmen hat sich dieser „Kampf“ auf eine so komplexe Ebene bewegt, dass die meisten Nutzer technisch überfordert sind.

Viele Abwehrmaßnahmen sind zwischenzeitlich so ausgeklügelt, dass die meisten erfolgreichen Angriffe auf falsche Einstellungen von Programmen oder einfache Unkenntnis der Nutzer zurückzuführen sind. Um dieses Angriffsstor zu schließen, werden nachfolgend zuerst die Angriffe und dann mögliche Abwehrmaßnahmen erläutert, mit dem Ziel, dass ein normaler Nutzer in der Lage ist, häufige Massenangriffe zu erkennen und sich passend zu schützen.

10 Begriffliche Abgrenzung

Zum Verständnis trenne ich die Begriffe Schutz und Sicherheit gemäß Heiß [Heiß99, 1-7] wie folgt:

Sicherheitsmaßnahmen: Die Gefahr wird an der Quelle unwirksam gemacht, so dass sie gar nicht mehr entstehen kann. Diese Maßnahmen sind meistens gründlicher, aber auch aufwendiger als vergleichbare Schutzmaßnahmen. Zur Vermeidung der vielen Verkehrstoten wäre z.B. eine Sicherheitsmaßnahme, die Nutzung von Autos zu verbieten.

Schutzmaßnahmen: Diese vermeiden nicht die Entstehung einer bedrohlichen Situation, sondern verhindern, dass diese eine Auswirkung auf das bedrohte Objekt hat. Diese Maßnahmen sind nicht so aufwendig, dafür aber auch nicht so grundsätzlich wie Sicherheitsmaßnahmen. Zu dem obigen Beispiel passend könnte man die Schutzmaßnahmen Airbags, Sicherheitsgurte oder Seitenaufprallschutz wählen.

Schutzwürdige Interessen aus der Sicht des Nutzers sind:

- **Integrität:** Schutz vor Beschädigungen oder unerwünschten Modifikationen von Daten, z.B. Schutz vor einem Programm, welches im Internet übertragene Daten beliebig ändert.
- **Vertraulichkeit:** Schutz vor unerwünschter Preisgabe oder Annahme veränderter Daten, z.B. Schutz vor Seiten im Internet, die vertrauenswürdige Seiten vortäuschen.
- **Verfügbarkeit:** Schutz vor unbefugtem Vorenthalten von Daten, z.B. Schutz vor einem Virus, der die Daten auf der Festplatte löscht.

Jeder Angriff hat das Ziel, einen oder mehrere der oben genannten Punkte zu unterlaufen. Folglich resultiert aus Angriffen ein direkter oder indirekter Schaden.

11 Angriff auf Vertraulichkeit: Datenspuren

11.1 Einleitung

Zu einer Zeit, in der in Talkshows intimste Details eines Lebens einem Millionenpublikum zugänglich gemacht werden und die öffentlich zugänglichen Informationen der meisten Homepages gegen Datenschutzgesetze verstoßen würden, stellt sich die Frage, ob so etwas wie ein Datenschutz überhaupt noch notwendig oder durchsetzbar ist.

Aus folgenden zwei primären Gründen ist der Datenschutz trotzdem gesetzlich sehr stark und umfassend geregelt. Erstens sollte jeder frei entscheiden können, wer welche persönlichen Informationen erhält und wie diese verwendet werden. Dieses Recht auf *informellen Selbstbestimmung* ergibt sich gemäß Bundesverfassungsgericht aus dem Grundgesetz. Und zweitens ist Datenschutz im Internet besonders wichtig, da Nutzer gezielt und automatisiert beobachtet werden können. In der realen Welt gehen einzelne Personen in der Masse unter und können nur mit erheblichem Aufwand verfolgt werden. Zudem sollen folgende Beispiele zeigen, dass für den Datenschutz Regelungen notwendig sind:

- „**Tracking-System findet verurteilte Pädophile**“, eine holländische Organisation will den Weg von verurteilten Pädophilen über das Internet verfolgbar machen. [SpiegelT00]

- **„Spielzeughändler wegen Verkauf von Kundendaten verklagt“**, der Internet-Spielzeughändler Toysmart.com ist von der US-Handelskommission FTC wegen Datenmissbrauchs verklagt worden. Das Unternehmen hat Kundendaten verkauft, obwohl deren vertrauliche Behandlung zugesichert worden war. [SpiegelV00]
- **„Der gläserne Konsument nimmt Formen an“**, die weltweit größte Online-Marketingagentur DoubleClick plant den Aufbau einer Datenbank, die Verbindungs- und Stammdaten von Konsumenten zusammenführt. [HeiseK00]
- **„Neues Überwachungszentrum und umfassende rechtliche Zugeständnisse“**, um die elektronische Kommunikation in England vollständig abzuhören, wird ein neues und für jede Kommunikation geeignetes Überwachungszentrum aufgebaut und den Geheimdiensten sowie den Strafverfolgern werden umfassende Rechte eingeräumt. [HeiseZ00] [HeiseL00]
- **„Echelon“**, dieses System wird von der US-amerikanischen National Security Agency (NSA) genutzt, um die weltweite internationale Kommunikation abzuhören. [Campbell00] Parallel wurde die NSA dazu ermächtigt, bei US-Geschäften mit ausländischen Vertragspartnern unterstützend tätig zu sein. [Christ00, S 67]
- **„Big Brother Bill“**, jeder Nutzer von Microsoft Office erhielt eine eindeutige ID, die sogenannte Globally Unique Identifier (GUID), womit es dem Konzern ermöglicht wurde, beobachtbare Bewegungen im Internet sowie erstellte Dokumente eindeutig zuzuordnen. [Siering99]

Wenn die Handlungen einer Person nicht elektronisch erfasst werden, so muß dies manuell erfolgen. Jemand muß der Person überallhin folgen, darf dabei nicht auffallen, Telefone müssen angezapft, Lauschgeräte installiert werden, usw. . Bewegt sich dagegen die Zielperson im Internet, hinterläßt jede Handlung automatisch elektronische Spuren, die mit Hilfe von Programmen ausgewertet werden können. Den Vorgang, eine Person soweit wie möglich elektronisch zu beobachten und die Ergebnisse dauerhaft zu speichern, wird als *tracking* bezeichnet.

Die Nachteile des Trackings für den Nutzer sind nicht sofort greifbar. Die Unternehmen werben damit, dass der Nutzer nur Vorteile hat, keine Massenmails oder uninteressante Werbung mehr, bessere Betreuung durch höhere Datenbasis, schnellere Reaktion bei einer Reklamation usw. . Ob diese angepriesenen Vorteile tatsächlich vorhanden sind, ist sehr zweifelhaft und noch nicht belegt. Eher scheint das Gegenteil der Fall zu sein. So müßten eigentlich die meisten Computerzeitschriften bei einem funktionierenden Support

der Hersteller eingestellt werden, da diese schwerpunktmäßig in ihren Artikeln Hilfestellung rund um den PC anbieten. Auch die Kaufunterstützungen und Serviceleistungen sind in den meisten Fällen bestenfalls mangelhaft. [HeiseGS00, S. 238] Sicher ist dagegen, dass die genaue Beobachtung der Kunden in erster Linie dem Unternehmen dient, da dieses kalkuliert mit den besseren Kenntnissen über mögliche Kunden, deren Wünsche abschätzen und so mehr verkaufen zu können. Mögliche und konkrete Nachteile des Trackings sind:

- Über viele Personen liegen genaue und automatisch bearbeitbare Daten vor. Eine beobachtete Person kann nicht kontrollieren oder verhindern, dass diese bewußt, wie z.B. durch Datenhandel [SpiegelV00] oder ungewollt, wie durch einen Datengau¹⁵ an Dritte weitergegeben werden. Der Nutzer hat keine Möglichkeit, den Transfer seiner Daten zu beobachten und verliert somit das ihm zugesprochene Recht auf informelle Selbstbestimmung. In Amerika gibt es keinen umfassenden Datenschutz, dadurch ist es beispielsweise üblich, dass Supermärkte Listen mit Zigaretenkäufern an Krankenversicherungen weitergeben. Ebenso überprüfen große Kreditkartenunternehmen anhand des Einkaufsprofils ihrer Kunden, ob Diebstahl oder Mißbrauch der Kreditkarte vorliegt. [Christ00, S. 146] Dazu müssen diese Daten langfristig gespeichert werden.
- Ein sogenannter „Big Brother“, der Zugriff auf die Datenbanksysteme hätte, könnte jede beliebige Information über eine bestimmte Person innerhalb von Sekunden gewinnen. Vor allem würde durch Automatisierbarkeit ermöglicht, alle Personen, die definierte Kriterien erfüllen, zu beobachten. Der mögliche Mißbrauch dieser Datensammlung würde totalitäre Systeme ermöglichen oder stärken.

Personenbezogene Daten lassen sich nach Buhlmann [Buhlmann96, S. 212ff] in drei Kategorien einteilen:

- **Inhaltsdaten:** Gemeint ist die eigentliche Nachricht, z.B. der Inhalt einer EMail, ein Artikel eines Diskussionsforum oder die Bestellung bei einem Online-Shop.
- **Stammdaten:** Dies sind personenbezogene Daten z.B. Name, Adresse, Bankverbindung, Geburtsjahr, Status, etc. .
- **Verbindungsdaten:** Hierbei handelt es sich um Informationen darüber, wer wann welchen Dienst von wo und wie lange nutzt oder genutzt hat.

¹⁵Am 4. Mai 2000 führte eine Sicherheitslücke bei Surf1 dazu, dass die Anmeldedatenbank mit knapp 20000 Kundendaten im Internet offen einsehbar war. Diese enthielt auch Bankverbindungen bzw. Kreditkarteninformationen. [HeiseSI00, S. 76]

Viele Kommunikationspartner verfügen über einen Teil der obigen Daten. So verfügen Telekommunikationsunternehmen beispielsweise, für ihre Abrechnungen über sämtliche Verbindungsdaten, während Online-Shops viele Inhaltsdaten und dazugehörige Stammdaten halten. Marketinggesellschaften wie z.B. DoubleClick verfügen wiederum über Verbindungsdaten. Die meisten Unternehmen versuchen ein möglichst vollständiges Kundenprofil zu erstellen und entsprechend die vorhanden Datenbestände mit verschiedenen Methoden zu vervollkommen. Mögliche Methoden werden im Weiteren genauer erläutert.

11.2 Datensammeln: passive Methoden

Unter den passiven Methoden des Datensammelns werden hier alle Methoden verstanden, die dazu führen, dass der Internetnutzer von sich aus Informationen, z.B. mittels Browsers durch den Besuch von Internetseiten, preisgibt und diese integraler Bestandteil der verwendeten Techniken, wie z.B. des Übertragungsprotokolls HTTP, sind. Bei dem Besuch von Seiten im Internet können z.B. nur Verbindungsdaten ermittelt werden. Erst wenn der Nutzer sich registrieren läßt bzw. anmeldet, gibt er Stammdaten oder Inhaltsdaten von sich preis.

11.2.1 Dynamische Elemente

Mit Hilfe von sogenannten dynamischen Elementen im Internet, wie z.B. Perl, ActiveX, Java oder Visual Basic lassen sich auf einfache Weise viele Verbindungsdaten gewinnen. Dies wird auf bestimmten Seiten im Internet, wie z.B. www.anonymizer.com oder mit dem für diese Arbeit konstruierten Programm `informationen.pl` demonstriert. An Informationen können dies unter anderem sein:

- die eigene erhaltene IP-Adresse und somit Informationen über den verwendeten Provider, bzw. über die Domain (und somit in vielen Fällen über das Land)
- das genutzte Betriebssystem, z.B. Windows 95 oder OS/2
- der verwendete Internet-Browser, z.B. Netscape, Internet Explorer
- der Computername
- die zusätzlich installierten plug-ins, wie z.B. Shockwave Flash oder RealPlayer

Die Preisgabe jeder einzelnen Information für sich bedeutet kein größeres Risiko, auch das mögliche Erhalten eines Werbebanners in der entsprechenden

Landessprache ist eher vernachlässigbar. Von Bedeutung ist, dass aufgrund der großen Anzahl der Informationen diese in ihren Ausprägungen dazu geeignet sind, die Bewegungen eines Nutzers im Netz zu beobachten.

So kann mit Hilfe der IP-Nummer, der Nutzer direkt wiedererkannt oder bei dem sogenannten IP-Sharing¹⁶ doch zumindest einer Gruppe zugeordnet werden. Möglich wäre dann eine weitere Aufteilung der Gruppe anhand der restlichen Merkmale mit dem Ergebnis, dass die Bewegungen eines Nutzers sehr detailliert aufgezeichnet werden können.

11.2.2 Cookie

Cookies sind generell reine Informationsdateien, die somit keinerlei schadhafte Funktionen ausüben können.¹⁷ Mit ihrer Hilfe läßt sich aber ein Internetnutzer eindeutig identifizieren, wodurch es sehr einfach wird, seinen Weg im Internet, das Clickverhalten und die Verweildauer auf einzelnen Seiten zu beobachten. Das heißt, Cookies ermöglichen das Sammeln von Verbindungsdaten.

Wenn jemand zum ersten Mal auf eine beliebige Seite einer bestimmten Domain gelangt, erhält er ein neues Cookie, mit möglichst langer Haltbarkeitsdauer und einer eindeutigen Identifizierungsnummer. In einer internen Datenbank wird diese Nummer als vergeben markiert und gleichzeitig wird für diese Nummer vermerkt, welche Seite wann besucht wurde. Folgt der Nutzer nun einem der angebotenen Links dieser Seite zu einer anderen der gleichen Domain, so wird bei Erreichen der neuen Seite das Cookie abgefragt und gleich ein identisches neu angelegt, um die Haltbarkeit des Cookies zu erhöhen. Mit den Daten des abgefragten Cookies erfährt der Seitenbesitzer die ID des Nutzers und überprüft diese in seiner Datenbank. Somit hat er nun drei Informationen: Welche beiden Seiten wurden besucht und wie lange auf der ersten Seite verweilt.

Eine Möglichkeit zum Mißbrauch der Cookies wurde auf den Internetseiten der Zeitung Spiegel [SpiegelW00] beschrieben. Die US-Regierung hatte zugegeben, die Privatsphäre der Bürger mit Hilfe von Cookies verletzt zu haben. Sobald jemand Anti-Drogen Banner von bestimmten Webseiten für Jugendliche anklickte, erhielt dessen Rechner ein Cookie, mit dem von nun an der Weg des Nutzers auf den Seiten der Drogenabteilung dokumentiert wurde.

¹⁶Bei diesem Verfahren teilen sich mehrere einen Internetzugang und treten mit dessen IP-Nummer im Internet auf. Typischerweise ist dies bei Firmen anzutreffen.

¹⁷Es ist aber sicherlich möglich, in Cookies einen schadhafte Code abzulegen und von einem anderen Programm ausführen zu lassen. [HeiseC00]

11.2.3 WebBug

Ein WebBug ist eine Grafik eingebunden durch das HTML IMG-Tag, auf einer Seite im Internet, mit der es möglich ist, die Bewegungen von Nutzern ähnlich zu beobachten, wie mit Hilfe von Cookies. Die WebBugs sind für den Nutzer meistens nahezu unsichtbar gestaltet, indem eine sogenannte „Ein-Pixel“ Grafik verwendet wurde. Ergänzend zur Größe kann die Farbe so gewählt sein, dass sie sich nicht vom Hintergrund abhebt. Jede andere (größere) Grafik, die von einem anderen Server stammt, insbesondere jedes Werbebanner, kann auch die Funktion eines WebBugs erfüllen.

Ein WebBug kann wie folgt erstellt sein:¹⁸

```
<IMG SRC="http://ad.doubleclick.net/ad/pixel.quicken/NEW"
width=1 height=1 border=0>
```

Dieser würde in folgender Weise funktionieren: Wählt der Nutzer eine Seite im Netz, erhält der Internet-Browser als Antwort eine Menge von Befehlen, durch deren Ausübung die gewünschte Seite entsteht. Ist ein Befehl wie oben dabei, lädt der Browser bei Befolgung dieses Befehls ein Bild von der Seite **http://ad.doubleclick.net/**. Dazu muß er eine Verbindung zu der angegebenen Seite aufbauen und übermittelt auf diese Weise bereits folgende Informationen: [SmithS99]

- die eigene IP Nummer,
- die URL der Seite, auf der der WebBug plaziert war,
- die Zeit, wann die Seite mit dem WebBug geladen wurde,
- welchen Internet-Browser der Nutzer benutzt und
- mögliche Cookies, die bei dem Nutzer plaziert wurden.¹⁹

Mit diesen Informationen kann DoubleClick nun ein Online Profil anlegen. Dieses beinhaltet genaue Angaben über den Nutzer, seine Wahl der Internetseiten und die Verweildauer.

Der eigentliche Unterschied zwischen WebBugs und Cookies liegt in dem Umgang des Internet-Browsers mit ihnen. Cookies sind in der Lage, mehr bzw. gezielter Informationen zu speichern und zu übermitteln, dagegen lassen sich

¹⁸Dieses entstammt der Domäne www.quicken.com. Eine Liste mit weiteren WebBugs ist auf den Internetseiten von Smith [Smith] einsehbar.

¹⁹Dies ist möglich, da bei dem Versuch ein Image zu laden ein zweiter, kompletter HTTP Request initiiert wird und somit der Seitenbesitzer Cookies abfragen bzw. setzen kann. [HTTP00, S. 6]

WebBugs vom Nutzer nicht explizit ausschalten.

Eine weiterführende Möglichkeit von WebBugs ist, dass diese in Microsoft Office Dokumente eingebunden werden können. Dazu wird einfach eine Grafik in ein Office Dokument mittels eines Links auf diese Graphik eingebunden. Jedesmal, wenn jemand das Dokument öffnet, baut sein Office eine Verbindung zu dem Ziel des Links auf und erfragt die Grafik. Das Ziel, typischerweise ein WebServer, erfährt auf diese Weise, wer wann von wo sein Dokument liest und hat die Möglichkeit den Weg seines Dokumentes zu verfolgen. [Smith]

Eine Gefahr für den Nutzer durch Cookies und WebBugs besteht dann, wenn Onlinefirmen Verbindungsdaten mit Stammdaten zusammen führen. Durch die Fusion der weltweit größten Online-Marketingagentur DoubleClick mit der Firma Abacus Alliance, die über zwei Millionen Kundenprofile hält, ist diese (in Deutschland gesetzlich verbotene) Zusammenführung realisiert worden. [HeiseZ00]

11.2.4 Beispiel: DoubleClick

DoubleClick kooperiert mit Suchdiensten, wie z.B. AltaVista in der Form, dass AltaVista in seinen Ergebnisseiten Bildaufrufe durch IMG Tags so gestaltet, dass diese von DoubleClick kommen und mit den Suchbegriffen inhaltlich übereinstimmen. Smith [SmithS00, S. 3ff] beschreibt einen Aufruf in der Ergebnisseite der Suche nach Sport und Auto wie folgt:

```
<IMG SRC=http://ad.doubleclick.net/ad/altavista.digital.com/result_
front;kw=sports+cars;cat=totext;ord= 1804224227?" border=0 height=60
width=468>
```

Mit der Eingabe und dem Abschicken des Suchstrings passiert folgendes:

- Der Internet-Browser des Nutzers erhält von AltaVista die HTML Befehle, welche die Ergebnisseite aufbauen.
- In der sequentiellen Ausübung der Befehle stößt der Internet-Browser auf obigen IMG Tag und meldet sich somit bei DoubleClick, um den Werbebanner zu erhalten.
- Durch den Kontakt des Internet-Browsers zu DoubleClick, erfährt diese Firma einiges über den Nutzer, z.B. den Inhalt des Suchstrings, in Schlüsselworten verpackt und hinter der **kw**-Anweisung, die IP und eventuelle Inhalte von Cookies, erhält also die Möglichkeit, Verbindungsdaten zu sammeln.

Als Vorleistung müssen sich DoubleClick und AltaVista nur auf eine Reihe von relevanten Schlüsselworten einigen. Mit Hilfe dieser einfachen Technik gelingt es DoubleClick, die Verbindungsdaten von allen Personen, die auf eine Seite mit einem Werbebanner von DoubleClick gehen, zu sammeln, ohne dass es diesen bewußt wird.

Um die Wirkung der Werbebanner zu verbessern und schnell vermutlich interessante Werbung einblenden zu können, wurde von DoubleClick für jeden Nutzer ein Onlineprofil erstellt. Dazu erhielt jeder Nutzer, um ein Tracking über mehrere Seiten, bei wechselnder IP und zu verschiedenen Zeiten zu ermöglichen, per Cookie eine eindeutige ID, die jedesmal übermittelt wird, wenn der Internet-Browser eine Anfrage an den Server von DoubleClick stellt. [DouCli] Das Profil wird in Form einer Tabelle angelegt, dauerhaft gespeichert und per ID einem Nutzer zugeordnet. In dieser Tabelle stehen bestimmte Stichwörter, die Interessensgebiete abstecken und eine Bewertung passend für die assoziierte ID. Jedesmal, wenn nun die Person mit einer bereits verteilten ID

- nach bestimmten Begriffen suchen läßt,
- bestimmte Seiten im Netz besucht oder
- Banner anklickt,

wird die Bewertung in der Tabelle verändert. [SmithS00]

Auf diese Weise gewinnt DoubleClick im Laufe der Zeit ein sehr genaues Persönlichkeitsprofil, welches bis jetzt fast ausschließlich anonymen IDs zugeordnet werden konnte. Durch die Fusion mit Abacus Allianz im November 99 erhielt DoubleClick viele Stammdaten, die mit den bereits vorhandenen Verbindungsdaten zusammengeführt werden können. Dies ist aber nicht die einzige Quelle von DoubleClick für Stammdaten. Auf Seiten von Tochtergesellschaften, wie z.B. www.NetDeals.com oder www.IAF.net werden Stammdaten von Nutzern mittels Zusagen auf bessere Betreuung und Werbung durch Abfragen gewonnen, die mit vorhandenen Verbindungsdaten zusammengeführt werden können. [DouCli]

Die Gefahren der Erstellung und Verbindung eines Onlineprofiles mit Stammdaten werden bei der Betrachtung folgenden Sachverhaltes ersichtlich. Beim Surfen verrät der Internetnutzer viel von sich selbst. Durch Beobachten seiner Eingaben in Suchmaschinen werden seine Interessen genauso deutlich, wie durch die Verweildauer auf bestimmten Seiten. Eine normale Marketinggesellschaft kann vielleicht herausfinden, welche Zeitung bezogen wird, oder ob und welche Computerspiele genutzt werden. Für sie müßte es aber immer ein Rätsel sein, welcher Artikel gelesen wird und wie lange ein bestimmtes

Spiel genutzt wird. Im Internet ist diese Information leicht zugänglich, und kann durch die Nutzung von WebBugs gewonnen werden, vor allem wenn diese von vielen Seiten eingesetzt werden. Die Werbebanner von DoubleClick werden derzeit auf ungefähr 12.000 Webseiten genutzt. [HeiseW00]

11.2.5 Weitere Marketinggesellschaften

Der geschilderte Versuch, genaue Kundenprofile zu gewinnen, beschränkt sich nicht nur auf DoubleClick. So sind viele Seiten und Suchmaschinen mit einer Marketinggesellschaft verbunden.²⁰ In Deutschland besonders stark vertreten ist die Werbeagentur quality-channel.de. Zu ihren Partner gehören unter anderem wissenschaft.de, funcity.de, heise.de, kicker.de, lifeline.de, manager-magazine.de, paperboy.de und spiegel.de. Alleine auf diese Seiten entfielen im Juni 2000 nach eigenen Angaben²¹ ungefähr 84 Millionen Zugriffe. Entsprechend groß ist die Möglichkeit, das Surfverhalten von vielen Internetnutzern zu beobachten.

Tabelle 1: Zusammenarbeitende Internetseiten mit Onlineagenturen

<i>Internetseite</i>	<i>Zusammenarbeit mit</i>
www.excite.com	ad.preferences.com
www.yahoo.de	eur.yimg.com
www.fireball.de	badservant.guj.de
www.t-online.de	banner.media-system.de
www.hotbots.com	akamai.net und doubleclick.net
www.go.com	ad.preferences.com
www.kostenlos.de	badservant.guj.de

11.3 Datensammeln: aktive Methoden

Als aktive Methoden werden im Folgenden alle Techniken aufgeführt, die aus der Sicht des Internet Nutzers nicht zu erwarten waren und bei denen ein Angreifer aktiv vorgegangen sein muß. Werden für die Gewinnung von Informationen Trojaner eingesetzt, also Programme mit gezieltem, schädigendem Verhalten, so werden diese aus Gründen der Vollständigkeit hier nur skizziert. Eine abschließende Betrachtung erfolgt im Kapitel Trojaner.

²⁰Die in der Tabelle aufgeführte Marketinggesellschaft preferences gehört dem Unternehmen MatchLogic an.

²¹<http://www.quality-channel.de/mediadaten/Partner.html>

11.3.1 Globally Unique Identifier

Der Globally Unique Identifier (GUID) wird nachfolgend genauer betrachtet, um einen Eindruck zu vermitteln, welche Mittel Unternehmen, vor allem solche, die über eine sehr breite Basis verfügen, einsetzen können, um persönliche Daten zu gewinnen.

Wenn in Microsoft Office 97²², z.B. in Word oder Excel ein Dokument das erste Mal gespeichert wird, erhält es eine eindeutige Nummer. Diese GUID besteht aus 32 Zeichen mit 4 trennenden Querstrichen, z.B. 4 1 2 D 4 C 2 0 - 6 F A D - 1 1 D 4 - 8 9 A B - C 9 3 0 2 9 C 1 A 0 3 B

In dieser Nummer sind unter anderem der Zeitstempel der Erzeugung und in den letzten zwölf hexadezimal Zeichen die MAC Adresse des Ethernet-Adapters enthalten. Gibt es in dem Rechner keinen Adapter, so wird eine Zufallszahl abhängig von der vorhandenen Hardware generiert und dadurch einem Rechner zuordnen. Eine genaue Beschreibung der GUID kann auf den Seiten von Microsoft [Microsoft00] nachgelesen werden.

Die GUID wird im Klartext, also unverschlüsselt, abgespeichert. Somit ist es relativ einfach sich diese anzusehen. Durch das Ablegen einer GUID läßt sich jedes Dokument einem Rechner zuordnen und der Zeitpunkt seiner Erstellung eindeutig festlegen. Auch eine Zuordnung verschiedener Dokumente untereinander ist problemlos möglich. Zusätzlich hat Richard M. Smith gezeigt, dass jeder Nutzer von Windows 98 betroffen ist, da die GUID bei diesem Betriebssystem mittels eines ActiveX Control weltweit auslesbar und interessanterweise änderbar ist, womit die eigentliche Idee hinter der GUID ad absurdum geführt ist.²³

Bei einer Verknüpfung der abgelegten GUID mit Stammdaten wäre eine Anonymität bei Veröffentlichungen von eigenen Dokumenten im Internet nicht mehr möglich. Jeder Autor ließe sich problemlos und in kürzester Zeit ermitteln. Ein (zufälligerweise) positiver Effekt war die Ermittlung des Melissa-Virusprogrammierers, da dieser Virus in Word erstellt wurde und so die GUID des Rechnerbesitzers vorlag. Andererseits ist es für Microsoft möglich, z.B. anhand der Firmendatenbank herauszufinden, welcher Nutzer mit welcher Software arbeitet, und ob diese registriert ist.

Ein Versuch, die mittels GUID²⁴ gewonnen Daten mit Stammdaten zusam-

²²Laut Siering [Siering99] ist die GUID auch vereinzelt in EMails von MS-OutLook aufgetaucht.

²³<http://users.rcn.com/rms2000/privacy/regwiz.htm>

²⁴In diesem Fall heißt es Microsoft ID, enthält aber auch die Adresse des Ethernet Adapters und ist somit im relevanten Bereich identisch zur GUID.

menzuführen, unternahm Microsoft mit dem Windows 98 Registration Wizard. Wenn im Internet Windows 98 bei Microsoft mit diesem Programm registriert wurde, so wurde auch gleichzeitig die GUID übertragen und lag so mit den Stammdaten bei Microsoft vor, automatisch dazu erhielt der Kunde ein Cookie mit der GUID, womit er auf jeder Seite von Microsoft sehr einfach identifiziert werden kann. Die GUID wurde, entgegen der Behauptung von Microsoft, auch dann übertragen, wenn der Anwender die Option „Systemdaten mit Registrierung einsenden“ nicht aktivierte. [Siering99]

Microsoft selber zeigte sich bei der Aufdeckung dieser Vorgehensweise desorganisiert. Zuerst wurde alles abgestritten, dann verharmlost und zuletzt als Programmfehler bezeichnet, der weder geplant noch bekannt war, und dessen gewonnene Daten sofort gelöscht würden. [Siering99]

11.3.2 Metadaten in Microsoft Office 97 Dokumenten

Mit Word ein leeres Dokument anzulegen und abzuspeichern, erzeugt eine Datei mit einer Größe von ungefähr 19 KByte²⁵. Dieselbe leere Datei in Excel hat noch 14KB. Da die Dokumente leer sind, stellt sich natürlich die Frage, welche Informationen so alles neben der GUID abgespeichert werden. Dieses kann man entweder bei Microsoft [Microsoft] oder mit Notepad selber nachlesen. Unter anderem befinden sich folgende Informationen, neben dem eigentlichen Dokumenteninhalt, in einer Datei:

- Name, Abkürzung und Firmenbezeichnung des Autors
- Netzwerk- oder Festplattenbezeichnung und Name des Computers
- Pfad und Dateiname der ersten Speicherung
- Aktueller Pfad und Dateiname
- Namen vorhergegangener Autoren
- Versionsnummer und persönliche Ansichten

Mit Hilfe der sogenannten Metadaten in Dokumenten, die mit Microsoft Office 97 erstellt werden, bieten sich viele für den Nutzer schadhafte Möglichkeiten. So kann mittels des vorhandenen Namens ein Dokument einem Autor zugeordnet werden und eine anonyme Veröffentlichung unwirksam gemacht werden. Andersherum ist es denkbar, dass jemand diese Angaben fälscht, um so z.B. eine Person mit einem anstößigen Dokument in Mißkredit zu bringen. Auch andere, vorhandene Angaben, wie Bezeichnung des Computers

²⁵1KByte = 1024 Byte

und Name von vorhergegangenen Autoren machen eine anonyme Veröffentlichung unmöglich.

Die angegebenen Pfad- und Dateinamen der Speicherung öffnen eine Sicherheitslücke, da sie einem Angreifer Einblick in den Aufbau des Dateisystems ermöglichen. So kann aus der möglichen Information, daß Microsoft Office in dem Standardordner gespeichert wurde, abgeleitet werden, daß sich vielleicht auch Windows in dem Standardordner befindet.

11.3.3 Eingesetzte Programme

Dieses Kapitel umfaßt den Einsatz von Programmen, um personenbezogene Daten zu erlangen. Da diese in den verschiedensten Ausprägungen möglich sind, wird nachfolgend nur ein kurzer Überblick, über die verschiedenen Versuche und eingesetzten Techniken aufgeführt, die von Unternehmen mit dem Ziel, genaue Daten über Nutzer zu erhalten, unternommen wurden.

- 11.11.1999: **Millionen-Klage gegen RealNetworks** Die Firma RealNetworks hat in ihrer Software RealJukebox einen Algorithmus eingearbeitet, der die GUID der Nutzer und ihre Hörgewohnheiten, laut Smith [SmithRJB99] einschließlich der CD-Bezeichnungen und der Art der Nutzung zu RealNetworks übertrug. [HeiseM99]
- 30.11.1999: **Curser überwacht Surfverhalten** Die Software der Firma Comet System, die den Mauszeiger auf bestimmten Webseiten in Cartoon-Figuren verwandelt, überträgt Nutzerdaten, unter anderem auch die GUID und die Adresse der Seite an den Hersteller. [SpiegelC99]
- 13.01.2000: **SendIt-Programmierer lesen jede EMail mit** Das EMail Programm SendIt verschickt von jeder Mail eine Kopie derselben an die Programmierer. [HeiseS00]
- 10.07.2000: **Netscapes SmartDownload belauscht Nutzer** Jedesmal wenn das Downloadtool eine Datei herunterlädt, überträgt es an Netscape, neben einigen anderen Daten, die EMail-Adresse des Nutzers, sowie die URL der heruntergeladenen Datei. [HeiseN00]
- 18.07.2000: **Windows Media Player 7 mit CD-Brenner und Sicherheitsproblemen** Der Media Player 7 überträgt bei „bestimmten Gelegenheiten“ Daten zu dem Medienserver von Microsoft. Diese werden mitprotokolliert und enthalten laut Microsoft unter anderem die GUID, die Verbindungszeit, IP-Adresse, Clientversion, usw.. [HeiseWM00]

Dies sind nur die bekanntgewordenen und großen Angriffe eines Jahres. Daneben gab es sicherlich noch eine Reihe weiterer Angriffe, die entweder unerkannt blieben oder in ihren Auswirkungen zu klein waren und somit kein Aufsehen erregten.

11.3.4 TRUSTe

Aufgrund der vielen Schlagzeilen über erfolgreiche Angriffe auf die Daten von Nutzern des Internets, verloren viele ihr Vertrauen in die Onlinefirmen und schränkten entsprechend ihre Auskunftsbereitschaft und Akzeptanz ein. Dieser Vertrauensverlust stellt Unternehmen vor immer größere Schwierigkeiten und so wurden Konzepte entwickelt, um diesem entgegenzusteuern.

Ein Ergebnis dieser Bemühungen ist die Organisation TRUSTe. Sie wurde im Oktober 1998 mit dem Ziel gegründet, die Onlinenutzer bezüglich des Gebrauchs ihrer persönlichen Daten zu sensibilisieren und Webseitenbetreiber zu ermutigen, Erklärungen abzugeben, wie sie mit den personenbezogenen Daten umgehen.²⁶ Darüber hinaus überprüft TRUSTe das Verhalten ihrer Mitglieder und gibt bei Nichtbeanstanden des Umganges mit sensiblen Daten ein Datensiegel aus, das auf den Seiten angebracht werden kann, um den Nutzern zu zeigen, das diese Firma bestimmte Datenschutzrichtlinien einhält. [Rötzer99]

Diese Vorgehensweise mag in einem Land ohne gesetzlich geregelten Datenschutz angebracht und vernünftig erscheinen, Zweifel kommen aber spätestens bei der Durchsicht der Gründer und Sponsoren. Unter anderem sind dies AltaVista, AOL, Excite, IBM, Intel²⁷, Lycos, Microsoft, RealNetworks, Yahoo und andere. Die meisten dieser Firmen mußten seit der Gründung und der Erteilung des Datenschutzesiegels Verletzungen der Vertraulichkeit einräumen. Das Siegel durften diese Firmen mit abwegigen Begründungen wie z.B. in dem Fall RealNetworks [HeiseR99], auf Kosten des allgemeinen Vertrauens in TRUSTe, behalten.

11.4 Bewußte Informationsweitergabe

Nachfolgend werden die Informationen behandelt, die ein Nutzer im Internet möglicherweise freiwillig preisgibt, ohne sich vielleicht darüber im Klaren zu sein, das diese unter Umständen dauerhaft gespeichert werden und vielen frei zugänglich sind.

²⁶http://www.truste.org/about/about_faqs.html

²⁷An dieser Stelle soll eine kurze Erläuterung erfolgen, da Intel ansonsten in dieser Diplomarbeit nicht weiter behandelt wird: Intel hat seinen Pentium III Prozessor mit einer per Software lesbaren, eindeutigen Seriennummer ausgestattet, mit dessen Hilfe Nutzer eindeutig identifiziert werden können. [HeiseP99]

11.4.1 EMail

EMails werden gewöhnlich im Klartext, d.h. unverschlüsselt und für jeden einsehbar im Internet übertragen. In den meisten Fällen haben der Sender und der Empfänger keine direkte Verbindung, so dass die EMail über viele, z.T. dem Sender unbekannt Server übertragen wird, die, jeder für sich, Zugriff auf alle Daten der EMail, wie Inhalt, Empfänger oder Sender haben. Aus diesen Gründen sind EMail sehr unsicher und wichtige Informationen sollten auf keinen Fall übertragen werden.

Rechtlich betrachtet ist das Ausspähen von EMail selbst in Deutschland umstritten, da sie wie Postkarten gehandhabt werden. Wer eine EMail verschickt, nimmt billigend in Kauf, dass andere von dem Inhalt erfahren. Eine EMail ist weder rechtlich noch technisch geschützt und so jedem Zugriff ausgeliefert. Selbst wenn EMail in Deutschland geschützt wären, könnten sie über Router oder Provider vermittelt werden, die in Ländern liegen, die ein Ausspähen von EMail nicht verbieten.

11.4.2 Homepage

Die Möglichkeit, sich weltweit zu präsentieren, nehmen viele gerne wahr. So werden schon in der Suchmaschine von altavista.de, bei einer Anfrage nach *Home* ungefähr zwei Millionen Seiten angezeigt. Sehr viel genauer werden die Ergebnisse, wenn direkt bei den Speicherplatzprovidern nach privaten Seiten gesucht wird.²⁸

Diese privaten Seiten beinhalten mit ihren Angaben zu Hobby, Freunde, Links, Adressen, vielleicht Lebenslauf und derzeitige Tätigkeit genau die Informationen, die sich Gesellschaften zur zielgerichteten Kundenwerbung wünschen. Entsprechend groß ist das Interesse der Marketinggesellschaften, diese Daten zu erhalten. Aufgrund ihrer unterschiedlichen Präsentation eignen sie sich noch nicht dazu, automatisch gewonnen zu werden. Dieses ändert sich, sobald ein Algorithmus entwickelt wird, der in der Lage ist, die Informationen in Form von Metadaten zur Verfügung zu stellen und ein Interesse seitens der Gesellschaften besteht, diesen Algorithmus auch einzusetzen.

11.4.3 Usenet

Diese Kommunikation, auch als Newsgroups bekannt, basiert auf dem *Network News Transfer Protocol*, kurz NNTP und funktioniert ähnlich wie eine Mailinglist. Um Nachrichten zu erhalten, muß sich der Nutzer bei sogenann-

²⁸Auf der Seite <http://www.kostenlos.de/internet/> gibt es z.B. eine Liste von Webspaces Anbietern.

ten News-Servern einloggen. [Lauer98, S. 283]

Der Vorteil dieses Dienstes gegenüber normalem Mailen ist die Möglichkeit mit seinem Beitrag viele Personen zu erreichen, bzw. auf die Beiträge von vielen zugreifen zu können. Um dieses zu gewährleisten, werden alle Beiträge archiviert und sind per Suchdienst, wie z.B. <http://www.deja-news.de/>, nach Suchbegriffen sortiert, abrufbar.

Dieser Suchdienst reicht derzeit bis 1995 zurück mit der Bemühung noch weiter zurückliegende Beiträge in das Archiv aufzunehmen. Auf diese Weise ist es sehr einfach möglich, alles, was eine Person jemals in die Newsgroups gepostet hat, anzeigen zu lassen, und so seine Meinung zu bestimmten Themen kennenzulernen.

Aufgrund der im Vergleich zu den Homepages noch chaotischeren Darstellung der Informationen und ihrer Bedeutung liegt ein automatisches Auswerten noch in weiter Zukunft. Eingesetzt wird dieses Verfahren der Informationsgewinnung bis jetzt bei Bewerbungen, um so möglichst viel über den potentiellen Kandidaten zu erfahren.

12 Angriff auf Vertraulichkeit: Spoofing

Die sogenannten spoofing²⁹ Angriffe täuschen dem Opfer einen vertrauenswürdigen Kommunikationspartner vor, so dass dieser bereitwillig Informationen übermittelt oder aber erhaltene Informationen als glaubwürdig einstuft. Diese Angriffe sind somit gegen die Vertraulichkeit gerichtet.

12.1 Domain Name System Spoofing

Das *Domain Name System* (DNS) ist der dezentrale Auskunftsdienst im Internet, zuständig für die Zuordnung des Domain Namens im *Uniform Resource Locators* (URL), wie z.B. www.beispiel.de, zu der IP-Nummer des Servers mit dieser Adresse und somit vergleichbar mit einer Vermittlungsschaltstelle im Telefonnetz.

Ein Spoofing Angriff versucht, die Zuordnung der Einträge zu verändern. Die Auswirkungen wären so, als ob jemand die Einträge im Telefonbuch beliebig verändern könnte. Beispielsweise wäre es einem Angreifer möglich, den Notrufnummern einen (kostenpflichtigen) 0190er-Anschluß zuzuordnen und so alles mitzuhören, bzw. den Inhalt frei zu editieren und noch viel Geld damit zu verdienen, da alle Notrufe nun über eine kostenpflichtige Leitung gehen.

²⁹engl.: Humbug, Schwindel

Gegen mutwillige Änderungen ist das DNS zudem sehr schlecht gesichert.

Besonders gefährlich macht solche spoofing Angriffe, dass sie nur schwer zu entdecken sind. DNS Aktivitäten werden aufgrund ihrer Vielzahl normalerweise nicht protokolliert, pro Web-Zugriff oder geladenem Bild fällt mindestens ein DNS Aufruf an, also bei typischen, größeren Nameservern viele Tausend pro Sekunde. [Weidner97, S. 1f] [Fuhrberg98, S. 56]

12.1.1 Domain Name Lookup

Die Auflösung der Adresse erfolgt in mehreren Schritten. Die Adresse vom Format `www.beispiel.de` wird vom Betriebssystem an eine Bibliotheksfunktion übergeben, welche daraus ein DNS Anfragepaket konstruiert und dieses an den DNS Port des vordefinierten Nameservers schickt.

Diese Anfrage ist rekursiv, d.h. der Client erfährt nur die endgültige Antwort und wird nicht an einen Name Server, der die Antwort kennt weitergeleitet. Untereinander kommunizieren die Nameserver nicht-rekursiv, d.h. jeder Server gibt nur Antworten, die er selber kennt. Fragen, die er nicht beantworten kann, werden an andere, übergeordnete Nameserver verwiesen.

Die Kommunikation im DNS erfolgt aus Gründen der Effizienz nicht über TCP sondern über das paketorientierte UDP (user datagram protocol). Da UDP-Pakete unterwegs verlorengehen können, bedienen sich die Server und Clients spezieller Logik zum Wiederholen unbeantworteter Anfragen; unerwartete Antwortpakete werden stillschweigend ignoriert. [Weidner97, S. 2]

12.1.2 Wirkung eines DNS Spoofings

Mittels eines erfolgreichen Zugriffes auf einen DNS Server, kann der Angreifer einer Adresse wie `www.bank.de` eine beliebige IP-Nummer, also auch die seines Servers, zuordnen. Das gefährliche an folgendem Angriffsszenario ist, dass es vollständig automatisiert ablaufen und somit gleichzeitig beliebig viele Opfer betreffen kann.

1. Ein Opfer möchte auf `www.bank.de` zugreifen. Sein Internet-Browser lenkt die DNS Anfrage an den eingestellten Name Server.
2. Der Name Server ist erfolgreich angegriffen worden und gibt als Antwort nicht die IP der Bank, sondern die IP des Angreifers aus.
3. Der Browser des Opfers öffnet eine Verbindung mittels *Hypertext Transfer Protocol* (HTTP) zu der angegebenen Adresse. Der Server des Angreifers kann nun mit dieser Anfrage auf zwei verschiedene Arten umgehen.

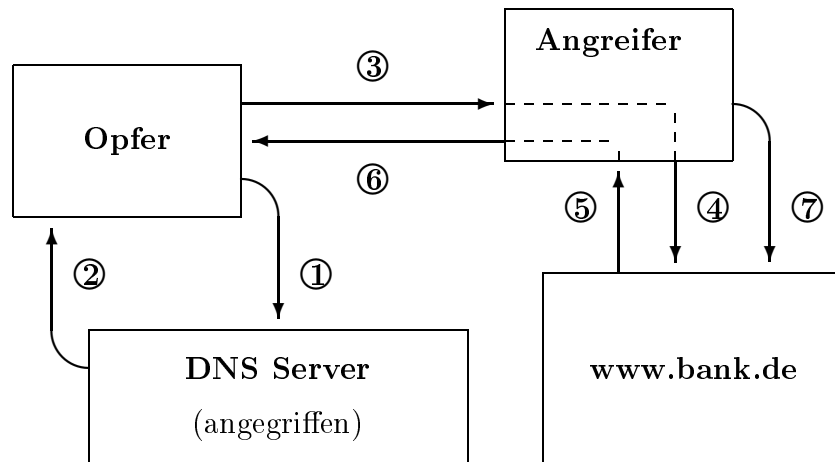


Abbildung 3: Erfolgreiches DNS Spoofing

- Der Angreifer hat die Seiten der Bank lokal kopiert und hält sie bei sich bereit. Das Opfer bewegt sich nun nur noch in dieser lokalen Kopie.
 - Der Angreifer leitet alle Anfragen des Opfers zum Server der Bank durch und gibt dessen Antworten an das Opfer weiter.³⁰ Dies ist auch die in der Abbildung behandelte Variante.
4. Der Angreifer leitet alle Anfragen an die Bank weiter. Der (gebräuchliche) Sicherheitsmechanismus, die Verbindung zu verschlüsseln, ist in diesem Fall wertlos, da die Verbindung zwischen Server des Angreifers und Bank verschlüsselt ist und der Angreifer problemlos Zugriff auf die Konten des Opfers hat. Möchte das Opfer eine Transaktion abschließen, so übermittelt der Angreifer dem Opfer nur eine nichtssagende Fehlermeldung, mit der Bitte es in beispielsweise drei Tagen noch mal zu versuchen.
 5. Die Bank übermittelt alle geforderten Seiten an den Server des Angreifers.
 6. Die von der Bank übermittelten Seiten werden zum Opfer durchgereicht.
 7. Nach ein bis zwei Tagen Datensammelns (Kontonummer, PIN (Personen Identifizierungsnummer) und TAN (Transaktionsnummer)) der Opfer, überweist der Angreifer sich von den Konten seiner Opfer belie-

³⁰In diesem Fall handelt es sich um eine man-in-the-middle attack, da der Angreifer zwischen dem Opfer und dessen Ziel sitzt.

bige Beträge bis zum Höchstsatz auf sein Konto und räumt dieses am nächsten Tag.

12.1.3 Cache Pollution

Aufgrund der Größe des Internets kann kein DNS Server alle *Resource Records* (RR)³¹ halten, deshalb muß bei einer Anfrage, deren Antwort nicht vorliegt, ein anderer Name Server gefragt werden. Die Antwort wird aus Gründen der Effizienz in einem Cache gespeichert, um bei einer erneuten Anfrage des gleichen Ziels Zeit zu sparen. Da Cache nur begrenzt vorhanden ist, sind alle Einträge mit einem *time-to-live* (ttl) Feld ausgestattet, in dem die Zeit in Sekunden bis zur Löschung des Eintrages gezählt wird.³²

Bei der sogenannten Technik des *cache pollution*³³ nutzt der Angreifer aus, dass manche Nameserver erhaltene Daten, ohne diese angefordert zu haben, gutgläubig im Cache verstauen. Bei einer späteren Anfrage nach diesen Daten liefert der Nameserver dann zwangsläufig falsche Antworten aus dem Cache zurück.

Wenn zum Beispiel jemand wissen will, wer der EMail Exchanger (MX) einer Domain ist, interessiert er sich oft auch für dessen Namen und die IP-Nummer. Um den Datenstransfer gering zu halten, werden diese Informationen bei der ersten Anfrage oft zusätzlich mitgeschickt, ohne dass sie angefordert wurden. Nun kann ein Angreifer aber auch Daten schicken, die mit der ursprünglichen Anfrage gar nichts zu tun haben und eventuell gefälscht sind, dass zum Beispiel die zugehörige IP Nummer der Adresse `www.bank.de` die IP Nummer des Hackers sei. Die falschen Daten werden ohne eine Überprüfung in den Cache des Name Servers geladen. Wenn dieser nun nach der IP Nummer von `www.bank.de` gefragt wird, liefert er zwangsläufig die falsche Adresse aus dem Cache und das Opfer wird auf die Seite des Angreifers geleitet. [Weidner97]

12.1.4 Query-ID guess

Der wohl derzeit gefährlichste Angriff auf DNS-Server besteht darin, die Query-IDs von Anfragen zu erraten. Dies sind 16-Bit Zahlen, die der Absender frei wählt. Diese sorgen dafür, dass die Antwortpakete richtig zugeordnet werden und sollen auch vor gefälschten Antworten schützen.

Wenn ein Nameserver eine Anfrage an einen anderen Nameserver gestellt hat, und ein Angreifer weiß die Query-ID dieser Anfrage, kann er versuchen,

³¹genauere Erläuterung im Anhang

³²Eine Abfrage ist mit Hilfe des Programms `ttl.pl` möglich.

³³engl.: den Cache verschmutzen

der Antwort zuvorzukommen und die Anfrage selber zu beantworten, mit manipuliertem Inhalt, aber richtiger Query-ID. Gelingt es ihm, wird diese Antwort als richtig gewertet, und die Originalantwort verstoßen, weil sie zu spät angekommen ist. Diese falsche Antwort wird der fragende Nameserver dann für weitere Anfragen speichern. [Weidner97]

Zur Durchführung bedarf es einiger Vorbereitungen: Der Angreifer benötigt eine eigene Domain, z. B. harmlos.de, dessen Namensraum (dieser beinhaltet die Computer einer Domäne, wie z.B. eins.harmlos.de oder stargate.harmlos.de) er selber verwaltet. Seinen Nameserver ersetzt er durch ein spezielles Programm, das die Pakete auf Port 53/UDP entgegennimmt. Der Angreifer ermittelt die echten Nameserver, deren Antworten er fälschen will, über eine einfache domain name Anfrage mit dem Anfragetyp 'query=NS' (zuständige Nameserver). Er bekommt daraufhin eine Liste, zum Beispiel ns.bank.de und ns.secondary.de.

Die Query-ID zu erhalten, ist derzeit für einen Angreifer relativ einfach, da die Name Server diese sequentiell numerieren. Sie besitzen einen internen Zähler, den sie nach jeder Anfrage um eins erhöhen. Der Angreifer fragt den Name Server zunächst nach einem eigenen Rechner, z.B. www.harmlos.de. Der Server stellt darauf eine eigene nicht rekursive Anfragen, um die Frage zu beantworten, und kurz danach bekommt der Angreifer ein entsprechendes Paket an seinen Nameserver geschickt. Er merkt sich die Query-ID dieses Pakets und kennt damit die ID der nächsten Anfragen seines Ziels. [Weidner97, S. 2f]

Anschließend stellt der Angreifer dem Angegriffenen eine übliche rekursive Anfrage und schickt sofort danach die passenden gefälschten Antworten an den erwarteten Ziel Name Server. Dieser schickt nun eine Anfrage an dem richtigen Server los, bekommt aber früher die gefälschten Antworten und hält daher diese für richtig, da die Query-ID übereinstimmt, und wartet nicht mehr auf die echte Antwort des eigentlich zuständigen Nameservers. [Weidner97]

Von nun an beantwortet der angegriffene Nameserver alle Anfragen nach www.bank.de mit den gefälschten Daten. Insbesondere wird auch die ursprüngliche Anfrage des Angreifers beantwortet - der sieht also sofort, ob das Manöver erfolgreich war. Falls nicht, waren noch andere Daten im Cache. Dann sagt das TTL-Feld (Time To Live) dem Angreifer auf die Sekunde genau, wie lange diese noch gültig sind. Dieser muß nur abwarten und kann dann einen neuen Versuch unternehmen.

12.2 WebSpoofing

12.2.1 Einleitung

In einem Internet-Browser wie z.B. Netscape oder Internet Explorer gibt es verschiedene Möglichkeiten, eine Internetseite zu identifizieren und seine eigene Position somit zu bestimmen. Unter anderem sind dies: [Felten96, S.2]

- *Aufmachung der Seite* wie Logo, Text, Layout,
- *Locationzeile*
- *Statuszeile*
- *Bezeichnung des Links im Text*
- *Source Code*

Bei einem DNS Spoofing spielen diese Hilfsmittel keine Rolle, da die Zuordnung URL zu IP-Nummer geändert wurde und der Nutzer keine Möglichkeit hat, den Angriff mit diesen Mitteln zu bemerken.

Im Vergleich zum DNS Spoofing ist das sogenannte WebSpoofing auf einer „höheren“ Ebene angesiedelt, da die Zuordnungen selber nicht verändert werden, sondern dem Nutzer eine falsche Adresse als echt glaubhaft gemacht wird. Dabei gibt es zwei unterschiedliche Methoden. Bei der Ersten versucht der Angreifer ähnlich dem DNS Spoofing einen sogenannten man-in-the-middle Angriff. Dabei werden Links so konstruiert und plziert, dass das Opfer diese nutzt und sich auf einer vertrauenswürdigen Seite wähnt. Die zweite Variante geht in die Richtung eines sozialen Angriffes. Der Angreifer konstruiert Seiten, die nicht andere vortäuschen, sondern selber vom Nutzer als vertrauenswürdig eingestuft werden.

12.2.2 URL Rewriting

Der Angreifer versucht dem Opfer einen Link zu präsentieren, den dieser anklickt und sich danach auf einer sicheren und vor allem vertrauenswürdigen Seite wähnt. Klickt der Nutzer auf so einen Link geschieht folgendes:

1. Der Internet-Browser des Opfers fragt den Server des Angreifers nach der gewünschten Zieladresse.
2. Der Server des Angreifers sendet nun wiederum eine Anfrage zum eigentlichen Zielservers.
3. Der Zielservers antwortet dem Angreifer auf die Anfrage.

4. Der Server des Angreifers leitet die Daten zum Opfer durch, dabei kann er diese beliebig verändern oder protokollieren.

Dies entspricht in etwa auch dem Verfahren, das man auf den Seiten sogenannter Anonymisierungsdienste verwendet. Das dort angebotene „anonyme Surfen“ beruht darauf, dass die gewünschte Adresse über den Anonymisierer angefordert wird und somit dem Zielsystem keinerlei Informationen über den eigentlichen Nutzer preisgegeben werden, da dieser im Internet nicht aktiv ist.

Obiger Angriff ist in dieser Form noch sehr leicht zu durchschauen, da sowohl in der Status- als auch in der Location-Zeile die gefälschte URL mit `http://www.angreifer.de/http://www.bank.de/` angezeigt wird. Durch den Einsatz von Java oder ActiveX lassen sich aber diese Anzeigen verändern oder abschalten, so dass nur noch die Durchsicht des Source Codes der Seite helfen würde.

Ein einfaches Beispiel für Angriffe dieser Art ist mit dem Programm `laurin.html` bereitgestellt. Dabei wird der Nutzer bei Bestätigung einer der angebotenen Links wahlweise auf lokale Kopien der anvisierten Seiten gelenkt oder aber mittels eines Programms auf die Originalseiten bewegt. In beiden Fällen ist es theoretisch möglich, alle Eingaben des Nutzers beliebig zu modifizieren und alle Ausgaben an den Nutzer beliebig zu verändern.

Eine andere Methode ist, Links so umzubenennen, dass ein Unterschied zum Original nicht auffällt. So ist sicherlich mit einem geeigneten Zeichensatz kein Unterschied zwischen **www.MICROSOFT.com** und **www.MICROSOFT.com** zu erkennen, einmal mit dem Buchstaben „o“ und einmal mit der Ziffer Null. Auch ist es möglich, syntaktisch verwandte Bezeichnungen, wie z. B. **www.sparkassepaderborn.de** anstelle von **www.sparkasse-paderborn.de** oder der IP-Adresse zu verwenden. Letztere Methode funktioniert, da eine IP-Adresse nur selten angezeigt oder von dem Nutzer memorisiert wird.

Die Schwierigkeit besteht darin, den Nutzern die veränderten Links so zu präsentieren, dass diese genutzt werden. Dazu gibt es mehrere Möglichkeiten. In einer Linksammlung auf einer Homepage können falsche Links zu diversen vertrauenswürdigen Seiten gesetzt sein. Dabei erscheint für das Opfer im Internet-Browser z.B. **www.bank.de**, während im Source Code der Link angegeben ist mit:

`http://www.harmlos.de/http://www.bank.de/`

In einer Linksammlung einer Homepage ist obiger Angriff auf eine relativ kleine Personengruppe beschränkt, hat folglich nur einen geringen Wirkungsbereich. Dieser lässt sich aber mit relativ einfachen Mitteln erweitern.

- Im Header und der Beschreibung einer Seite werden Bezeichnungen so gewählt, dass Suchmaschinen diese Seite zu den möglichen Suchbegriffen potentieller Opfer assoziieren und entsprechend anzeigen.
- In einer EMail an möglichst viele Personen mit z.B. folgendem Text: *“Achtung an alle Windows 9x Benutzer: eine neue Sicherheitslücke im Betriebssystem Windows 9x ermöglicht Viren uneingeschränkten Zugriff. Um Schaden zu vermeiden holen sie sich bitte das neueste Patch von Microsoft.“* Der falsche Link oder ein Link zu der Seite mit den veränderten Links wird gleich mitgeschickt.

Die Technik des WebSpoofing ist sehr einfach und wird bereits eingesetzt, so hat beispielsweise ein Angestellter der kalifornischen Firma Pairgain Technologies eine gefälschte Pressemitteilung zu einer angeblichen Übernahme seiner Firma durch eine Andere, in dem Message-Board von Yahoo plaziert. Als Beweis fügte er einen Link zu der angesehenen amerikanischen Agentur Blomberg hinzu. Durch das Anklicken dieses Links gelangte der Betrachter zu einer Webseite, die nahezu identisch zu Blomberg aber unter der Kontrolle des Angestellten war. Statt einer Klartext-URL war jedoch nur die IP-Nummer des Servers und eine Bestätigung der Meldung zu sehen. Kurz nach der Veröffentlichung fiel der Kurs der Aktie der betroffenen Firma um 31%. [HeiseP00, S. 163]

12.2.3 Vortäuschen einer Seite

Bei diesem Angriff wird dem Nutzer eine scheinbar normale Internetseite präsentiert, mit z.B. besonders günstigen Angeboten. Die Präsentation kann wie oben problemlos über Suchmaschinen oder Werbemails eine größere Anzahl Surfer erreichen. Hinter den Seiten steht aber keine Firma, sondern ein Angreifer, der sich für Daten, wie z.B. Kreditkarteninformationen oder Bankverbindungen interessiert. Der Surfer wähnt sich dabei auf der Seite eines Unternehmens mit besonders günstigen Angeboten, bestellt und gibt im Zuge der Bestellung persönliche Daten preis.

13 Schadhafte Programme

13.1 Einleitung

Am 4.Mai 2000 verbreitete sich der I LOVE YOU Virus mit einer bis dahin unbekanntem Geschwindigkeit innerhalb weniger Stunden über das gesamte Internet. Betroffen waren beispielsweise Bundes- und Länderministerien, das ZDF in Mainz, die Mittelbayrische Zeitung, Siemens, ca. 80 % aller Rechner in Spanien, der Kongress, das Verteidigungsministerium, die Zentralbank usw. in den USA. Alleine dort entstand nach Schätzungen ein Schaden von

ungefähr einer Milliarde Dollar. [HeiseILY00]

Entscheidend für die Ausbreitung des Virus war nicht seine technische Raffinesse, sondern die Unbekümmertheit der Nutzer und mangelhaft eingestellte Programme, vor allem MS-Outlook. Die eingesetzte Technik zur Verbreitung des Virus war generell bekannt und wurde auch schon von vorhergegangenen schadhafte Programmen, wie z.B. Melissa und Word.Share.Fun eingesetzt.

Im weiteren Verlauf wird versucht, alle möglichen Ausprägungen schadhafte Programme in vier Kategorien einzuteilen, um so einen einfachen Gesamtüberblick zu vermitteln und spezifische Merkmale besser darstellen zu können.

- **Viren:** Zu den Viren gehört jeder Algorithmus, dessen Zweck eine möglichst hohe Verbreitung über möglichst viele PCs ist. Weder muß dieser Algorithmus einen schadhafte Teil beinhalten, noch muß die Verbreitung automatisch geschehen.
- **Trojaner:** Ein Trojanisches Pferd ist ein Programm, das über eine nützliche oder interessante Funktion verfügt. Darüber hinaus aber einen Teil beinhaltet der etwas Unerwartetes macht, wie beispielsweise heimlich Dateien kopieren oder Paßwörter stehlen. [RFC1244]
- **Fehlerhafte Programme:** In die Gruppe fehlerhafter Programme kann jedes Programme eingeordnet werden, dass in seiner normalen Benutzung Fehler verursacht und sich so schadhafte auswirkt.
- **Gefährliche Programme:** Die gefährlichen Programme werden bewußt eingesetzt, um jemandem zu schaden.

Grenzfälle, deren Angriffsstruktur mehrere Zuteilungen bzw. keine erlauben, werden so weit wie möglich eingeteilt, um zu vermeiden, mit zusätzlichen Regeln, die eine genauere Einteilung erlauben würden, den Überblick zu verlieren. Beispielsweise ist ein Angriff bekannt, bei dem mit Dokumenten im RTF-Format mittels WordPad in das Dokument eingebundene Befehle an die Systemumgebung abgegeben werden können. [HeiseD00] Dieser Angriff beruht nicht auf einem Fehler, denn diese Funktion ist gewollt, auch ist es kein Trojaner, denn kein beteiligtes Programm gibt etwas anderes vor. Auch die anderen aufgelisteten Angriffe scheiden aus unterschiedlichen Gründen aus. In so einem Fall würde der Hauptaspekt zur Einteilung herangezogen werden. Dies die Erwartung, den Nutzer mit einem Programm, von dem dieser dies nicht erwartet, zu schaden und somit ausschlaggebend für die Einteilung als Trojaner.

13.2 klassische Viren

Die Frage, wie Viren entstehen, führt zur Betrachtung der Motivation von Virenprogrammierern.

- Ein Virus wird programmiert, weil der Programmierer es kann (oder können möchte). Hier steht die Lösung eines Problems im Vordergrund. Zu Testzwecken wird der Virus dann „freigelassen“.
- Der zweite Ansatz erklärt die Programmierung von Viren mit der scheinbaren „Macht“, die der Ersteller hat. Der Gedanke, etwas ausrichten zu können, bzw. Verursacher von Schäden in Millionen Höhe zu sein, ist hier ausschlaggebend.
- Im drittem Fall werden die Programme aus wirtschaftlichen oder wissenschaftlichen Gründen erstellt, die sich dann aufgrund eines Unfalles verbreiten.

13.2.1 Definition

Die hier verwendete Definition für einen Computervirus³⁴ leitet sich von den wortverwandten „echten“ Viren ab. Diese haben keinen eigenen Stoffwechsel und sind für die Vermehrung auf Wirtszellen angewiesen. [Bert98, S. 10365] Ebenso sind klassische Computerviren, um sich zu vermehren, auf die Ausführung von Wirtsprogrammen oder bestimmte Sektionen der Festplatte angewiesen. Ein anschauliches Beispiel für den Aufbau eines Virus ist nach Heiß [Heiß99, 3-5] aufgeführt.

```
procedure virus;
begin
Kennung:=3728593;
suche eine nicht infizierte Datei;
wenn gefunden, dann infiziere diese mit dem Virus;
wenn heute=Freitag der 13te, dann formatiere Festplatte;
starte das Wirtsprogramm;
```

Dieser Virus wird als Prozedur während der Ausführung des Wirtsprogrammes aufgerufen, vermehrt sich, führt vielleicht einen schadhafte Code aus und springt zum eigentlichen Programm zurück, so dass ein Anwender nicht bemerkt, dass dieses Programm infiziert ist und gerade ein Virus aktiv war.

³⁴lat.: Gift, giftiger Schleim

13.2.2 Einteilung

Derzeit gibt es laut dem Anti-Viren Programm F-Prot³⁵ ca. 28.000 Viren mit unterschiedlichsten Ausprägungen, für die verschiedenste Einteilungen in der Literatur und im Internet vorgenommen werden. Aus verschiedenen Virentypen erwachsen unterschiedliche Gefahren mit entsprechend passenden Schutzmaßnahmen, weshalb eine richtige Einteilung erforderlich ist. So läßt sich die Verbreitung von System- respektive Bootviren verhindern, wenn nicht von infizierten Datenträgern gebootet wird, während EMail-Viren sich mittels Attachment in E-mails übertragen.

Viren lassen sich nach Dragers gemäß dem Ort ihrer Speicherung wie folgt unterscheiden: [Dargers95]

- **Programm-viren** binden sich an ein Programm. Wird dieses aufgerufen und ausgeführt, startet auch der Virus.
- **Systemviren** befallen Systembereiche von Disketten und Festplatten. Bei diesen handelt es sich in der Regel um sogenannte Bootsektoren, bzw. *Master-Boot-Sektoren* (MBR). Diese Sektoren werden beim Start des Computers ausgelesen und die beinhalteten Anweisungen ausgeführt, wodurch auch der Virus gestartet wird.
- **Macro-viren** befinden sich in Dateien und werden meistens durch Lesen oder Aufrufen dieser Datei von dem entsprechenden Programm, wie z.B. Word, automatisch ausgeführt. Aufgrund der immer stärker voranschreitenden Integration von EMail Clients in die allgemeine Systemumgebung, wie z.B. Microsoft Outlook, Microsoft Office und Betriebssystem verbreiten sich diese Viren zwischenzeitlich innerhalb von Stunden über das gesamte Internet.

Programm-viren unterscheiden sich wiederum in der Art und Weise, in der sie sich an Programme binden. [Heiß99, 3-6]

- **Schalen Viren** bilden eine virtuelle Schale um das infizierte Programm. Sie treten an die Stelle des Programms, welches selbst als internes Unterprogramm aufgerufen wird.
- **Additive Viren** hängen sich an das Programm und verlängern es entsprechend. Die Startadresse wird auf den Virencode umgelenkt. Nach Ausführung des Virus wird zur ursprünglichen Startadresse gesprungen und das eigentliche Programm gestartet.
- **Ersetzende Viren** überschreiben einen Teil des infizierten Programms mit ihrem Code. Die Länge des Programms bleibt somit konstant, aber es wird in aller Regel unbrauchbar.

³⁵<http://www.data-fellows.com/>

Neben diesen Klassifizierungsmerkmalen gibt es eine Reihe weiterer Eigenschaften, die sich an Viren beobachten lassen: [Dargers95]

- **Direct Action Viren** werden sofort bei der Ausführung von infizierten Programmen aktiv, verbreiten sich und führen gegebenenfalls Schadensroutinen aus. Danach beendet sich der Virus und übergibt die Kontrolle wieder dem ursprünglichen Programm.
- **Residente Viren** bleiben nach ihrem Start im Hauptspeicher, um so jederzeit das System kontrollieren und unter Umständen eine Schadensroutine zu einem späteren Zeitpunkt ausführen zu können.
- **Stealth Viren** versuchen beispielsweise ihre Anwesenheit im System zu verschleiern. Dazu überwachen diese bestimmte Prozesse im System, wie z.B. Zugriffe auf Programmdateien und Inhaltsverzeichnis und verändern gegebenenfalls die Resultate dieser Zugriffe.
- **Polymorphe Viren** verschlüsseln sich bei einer Infektion selbst, um so zu verhindern, dass sie anhand einer speziellen Bytefolge von Antivirenprogrammen erkannt werden.

13.2.3 Schäden

Jeder Virus hat prinzipiell die Rechte und Möglichkeiten der Person, die das infizierte Programm gestartet hat. Die möglichen Schäden lassen sich in vier Kategorien einteilen:

1. **Harmlos** ist ein Virus, wenn seine Schadensroutinen keine Auswirkungen auf die Benutzung der Hard- und Software haben.
2. **Lästig** gilt für einen Virus, der die tägliche Benutzung des Computers beeinträchtigt, aber weiter ermöglicht und die Auswirkungen relativ einfach rückgängig gemacht werden können.
3. **Lethal** ist ein Virus, der Daten oder Dateien löscht, umbenennt³⁶ oder auf andere Weise unzugänglich macht.
4. **Massiv lethale** Viren löschen nicht nur Dateien oder ähnliches, sondern versuchen dauerhaft die Nutzung des Computers zu verhindern.

Diese Einteilung soll nicht in Sicherheit wiegen. Wird in einem System ein Virus entdeckt, sollte er sofort entfernt werden, auch wenn er offensichtlich nur harmlos erscheint. Es ist nicht vorhersagbar, ob vielleicht nach dem 100sten

³⁶Nach einer normalen Betriebssysteminstallation, wie z.B. von Windows 95, befinden sich mindestens 5000 Dateien auf der Festplatte. Ob eine Datei hier umbenannt oder gelöscht wurde ist unerheblich, denn ein Nutzer wird diese vermutlich nie wiederfinden.

harmlosen Aufruf des Virus eine massiv lethale Aktion startet.

Nach einer Studie des US-Fachmagazins InformationWeek Research entstehen der Weltwirtschaft im Jahr 2000 durch Viren mehr als drei Billionen DM Schaden [SpiegelCV00], wobei solche Angaben mit Vorsicht betrachtet werden müssen, da der Begriff Schaden sehr weit gedehnt werden kann und in den meisten Fällen nicht oder nur sehr schwer meßbar ist.

13.2.4 Beispiele

Eine vollständige Auflistung aller Viren ist hier selbstverständlich nicht möglich, so dass nur einige Beispiele, entsprechend den vorgestellten Schadenskategorien, aufgeführt werden.³⁷

1. Form-Virus

- Infizierung: Wenn von einer infizierten Diskette gebootet wird, befällt dieser Virus den Bootsektor der Festplatte und bleibt resident im Hauptspeicher. Jede weitere eingelegte Diskette wird von nun an, falls möglich, befallen. Der Virus gehört zu den am meisten verbreiteten.
- Schaden: Am 18ten eines jeden Monats wird für jeden Tastendruck ein „Klick“ von dem PC Lautsprecher ausgegeben. Dies funktioniert nicht, wenn ein Keyboard-Treiber, wie z.B. keyb.com geladen wurde.

2. Melissa

- Infizierung: Wenn eine Datei, z.B. LIST.DOC, in der sich der Virus befindet, per EMail erhalten, heruntergeladen und in Word geöffnet wird, startet der Virus und schickt sich selber an 50 andere Adressen aus dem Adressbuch von MS Outlook.
- Verbreitung: Dieser Virus, der ohne die aktive Hilfe von Nutzern keine Möglichkeit hat sich zu verbreiten, verteilte sich innerhalb weniger Stunden über das gesamte Internet. Viele Firmen, so auch Intel und Microsoft, berichteten von einer Infizierung und schlossen ihr EMail-System, um eine weitere Verteilung zu verhindern.
- Schaden: Der Virus verfügt nicht über eine explizite Schadensroutine. Der Schaden entsteht nur durch die massive Verbreitung.

³⁷Eine nahezu vollständige Liste steht auf folgenden Seiten zur Verfügung:
<http://www.Europe.DataFellows.com/v-descs/>
<http://www.uni-siegen.de/security/viren/index.html>
<http://www.avp.ch/avpve/>.

Ein Nutzer, der den Virus aktiviert, verbreitet diesen gleich an 50 Personen. Aufgrund der massiven Zunahme von E-Mails sind viele Verbindungen und Mailsysteme zusammengebrochen, entsprechend einem *Denial-of-Service* Angriff. Zusätzlich kopiert sich der Virus noch in andere DOC Dateien und verbreitet auch diese, wie die LIST.DOC, an 50 Personen und ermöglicht diesen sozusagen einen Einblick in private Informationen.

3. Michelangelo

- Infizierung: Der Virus befällt den Partitionssektor der Festplatte, wenn der Rechner von einer infizierten Diskette gebootet wird. Der Virus bleibt im Hauptspeicher resident und schreibt sich auf jede Diskette, die in das Laufwerk gelegt wird.
- Schaden: Jeden 6ten März versucht der Virus die Festplatte mit Nullen zu überschreiben.

4. CIH

- Infizierung: Der Virus befällt Windows 95 und 98 EXE Dateien und bleibt nach seinem Aufruf im Hauptspeicher resident. Von dort wird jedes andere Programm, das aufgerufen wird, infiziert.
- Verbreitung: In kürzester Zeit gehörte der CIH Virus weltweit zu den zehn verbreitetsten Viren. Diese hohe Verbreitung verdankte der Virus vor allem dem Umstand, dass er von mindestens vier Raubkopiergruppen unabsichtlich weitergegeben wurde. Zusätzlich gab es zahlreiche kommerzielle Unternehmen, wie z.B. das Magazin PC Games, Yamaha, Activision und IBM die den Virus unabsichtlich auf CDs verbreitet hatten.
- Schaden: Der Virus ist massiv lethal. Zum einen löscht er die Daten auf der Festplatte, zum anderen versucht er das Flash-ROM für das BIOS zu überschreiben. Wenn dies gelingt, läßt sich der Computer nicht mehr booten.³⁸

13.2.5 Infizierung

Ein Computersystem kann sich auf verschiedene Art und Weise mit einem Virus infizieren, abhängig von der Art des Virus. Bei einer Umfrage auf <http://www.icsa.com/> wurden dazu folgende Übertragungswege und deren Häufigkeit genannt:

- Infizierung über Disketten: 52,8%

³⁸Erfolg hatte der Virus unter anderem bei Motherboards mit dem Intel 430 TX Chip-satz.

- Infizierung über EMail-Attachments 32%
- Infizierung über Downloads 9,4%
- Sonstige 5,8%

Die Verbreitung eines Virus über Disketten ist nur möglich, wenn ein bereits infiziertes Programm von Diskette gestartet, oder der Rechner von einer infizierten Diskette gebootet wird.

Eine Vireninfiltration über EMail-Attachments, die zweithäufigste Möglichkeit, tritt immer stärker in den Vordergrund, da sich die meisten entsprechenden Viren selber nach Einträgen im Adressbuch des Opfers verschicken und so die EMail an jemanden gesendet wird, der das Opfer kennt und diesem vertraut und ein Attachment bedenkenlos öffnet.

Eine weitere und oft unbeachtete Möglichkeit, den Computer mit einem Virus zu infizieren, ist die Verwendung von Originalmedien, die vermeintlich sicher und somit vertrauenswürdig sind. So berichtete das Bundesamt für Sicherheit in der Informationstechnologie [BSI99] unter anderem von folgenden Vorfällen:

- Die Zeitschrift PC-Professionell verschickte im September 1994 an Abonnenten eine Diskette mit einem Scherzprogramm. In einer Kopierstation wurde diese mit dem Parity Boot B Virus infiziert, so dass 20.000 infizierte Disketten (von 30.000) ausgeliefert wurden.
- Microsoft Großbritannien übergab Ende 1995 zur geplanten Einführung von Windows 95 an rund 200 führende britischen Softwareentwickler eine Diskette, die von dem Form-Virus befallen waren.
- Mercedes Deutschland verteilte Ende April 1995 an rund 2000 Journalisten eine Pressemappe mit Informationen zur neuen E-Klasse, die eine Diskette enthielt. Diese war mit einem Stoned-Virus infiziert.

Allen Fällen gemein ist allerdings, dass das Original auf Viren überprüft wurde und sich diese erst durch nachträgliche Änderungen oder Kopieren der Diskette auf unsicheren Rechnern übertragen konnten. Generell kann ein Computer nur infiziert werden, wenn der Virus auf dem Rechner mindestens einmal aktiv ist. So ist es ohne weiteres möglich, Dateien, die einen Virus enthalten, auf den Computer zu kopieren oder aus dem Internet zu laden, ohne dass dieser sich je ansteckt.

Dass sich Viren im Internet zwischenzeitlich immer stärker verbreiten können, liegt vor allem an der fast Monokultur der Betriebssysteme auf Clientebene. So ist das System von mehr als 90% der Computer, auf denen

E-Mail-Clients laufen, ein MS-Windows Betriebssystem. Dadurch fällt es Viren leicht, Schwachstellen zur Verbreitung oder bestimmte Verbreitungsmechanismen auf möglichst vielen Rechnern zu nutzen. [StalderVi00] Nicht nur die technische Seite in Betriebssystemmonokulturen ermöglicht es Viren, sich massiv zu verbreiten. Vor allem die Möglichkeit, ein Programm zu erstellen, dessen Schadensauswirkungen möglichst hoch sind, zieht viele Virenprogrammierer in Richtung MS-Betriebssysteme.

13.3 Würmer

Die Idee von sogenannten Wurm-Programmen wurde das erste Mal in der Novelle „The Shockwave Rider“ von Brunner 1975 veröffentlicht. Ein Programm ist dann ein Wurm, wenn es versucht, möglichst viele Kopien von sich selber zu erzeugen, ohne dass diese dabei explizit schadhafte Routinen haben. Der Schaden entsteht in den meisten Fällen durch den Erfolg der Kopierfunktion, da so viele Replikationen erzeugt wurden, dass die Ressourcen des Computers belegt sind und keine anderen Programme mehr ausgeführt werden können. [Denning90, S. 140]

Der bekannteste Computerwurm ist auch gleichzeitig der erste, der ins Internet gelangte. Am 2ten November 1988 erschien erstmalig ein Wurm im Internet (damals noch ARPANET). Dieser eignete sich sofort die Ressourcen der infizierten Computer an, um möglichst viele Kopien von sich selber zu generieren. Innerhalb von acht Stunden befiel dieser, nach seinem Programmierer Robert Morris benannte Morris-Wurm, 2500 bis 3000 an das Netz angeschlossene Computer, also fast alle, die zu der Zeit ans Netz angeschlossen waren, und lastete diese so stark aus, dass keine andere Tätigkeit auf den infizierten Rechnern mehr möglich war. [Denning90, Artikel 10]

13.4 Hoax

Die sogenannten Hoax-Meldungen³⁹ werden unter Viren aufgeführt, da sie sich massiv verbreiten (oder zumindest den Versuch unternehmen), um auf diese Weise Schaden anzurichten. Sie verfügen weder über eine automatische Verbreitungs- noch über Schadensroutinen und bestehen derzeit nur aus einer E-Mail mit einem Text, der so gewählt wird, dass der Empfänger diesen an möglichst viele weiterreicht. Aufgrund des Aufbaus entspricht dies somit einem sozialen Angriff, da ohne die aktive Unterstützung des Nutzers kein Schaden entstehen kann.

³⁹ engl.: Ulk

13.4.1 Arten

Streng genommen kann jeder Kettenbrief zu den Hoax gezählt werden, abgrenzend sind also nur die Meldungen gemeint, deren Inhalt sachlich falsch ist. Im Laufe der Anwendung von Hoaxmails haben sich verschiedene Arten herausgebildet. Fast alle Hoax lassen sich daran erkennen, dass sie den Leser auffordern, die EMail an möglichst viele zu verbreiten und diese Verbreitung moralisch "gut" ist, oder direkt zu einem Vorteil führt. Vorkommende Schlagwörter sind kursiv gedruckt.

- **Viruswarnung:** In dieser EMail wird vor einem *neuen* Virus gewarnt. Dieser verbreite sich *sehr schnell* meist per *EMail*. Derzeit gibt es *keine Abwehr* und der Virus ist *sehr zerstörerisch*. Auch große Firmen, wie z.B. *Netscape, Microsoft, AOL oder andere* haben vor diesem Virus gewarnt. [Hoax96] Ein Beispiel für dieses Schema ist die Good Time oder die WIN A HOLIDAY Meldung.
- **EMail Tracking:** Bei dieser Version wird in der EMail berichtet, das eine größere Firma, wie z.B. *Microsoft* etwas *neues* ausprobieren möchten, oder einfach nur wissen möchten, wie verbreitet ihr Produkt ist. Dazu *erhält* jeder Nutzer, der diese EMail weiterleitet oder empfängt, einen bestimmten *Geldbetrag*. Um Zweifel auf Seiten der Nutzer auszuräumen wird auch oft darauf verwiesen, dass z.B. Bill Gates richtig viel Geld hat und damit machen kann, was er will, bzw. dass der Sender es selber nicht glauben wollte, aber tatsächlich nach einer gewissen Zeit Geld erhielt. Ein Beispiel zu dieser Hoax hat den Namen Microsoft E-Mail Tracking System.
- **Helft Mir:** In dieser Meldung, wird von einem *Kind* berichtet, welches *todkrank* ist und im Sterben liegt. Sein letzter Wunsch ist, *Beachtung zu finden, im Guinness-Buch der Rekorde aufgenommen zu werden oder etwas zu erreichen* und bittet darum, diese EMail so oft wie möglich zu verschicken, wie beispielsweise in der Meldung „A moment of silence“⁴⁰.

Jede dieser Möglichkeiten versucht den Nutzer auf verschiedene Art und Weise davon zu überzeugen, die EMail zu verbreiten. Die Viruswarnungen wenden sich an die Hilfsbereiten, die sich durch die Verbreitung solcher EMail gleichzeitig zu Experten machen wollen. Die EMail Tracking Meldungen versuchen vor allem die Nutzer zu überzeugen, die der Meinung sind, dass alle mit dem Internet Geld verdienen, nur sie selber nicht, die EMail weiterzuleiten. Die letzte Hoax bezieht sich auf die, die generell hilfsbereit und der Meinung sind, für mich nur ein kleiner Klick, für einen anderen eine Erfüllung.

⁴⁰<http://www.tu-berlin.de/www/software/hoax/slowdance.shtml>

13.4.2 Schaden

Der entstehende Schaden der Hoax Meldungen ist in den meisten Fällen für private Anwender marginal. Nur wenn eine EMail so oft verschickt wird, dass der Datentransfer gestört wird und so vielleicht bestimmte Seiten im Internet nicht erreichbar sind, oder der EMailverteiler zusammenbricht und gegebenenfalls EMails nicht mehr weiterleitet, tritt meßbarer Schaden ein.

Für Firmen können Hoax Meldungen dagegen schwere Beeinträchtigungen bedeuten. In den meisten Fällen dürfte ein zusammenbrechender EMailverteiler, der einige EMails verschluckt für sinkendes Vertrauen seitens der Anwender sorgen, auch wenn diese vielleicht den Zusammenbruch bewirkt haben. Gravierender noch sind z.B. falsche Meldungen über die Lage von Firmen. So hat sich eine Falschmeldung über die Firma Emulex mit folgendem Inhalt rasend an der Börse verbreitet: Statt eines Gewinns von drei Millionen US-Dollar müsse man für das letzte Quartal einen Verlust ausweisen, der Unternehmensführer sei zurückgetreten und die Bilanz der letzten Jahre müsse ebenfalls überarbeitet werden. Sofort kam es zu Panikverkäufen, die den Kurs um bis zu 62 Prozent einbrechen ließen, bis die US-Hightech-Börse Nasdaq den Handel aussetzte. Durch diese Kursmanipulation ging der Firma weit über eine Milliarde US-Dollar Marktkapitalisierung verloren. [HeiseG00]

13.5 Trojaner

Streng genommen muß jedes Programm, das über Funktionen verfügt, die vor dem Nutzer geheimgehalten werden, zu den Trojanern gezählt werden. Da dies aber für die meisten Programme gilt, beschränkt sich dieses Kapitel auf all diejenigen, deren verdeckte Funktionen für den Nutzer schadhaft sind.⁴¹ Anzumerken ist, dass hier nur von Programmen berichtet werden kann, von denen diese schadhaften Routinen bekannt geworden sind.

Ein Trojaner kann in jeder Form in Erscheinung treten. Es kann ein Utility sein, das angeblich Dateiverzeichnisse indiziert oder Registrierungscode von Software extrahiert. Es kann sich in einer normalen Textverarbeitung oder einem Netzwerktool verstecken. Bei keinem Programm kann ein Trojaner ausgeschlossen werden, solange nicht der Quellcode überprüft wurde. [Anon99, S. 259]

13.5.1 Beispiele von Trojanern

Nachfolgend werden einige Beispiele von Trojanern aufgeführt:

⁴¹Eine Liste von nicht schadhaften Funktionen, sogenannten Easter Eggs, gibt es unter www.eastereggs.de.

- **AOL.Buddy:** Dieser Trojaner ist seit dem Mai 1999 bekannt. Das Programm wird in Word Dokumenten verteilt, mit der Werbung, einen freien AOL Zugang zu erhalten. Wird auf das AOL Logo geklickt, infiziert sich das System. Wird Windows gestartet, startet auch der Trojaner und sendet das AOL login und Password als EMail zu qware4019@hotmail.com, ha015312@hotmail.com oder liighthack@yahoo.com, abhängig von der Version des Trojaners. [VIR]
- **IRC-Hack:** Dieses besteht aus einer selbstextrahierenden Datei, mit der ein Programm, mit dem IRC-Clients attackiert werden können, auf der Festplatte installiert wird. Daneben wird ein Serv-U FTP Server auf dem Computer installiert, der die Festplatte C: für vollen Zugriff aus dem Netz einrichtet. Dieser startet automatisch bei jedem Systemstart. [VIR]

Die aufgeführten Trojaner sind in ihrer Funktion bekannt und werden von den meisten Anti-Viren Programmen gefunden und entfernt. Schwieriger wird die Entfernung dieser Programme, wenn in bekannten und von vielen Personen eingesetzten Produkten geheime Funktionen entdeckt werden. Hier ist eine automatische Entfernung durch ein Anti-Viren Programm nicht möglich, da Anwender unter Umständen dieses Programm trotz der schadhaften Funktionen einsetzen möchten. Das Anti-Viren Programm wäre im Fall einer Entfernung des Trojaners der Schädling.

- Das Programm **Send It** verschickt EMail Rundschreiben. Insgeheim geht von jeder versendeten EMail eine Kopie an die Programmierer dieser Freeware, um so nach deren Angaben den Verbreitungsgrad des Programmes kontrollieren zu können. [HeiseS00]
- Der **Comet Cursor** verwandelt auf bestimmten Webseiten den Mauszeiger in eine Cartoon-Figur. Insgeheim werden Bewegungsdaten, wie eine eindeutige Seriennummer (GUID), Aufenthaltsort und somit auch Verweildauer an die Betreiber der Seiten übermittelt. [SpiegelC99]
- Der **Multimedia-Player** von Microsoft ist geeignet, sehr viele verschiedene Medienformate wiederzugeben und befindet sich nach jeder Windowsinstallation automatisch auf dem Computer. Wie Untersuchungen der Computerzeitschrift c't ergeben haben, überträgt dieser, wie auch der RealPlayer von RealNetworks, bei jedem Abspielen von Multimedia-Dateien aus dem Internet heimlich die GUID an den entsprechenden Server. [HeiseM00]

Trojaner werden häufig als Attachment per EMail verschickt, mit der Intention, dass dieses vom Nutzer ausgeführt wird. Eine andere Variante, die mit dem EMail Programm Eudora funktioniert, ist, Attachments nicht ausführen, sondern nur abspeichern zu lassen und dieses dann mit einem in der

E-Mail erhaltenen Link zu referenzieren, so dass der Nutzer, wenn er den Link in dem Glauben nutzt, damit irgendwo ins Netz zu gelangen, in Wirklichkeit ungewollt ein Programm auf seinem Computer aufruft. [EMail00, S. 76]

13.6 Fehlerhafte Programme

Für die meisten Nutzer dürfte der Aufwand, der durch fehlerhafte Programme entsteht, wie z.B. Abstürze einschließlich Datenverlust eines Betriebssystems oder ein Textverarbeitungsprogramm, das das Layout einer längeren Arbeit durcheinanderwirbelt, über einen längeren Zeitraum betrachtet, aufwendiger sein, als die Beseitigung entstandener Schäden durch Viren.

Fehler gibt es in fast jedem Programm, egal wie umfangreich es getestet wurde.⁴² In Windows 2000 werden beispielsweise ungefähr 63.000 Fehler vermutet, davon lt. Angaben von Microsoft 23.000, die zu echten Problemen führen könnten. [HeiseF00] Nicht jeder Fehler hat fatale Folgen, doch wird ein Produkt bei steigender Anzahl instabil und die Bedienerfreundlichkeit sinkt.

13.6.1 Beispiele

Bekanntgewordene Beispiele für fehlerhafte Programme beziehen sich in den meisten Fällen auf Sicherheitslücken, die durch diese Programme entstehen. Nachfolgend wird nur ein kleiner Ausschnitt der vielen Fälle von fehlerhafter Software wiedergegeben:

- **Internet Explorer:** Durch eine im Internet Explorer 5 gefundene Sicherheitslücke können beliebige Dateien auf der eigenen Festplatte, deren Speicherort bekannt ist, aus dem Internet gelesen werden. [HeiseIE99]
- **MS-Office 97:** Durch einen fehlerhaften Treiber in der ODBCJT32.DLL können aus MS-Excel Tabellen heraus Befehle an das Betriebssystem abgesetzt werden.⁴³
- **fingerd:** Der berühmte Morris-Wurm nutzte einen Fehler in der Implantierung der Software fingerd, um mittels eines Speicherüberlaufes, der entsteht, wenn mehr als die erwartete Anzahl Zeichen übergeben werden, Administratorrechte zu erhalten. [Fuhrberg98, S.70]

⁴²Am 4. Juni 1996 explodierte die Ariane 5 Rakete 40 Sekunden nach ihrem Start aufgrund eines Softwarefehlers. Die einzelnen verwendeten Komponenten waren aufwendig sowie fehlersicher konstruiert und als korrekt bewiesen, nur das Zusammenspiel funktionierte nicht. [Engels98, S. 17]

⁴³<http://pages.whowhere.com/computers/cuartangojc/>

- **PPTP**: Das für virtuelle, private Netzwerke von Microsoft entworfene und implementierte *Point-to-Point-Tunneling Protocol* wurde als eine der solidesten Sicherheitsmaßnahmen am Markt angepriesen. Zwischenzeitlich sind fünf verschiedene Fehler in der Implementierung bekannt geworden. Jeder dieser Fehler ermöglicht es in das Sicherheitskonzept einzubrechen. [Anon99, S. 21f]
- **Y2K**: Das Jahr-2000-Problem entstand aufgrund zweier Fehler. Der erste war ein Konstruktionsfehler, da die Datumsspezifikation in vielen Programmen nur sechs Stellen vorsah und ein Datum entsprechend als beispielsweise 09.09.90 abgebildet, das Jahrhundert aber nicht beachtet wurde. Der zweite Fehler beruht auf schlechter Programmierung, da in den betroffenen Programmen viele, nicht dokumentierte Zugriffe auf dieses Datum stattfanden, die sechs Stellen erwarteten und bei acht diverse Fehler produzierten.

13.7 Gefährliche Programme

Als gefährliche Programme werden hier die aufgeführt, die gezielt eingesetzt werden, oder eingesetzt werden können, um viele Nutzer auf einmal anzugreifen. Diese Programme lassen sich generell in drei verschiedene Kategorien einteilen.

13.7.1 Hintertürprogramme

Hintertürprogramme installieren sich, meistens aufgrund eines Aufrufes durch unachtsame Anwender, selbst auf dem Computersystem. Einmal installiert öffnen sie das PC-System nahezu jedem beliebigem Angreifer. Dieser ist dann in der Lage, alle Handlungen, die der Nutzer selber machen kann, nachzuvollziehen oder auszuüben. Darüber hinaus können Tastaturanschläge aufgezeichnet und übertragen, Viren installiert werden und vieles mehr. Wer einen Multimedia-Computer mit Kamera und Mikrofon besitzt, liefert dem Angreifer eine zusätzliche Überwachungsmöglichkeit mit Bild und Ton. [Luckh99, S. 88]

Zu den Programmen dieser Art gehören: SubSeven, Deep Throat, NetSphere und BackOrifice.⁴⁴ Dieses umfangreiche Programm ist beispielsweise seit dem 03.08.1998 im Internet verfügbar und kann per Email verschickt werden. Aktiviert der Empfänger dieses Programm, so installiert es sich und ermöglicht von nun an, das der PC über das Netz kontrolliert und ausgespäht wird. So werden die Tastatureingaben aufgezeichnet, Screen-Shots erstellt, Systeminformationen ausgelesen, Einträge in der Registry beliebig modifiziert, das

⁴⁴Eine umfassende Liste findet man auf <http://www.multimania.com/ilikeit/>.

Filesystem manipuliert und vieles mehr.

Hintertürprogramme werden häufig als Trojaner bezeichnet. Diese generelle Bezeichnung ist aber meistens falsch, da diese Programme nicht vorgeben etwas anderes zu sein. Hersteller von sogenannter Fernwartungssoftware, die über die gleiche Funktionalität verfügt, wie Hintertürprogramme bedienen sich oft des Ausdruckes Trojaner für diese Programme, um so etwaige Kunden der Konkurrenz zu verunsichern. So verurteilt Microsoft ein Hintertürprogramm als bösertiges, da dieses nach einer Installation nur sehr schwer zu entdecken ist, bewerben aber ihre eigene Fernwartungssoftware damit, dass sie so konfigurierbar ist, dass es für Fernwartungszugriffe keine Anzeichen gibt. [Luckh99, S. 89]

13.7.2 Überwachungsprogramme

Überwachungsprogramme werden meistens von staatlichen Organisationen, wie der *National Security Agency* (NSA) oder dem *Bundesnachrichtendienst* (BND) eingesetzt, um verdachtsunabhängig möglichst viele elektronische Kommunikationsverbindungen, wie z.B. EMail, Telefon oder Fax abzuhören, aufzuzeichnen und auszuwerten. Die Leistungsfähigkeit dieser Systeme ist zwischenzeitlich so gut, dass davon ausgegangen werden muß, dass jede Kommunikation von mindestens einem Dienst aufgezeichnet wird, insbesondere jede EMail. Aufgrund des hohen täglichen EMail Aufkommens werden aber nur die EMails längere Zeit gespeichert, in denen bestimmte Schlagwörter, wie z.B. Mord, Attentat, Schnee, etc. auftauchen.

Bekannt gewordene Programme dieser Art sind z.B.:

- **Echelon**⁴⁵: Dieses System wird von der amerikanischen NSA z.T. seit 50 Jahren genutzt, um fast jede elektronische Kommunikation abzuhören. Zu dem System gehören auch Stationen, die von Großbritannien, Kanada, Australien und Neuseeland unterhalten werden. [Campbell00]
- **Carnivore**⁴⁶: Das System wird vom FBI eingesetzt, um die elektronische Kommunikation eines einzelnen eingehend zu überprüfen. Dazu wird ein PC des FBI, mit der entsprechenden Software bei dem Provider des Ziels installiert. Dieser überprüft die Kommunikation und leitet diese gegebenenfalls an den Server des FBI's weiter. [Christ00, S. 96]

⁴⁵engl.: Staffelung

⁴⁶engl.: Fleischfresser

13.7.3 Aktive Elemente

Unter dem Begriff ausführbare Inhalte, bzw. aktive Elemente von Webseiten werden Programme bezeichnet, die in HTML-Dokumente integriert sind und automatisch vom Internet-Browser nach dem Laden gestartet werden. Diese Programme werden folglich auf der Seite des Client ausgeführt. Es gibt sie in verschiedenen Sprachen, z.B. ActiveX, Java, JavaScript, VBScript, mit unterschiedlichen Eigenschaften und verschiedenen Sicherheitskonzepten.

Java wurde 1991 entwickelt, mit dem Ziel, größtmögliche Plattformunabhängigkeit zu erhalten. Um dies zu gewährleisten, generiert ein Java Compiler keine prozessorabhängigen Maschinenbefehle, sondern einen neutralen Bytecode (Applet), der bei einem Seitenaufruf an den Aufrufenden gesendet wird. Ein spezieller Interpretor, die sogenannte Java Virtual Machine (JVM), setzt den Bytecode auf der Seite des Empfängers in Maschinenbefehle um. Java wurden bereits bei der Konzeption starke Sicherheitsmechanismen mitgegeben, unter anderem die sogenannte *Sandbox*. Bei dieser wird ein Java Applet in einer sicheren Umgebung, genannt Sandbox, ausgeführt. Bestimmte Zugriffe aus dieser Sandbox auf das Computersystem werden nicht gestattet. [Raeppe98, S. 53f]

Im Vergleich zu Java gilt ActiveX als sehr unsicher, da die sogenannten ActiveX Objekte weitreichende Zugriffsrechte auf einem Computersystem erhalten. ActiveX basiert auf einer von Microsoft entwickelten Technologie und ist entsprechend an das Betriebssystem Windows gebunden. Das Sicherheitskonzept von ActiveX bezieht sich auf die AuthenticCode Technologien. Dabei wird ActiveX-Komponenten der Zugriff auf das Computersystem nur gestattet, wenn der Programmierer dies ausdrücklich erlaubt, oder wenn sie über eine Signatur verfügen und einem Programmierer folglich eindeutig zugeordnet werden können.

Die nachfolgende Liste zeigt einige Beispiele auf, wie Angriffe trotz bestehender Sicherheitsmechanismen durchgeführt wurden:

- Mit Java können die Eingaben in ein Formular der nachfolgenden Seite abgehört und an einen Server übertragen werden. [Anon99, S. 639]
- Der Chaos Computer Club hat ein ActiveX Programm auf einer Seite im Internet demonstrativ implementiert. Wird diese Seite aufgerufen und die Ausführung gestattet, überweist dieses Programm, falls auf dem Computer die Software Quicken installiert ist, mit Hilfe dieser Software per T-Online einen Betrag auf ein bestimmtes Konto. [Lauer98, S. 405]

Aufgrund der immer stärkeren Integration des Internet-Browsers in das Betriebssystem ist zu erwarten, dass Angriffe dieser Art häufiger und vor allem in ihren Auswirkungen stärker werden.

14 Sozialer Angriff

Mit sozialen Angriffen wird versucht, den Nutzer in irgendeiner Weise zu veranlassen, sicherheitsrelevante Daten preiszugeben. Dies geschieht nicht primär mit Hilfe eines Programmes oder ausgefeilter Technik, sondern ausschließlich durch Überzeugungsarbeit. Soziale Angriffe kommen in verschiedenen Formen mit Hilfe verschiedener Medien, wie z.B. Telefon oder EMail, vor. So registrierte allein der Zugangsdienst CompuServe im letzten Quartal 1998 rund zehn Versuche von Unbekannten, mit Hilfe von Massenmails an Zugangsdaten und Paßwörter von Nutzern zu kommen. Der Text dieser EMail ist ähnlich zu einem möglichen Gesprächsverlauf, falls der Angreifer das Telefon nutzen sollte. Darin berichtet ein angeblicher Systemadministrator oder eine ähnliche Person mit Vertrauensstatus, dass es zu Problemen gekommen ist und jetzt das Paßwort und die Zugangsdaten benötigt werden bzw. kurz das Paßwort auf ein angegebenes zu wechseln sei, damit das Problem behoben werden kann. Von diesem sozialen Angriff gibt es zahllose Varianten, so ist es auch denkbar, dass ein Problem erzeugt wird, und der Nutzer dann eine EMail mit obiger Aufforderung erhält.

In Amerika ist ein sehr trickreicher Fall eines sozialen Angriffes bekannt geworden. Telefonhacker hatten sich Zugang zu einer Vermittlungsstelle verschafft und viele von dort erreichbare Personen angerufen. Diesen wurde erzählt, dass es derzeit ein Sicherheitsproblem bei einem Kreditinstitut gäbe und entsprechend die PIN gesperrt werden müsse. Damit dies gemacht werden kann, muß die PIN dem Systemadministrator mitgeteilt werden. Da dies aber am Telefon jeder behaupten kann, sollten sie ihre Kreditkarte umdrehen und die Nummer für die Sperrung, die auf der Rückseite steht, anrufen. Gerade diese Nummer aber wurde zu diesem Zeitpunkt durch den Angriff auf eine andere umgeleitet, ohne dass dies den Anrufern auffiel, so dass die Hacker an etliche hundert Kreditkarteninformationen und PIN's gelangten.

Teil V

Gegenmaßnahmen

*Die Kunst des Krieges lehrt uns, nicht darauf zu hoffen,
dass der Feind nicht kommt, sondern darauf zu bauen,
dass wir bereit sind, ihn zu empfangen.*

Grundsätzlich gibt es zwei Möglichkeiten sich bzw. seinen Computer und die darauf befindlichen Daten vor unerwünschten Zugriffen zu schützen. Entweder durch bestimmte Verhaltensregeln oder durch die Nutzung unterstützender Programme.

15 Verhaltensregeln

Unter den Punkt Verhaltensregeln fallen sicherheitsfördernde Verhaltensweisen und vom Nutzer selbst vornehmbare Änderungen der vorhandenen Einstellungen des Computersystems. Mit restriktiven Verhaltensregeln läßt sich ein Computersystem für die behandelten nicht-gerichteten Angriffe nahezu beliebig sicher machen. In den meisten Fällen verliert der Nutzer dadurch aber auch gleichzeitig Bequemlichkeit. So werden z.B. bestimmte Seiten im Internet nur korrekt dargestellt, wenn dynamische Elemente, wie z.B. JavaScript oder ActiveX, erlaubt sind. Gleichzeitig sind dies sicherheitskritische Merkmale, deren Aktivierung viele Angriffe ermöglichen.

15.1 Allgemeine Verhaltensmaßnahmen

Im Folgenden werden fünf sicherheitsfördernde Verhaltensweisen erläutert, bei deren Einhaltung der Nutzer bereits eine gewisse Sicherheit erlangt, ohne bestimmte Einstellungen vornehmen oder Programme installieren zu müssen. Die aufgeführten Maßnahmen wirken gegen bestimmte Angriffe:

Tabelle 2: Abwehr durch Verhaltensmaßnahmen

<i>Verhaltensmaßnahme</i>	<i>geeignet gegen</i>
Schutz persönlicher Daten	Datenspuren, soziale Angriffe
vorsichtiges Surfen	Spoofing
umsichtiges Mailen	Datenspuren
Infizierungen vermeiden	Schadhafte Programme
Datensicherung	Schadhafte Programme

15.1.1 Schutz persönlicher Daten

Eine der ersten und wichtigsten Verhaltensmaßnahmen ist die Verweigerung der Preisgabe von persönlichen Daten. Da, wie erläutert, der Datenschutz in vielen Ländern gesetzlich nicht gewährleistet ist, empfiehlt es sich, seine persönlichen Stammdaten so selten wie möglich offen darzulegen. Auch lassen sich viele Präsentationen im Internet nicht eindeutig einer Rechtsprechung zuordnen, so muß beispielsweise nicht zwingend die Endung .de im Domain Namen auf ein Unternehmen in Deutschland und somit der Gültigkeit von deutschen Datenschutzrichtlinien hindeuten.

Diese Schutzmaßnahme verhindert so zwar prinzipiell kein Beobachten der Bewegungen im Internet, aber den beobachtenden Unternehmen fehlt die Möglichkeit, die gewonnenen Daten einer realen Person zuordnen zu können. Dies gilt auch für die Software auf dem eigenen Rechner. Erfährt diese nicht die korrekten Stammdaten, ist es ihr nicht möglich, diese gesteuert oder aufgrund eines Fehlers, wie z.B. durch die bekannten Metadaten in Microsoft Office Dokumenten, weiterzugeben.

Sozialen Angriffen kann in der gleichen Weise begegnet werden. Wird z.B. der Nutzer von einer ihm nicht bekannten Personen per Mail oder Telefon kontaktiert und aufgefordert sicherheitsrelevanten Daten preiszugeben oder irgendwelche Seiten im Internet zu besuchen, kann ein sozialer Angriff vorliegen. Unter keinen Umständen sollte der Nutzer solchen Aufforderungen Folge leisten.

15.1.2 Vorsichtiges Surfen

Die Web-Spoofing Angriffe zielen darauf ab, den Nutzer zu täuschen. Dabei sind diese keineswegs perfekt, denn oft werden Spuren hinterlassen, die dem Anwender zeigen, dass er gerade das Ziel eines Angriffes ist. So verschwindet unter Umständen die Locationzeile, es wird eine IP-Nummer anstelle des bekannten Namen angezeigt, der Sourcecode ist nicht einsehbar und anderes. Sollte es beim Surfen zu dem beschriebenen Verhalten des Internet-Browsers kommen, besteht der Verdacht, gerade erfolgreich getäuscht worden zu sein. Selbst wenn die betrachtete Seite unwichtig ist und die enthaltenen Informationen keinerlei Handlungen auslösen, ist ein solcher Angriff gefährlich, da damit zu rechnen ist, dass sich der Nutzer von nun an in einem beobachteten Raum bewegt, deshalb sollte der Browser neu gestartet werden. Weiter sollten keine Links zu sicherheitsrelevanten Seiten genutzt werden, solange man sich nicht davon überzeugt hat, dass diese korrekt sind, bzw. der Herkunft der Links vertraut werden kann. Auch die bei Suchmaschinen als Resultat einer Suche angegebenen Links können falsch sein, da diese nicht den Inhalt des Ziels überprüfen.

Eine einfache und effektive Möglichkeit, dieser Art von Angriff zu begegnen ist, sich die IP Nummer der kritischen Adressen zu besorgen und diese als Adresse einzugeben. So kann beispielsweise 'http://194.122. 76.131' statt 'http://www.heise. de' verwendet werden. [Weidner97, S. 2f] Durch das anschließende Setzen eines Bookmarks hat man die Möglichkeit, die Adresse zu speichern und kann sie leicht aufrufen.⁴⁷, ohne jedesmal die IP-Adresse eingeben zu müssen. Eine weitere Möglichkeit sich gegen Web-Spoofing zu schützen, besteht in der Deaktivierung von aktiven Inhalten, wie z.B. Java oder JavaScript, da die meisten Angriffe diese Elemente nutzen, um den Surfer zu täuschen. Genauere Anweisungen zur Deaktivierung sind in Kapitel 15.2.1 zu finden.

15.1.3 Umsichtiges Mailen

Da eine abgeschickte EMail theoretisch von jeder beliebigen Person, insbesondere einer, von der man es sich am wenigsten wünscht, abgefangen und gelesen werden kann, sollten niemals sicherheitsrelevante Informationen, wie z.B. Paßwörter, PIN's oder Bankverbindungen unverschlüsselt weitergegeben werden. Eine weitere Möglichkeit, mittels umsichtiges Verhaltens, Schaden zu verhindern, besteht darin, bestimmte Mails, sogenannte Hoax Meldungen als solche zu erkennen und nicht weiterzuleiten, damit diese keine auslastende Wirkung auf Mailverteiler haben und somit harmlos werden.

15.1.4 Infizierungen vermeiden

Ein Computer kann nur dann von einem schadhaften Programm infiziert werden, wenn dieses mindestens einmal auf dem System ausgeführt wird. Die aufgeführten Verhaltensregeln sollen ein erstmaliges Ausführen dieser Programme verhindern.

- Nicht mit einer „fremden“ Diskette den Computer starten. Auch wird eine Diskette häufig im Laufwerk vergessen und bei einem Neustart automatisch davon gebootet. Eine Möglichkeit das automatische Booten von Diskette zu verhindern, ist die Bootreihenfolge (Diskette, Festplatte) im BIOS so zu ändern, so dass immer zuerst von der Festplatte gestartet wird.
- Keine Attachments in erhaltenen Mails ausführen oder herunterladen, deren Erhalt nicht explizit abgesprochen war. Viele Makroviren verschicken sich selber anhand des Adressbuches, so dass der Sender beim Empfänger bekannt ist. Oft wird hier der Fehler gemacht und dem Attachment vertraut, da der Kommunikationspartner bekannt ist.

⁴⁷Das Programm name2ip.pl wandelt einen Namen in eine IP-Nummer.

- Erhaltene Dateien oder Programme vor dem Start im eigenen Computersystem unbedingt mit einem aktuellen Anti-Viren Programm auf Viren oder Trojaner überprüfen.

Viren können sich schneller verbreiten, wenn sie bestimmte Orte infizieren, von denen möglichst viele andere erreicht werden. So sind gerade immer wieder Raubkopiergruppen, die einen hohen Umschlag an Programmen haben, als Hauptverbreitungsquellen von Viren bekannt geworden. Eine Sicherungsmaßnahme ist entsprechend einfach, man muß lediglich auf den Einsatz von Raubkopien verzichten.

15.1.5 Datensicherung

Aufgrund ihrer Konzeption und Durchführung stellt eine Datensicherung immer nur eine Schutzmaßnahme⁴⁸ dar, die erst dann benötigt wird, wenn alle anderen Maßnahmen nicht gegriffen haben und ein Angriff wichtige Dateien zerstört hat.

Die richtige Methode zur Datensicherung ist von individuell verschiedenen Parametern abhängig. Auf der Seite des Nutzers sind die Punkte Wahrscheinlichkeit und Bedrohungsschwere eines Angriffes wichtig. Die Bedrohungsschwere richtet sich nach dem möglichen Schaden, meßbar an dem Aufwand, alle verlorenen Daten zu restaurieren, und muß für jeden individuell festgesetzt werden, kann also als Antwort auf die Frage: "Wieviel Aufwand wäre notwendig, wenn jetzt alle Daten unrettbar gelöscht sind?" verstanden werden. In diesem Kontext sind die Daten eines Druckerservers hinter einer Firewall vermutlich nicht so gefährdet und entsprechend redundant vorhanden, wie die Daten eines Systems mit einer Habilitation, auf dem Kinder regelmäßig neueste Raubkopien ausprobieren.

Die wählbaren Komponenten einer Datensicherung sind Umfang, Zeitpunkt und Intervall und richten sich ganz nach den technischen Möglichkeiten und der allgemeinen Gefahrensituation, die aus Bedrohungsschwere und Wahrscheinlichkeit eines Angriffes resultieren. Zum möglichen Vorgehen gibt es verschiedene Prinzipien:

- Das sogenannte „Großvater-Vater-Sohn-Prinzip“ besagt einfach, das eine Datensicherung eine gewisse Zeit gehalten wird. So kann bspw. für jeden Wochentag eine Sicherung erstellt werden, um zu verhindern, dass bei einer ungültigen Sicherung eine Restaurierung unmöglich wird.

⁴⁸Der allgemeine Begriff Datensicherung hat seinen Bezugspunkt auf die Daten, während sich die hier erläuterten Begriffe Sicherungs- und Schutzmaßnahmen auf ein Computersystem allgemein beziehen, daher die verschiedenen Betrachtungen.

Dies sollte mit längerfristigen Zeitrhythmen ergänzt werden, da so verhindert wird, dass z.B. ein längere Zeit unbemerkt gebliebener Virus die gesamte Datensicherung kontaminiert. So kann zu obiger Tagessicherung noch Wochen-, Monats- und Jahressicherung hinzugenommen werden.

- Bei der Inkrementellen oder Vollsicherung muß unterschieden werden, ob nur die Dateien gesichert werden, die sich seit der letzten Datensicherung verändert haben, bzw. neu hinzugekommen sind, oder ob alle Dateien gesichert werden. Das erste Verfahren ist deutlich schneller und kostengünstiger, da weniger Daten gesichert werden, während das zweite Verfahren etwas sicherer ist und schnellere Wiederherstellung ermöglicht. Für das erste Verfahren müßte jede Sicherung eines Zyklus in der richtigen Reihenfolge zurück gespielt werden, während bei der Vollsicherung eine Rückspielung genügen würde.

15.2 Veränderte Einstellungen

In den meisten Fällen sind die Grundeinstellungen neu installierter Programme unzureichend und erlauben unnötigerweise viele Angriffe. Die nachfolgenden Punkte sollen einfache Möglichkeiten erläutern, mit denen ein Nutzer, ohne zusätzliche Programme zu nutzen, die Sicherheit seines Computers erhöhen kann. Neben den aufgeführten, gibt es viele weitere Einstellungsmöglichkeiten, abhängig von dem genutzten Programm, die die Sicherheit erhöhen. Aufgrund der Vielfalt der Möglichkeiten und des daraus folgenden steigenden Umfangs beschränkt sich diese Ausarbeitung auf folgende Punkte, die ausgewählt wurden, um so einen großen Bereich abzudecken und mögliche Lücken durch fehlerhafte Einstellungen in anderen, nicht behandelten Programmen anzudeuten.

Tabelle 3: Abwehr durch veränderte Einstellungen

<i>Einstellungen</i>	<i>geeignet gegen</i>
Internet-Browser	Spoofing, Datenspuren, schadhafte Programme
Microsoft Office	schadhafte Programme
Windows-Explorer	Schadhafte Programme

15.2.1 Internet-Browser

In den verwendeten Browsern läßt sich die Gefahr mit Hilfe von Cookies, beobachtet zu werden, relativ einfach vermeiden, da in vielen Browsern eine

Verbotsvorschrift für Cookies vorgesehen ist. Bei deren Aktivierung verweigert der Browser die Plazierung von Cookies auf dem Computer bzw. erlaubt keinen Zugriff mehr auf bereits abgelegte, was somit eine Sicherungsmaßnahme darstellt. Bei Netscape findet man diesen Schalter unter Bearbeiten, Einstellungen, Erweitert und dann Cookies deaktivieren. Im Internet Explorer befindet sich dieser Schalter bei Extras, Internetoptionen, Sicherheit, Internet(Stufe anpassen) und wieder Cookies deaktivieren.

Bereits auf der Festplatte abgespeicherte Cookies lassen sich wiederum abhängig vom Internet-Browser löschen. Netscape speichert alle Cookies in die Datei cookies.txt im Verzeichnis /Netscape/Users/<name>/. Wird diese Datei gelöscht, so werden auch die entsprechenden Cookies gelöscht. Der Internet Explorer speichert alle Cookies in den Ordner /Windows/Cookies/. Es genügt, die Dateien in diesem Ordner zu löschen, um alle Cookies zu entfernen.

Dem Internet-Browser die Ausführung von dynamischen Elementen, wie z.B. Java, JavaScript, ActiveX und anderen zu gestatten, ermöglicht viele verschiedene Angriffe im Internet. Unter anderem sind dies :

- Ausführung von schadhaften Programmen aufgrund fehlerhafter Implementierung dieser Sprachen.
- Ein automatisiertes Beobachten der Bewegungen des Nutzers durch auswertbare Datenspuren.
- Viele Täuschungsmannöver, sogenanntes Web-Spoofing, werden durch Java und JavaScript ermöglicht und wirkungslos, sobald die Ausführung verboten wird.

Diese Sprachen lassen sich einfach deaktivieren, allerdings mit dem Nachteil, dass dann viele Seiten im Internet nicht korrekt dargestellt werden, da sie gerade diese Elemente einsetzen. Hier muß jeder selber entscheiden, welches Risiko er bereit ist einzugehen, bzw. wie weit er auf bestimmte Seiten verzichten möchte.

Unter Netscape läßt sich die entsprechende Einstellung unter Bearbeiten, Einstellungen, Erweitert und dort Java und JavaScript deaktivieren⁴⁹, bei dem Internet Explorer unter Extras, Internetoptionen, Sicherheit, Internet, Stufe anpassen, ActiveX (deaktivieren), Java (deaktivieren) und Scripting (deaktivieren).

⁴⁹Andere Sprachen, wie z.B. ActiveX oder VisualBasic werden von Netscape nicht interpretiert.

WebBugs stellen so etwas wie eine kreative Anwendung einer Technik dar, die eigentlich etwas anderes bewirken sollte, und mit der keiner gerechnet hat. Aus diesem Grund gibt es im Internet Explorer oder bei Netscape keinen Schalter, wie bei den Cookies, mit denen sich WebBugs ausschalten lassen. Diese lassen sich auch nicht über die Größe von normalen Bildern unterscheiden, da theoretisch jedes Bild ein WebBug darstellen kann. Die Vermutung, dass ein Bild ein WebBug ist, liegt dann nahe, wenn das Ziel des IMG Tags nicht mit der eigentlichen Domäne übereinstimmt.

Eine Möglichkeit, das Laden von WebBugs zu verhindern, ist somit generell das Laden von Bildern zu verbieten und nur solche manuell nachzuladen, die für relevant gehalten werden. Bei Netscape läßt sich das automatische Laden ein- bzw. ausschalten unter Bearbeiten, Einstellungen, Erweitert (Grafiken automatisch laden). Bei dem Internet Explorer findet man diese Möglichkeit unter Extras, Internet Optionen, Erweitert, Multimedia (Bilder anzeigen), außerdem kann beim Internet Explorer das Zugreifen auf Inhalte über Domaingrenzen hinweg unter Extras, Internet Optionen, Sicherheit, Stufe anpassen, Verschiedenes (Auf Datenquellen über Domaingrenzen hinweg zugreifen) verboten werden. Darüber hinausgehende Einstellungsveränderungen sind teilweise Geschmackssache und deren Erläuterung würde aufgrund des Umfangs den Rahmen dieser Ausarbeitung sprengen. Bei der Adresse <http://www.heise.de/ct/browsercheck/> lassen sich die Einstellungen seines Browser überprüfen.

15.2.2 Microsoft Office

Die Ausführung und somit Verbreitung von Makroviren läßt sich in Microsoft Office unterbinden, wenn bestimmte Einstellungen vorgenommen werden. Unter dem Menüpunkt Extras, Allgemein, Makrovirus-Schutz läßt sich ein Kontrollkästchen aktivieren. Durch setzen eines Häkchens erscheint von nun an eine Warnmeldung, wenn der Nutzer ein Dokument öffnet, welches einen Makrocode und somit potentiellen Virus enthält. In dieser Meldung hat der Nutzer die Möglichkeit, die Ausführung des Makros zu gestatten, bzw. abzulehnen.⁵⁰ Niemals sollte Makros, die nicht selber erstellt oder deren Wirkung nicht genau bekannt ist, die Ausführung gestattet werden. Makros aus bekannten Quellen, deren Wirkung aber unbekannt sind, könnten sich selber verschickt haben, wie bei dem I LOVE YOU Virus und stellen somit auch eine Gefahr dar. Das Deaktivieren dieses Virenschutzes von Microsoft Office läßt sich über die Registry problemlos vornehmen, was sich bereits einige Viren zunutze gemacht haben. Um zu verhindern, dass der Schutz über längere Zeit ausgeschaltet ist, sollte immer wieder überprüft werden, ob das

⁵⁰In dieser Meldung hat der Nutzer auch die Möglichkeit, diese Warnmeldung generell abzustellen. Einmal angeklickt, erhält der Nutzer keine Warnmeldungen mehr.

Kontrollkästchen noch aktiv ist.

15.2.3 Windows-Explorer

Der Windows-Explorer zeigt nach einer Neuinstallation die Dateiendungen, wenn diese bekannt, d.h. einem Programm zugeordnet sind, nicht an. Durch die Verzahnung von Internet-Browser und Betriebssystem macht sich dieses auch in den Internetdiensten unter den Betriebssystemen der Windows-Reihe, vor allem Windows 98 und nachfolgende bemerkbar. So wird z.B. die Datei HARMLOS.TXT.exe als HARMLOS.TXT angezeigt und sicherlich unbedenklicher erscheinen, als wäre hier EXE, also ausführbar, zu sehen. Eine Textdatei wird unter Windows mit Notepad geöffnet und stellt keine Gefahr für das System dar, selbst wenn der Inhalt ein Virus ist. Das Ausführen einer EXE Datei mittels Doppelklick liefert das System vollständig an dieses Programm aus. Um solche Angriffe zu verhindern sollten die Grundeinstellungen im Explorer geändert werden. Unter MS-Windows ist dies der Punkt Ansicht, Optionen, (keine MS-Dos Erweiterungen für registrierte Dateien).

16 Programme

Unterstützung findet der Nutzer in vielen Programmen, die ihm Helfen, bestimmte Angriffe abzuwehren. Programme können eine sehr mächtige Unterstützung darstellen, aber den Programmierern muß unbedingt vertraut werden, da man ihnen durch das Starten der Programme in vielen Fällen Zugriff auf die eigenen Daten gewährt.

Die möglichen Programme zum Schutze des Nutzers lassen sich generell in zwei Kategorien einteilen: Einmal Programme, die auf dem Computer des Nutzers laufen, und einmal Programme, die auf einem Server irgendwo im Internet laufen. Beide Versionen haben Vor- und Nachteile. Die serverseitigen Programme können eigentlich keine Schäden auf dem Rechner des Nutzers anrichten, während sie ohne weiteres ihrem Betreiber alle erhaltenen Informationen über den Nutzer mitteilen können. Die clientseitigen Programme können direkt Schaden anrichten, da sie in den meisten Fällen uneingeschränkten Zugriff auf das Computersystem haben, aber nur dann Informationen übermitteln, wenn eine Verbindung zwischen Computer und Ersteller besteht.

16.1 Clientseitige Programme

Die Wirkung der Client-Programme läßt sich grob an folgender Tabelle erkennen:

Tabelle 4: Abwehr durch Client-Programme

<i>Programm</i>	<i>geeignet gegen</i>
Cookie finder	Datenspuren
Viren und Trojaner	Schadhafte Programme
Viewer	Schadhafte Programme
GUID	Datenspuren
Firewalls	Datenspuren, Schadhafte Programme

16.1.1 Cookie finder

Es gibt zwischenzeitlich viele Programme, die das Speichern von Cookies verhindern, einschränken, bzw. gespeicherte Cookies löschen, zum Beispiel auf der Seite www.winfiles.com. Programme dieser Art löschen einfach die bereits vorhandenen Cookies auf der Festplatte und verhindern das Ablegen neuer Cookies.

16.1.2 Viren und Trojaner

Programme stellen eine hilfreiche und mächtige Unterstützung gegen Viren bzw. Trojaner dar. Diese Programme können regelmäßig oder aber, was häufiger vorkommt, aufgrund des Verdachtes, dass ein schadhaftes Programm auf dem Computersystem aktiv ist, verwendet werden. Ein Programm, welches immer aktiv nach Viren oder Trojaner sucht, bzw. deren Zugriff auf die Festplatte verhindern möchte, ist zwar regelmäßig in Benutzung, wird aber in den meisten Fällen, wenn überhaupt, nur unregelmäßig, mit den neusten Dateien über Viren und Trojaner versorgt und muß entsprechend auch als unregelmäßig angesehen werden.

16.1.3 Schadhafte Programme entdecken

Viren lassen sich aufgrund ihrer meist offenen⁵¹ schadhafte Funktion leichter aufspüren, als Trojaner. Sobald der Computer anormales Verhalten zeigt, wie z.B. vertauschen von Buchstaben auf einem Ausdruck (Herbstlaubvirus) oder unerwartete Abstürze des Computers, kann die Ursache ein Virus sein. Sehr wahrscheinlich ist die Existenz eines Virus, wenn die Aktivitäten des Computers in keinem Zusammenhang zu den gerade genutzten Programmen stehen. So ist z.B. während der Nutzung von Word ein plötzlich erscheinender Lauftext ein relativ eindeutiges Zeichen für einen Virus.⁵²

⁵¹Nur die wenigsten Viren versuchen den entstandenen Schaden zu verbergen.

⁵²Gleiches gilt natürlich ebenso für eine plötzlich formatierte Festplatte oder gelöschte Dateien, nur ist dann die Erkennung des Virus vermutlich zu spät.

Die Entdeckung von Trojanern ist in vielen Fällen ungleich schwerer, da sie sich auf zwei verschiedene Weisen tarnen. Zuerst täuschen sie dem Nutzer vor, ein sinnvolles Programm zu sein, dessen Funktionalität genutzt wird und zweitens werden in den meisten Fällen die schadhafte Auswirkungen verborgen. Unter Windows gibt es viele Möglichkeiten, gerade laufende Programme oder solche, die mit dem Betriebssystem gestartet werden, aufzuspüren. Diese sind aber vielfach unzureichend, so dass dem möglichen Ergebnis: "kein aktives, schadhafte Programm" nur eingeschränkt vertraut werden kann.

- Mit dem sogenannten **Task Manager**⁵³ können laufende Tasks (Programme) angezeigt werden. Da jedes Programm aber selber entscheiden kann, ob es angezeigt werden möchte, ist diese Möglichkeit sehr unzuverlässig.
- In dem Ordner **autostart** des Verzeichnisses `c:\windows\startmenü\programme` sind Programme aufgeführt, die mit Windows automatisch gestartet werden. Diese Liste ist aber nicht vollständig.
- In der **Registry** von Windows, anzeigbar mit dem Tool Regedit, sind unter den Punkten `HKEY_LOCAL_MACHINE/Software/Microsoft/Windows /CurentVersion/Run` und `HKEY_CURRENT_USER/Software/Microsoft/Windows /CurrentVersion/Run` Programme aufgeführt, die automatisch gestartet werden. Diese Listen sind zwar sehr genau, trotzdem aber unzureichend, da erstens nicht alle Programme verzeichnet sind und zweitens Viren bzw. Trojaner in den meisten Fällen als nützliches oder bekanntes Programm, wie beispielsweise `command.com` aufgeführt werden.

Neben diesen unzuverlässigen Methoden gibt es noch weitere, die in den meisten Fällen sehr genau aktive schadhafte Programme anzeigen, gleichzeitig aber auch viele andere Prozesse, so dass schadhafte Programme auch hier unentdeckt bleiben dürften.

- Mit der sogenannten **Objektvergleichsmethode** werden von einem Programm Prüfsummen zu allen wichtigen, eingesetzten Programmen gebildet. In gewissen Zeitintervallen werden diese neu gebildet und mit den alten, gespeicherten verglichen. Hat sich die Prüfsumme verändert, so kann die Ursache darin begründet sein, dass ein schadhafte Programm an dem überprüften Programm Veränderungen vorgenommen hat. In den meisten Fällen haben aber legale Operationen, wie z.B.

⁵³unter Windows durch gleichzeitiges Drücken der Tasten alt, strg und entf aktivierbar

Änderung des Datums, Paßwortes oder Anzahl der Aufrufe den Source Code des Programmes verändert, so dass der Nutzer die Meldung bei der Objektvergleichsmethode bewerten muß, was er in den meisten Fällen nicht kann.

- Das **Tätigkeitsmonitoring** überwacht auf einem Computersystem sämtliche Aktivitäten, wie z.B. Zugriffe auf das Filesystem, die Registry und andere zentrale Komponenten. Ein aktiver Virus oder Trojaner wird hier angezeigt, wie aber auch alle anderen Programme, so erfolgen z.B. alleine durch den Start von MS Word 97 über 4200 Zugriffe auf die Registry.

16.1.4 Schadhafte Programme entfernen

Da sich residente Viren vor einer Entdeckung schützen können, ist es unerlässlich, deren Start zu verhindern, bevor Anti-Viren Programme oder andere zur Entdeckung, bzw. Bekämpfung von Viren gestartet werden. Entsprechend muß der Computer von einer nicht infizierten Bootdiskette gestartet werden.

Die meisten Trojaner verfügen über bekannte Funktionen, aufgrund derer sie eingesetzt und nicht als Trojaner erkannt werden. Hier fällt das Erkennen eines schadhaften Programmes sehr schwer und die beste Methode ist zu Wissen, welche Programme allgemein als Trojaner bekannt sind. Dies kann durch regelmäßiges Lesen bestimmter Seiten im Internet, wie z.B. www.heise.de, www.dr Solomon.de oder anderer, die sich mit diesem Thema beschäftigen, geschehen.

Die einzige anwendbare Methode, Viren und Trojaner zu entdecken und zu entfernen, ist der Einsatz sogenannter Anti-Viren Programme. Diese vergleichen Dateien und Programme mit bestimmten Suchmustern. Diese Muster sind eindeutige Merkmale von Viren. Taucht in einer Datei so ein Muster auf, gilt diese als Befallen und der Virus wird nach einem entsprechenden Algorithmus entfernt. Anti-Viren Programme sind nur so gut, wie ihre vorhandene Suchmusterbibliothek, dadurch ist es notwendig diese immer aktuell zu halten. Bekannte Anti-Viren Programme sind z.B. F-Prot, eSafe Desktop oder McAfee.⁵⁴

Neben diesen vergleichenden Anti-Viren Programmen gibt es andere, die ständig im Hintergrund aktiv laufen und alle Aktivitäten und startende Programme auf dem Computer überwachen. Kommt es dabei zu einer Anomalität oder wird ein schadhafte Programm entdeckt, verbietet das Programm

⁵⁴Einen Vergleich der Anti-Viren Software findet man in dem Artikel „Schutz vor Ungeziefen“ der Computerzeitschrift c't Heft 13/2000 S. 114 des Heise Verlages.

den entsprechenden Zugriff. Diese Programme benötigen ebenso zur Erkennung der Viren, möglichst aktuelle Bibliotheken.

16.1.5 Viewer

Die jüngsten Virenepidemien gehen auf das Konto sogenannter Makroviren. Diese benötigen zur Ausführung in vielen Fällen Microsoft Office. Eine Möglichkeit, dieser Gefahr zu begegnen ist der Einsatz sogenannter Microsoft Office Viewer, mit denen Dokumente betrachtet werden können, ohne dass dabei ein schadhafter Code ausgeführt wird.⁵⁵ Generell sollten die Einstellungen in dem Explorer so sein, daß potentiell gefährlichen Attachments von E-Mails zuerst in einem Viewer betrachtet werden.

16.1.6 Abwehrmaßnahmen gegen GUID

Um sich vor den Beobachtungen durch Ausnutzen der GUID zu schützen, gibt es mehrere Ansätze:

- Mit der Installation eines **Patches** von Microsoft speichert Office 97 keine GUID mehr in den Dokumenten.⁵⁶
- Mit **falschen Angaben** einem Installationsprogramm oder einer Registrierung gegenüber, bei persönlichen Fragen, verschafft man sich eine Deckidentität. Die Dokumente lassen sich zwar immer noch einem Rechner, aber nicht mehr einer Person zuordnen.
- **Erstellte Programm GUID.cpp**, dieses verändert entdeckte GUIDs in den Dokumenten zufällig, mit dem Vorteil, dass dieses Dokument nur noch sich selbst zugeordnet werden kann und so jeder Versuch, eine Datenbank mit den Zuordnungen aufzubauen, sinnlos ist.
- **Hexeditor**, die GUID läßt sich einfach von Hand entfernen. Dazu genügt ein HexEditor oder Notepad. In diesem das Dokument, in der die GUID gespeichert ist, öffnen und diese suchen und löschen oder bearbeiten.

16.1.7 Metadaten

Ohne bestimmte Maßnahmen werden ausführliche Informationen in den Dokumenten, die mit Microsoft Office erstellt werden, gespeichert. Folgende Einstellungen schränken die Speicherung dieser Informationen ein:⁵⁷

⁵⁵Download unter <http://www.eu.microsoft.com/msdownload/>

⁵⁶<http://officeupdate.microsoft.com/downloaddetails/off97uip.htm>

⁵⁷nachzulesen unter <http://officeupdate.microsoft.com/articles/medadata.htm>

- Der Name des Autors ist unter Extras, Optionen, Benutzer-Info frei editierbar.
- Weitere persönliche Informationen sind unter Datei, Eigenschaften, Datei-Info einstellbar.

Neben diesen offensichtlichen Plätzen können Metadaten laut Microsoft auch in Kommentaren, Kopf- und Fußzeilen, Hyperlinks, Styles, versteckten Feldern, Ansichten (Views) und weiteren abgelegt sein.

Microsoft Office beinhaltet die Möglichkeit beim Abspeichern nicht das gesamte Dokument, sondern die Änderungen zu dem vorhergegangenen Dokument zu speichern. Dies hat zwei große Nachteile. Zuerst nimmt die Größe des Dokumentes mit der Zeit kontinuierlich zu, da alle Änderungen gespeichert werden und zweitens kann jeder Leser einsehen, welche Veränderungen das Dokument durchgemacht hat. Dieser Mechanismus kann unter Extras, Optionen, Speichern (Schnellspeicherung zulassen) an- oder ausgeschaltet werden.

16.1.8 Firewalls

Sogenannte Firewalls⁵⁸ sollen den Datenstrom zu und von einem Rechner überwachen und unerlaubte Zugriffe unterbinden. Technisch gesehen gibt es zwei verschiedene Typen von Firewalls. [Raepple98, S. 167]

Die *Paketfilter* arbeiten auf der Netzwerkschicht und lassen nur solche IP-Pakete passieren, für deren Ursprungs- oder Zieladressen Erlaubnisse erteilt wurden oder bestimmte andere Regelungen bezogen auf die Protokoll-Header zutreffen. Alle anderen Pakete werden verworfen. Diese Firewallvariante ist relativ billig und schnell einsetzbar. Gleichzeitig ist diese Variante aber auch sehr restriktiv, da sich komplexe Regeln nicht einsetzen lassen. Zudem kann sie bei bestimmten Angriffen, wie z.B. sogenanntem IP-Spoofing schnell unterlaufen werden. [Anon99, S. 304]

Auf den sogenannten *Proxy Gateways* läuft der gesamte Datenverkehr zwischen dem Computersystem (Innen) und der restlichen Welt (Außen). Im Unterschied zu den Paketfiltern wird jedoch die Verbindung zwischen Innen und Außen getrennt und keinem Paket der direkte Transfer gestattet. Wird versucht eine Verbindung aufzubauen, so überprüft der Proxy Gateway erst einmal, ob diese überhaupt erlaubt ist, bevor dieser stellvertretend die Verbindung aufbaut. Nach außen tritt also nur der Proxy auf und das Ziel erfährt nichts über den oder die dahinter liegenden Computer. Auf dem Proxy können beliebige, auch komplexe Regelungen für die Verbindung nach draußen

⁵⁸engl.: Brandschutzmauer

erstellt werden.

Eine Firewall hilft dem Nutzer gegen viele Angriffe.

- Die Übertragung von Informationen zur Identifizierung, wie ID, GUID, persönliche Daten usw. kann zu bestimmten Adressen erlaubt und zu allen anderen verboten werden.
- Das eigene System ist für Außenstehende nahezu unsichtbar und bietet so nur sehr wenig Angriffsfläche.
- Auf dem Proxy Gateway können Virentfilter installiert und auf diese Weise schadhafte Programme abgefangen werden, bevor diese relevante Daten erreichen.
- Die Firewall unterbindet oder protokolliert Datenströme von Trojanern, Hintertüren oder ähnlichen schadhaften Programmen nach draußen.

16.2 Serverseitige Programme

Tabelle 5: Abwehr durch Serverseitige Programme

<i>Programm</i>	<i>geeignet gegen</i>
Anonymizer	Datenspuren
kryptographische Verfahren	DNS-Spoofing
zufällige Query-IDs	DNS-Spoofing
Domain Namen überprüfen	DNS-Spoofing
EMail	Datenspuren

16.2.1 Anonymizer

Viele Gefahren durch passive und auch aktive Methoden des Datensammelns, wie z.B. mit WebBugs oder Cookies lassen sich vermeiden, wenn Anonymisierungsdienste, wie z.B. www.anonymizer.com genutzt werden. Diese funktionieren ähnlich, wie ein Web-Spoofing. Durch Zwischenschalten tritt der Nutzer im Internet nicht in Erscheinung, sondern der beauftragte Rechner des Anonymisierungsdienstes, so dass der Versuch, personenbezogene Daten über den Nutzer zu sammeln, mit den meisten Techniken erfolglos ist. Diesen Dienst kann jeder nutzen. Vor der Zieladresse, z.B. www.beispiel.de muß der Server des Anonymisierungsdienstes angegeben werden, eine vollständige Anfrage sähe also wie folgt aus: <http://anon.free.anonymizer.com/http://www>

.beispiel.de/. Auf der erhaltenen Seite sind bereits alle Links geändert, so dass man sich von nun an in einem "sicheren Raum" bewegt.

Hier muß man sich aber vor Augen halten, dass die Möglichkeit, vielleicht auf einigen Seiten, in seinem Surfverhalten beobachtet werden zu können, gegen die Gewissheit, auf jeden Fall von `www.anonymizer.com` beobachtet zu werden, getauscht wird. Dies kann vermieden werden, wenn z.B. das erstellte Programm `socket.pl` genutzt wird. Dieses legt keine Logfiles an und der Quellcode ist frei einsehbar. Seine Funktionsweise ist nahezu identisch zu der von Anonymisierern. Bei diesen werden verdächtige Elemente in den Anfragen und Antworten entfernt. Das Programm dagegen konstruiert ein ganz neues Anfragepaket, das die gewünschte URL des Nutzers beinhaltet und schickt dieses an das Ziel. Aus der Antwort werden dann bestimmte Elemente, wie z.B. IMG-Anweisungen und Cookies entfernt und dieses wird an den Nutzer weitergereicht. Die HTTP-Anweisungen werden dabei so geändert, dass der Nutzer von nun an, automatisch durch bestätigen eines Links, die Anfrage immer über das Programm stellt.

16.2.2 Kryptographische Verfahren

Hierbei gibt es zwei Ansätze, die notwendigen Sicherheitsmaßnahmen zu plazieren. Einmal zwischen Client und Ziel-Server und einmal zwischen Quell- und Ziel-Server.

Werden die Maßnahmen zwischen Client und (Ziel)Server plaziert, ist dies eine Schutzmaßnahme, da ein möglicher Einbruch an einer unzulänglichen Authentisation des (Ziel)Servers scheitert. Statt die Adressen zu prüfen, könnten sich Server und Client untereinander durch kryptographische Schlüssel ausweisen und so eine vertrauenswürdige Verbindung ermöglichen. [Weidner97, S. 2f] Allen voran scheinen Public Key Verfahren dafür besonders gut geeignet, da Authentisation und Verschlüsselung mit dem selben Verfahren ermöglicht wird.

Das bisherige Manko einer gesicherten Verbindung zwischen einem Client mit z.B. Netscape oder Internet Explorer und einem Server ist, dass diese Verfahren nur eine gesicherte Verbindung ermöglichen, nicht aber eine eindeutige und für den Nutzer transparente Authentisation. Dieser erfährt anhand eines Symbolen nur, dass eine Verbindung gesichert ist. Dem Angreifer fällt es darum nicht schwer, selber ein Zertifikat zu erzeugen und die Verbindung zwischen Client und seinem Server zu verschlüsseln. Dem normalen Nutzer dürfte der Unterschied kaum auffallen, zumal die verwendeten Zertifikate nahezu identisch sein können. Abhilfe wäre geschaffen, wenn die Internet-Browser zu jeder Adresse ein Zertifikat fest abspeichern und den

Zugriff verweigern oder zumindest eine Fehlermeldung ausgeben kann, wenn das erhaltene Zertifikat von dem gespeicherten abweicht.

Ein Problem dieser Client-Server Sicherungsmaßnahme ist der Nutzer auf der Client Seite. Durch Fehlverhalten oder unzureichende Einstellungen auf seiner Seite ist es ohne weiteres möglich, dass Trojaner, als Vorstufe zu einem komplexen Angriff, die Zuordnungen im Internet-Browser, Adresse zu Zertifikat ändern, bzw. die Abfrage immer mit wahr beantworten. Aus diesem Grund ist die Plazierung der Sicherungsmaßnahmen zwischen zwei Servern sicherer.

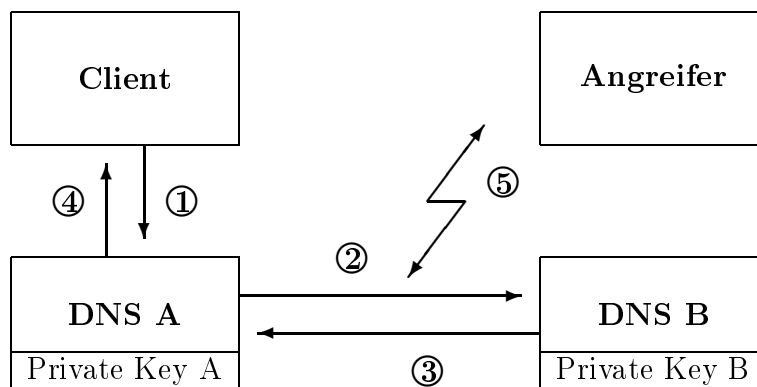


Abbildung 4: Verschlüsselung zwischen zwei Servern

Bei einer sicheren Server-zu-Server-Verbindung gelingt es dem Angreifer nicht, die Verbindung zu belauschen, bzw. eine falsche Antwort einzuspielen.

1. Der Client hat eine Adresse wie z.B. `www.bank.de` und möchte diese in die zugehörige IP Adresse umwandeln, wofür diese an den eingetragenen Name Server übermittelt wird.
2. Dieser kennt die Adresse nicht und fragt einen weiteren Name Server. Dazu verschlüsselt er die Anfrage mit seinem Private Key, mit der Wirkung, dass er als Frager authentisch ist, da sich nur mit dem Public Key des Name Servers A die Frage entschlüsseln lässt. Da der ZielServer bekannt ist, kann A das Paket zusätzlich mit dem Public Key des Name Servers B verschlüsseln, um zu verhindern, dass andere an dir Informationen der Anfrage kommen, z.B. Query-ID, Inhalt der Frage, etc. .
3. Der Name Server B erhält die verschlüsselte Anfrage, wandelt diese mit Hilfe seines Private Key und dem Public Key von A in Klartext um und kann auf diesem Weg den Name Server von A eindeutig identifizieren.

B schickt die Antwort auf gleiche Weise verschlüsselt, zu A. Zuerst mit seinem Private Key, damit A genau weiß, dass die Antwort nur von B sein kann und dann mit dem Public Key von A, um jedem anderen die Möglichkeit zu nehmen, den Inhalt der Antwort in Erfahrung zu bringen.

4. Die Antwort wird an den Client weitergereicht.
5. Durch die zweifache Verschlüsselung ist es dem Angreifer nicht möglich, die Antwort zu entziffern oder selber Antworten erfolgreich einzuspeisen, da die Server über die jeweiligen Public Key verfügen und so eine fremde Antwort sofort auffallen würde.

16.2.3 Zufällige Query-IDs

Die Verwendung von zufällig gewählten Query-IDs ist als Gegenmaßnahme zu dem Query-ID-guess Angriff anzusehen. Bei diesem bringt der Angreifer die verwendete Identifizierungsnummer in Erfahrung und kann so auf die zukünftige schließen, da die IDs immer sequentiell verlaufen. Bei einer zufälligen Wahl der Query-ID seitens des Name Servers kann der Angreifer diese nicht mehr oder nur sehr schwer erraten.

Diese Sicherungsmaßnahme ist alleine aber nicht ausreichend, denn selbst bei einer gewählten Zufallszahl, die nicht zu erraten ist, kann der Angreifer immer noch einen brute-force Angriff starten, da es höchstens 65536 verschiedene Query-IDs gibt. Die Erfolgchancen eines solchen Angriffes hängen von der verfügbaren Zeit für die Antwort ab. Dabei hilft natürlich, wenn die echten Nameserver nicht antworten können, weil sie mit einer Unmenge sinnloser Anfragen oder anderen denial-of-service Angriffen beschäftigt sind. [Weidner97, S. 2f]

16.2.4 Domain Namen überprüfen

Das sogenannte *reverse dns lookup* macht sich eine mögliche Nachlässigkeit des Angreifers zunutze und zielt darauf ab, eine Verschmutzung eines Name Servers zu erkennen, bzw. zu umgehen. In den *Resource Records* (RR) des Name Servers steht die Zuordnung Name -> IP Adresse und IP -> Name. Wenn der Angreifer nur den Eintrag Name -> IP Adresse ändert, also dem Namen `www.bank.de` die IP seines Rechners zuweist, und dabei nicht die IP seines Rechners dem Namen der Bank zuordnet, ergibt eine Rückabfrage eine unterschiedliche Adresse. So würde die Frage nach `www.bank.de` z.B. die Adresse `187.152.130.22` liefern (Adresse des Angreifers), die Frage nach `187.152.130.22` aber nicht `www.bank.de` sondern z.B. `www.angreifer.de`.

Eine weitere Möglichkeit, sich vor DNS-Angriffen zu schützen, besteht darin, möglichst viele Name Server nach der gewünschten Adresse zu befragen. Wurde der Eintrag eines Name Servers durch einen Angriff verändert, so würde dies sofort auffallen, da die Antworten der Name Server nicht einheitlich sind. Ein Angreifer müßte alle Name Server die befragten werden erraten und erfolgreich angreifen, was bei einer günstigen Wahl von Name Server, wie z.B. solche, die in gut gesicherten Organisationen⁵⁹ liegen, erheblich erschwert werden kann. Genau dies macht das erstellte Programm `dnslookup.pl`. Aus einer vorhandenen Liste von Name Server, die beliebig erweitert werden kann, werden zufällig Einträge herausgesucht und per DNS-Anfrage nach einer bestimmten Adresse befragt. Die erhaltenen Antworten werden für einen besseren Vergleich gegenübergestellt.

16.2.5 EMail

Mit dem Versenden von EMail verrät jeder Nutzer, wie gezeigt, viel von sich selbst. Inhalt der EMail und Adresse des Senders und Empfängers sind für viele Personen im Internet frei einsehbar. Viele Geheimdienste, wie beispielsweise die National Security Agency fangen jede EMail ab. Es gibt eine Reihe von Programmen, die auf unterschiedliche Art und Weise die Daten (Verbindungs- und Inhaltsdaten) einer EMail schützen.

Eine Möglichkeit, die Inhaltsdaten einer EMail zu schützen, besteht darin, diese zu verschlüsseln. Dafür bietet sich unter anderem das Programm PGP (Pretty Good Privacy) an. In der Version 5 unterstützt das Programm folgende Verschlüsselungsalgorithmen: RDA, IDEA, DSS CAST und SHA. [Fuhrberg98, S. 111] Vorrangig schützt die Verschlüsselung eine EMail davor, automatisch mit Hilfe von Überwachungsprogrammen erfaßt und ausgewertet zu werden.

Die Verbindungsdaten, also wer mit wem, bzw. ob überhaupt kommuniziert wurde, lassen sich mit Hilfe sogenannter *Remailer* schützen. Dabei wird die EMail dem Remailer geschickt, der diese weiterleitet. Wie bei einem Anonymisierungsdienst steht auch hier ein Programm zwischen dem Sender und dem Empfänger. Von den Remailern gibt es verschiedene Arten: [Fuhrberg98, S. 314]

- Die pseudonymen Remailer ersetzen die Absenderadresse durch ihre eigene, so dass das Ziel und alle Stationen dazwischen nicht wissen, wer diese EMail verschickt hat. (Remailer Typ 0)
- Mit kryptographischen Verfahren und verschiedenen Remailer lassen sich die Verbindungsdaten auch vor dem Betreiber selber verbergen.

⁵⁹BSI, NSA, CIA, BND, BKA, ...

Dazu wird eine Nachricht an einen Remailer geschickt, der diese nach einiger Zeit an den nächsten weiterleitet. Die Nachricht ist dabei mehrfach verschlüsselt, damit nur das eigentliche Ziel an den Inhalt gelangt. Sei N die Nachricht. Dann erzeugt der Absender beispielsweise eine EMail $R_A, K_A(R_B, K_B(R_C, K_C(N)))$, wobei R_x für die Adresse des Remailers x steht und K_x für eine Verschlüsselung mit dem öffentlichen Schlüssel des Remailers x . Der Remailer A erhält die EMail, entschlüsselt diese und findet die Anweisung, diese an den Remailer B zu schicken. Dieser erhält folgende Nachricht: $R_B, K_B(R_C, K_C(N))$ und fährt, wie A fort. Der Remailer C sendet schließlich die Nachricht an den eigentlichen Adressaten. (Remailer Typ 1)

Teil VI

Abschließende Betrachtung

Bei der abschließenden Betrachtung der drei vorgestellten Angriffsformen fällt auf, daß diese teilweise voneinander abhängig sein können bzw. sich in der genutzten Technik oder Auswirkung überschneiden. So können z.B. Trojaner Spoofing Angriffe einleiten, die dann zum Zweck des Datensammelns eingesetzt werden. Diese Überschneidungen sind möglich, da den geschilderten Kategorien unterschiedliche Bedeutungen zugrunde liegen. So werden schadhafte Programme in dieser Arbeit schwerpunktmäßig anhand ihrer Mitteln beschrieben, während bei Datenspuren das Hauptaugenmerk auf den Zielen liegt. Spoofing Angriffe beziehen sich sowohl auf die Ziele, als auch auf die eingesetzten Mittel.

Das Ziel dieser Ausarbeitung war es, dem Leser die derzeit gebräuchlichsten nicht-gerichteten Angriffsformen

- Spoofing
- Datenspuren
- Schadhafte Programme

verständlich zu erläutern und vor allem Möglichkeiten zur wirkungsvollen Prävention oder Abwehr zu vermitteln. Dabei sollte keineswegs eine Beschränkung auf konkrete Gegenmaßnahmen erfolgen, sondern durch eine ausführliche Darstellung der technischen Prozesse auch Angriffsvarianten erkennbar und wirkungslos gemacht werden.

Die diesem Konzept zugrundeliegende Idee ist, dass es unabhängig von der Qualität des Massenangriffs einen nicht erfassten Prozentsatz gibt. Jeder Nutzer kann durch sein Verhalten bzw. die Wahl der Mittel beeinflussen, ob er erfolgreich angegriffen wird oder nicht. Der Schwerpunkt liegt folglich nicht auf Vermeidung von Angriffen (was vermutlich auch gar nicht möglich ist), sondern darauf nicht betroffen zu sein. Dies ist möglich, da bei einem Angriff mit mehreren Millionen Zielen keine Ressourcen oder Möglichkeiten zur Verfügung stehen, die nicht Erfassten nachträglich, sozusagen von Hand, anzugreifen (da auch diese Zahl in die Millionen gehen dürfte).

Für das Spoofing mit seinen Teilbereichen

- Domain Name System - Spoofing
- Web - Spoofing

gibt es relativ einfache Sicherungsmaßnahmen, zudem ist der Wirkungsradius im Falle eines erfolgreichen Angriffs vermutlich auf wenige Opfer beschränkt. Denn die Information über ein sehr erfolgreiches Spoofing dürfte sich so schnell verbreiten, dass sich die Zahl der noch zusätzlichen Opfer stark verringert. Es ist also zu erwarten, dass diese Angriffsform in Zukunft keine große Rolle spielen wird.

Die schadhaften Programme unterteilt in

- Viren
- Trojaner
- Gefährliche Programme
- Fehlerhafte Programme

stellen Angriffsmittel zur Verfügung. Aufgrund ihrer Vielfältigkeit und Wandlungsfähigkeit wird es sie wohl solange geben, wie Menschen des Programmierens mächtig sind. Die Gefährlichkeit von Viren wird im Vergleich zu Softwarefehlern in Programmen allerdings häufig überschätzt. Für den Einzelnen ist natürlich ein Virus, der alle Daten löscht um einiges schadhafter, als ein fehlerhaft erstelltes Betriebssystem, welches alle zwei Stunden abstürzt. Volkswirtschaftlich läßt sich dagegen nicht sagen, ob ein Virus oder fehlerhafte Software mehr Schaden anrichtet. Abschließend betrachtet, ist zu sagen, dass es immer wieder erfolgreiche Angriffe mit erheblicher Schadenswirkung geben wird. Mit Hilfe einer guten Datensicherung dürfte sich der entstandene Schaden allerdings eindämmen und in vielen Fällen sogar rückgängig machen lassen.

In den Augen des Autors ist auf lange Sicht die Angriffsart Datenspuren mit den Formen:

- passive Methoden
- aktive Methoden

als die Gefährlichste einzustufen. Das eigentlich bedrohliche ist die schleichende Entwicklung der zunehmenden Überwachung, ebenso in der realen Welt, wie auch im Internet. Die Möglichkeiten nehmen mit der Steigerung der Prozesse über das Internet stetig zu, wobei hier das Augenmerk, wie in der gesamten Diplomarbeit, nicht auf einem Einzelnen, sondern auf vielen (allen) Betroffenen liegen soll. Beispielsweise ist die genaue Beobachtung und Aufzeichnung der Aktivitäten eines Einzelnen tragisch, aber unter Umständen nicht zu verhindern, wenn z.B. Firmen Privatdetektive anwerben, oder die Exekutivorgane eines Staates durch eine Genehmigung eine Überwachung

mit entsprechenden technischen und personellen Ressourcen beginnen. Werden aber alle Personen eines Landes nahezu vollständig überwacht, sind die vermutlichen Folgen gravierend: Verlust der Meinungsfreiheit, der freien Willensbildung, Notwendigkeit alle Gesetze und Verordnungen zu kennen, da ein Übertreten sofort registriert werden kann, u. ä.

Auf eine ausführlichere Darstellung wird an dieser Stelle verzichtet, vor allem um das Gesamtbild der Ausarbeitung nicht zu stören. Folgende kurze Ausschnitte sollen diesen Aspekt jedoch andeuten:

- **Gelder für DataWarehouses** Das FBI forderte in seinem Budgetantrag für das Haushaltsjahr 2001 u. a. Gelder für eine Datenbank mit dem Codenamen „Casa de Web“. Wird der Antrag bewilligt, bedeutet dies die Legitimation zur dauerhaften Speicherung abgefangener Kommunikation, wie Audiodateien und Abhörprotokolle mit dazugehörigen Berichten, in großen Datenbanken. [Christ00, S. 96]
- **lifeShirt:** Zur Erstellung einer genaueren Diagnose und als Hilfsmittel bei der Behandlung von Krankheiten hat die Firma lifeShirt einen Prototyp eines Hemdes vorgestellt, das mittels unterschiedlicher Sensoren und Elektroden kontinuierlich Atemfrequenz, Körperposition, Blutdruck und andere Werte mißt. Auf einer gesicherten Webseite sollen die Daten gespeichert werden und autorisierten Personen, z.B. dem behandelnden Arzt, zugänglich sein. [Christ00, S.110f]
- **2/3 der Bevölkerung überwacht:** Die Angst vor der IRA bewirkte, dass jeder als Terrorist eingestufte Ire, seine Verwandten, Freunde und Bekannten sowie jede Person, mit der dieser je gesprochen hat, bei der einen oder anderen Sicherheitsabteilung in Nordirland gespeichert wird. So waren 1996 Daten von ungefähr einer Million Personen elektronisch erfaßt, das entspricht zwei Dritteln der Bevölkerung. [Christ00, S.131]
- **Forderungen zum Ende der Anonymität:** In der Vergangenheit sind von verschiedenen Seiten Ansprüche gestellt worden, die Anonymität im Internet zu verhindern oder doch so weit es geht zu vermeiden. So forderte das Komitee für Bürgerrechte, Inneres und Justiz des Europaparlamentes in einem Bericht, Provider zur Identifikation von EMail-Benutzern zu zwingen und die Verbindungsdaten mindestens drei Monate zu speichern.⁶⁰ In Frankreich will man noch einen Schritt weiter gehen. Ein Gesetz, das eine vom Provider zwanghaft vorgenommene Identifikation des Verantwortlichen bei nicht-privaten Veröffentlichungen im Internet vorsieht, ist am 28. Juni 2000 verabschiedet worden.⁶¹ Auch in Deutschland werden Forderungen nach weniger Anonymität

⁶⁰<http://www.heise.de/newsticker/data/fr-06.04.00-000/>

⁶¹<http://www.heise.de/newsticker/data/fr-29.03.00-000/>

gestellt. So ist beispielsweise das BKA der Meinung, zur besseren Bekämpfung der Kriminalität im Internet, müsse unter anderem die Anonymität beim E-Commerce eingeschränkt werden.⁶²

⁶²<http://www.heise.de/newsticker/data/jk-24.02.00-003/>

Teil VII

Anhang

*Auch das kleinste Licht anzuzünden ist besser,
als sich über die Dunkelheit zu ärgern.*

Nachfolgend werden unter anderem auch Inhalte aufgeführt, die in der eigentlichen Arbeit nicht referenziert wurden. Dies dient dem Zweck eines möglichst vollständigen Überblicks.

A Grundlage verwendeter Protokolle

A.1 Das OSI-Referenzmodell

Aufgrund der Komplexität der Kommunikation zwischen Datenverarbeitungsanlagen ist es nicht sinnvoll, alle notwendigen Aufgaben in einem einzigen Protokoll abzuwickeln. Daher kommen in der Regel mehrere Protokolle in Form von übereinandergelegten Schichten mit unterschiedlichen Funktionen zum Einsatz.

Damit es hinsichtlich der in jeder Schicht zu leistenden Funktionen eine einheitliche Betrachtungsweise und Aufgabenumfang gibt, hat die *Internationale Standardisation Organisation (ISO)* ein Modell einer Protokollschichtung entworfen, das sogenannte *Open Systems Interconnection (OSI) 7-Schicht Referenzmodell*. Auf das OSI Modell wird hier kurz eingegangen, da es gewissermaßen die Grundlage für die Datenübertragung im Internet bildet und somit das Gesamtverständnis erleichtert. [Lauer98, S. 65]

Das OSI Modell besteht aus folgenden aufeinander aufbauenden Schichten [Fuhrberg98, S. 7]:

1. In der **physikalischen Schicht** werden die Parameter für eine physikalische Übertragung festgelegt.
2. Die **Sicherungsschicht** ist für die fehlerfreie Übertragung von Daten zuständig. Hierzu gehört z.B. die Verwendung von Prüfsummen. Außerdem erfolgt eine Adressierung des mit dem Übertragungsmedium verbundenen Gerät, z.B. durch die sogenannte Ethernet- oder MAC-Adresse.
3. In der **Verbindungsschicht** werden Pakete mit Hilfe definierter Netzadressen von einem Teilnehmer zum anderen geschickt. Ein Protokoll dieser Schicht ist das Internet-Protokoll (IP).

4. Die **Transportschicht** stellt den Übergang zwischen den hardwarenahen Schichten eins bis drei und den anwendungsbezogenen Schichten fünf bis sieben her. Sie soll den Transport der Daten zuverlässig sicherstellen. Zur Netzadresse der Schicht drei werden Angaben über beteiligte Instanzen (z.B. Prozesse) hinzugefügt. Beispiele für Protokolle sind das *transmission control protocol* (TCP) oder das *user datagram protocol* (UDP).
5. Die **Sitzungsschicht** hat die Aufgabe, Verbindungen zwischen Sitzungsbenutzer wie z.B. Benutzerprozesse zu kontrollieren.
6. Die Aufgabe der **Darstellungsschicht** ist, verschiedene Datenformate rechnerunabhängig darzustellen. Hierzu gehören Funktionen zur Verschlüsselung, Komprimierung oder Konvertierung.
7. In der **Anwendungsschicht** werden die Daten der jeweiligen Anwendung, wie z.B. FTP, HTTP, SMTP übertragen.

Die Daten einer Verbindung über das OSI Modell wandern dabei bildlich betrachtet im Quellrechner von oben durch alle Schichten nach unten, werden dann übertragen und bewegen sich analog im Zielrechner wieder von unten nach oben.

A.2 Aufbau des IPv4 Headers

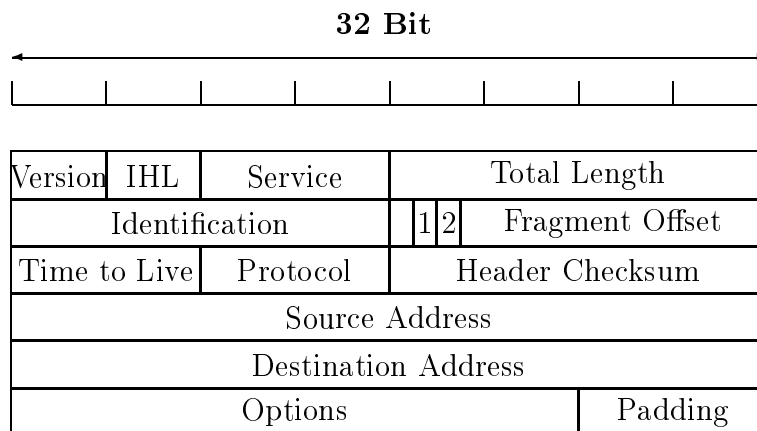


Abbildung 5: IP Head

- **Version** (4 Bit): Hier wird die verwendete Version des IP Protokolls angegeben.

- **Internet Header Length** (4 Bit): Dieses Feld gibt die Länge des IP Headers in Vielfachen von 32 Bit an.
- **Service** (8 Bit): Dieses Feld ist mehrfach unterteilt und spezifiziert die Priorität des Datagramms, die Verzögerung, Zuverlässigkeit und Wegewahl. Da gegenwärtige Implementierungen des IP-Protokolls dieses Feld ignorieren, wird hier auch nicht weiter darauf eingegangen.
- **Total Length** (16 Bit): Dieses Feld gibt die Länge des Paketes inklusiv des IP Headers an. Aus den 16 Bit ergibt sich somit eine maximale Gesamtlänge von $2^{16} = 65535$ Byte.
- **Identification** (16 Bit): Alle Pakete einer Nachricht besitzen die gleiche Identifikationsnummer, um am Ziel eine eindeutige Zuordnung zu ermöglichen.
- **Flags** (2 Bit): Hier stehen die Kontroll Flags für 1) Don't Fragment und 2) More Fragment. Das erste weist einen Router an, das Datagramm nicht zu fragmentieren, das 2te zeigt, ob noch weitere Fragmente folgen.
- **Fragment Offset** (13 Bit): Dieses Feld gibt an, an welcher Stelle das Paket in die Nachricht gehört. Dadurch kann der Zielrechner die Pakete richtig zusammensetzen. Die Lage wird als ein Vielfaches von 8 Byte bestimmt, woraus sich ein Maximum von 8192 Paketen pro Nachricht ergibt.
- **Time to live** (16 Bit): Hier wird die verbleibende Lebenszeit eines Paketes in Sekunden angegeben.
- **Protocol** (16 Bit): Hier erfolgt die Zuordnung zum Protokoll der höheren Schicht.
- **Header Checksum** (16 Bit): Prüfsumme für den IP Header
- **Source Address** (32 Bit): Internet Adresse des Senders
- **Destination Address** (32 Bit): Internet Adresse des Empfängers
- **Options**: Dieses Feld hat eine variable Länge und dient zur möglichen Anpassung an Anforderungen höherer Protokolle.
- **Padding**: Dieses Feld dient zum Auffüllen des IP Headers, um sicherzugehen, dass dieser immer die geforderte Mindestgröße hat.

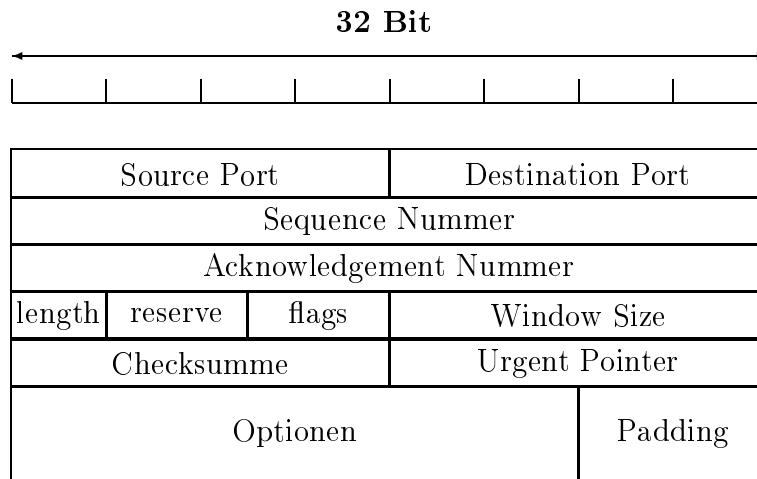


Abbildung 6: TCP Head

A.3 Aufbau des TCP Headers

- **Source Port** (16 Bit): Die Absenderadresse des Prozesses oder Dienstes, z.B. FTP 21, Telnet 23
- **Destination Port** (16 Bit): Hier wird der Port des Zielprozesses angegeben.
- **Sequence Nummer** (32 Bit): Mit der Sequence Nummer wird die Position der Daten im ausgetauschten Datenstrom angegeben.
- **Acknowledgement Nummer** (32 Bit): Hier bestätigt der Empfänger, bis zu welchem Datenbyte er die Daten empfangen hat, bzw. welches er als nächstes erwartet.
- **length** (4 Bit): In diesem Feld wird angegeben, wieviel 32 Bit Worte der TCP-Header enthält.
- **reserve** (6 Bit): Dieses Feld wird derzeit nicht genutzt.
- **flags** (6 Bit): Dieses Feld enthält sechs 1 Bit lange Control Flags. Im einzelnen sind dies der Urgent Pointer, womit gezeigt wird, dass das gleichnamige Feld beachtet werden muß, der ACK, womit bei Bedarf auf die Acknowledgement Nummer verwiesen wird, das Push Feld, bei Setzung eines Bits sollen die Daten sofort zum Anwendungsprotokoll weitergegeben werden, das Reset Feld steht für eine sofortige Beendigung der Verbindung, das Synchronisationsfeld steht für den Aufbau einer Verbindung und das Final Flag steht für das letzte Paket.

- **Window Size** (16 Bit): In diesem Feld wird dem Sender mitgeteilt, wieviel verfügbaren Puffer der Empfänger hat, um ein Überlaufen des Speichers zu verhindern. Eine Fenstergröße von null stoppt den Datentransfer.
- **Checksumm** (16 Bit): Dieses Feld enthält die Prüfsumme des TCP-Headers und der Daten.
- **Urgent Pointer** (16 Bit): Mit diesem Feld wird die Dringlichkeit des Pakets angezeigt.
- **Optionen**: Dieses Feld hat eine variable Länge und ermöglicht das Schalten mehrerer Optionen.
- **Padding**: Dieses Feld enthält Füllinformationen um sicherzustellen, dass der TCP Header im 32 Bit Format endet.

[Hartmann, Punkt 4]

A.4 Funktion des TCP/IP Protokolls

Mit seinen Funktionen stellt das IP Protokoll im Internet die Grundlage für eine einheitliche, paketerorientierte Kommunikation dar. Zu große Datenpakete werden automatisch in kleinere zerlegt und übertragen. Außerdem erhält jedes Paket eine eindeutige Nummer, so dass die einzelnen Pakete am Zielort wieder korrekt zusammengesetzt werden können und eine Prüfsumme (nach dem CRC Verfahren) mit der eine korrekte Übertragung festgestellt werden kann.

Das Internet Protokoll garantiert nicht, dass ein Paket sein Ziel korrekt oder überhaupt erreicht. Es gibt auf IP Ebene auch keine Möglichkeit ein fehlerhaftes Paket erneut anzufordern bzw. eine Quittung zu senden, wenn ein korrektes Paket erhalten wurde. Dies sind Aufgaben von Protokollen auf höheren Ebenen, wie dem TCP.

Die IP Schicht dient generell nur der schnellen Zustellung von Paketen und genügt keinen Ansprüchen an Stabilität und Sicherheit. [Lauer98, S. 67f]

TCP schafft die Voraussetzung für eine stabile und sichere Verbindung mittels eines *Handshake*-Verfahrens. Das Prinzip sei hier kurz umrissen:

1. A sendet an B ein IP Paket, Inhalt: Absicht eine TCP-Verbindung aufzubauen.
2. B erhält dieses und sendet ein sogenanntes *positive acknowledgement*, also eine Quittung.

3. A sendet zur Bestätigung seinerseites ein *positive acknowledgement* zurück.
4. Erst wenn B dieses erhält, ist auch für ihn die Verbindung aufgebaut.
5. A sendet nun die Datenpakete mit einer fortlaufenden Nummer, B muß den Erhalt dieser Pakete mit der gleichen Nummer quittieren.

Erreicht ein Paket nicht das Ziel, so läßt sich dies feststellen, da die Quittung ausbleibt. Bleibt eine Quittung aus, so kann dies zwei Gründe haben: a) das Paket hat das Ziel nicht erreicht oder b) die Quittung hat das Ziel nicht erreicht. In beiden Fällen wird von A das Paket nach einer definierten Zeit noch mal gesendet, bis er von B eine Quittung erhält oder eine bestimmte Anzahl Versuche gemacht wurden.[Lauer98, S. 77ff]

A.5 Aufbau der HTTP Header

Nahezu jede HTTP Verbindung läuft nach folgendem Schema ab: Ein Computer stellt die Anfrage und sendet somit einen Request und der andere antwortet mit einem Response. Jede dieser Nachrichten verfügt über einen Header, der die genauen Bedingungen des Datenaustausches klären soll.

A.5.1 HTTP Request Header

Ein Request Header ist zeilenweise wie folgt aufgebaut: [HTTP00, S. 3]

- **command line**: weiter unten erläutert
- **Accept**: welche Dokumente von dem Anfrager akzeptiert werden
- **Accept-Language**: bevorzugte Sprachen des Anfragers
- **Accept-Encoding**: teilt dem Server mit, welche Kompressionsmethoden verstanden werden
- **User-Agent**: genaue Beschreibung des Internet-Browsers bei dem Anfrager
- **Host**: genaue Adressierung des Zielcomputers
- **Connection**: ob die Verbindung offen oder geschlossen ist (close oder Keep-Alive)

Der Request Header von dem Client zu einem Server beinhaltet in der command line die Methode des Zugriffs, die Identifizierung der bezogenen Resource und die genutzte Protokollversion getrennt durch ein Leerzeichen.

Zum Beispiel: *GET /beispiel/index.html HTTP/1.0*

Zulässige, normale Methoden sind GET, HEAD und POST. Darüber hinaus gibt es noch die ergänzenden Methoden PUT, DELETE, LINK, UNLINK [RFC1945, D.1.1] und TRACE. [HTTP00, S. 20]

Die Funktion dieser Methoden sind:

- **GET**: Der Server wird angewiesen, die bezogene Ressource, unabhängig ihrer Art, an den Client zu senden. [RFC1945, 8.1]
- **HEAD**: Diese Methode ist identisch zur GET Methode, außer dass der Server kein Entity-Body in der Antwort mit angeben muß, sondern nur den Header der bezogenen Ressource übermittelt, so dass diese Methode hauptsächlich genutzt wird, um Links auf ihre Gültigkeit hin zu prüfen. [RFC1945, 8.2]
- **POST**: Die POST Methode wird genutzt, damit der angegebene Zielserver die Daten dieses Requests als neue, untergeordnete Information der bezeichneten Ressource akzeptiert. Damit werden folgende Funktionen unterstützt: [RFC1945, 8.3]
 - Kommentierung vorhandener Ressourcen
 - Senden einer Nachricht zu einer Newsgroup, Mailing Liste, Bulletin Board usw. .
 - Einen Datenblock übermitteln, wie z.B. senden einer FORM zu einem Prozess, der Daten verarbeitet.
 - Eine Datenbank mit Daten erweitern.
- **PUT**: Der Server wird angewiesen, die anhängenden Daten unter der angegebenen Adresse zu speichern. Der Unterschied zu POST besteht darin, dass bei POST der Server die anhängenden Daten der Adresse zur Bearbeitung übergibt. [RFC1945, D 1.1]
- **DELETE**: Hiermit wird die angegebene Adresse gelöscht. [RFC1945, D 1.2]
- **LINK**: Die angegebene Adresse wird mit anderen verlinkt.
- **UNLINK**: Bestehende Links werden gelöscht.
- **TRACE**: Erlaubt dem Nutzer, den Weg der Daten zu beobachten. [HTTP00, S. 20]

A.5.2 HTTP Response Header

Die Antwort des befragten Computers ist zeilenweise vergleichbar mit der Anfrage aufgebaut: [HTTP00, S. 4]

- **Return Code:** Diese Zeile beinhaltet das Protokoll und vor allem einen Status Code der Verbindung, mit deren Hilfe der Empfänger den Erfolg seiner Anfrage mitgeteilt bekommt.
- **Date:** aktuelle Zeit des Senders
- **Server:** von dem Server verwendete Software (z.B. Apache on Unix)
- **Last-Modified:** Zeitpunkt, wann das Dokument zum letzten Mal modifiziert wurde
- **Etag:** eindeutige Bezeichnung der erfragten Ressource
- **Accept-Ranges:** teilt dem Empfänger mit, daß der Server Teile der Ressource übermitteln kann, vor allem für Stream-Technologien genutzt
- **Content-length:** wie lang das erfragte Dokument ist
- **Connection:** aktueller Status der Verbindung, also offen oder geschlossen
- **Content-type:** Art des Dokumentes (z.B. Text)

Besonders wichtig in dem Header ist der übermittelte Status Code. An diesem kann der Empfänger erkennen, ob seine Anfrage erfolgreich war oder nicht, bzw. was genau nicht funktioniert hat. Um einen kleinen Einblick zu gewähren, werden nachfolgend die festgelegten Status Code Bereiche erläutert. [HTTP00, S. 22]

- **100-199:** Informativ, z.B. dass der Client mit seinen Anfragen fortfahren kann (100).
- **200-299:** Request ist erfolgreich, z.B. die Daten werden übermittelt (200), erschaffen (201) oder akzeptiert (202).
- **300-399:** Request ist umgeleitet, z.B. wenn mehrere Ziele zur Auswahl stehen (300), das Ziel permanent zu einer anderen Adresse bewegt wurde (301) oder ein Zugriff über einen Proxy notwendig ist (305).
- **400-499:** Request ist nicht erfolgreich, z.B. Syntaxfehler im Request (400), keine Erlaubnis der Frage für dieses Dokument (401), Dokument nicht gefunden (404) oder unerlaubte, genutzte Methode (405).

- **500-599**: Serverfehler, wenn z.B. ein interner Fehler vorliegt (500), die erfragte Aktion nicht möglich ist (501) oder die HTTP Version nicht unterstützt wird (505).

B Grundlage der Adressierung

B.1 IP Adressen

IP-Adressen bestehen aus 32 Bit, die in Tupeln zu je 8 Bit zusammengefaßt werden. Die übliche Darstellungsweise ist die sogenannte 4-Byte-Dezimalpunkt schreibweise z. B. 207.201.156.106.

Diese IP-Adresse setzt sich immer aus einer Netzwerkadresse (Net-ID) und einer Hostadresse (Host-ID) zusammen. Ursprünglich wurde die Vergabe der Adressen durch das sogenannte *Network Information Center* (NIC) geregelt. Diese Organisation des Defense Data Network hielt auch die zentrale Host-Tabelle, die eine Zuordnung von Domain Namen zu IP Adressen ermöglichte. [HeiseF97, S. 346] Da bei der hohen Verbreitung und Ausdehnung des Internets eine zentrale Verwaltung nicht mehr effektiv war, wurden die Aufgaben verteilt. Die Host-Tabellen wurden durch das verteilte Domain Name System ersetzt und der Netzteil wird von nationalen Organisationen, in Deutschland z.B. DENIC, an Provider oder Endanwender vergeben und in fünf Klassen unterteilt, wobei die ersten Bit der Adresse die Zugehörigkeit zu einer Klasse festlegen. [Raepple98, S. 33f]

In der Abbildung entsprechen dabei die Notationen mit einem * folgenden Bedeutungen:

1. max. Anzahl der möglichen Netze
2. max. Anzahl der möglichen Rechner pro Netz

Die Netze der Klasse A sind an einige große Organisationen vergeben (z.B. Militär oder Forschungseinrichtungen), Adressen der Klasse B und C werden für alle übrigen Internet-Nutzer vergeben. Multicast-Adressen sind Adressen, mit deren Hilfe es möglich ist, nicht nur einzelne Rechner zu adressieren, sondern alle Rechner einer Multicast-Gruppe gleichzeitig. Die Adressen der Klasse E waren für einen speziellen Einsatz reserviert worden, werden aber zur Zeit nicht verwendet. [Fuhrberg98, S. 12]

Für private Netzwerke sind die Adressbereiche 10.0.0.0 bis 10.255.255.255, 172.16.0.0 bis 172.31.255.255 und 192.168.0.0 bis 192.168.255.255 reserviert. [RFC1918]

K l a s s e	Adressraum		Adresslänge in Bit				1*	2*
	von	bis	1-8	9-16	17-24	25-32		
A	0.0.0.0	127.255.255.255	0 Netz- anteil	Rechneranteil			2^7	2^{24}
B	128.0.0.0	191.255.255.255	1 0 Netzanteil		Rechneranteil		2^{14}	2^{16}
C	192.0.0.0	223.255.255.255	1 1 0 Netzanteil			Rechner- anteil	2^{21}	2^8
D	224.0.0.0	239.255.255.255	1 1 1 0 Multicast-Adressen				2^{28}	
E	240.0.0.0	247.255.255.255	1 1 1 1 0 Reserviert				2^{27}	

Abbildung 7: Format der IP-Adressklassen

B.2 Ressourcen Records

RR)

Alle Resource Records (RR) innerhalb des Domain Name Systems gehorchen folgendem Schema:

- **Name:** i.a. der Name des Knotens, zu dem dieser Eintrag gehört
- **Type:** 2 Byte, die den RR Type beschreiben, z.B. NS für Name Server oder A für eine Host Adresse
- **Class:** 2 Byte, die die RR Class beschreiben, z.B. IN für Internet
- **TTL:** 32 Bit, welche die Zeit spezifizieren, die dieser RR noch im Speicher bleibt, bevor die Quelle dieser Information erneut befragt wird.
- **RData:** ein 16 Bit Wert, welcher die Länge in Bytes des RData Feldes spezifiziert.
- **RData:** ein Feld variabler Länger, das die Resource beschreibt.

[RFC1035, S. 11f]

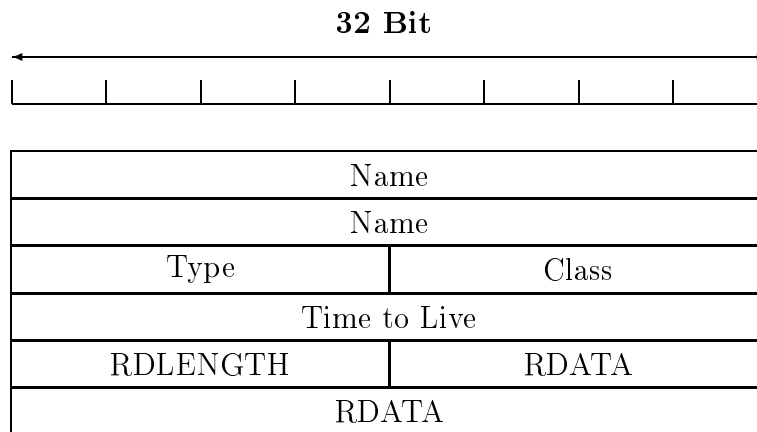


Abbildung 8: Aufbau der Resource Records

B.3 TCP Adressen

Die IP-Adressen ermöglichen Datenpaketen, über das Internet von einem Rechner zu einem anderen zu kommen. Damit dieser die Möglichkeit hat, zwei oder mehrere parallele Verbindungen aufzubauen, gibt es im TCP die *Port* Nummern. Ports sind im Computer keine physischen Anschlüsse, sondern schlichte 16-Bit Nummern, also eine zusätzliche Identifikation, um eine TCP Verbindung eindeutig kennzeichnen zu können. Port Nummern sind grundsätzlich frei wählbar, für die wichtigsten Internet-Dienste haben sich allerdings bestimmte Port-Nummern, sogenannte *well known ports*, etabliert.

Tabelle 6: well known ports

<i>Nummer</i>	<i>Dienst</i>	<i>Bedeutung</i>
21	FTP	Transfer von Dateien
23	telnet	Remote Login
25	SMTP	E-Mail
53	DNS	Domain Name System
80	HTTP	Protokoll des WWW
110	POP3	E-Mail

C Grundlage der Verschlüsselung

Moderne Kryptographie beruht meistens darauf, dass es ein einfaches und schnelles Verfahren zur Verschlüsselung einer Nachricht und Entschlüsselung

mittels eines Schlüssels gibt, während die inverse Funktion dieses Verfahrens, das „Knacken“ der Verschlüsselung, aber sehr viel aufwendiger ist. Generell lassen sich alle Verschlüsselungsverfahren in zwei Kategorien einteilen, einmal die symmetrischen und einmal die asymmetrischen Verfahren.

C.1 Sichere Verschlüsselung

Ein Verfahren gilt dann als sicher, wenn ohne das Wissen des verwendeten Schlüssels, der Inhalt einer verschlüsselten Information in einem vertretbaren Zeitraum nicht lesbar gemacht werden kann. Perfekt sicher ist ein Verfahren dann, wenn es generell ohne Kenntnis des Schlüssels nicht möglich ist, an die enthaltenen Informationen zu gelangen.

Es gibt sicherlich zahllose Möglichkeiten für perfekt sichere Kryptosysteme. Zur Erläuterung des Konzeptes, wird hier das 1917 von Vernam entwickelte und patentierte Kryptosystem *One-Time Pad* vorgestellt. [Stinson95, S. 50]

Sei $x = (x_1, \dots, x_n)$ der Klartext und $K = (K_1, \dots, K_n)$ der korrespondierende Schlüssel, mit $x_i, K_i \in \{0, 1\}$. Dann gelte für die Verschlüsselung:

$$d_k(x) = (x_1 + K_1, \dots, x_n + K_n) \text{ mod } 2$$

und für die Entschlüsselung:

$$e_k(y) = (y_1 + K_1, \dots, y_n + K_n) \text{ mod } 2$$

Bei einmaliger Verwendung eines Schlüssels K ist dieses Verfahren aufgrund der Betrachtung des verschlüsselten Textes nicht knackbar, da jeder beliebige Klartext mit gleicher Länge möglich ist. Folgendes Beispiel soll dies verdeutlichen: sei der zufällig gewählte Schlüssel 100 gegeben. Die Nachricht 110 wird damit gemäß dem obigen Verfahren zu 010 verschlüsselt. Aus dem chiffrierten Teil lassen sich nun, ohne Kenntnisse über den Schlüssel, folgende mögliche Nachrichten bestimmen: 111, 110, 101, 100, 011, 010, 001, 000. Jede dieser Möglichkeiten ist gleichwahrscheinlich zu den anderen, woraus folgt, dass ein Angreifer ausschließlich die Länge der möglichen Nachricht bestimmen kann, nicht aber den Inhalt, da jedes denkbare, gleichlange Ergebnis möglich ist.

Obwohl dieses Verfahren beweisbar sicher ist, wird es allgemein aus mehreren Gründen nicht verwendet. Wenige Ausnahmen im militärischen und diplomatischen Bereich beruhen auf der schlichten Notwendigkeit eines perfekt sicheren Verfahrens in diesen Umfeld. So benötigt dieses Verfahren einen Schlüssel, der beiden Seiten bekannt und der mindestens so lang, wie die Nachricht selber sein muß. Zu dem muß dieser Schlüssel auf einem sicheren

Kanal ausgetauscht werden. Mit dieser Notwendigkeit, einen Schlüssel für jede Nachricht auszutauschen, der mindestens die Länge der Nachricht hat, ist dieses Verfahren sehr aufwendig bzw. hinfällig, da auch gleich die Nachricht ausgetauscht werden könnte.

C.2 Symmetrische Verfahren

C.2.1 Funktion

Ein symmetrisches Verschlüsselungsverfahren beruht darauf, dass für die Ent- und Verschlüsselung einer Nachricht der gleiche Schlüssel verwendet wird. Formal betrachtet stellt sich ein symmetrisches Verfahren wie folgt dar: sei E das Verschlüsselungsverfahren, D das Entschlüsselungsverfahren, N die Nachricht, V die korrespondierende Verschlüsselung und K der Schlüssel.

Für jede Nachricht N gilt somit: [Stinson95, S. 1ff]

$$V = E_K(N)$$

$$N = D_K(V)$$

C.2.2 Data Encryption Standard

Das Data Encryption Standard (DES) Verfahren verschlüsselt (und entschlüsselt) einen Klartext mit der Länge von 64 Bit und nutzt dabei einen Schlüssel mit 56 Bit Länge. Der verschlüsselte Text hat wieder eine Länge von 64 Bit. [Stinson95, S. 70ff]

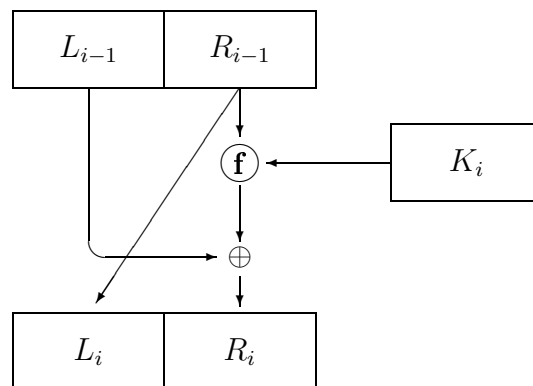


Abbildung 9: Eine Runde der DES Verschlüsselung

Das Verfahren läuft in drei Schritten ab:

1. Aus dem Klartext x wird ein Bitstring x_0 durch eine feste initial Permutation gewonnen. Es gilt: $x_0 = IP(x) = L_0R_0$ wobei L_0 entspricht den ersten 32 Bits und R_0 den letzten 32 Bits.
2. Sechzehn Iterationen der folgenden Funktion werden ausgeführt:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) \end{aligned}$$

\oplus ist eine exklusiv-oder Operation zweier Bitstrings und f ist eine Funktion, auf die später noch eingegangen wird. K_i ist die i te Permutation des Schlüssels K .

3. Abschließend ist noch die inverse Permutation IP^{-1} auf den Bitstring $R_{16}L_{16}$ vorzunehmen, also

$$y = IP^{-1}(R_{16}L_{16})$$

Die Funktion f , die das eigentliche Kryptoverfahren beinhaltet, erweitert den Bitstring von 32 auf 48 Bits, führt eine exklusive-oder Operation aus, permutiert das Ergebnis nach sogenannte *S-boxes* und permutiert erneut. Die genaue Vorgehensweise mit einem ausführlichen Beispiel wird von Douglas R. Stinson [Stinson95, S. 71ff] erläutert.

C.2.3 Sicherheit

Das 1981 als ANSI Standard normierte Verfahren beruht prinzipiell auf einer Permutation. Da das Verfahren zudem ein feste Schlüssellänge von 56 Bits einsetzt, wird der Aufwand, diese Verschlüsselung zu knacken, mit steigender Kapazität der Rechenanlagen immer geringer. So gelang es 1997 erstmals, eine Verschlüsselung durch ein Ausprobieren aller möglichen Schlüssel lesbar zu machen. Daneben gibt es zwischenzeitlich eine Reihe mathematischer Analysenmethoden, die das dechiffrieren vereinfachen, so dass heute das einfache DES Verfahren als sehr unsicher gilt. [Fuhrberg98, S. 82]

C.3 Asymmetrische Verfahren

C.3.1 Funktion

Bei den asymmetrischen Verfahren gibt es zwei verschiedene Schlüssel. Einer wird typischerweise genutzt, um eine Nachricht zu verschlüsseln, der andere um sie zu entschlüsseln. Zudem ist dieses Verfahren dazu geeignet, einen der Schlüssel, ohne die Sicherheit zu beeinträchtigen, als sogenannten *Public Key*

zu veröffentlichen.

Bei vielen dieser Verfahren können die Schlüssel ihre Funktion tauschen, solange nicht versucht wird, mit dem gleichen Schlüssel die Nachricht zu chiffrieren und dechiffrieren.

Für das Verfahren werden folgende Vereinbarungen benötigt:

Sei E das Verschlüsselungsverfahren, D das Entschlüsselungsverfahren, N die Nachricht, V die korrespondierende Verschlüsselung, a der Private Key und b der Public Key.

Für jeden Klartext N gilt:

$$N = D_a(E_b(N)) = D_b(E_a(N)) = N$$

Dieses Verfahren eignet sich auch zur Authentisierung. Wird eine Nachricht mit einem Private Key verschlüsselt, dann kann sie nur mit dem dazugehörigen Public Key a lesbar gemacht werden, womit nur der (öffentliche) Besitzer des Public Key b die Nachricht verfaßt haben kann.

C.3.2 Beispiel: RSA Kryptosystem

Auch bei dem RSA⁶³ Verfahren wird auf die genaue Betrachtung des mathematischen Hintergrundes und die Beweisführung zugunsten eines schnelleren Verständnisses verzichtet. Eine ausführliche Präsentation läßt sich bei Douglas R. Stinson [Stinson95, S. 114ff] nachlesen.

Das RSA Kryptosystem funktioniert wie folgt:

Alice produziert einen Geheimschlüssel S und einen öffentlichen Schlüssel K . Bob, der Alice eine Nachricht zukommen lassen möchte, kodiert diese mit K und Alice entschlüsselt diese mit S .

Das Schlüsselpaar von Alice besteht aus zwei (großen)⁶⁴ Primzahlen p und q mit $p \neq q$ und einer Zufallszahl e mit $3 \leq e \leq pq$ und $GGT(e, (p-1)(q-1)) = 1$.

Desweiteren ist die Bildung der Zahlen N und d , für die gelten muß $N = pq$, $d < N$ und $ed \equiv 1 \pmod{(q-1)(p-1)}$, notwendig. Außerdem gilt $S=d$ und $K=e$.

⁶³nach den Entwicklern dieses Verfahrens von 1977: Rivest, Shamir und Adleman

⁶⁴mit 200 und mehr Dezimalstellen

Die Verschlüsselungsfunktion für den Klartext x lautet:

$$y = x^e \bmod N$$

Die Entschlüsselungsfunktion für den Ciphertext y lautet:

$$x = y^d \bmod N$$

Als Zahlenbeispiel wählt Alice $q = 101$ und $p = 113$, damit gilt für $N = qp = 11413$. $e = 3533$ ist der private Key und $d = 6597$ ist der Public Key. Sei die Nachricht = 9726, dann gilt:

$$9726^{3533} \bmod 11413 = 5761$$

Die Entschlüsselung des Ciphertext = 5761 geht wie folgt:

$$5761^{6597} \bmod 11413 = 9726$$

C.3.3 Sicherheit

Die Sicherheit von RSA besteht darin, dass es einfach ist, zwei große Zahlen miteinander zu multiplizieren, dass aber die Faktorisierung einer großen Zahl extrem aufwendig ist.

So ist beispielsweise die Multiplikation zweier Primzahlen mit je 150 Dezimalstellen für keinen Computer ein größeres Problem, während die Faktorisierung des Ergebnisses selbst mit dem besten Algorithmus auf einer normalen Workstation mehr als 2000 Jahre dauern würde. Generell verdoppelt sich ungefähr die Rechenzeit, wenn das Ergebnis der Multiplikation um drei Dezimalstellen größer wird. [Buchmann99, S. 6]

Entsprechend gilt das RSA Verfahren als praktikabel sicher, aber nur so lange, bis ein schnelles Verfahren zur Faktorisierung gefunden wird. Derzeit werden Verfahren dieser Art nur mit sehr großem Aufwand dechiffriert. [SpiegelC00]

C.4 Symmetrische vs. Asymmetrische Verfahren

Die Unterschiede zwischen den Verfahren ergeben sich durch die unterschiedlichen Berechnungsweisen und äußern sich in verschiedenen Anwendungen der Verfahren.

Merkmale des DES Verfahrens

- + Im Vergleich zu asymmetrischen Verfahren außerordentlich schnell, mit besonderen Chips, bis zu 1 GBit/s. [Stinson95, S. 83]

- + Erfüllt das sogenannte strikte Avalanche-Kriterium, d.h. durch die Änderung eines Klartext- oder Schlüsselbit ändert sich mit einer Wahrscheinlichkeit von 0,5 jedes Chiffretextbit.
- Ein sicherer Kanal, über den der gemeinsame, geheime Schlüssel ausgetauscht werden muß, ist erforderlich.
- Jede an der Kommunikation beteiligte Instanz verfügt über den geheimen Schlüssel.
- Der Schlüsselraum ist mit höchstens 2^{56} Schlüsseln relativ klein und kann durch differentielle Kryptoanalyse bei frei wählbarem Klartext auf 2^{47} verschiedene Schlüssel weiter eingeschränkt werden.

[Fries93, S. 128]

Merkmale des RSA Verfahrens

- + Eine Authentisierung ist möglich, wenn öffentliche Schlüssel von einer vertrauenswürdigen Instanz zertifiziert werden.
- + Das Verfahren benötigt keine feste Schlüssellänge und kann somit derzeit beliebig sicher verschlüsseln.
- + Zum Austausch der Schlüssel ist kein sicherer Kanal erforderlich.
- Das Verfahren ist im Vergleich zu DES sehr zeitaufwendig. Bei einer Schlüssellänge von 512 Bit hat es unter normalen Bedingungen ungefähr eine Durchsatzrate von 100 KBit/s.
- Die Sicherheit von RSA hängt sehr stark mit der Schwierigkeit der Faktorisierung großer Zahlen ab, sollte ein Verfahren zur schnellen Faktorisierung gefunden werden, ist RSA unsicher.

[Fries93, S. 342]

Hieraus ergibt sich häufig folgender Einsatz der Verschlüsselungsalgorithmen: Das RSA Verfahren wird für den Aufbau einer sicheren Verbindung genutzt, da ein geheimer Austausch von Schlüsseln nicht erforderlich ist. In dieser wird dann der geheime DES Schlüssel ausgetauscht, um so die Möglichkeit zum schnellen Datenaustausch zu erhalten.

D Erstellte Programme

Im Laufe dieser Diplomarbeit entstanden einige Programme, die teilweise informativer Art sind, aber auch zur konkreten Angriffsabwehr herangezogen

werden können. Da diese Programme nicht zentraler Gegenstand der Ausarbeitung sind, werden sie nachfolgend kurz in ihrerer Wirkungsweise erläutert. Sie sind prinzipiell über das Internet unter folgender Adresse aufrufbar: <http://dsor.uni-paderborn.de/sendke/html/diplom/index.html>.

- **dnslookup.pl**: Dieses Programm hält eine beliebig erweiterbare Liste von IP-Adressen einzelner DNS Server. Die Adresse des Eingabefeldes wird als Adressanfrage an zufällig aus der Liste gewählte Name Server geschickt. Deren Antwort wird mit der Wirkung vergleichend gegenübergestellt, dass veränderte Einträge in den Name Servern auffallen.
- **domain2ns.pl**: Der Name Server der im Eingabefeld angegebenen Domain wird ermittelt.
- **ttd.pl**: Das time to live Feld eines RR wird angezeigt.
- **name2ip.pl**: Ein Name wird in eine IP-Adresse umgewandelt.
- **ip2name.pl**: Eine IP-Adresse wird in einen Namen umgewandelt.
- **anon.pl**: Die im Eingabefeld befindliche Adresse wird einem Anonymisierungsdienst übergeben und nachfolgend aufgerufen.
- **socket.pl**: Die URL im Eingabefeld wird an ein erstelltes Programm übermittelt, welches für den Nutzer im Internet eine HTTP Anfrage stellt und diesem somit anonymes bewegen ermöglicht.
- **laurin.html**: Diese Seite zeigt verschiedene Programme, die unterschiedliche Möglichkeiten demonstrieren, wie sogenanntes WebSpoofting funktionieren könnte.
- **informationen.pl**: Auf dieser Seite werden Informationen über den Aufrufer angezeigt.
- **guid.cpp**: Dieses Programm muß heruntergeladen werden. Bei einem Start durchsucht es alle Dateien des gleichen Ordners und verändert gefundene GUIDs zufällig.

E Verzeichniss der Abkürzungen

ARPA: Die *Advanced Research Projects Agency* ist eine Abteilung des amerikanischen Verteidigungsministeriums und hat die erste Vernetzung von räumlich getrennten Computern in Auftrag gegeben. Daraus entstand 1969 das sogenannte ARPANET, der Vorläufer des Internets.

BDSG: Das *Bundesdatenschutzgesetz* wurde am 20. Dezember 1990 verabschiedet, mit dem Zweck, den Einzelnen vor Beeinträchtigungen seines Persönlichkeitsrechtes zu schützen.

BND: *Bundesnachrichtendienst*, der Geheimdienst Deutschlands, zuständig für die Aufklärung im Ausland

BSI: Das *Bundesamt für Sicherheit in der Informationstechnologie* hat die Aufgabe, Konzepte, durch die der Umgang mit den neuen Technologien sicherer gemacht wird, zu erarbeiten und zu präsentieren.

CRC: *cyclic redundancy check* ist eine Methode, zur Bildung einer Prüfsumme, um Fehler in einem Datenblock zu entdecken. Eine genaue Erläuterung dieses Verfahrens gibt es in dem Buch *Error-Control Coding for Computer Systems* von T.R.N Rao, E. Fujiwara gedruckt von Prentice Hall 1989.

DES: *Data Encryption Standard* ein 1973 eingeführtes symmetrisches Blockverschlüsselungsverfahren

DNS: *Domain Name System* ein Verfahren, um Klartextbezeichnungen von Adressen, wie z.B. www.beispiel.de in IP-Adressen umzuwandeln

FTP: Das *File Transfer Protocol* ist ein Protokoll, mit dem Dateien über das TCP/IP übertragen werden können.

GG: Das *Grundgesetz* vom 23. Mai 1949, beschreibt die Grundrechte in Deutschland und findet seine Anwendung zwischen Bürger und Staat

GUID: Der *Globally Unique Identifier* ist eine weltweit eindeutige Identifizierungsnummer

HTML: Die *HyperText Markup Language* ist eine Seitenbeschreibungssprache für Darstellungen im Internet.

HTTP: Mit dem *HyperText Transfer Protocol* werden im Internet Seiten von einem Computer zu einem Anderen übertragen.

IMAP4: Das *Internet Message Protocol Version 4* vereinigt POP3 und SMTP zu einem Protokoll und wird in dem RFC 1730 beschrieben.

IP: Das *Internet Protocol* ist sozusagen die Grundlage im Internet und stellt ein simples, paketorientiertes Protokoll dar, welches zustandslos arbeitet.

ISO: Die *International Standardization Organization* sorgt für die weltweite Vereinheitlichung technischer Standards.

MAC-Adresse: Die *Medium Access Control* ist die weltweit eindeutige Adresse einer Netzwerkkarte. Alle anderen genutzten logischen Adressierungsarten basieren auf dieser.

MBR: Im *Master-Boot-Record* werden die Daten einer Festplatte gespeichert, die für grundlegende Startprozesse benötigt werden. Diese Informationen der Struktur der Festplatte werden Partitionstabelle genannt.

MIME: Das *Multipurpose Internet Mail Extensions* Verfahren ermöglicht EMail Attachments und beliebige 8-Bit Sonderzeichen.

MX-Record: In dem *Mail eXchange* Record eines Name Server steht die passende IP-Adresse zu einer EMail-Adresse.

NIC: Das *Network Information Center* hat früher die Vergabe der Adressen für das Internet vorgenommen.

NNTP: Auf dem *Network News Transfer Protocol* basiert der Austausch von Nachrichten in Newsgroups.

NSA: Der amerikanische Geheimdienst *National Security Agency* ist für die nationale Sicherheit zuständig, wozu das Abhören der gesamten weltweiten elektronischen Kommunikation gehört.

OSI: Das *Open Systems Interconnection* Modell beschreibt ein System von Schichten für den allgemeinen Datenaustausch.

PGP: Das weit verbreitete Programm *Pretty Good Privacy* ermöglicht im Internet durch Verschlüsselung eine sichere Kommunikation.

PIN: Mit der *Personen Identifizierungsnummer* wird eine Identität eindeutig festgestellt. Meistens erfolgt anschließend eine Authentisation, z.B. mittels einer TAN.

POP3: Das *Post Office Protocol, Version3* wird verwendet, um EMail, die für einen bestimmten Benutzer auf seinem EMail Server zwischengespeichert ist, abzuholen. Es ist in RFC 1939 IK, S. 951 beschrieben.

PPTP: Mit dem *Point-to-Point Protocol* wird ein Computer an das Internet angebunden.

RSA: Das nach den Entwicklern benannte *Rivest, Shamir und Adleman* asymmetrische Verschlüsselungsverfahren beruht auf der Schwierigkeit zur Faktorisierung großer Zahlen.

RR: In den *Resourcen Records* speichert ein Name Server die Daten für eine Domäne.

SMTP: Mit dem *Simple Mail Transfer Protocol* können EMail im Internet geschrieben und gesendet werden.

StGB: In dem *Strafgesetzbuch* sind sogenannte Straftaten aufgeführt.

TAN Die *Transaktionsnummer* wird genutzt, um eine Transaktion zu authentisieren.

TCP: Neben dem IP ist das *Transmission Control Protocol* die zweite Grundlage im Internet. Es nutzt das IP und realisiert eine sichere, paketorientierte Verbindung mit Fehlerkorrektur.

UDP: Neben dem TCP ist das *User Datagramm Protocol* ein Protokoll zur Datenübertragung in der Transportschicht.

URL: Mit Hilfe der *Uniform Resource Locator* werden Seiten, Dateien, Bilder und anderes im Internet adressiert.

WWW: Das *World Wide Web* ist die heutige Version des Internets.

Literatur

- [Anon99] anonymous: *Hacker's Guide, Sicherheit im Internet und im lokalen Netz*, Markt & Technik Buch- und Softwareverlag, Haar bei München, 1999
- [Bacon97] Bacon; Jean: *Conncurrent Systems, Operating Systems, Database and Distributed Systems: An Integrated Approach*, Addison-Wesley, Harlow, England, 2. Auflage 1997
- [Bert98] *Bertelsmann Lexikon, 23. Band*, Verlagshaus Stuttgart, 1998
- [BSI99] Felzmann, Frank W. : *Computer Viren - eine ständige Gefahr*, <http://www.bsi.de/literat/index.htm>, 29.9.1999
- [Buchmann99] Buchmann, Johannes: *Faktorisierung großer Zahlen*, Spektrum der Wissenschaft Digest, Spektrum der Wissenschaft Verlagsgesellschaft, Heidelberg, 2/1999
- [Buhlmann96] Bulmahn, E. et al. (Hg.): *Informationsgesellschaft - Medien - Demokratie*, BdWi-Verlag Marburg 1. Auflage 1996
- [Bundes95] Bundesbeauftragter für den Datenschutz: *Bundesdatenschutzgesetz - Text und Erläuterung -*, Gebr. Garloff GmbH, 3. Auflage 1995
- [Campbell00] Campbell, Duncan, 24.07.2000: *Inside Echelon* <http://www.heise.de/tp/deutsch/special/ech/6928/1.html>
- [Christ00] Schulki-Haddouti, Christiane (Hrsg.): *Vom Ende der Anonymität, Die Globalisierung der Überwachung*, Verlag Heinz Heise, Hannover, 1. Auflage 2000
- [Comer95] Comer, Douglas E.: *Internetworking with TCP/IP, Volume I, Principles, Protocols, and Architecture* Prentice-Hall, ORT, 3.Auflage 1995
- [Dargers95] Dargers, Torsten: *Computerviren - Ein Überblick* Virus-Test-Center Hamburg <http://agn-www.informatik.uni-hamburg.de/vtc/>
- [Denning90] Denning, Peter J. (Hrsg.): *Computers under Attack, Intruders, Worms and Viruses* Addison-Wesley, New York, 1990
- [DouCli] DoubleClick: *DoubleClick Privacy Statement*: <http://www.doubleclick.net:80/us/corporate/privacy>
- [EMail00] Heise: *E-Mails: Statt Hyperlink Trojanisches Pferd c't*, Heise Verlag, Hannover, 11/2000

- [Engels98] Engels, Gregor: *Technik des Software-Entwurfs I* Folienskript 1998
- [Feit98] Dr. Feit, Sidnie: *TCP/IP, Architecture, Protocols, and Implementation with IPv6 and IP Security* McGraw-Hill, NewYork 1998
- [Felten96] Felten, Edward W. et al.: *Technical Report 540-96* Department of Computer Science, Princeton University 1996
<http://www.cs.princeton.edu/sip/pub/spoofing.html>
- [Fries93] Fries, O. et al. (Hrsg.): *Sicherheitsmechanismen, Bausteine zur Entwicklung sicherer Systeme*, R. Oldenbourg Verlag, München Wien, 1993
- [Fuhrberg98] Fuhrberg, Kai: *Internet Sicherheit, Browser, Firewalls und Verschlüsselung*, Carl Hanser Verlag, München-Wien, 1998
- [Hare95] Siyan K., Hare C.: *Internet Firewalls & Netzwerksicherheit* SAMS, Haar bei München, 1995
- [Hartmann] Hartmann, Mike: *Die TCP/IP Protokoll Suite*
<http://www.iig.uni-freiburg.de/telematik/index.html>
- [HeiseB00] Heise Newsticker, 12.05.2000: *Office-2000-Bugfix mit Sicherheitsupdate für Outlook*, <http://www.heise.de/newsticker/data/atr-12.05.00-002>
- [HeiseC00] Heise Newsticker, 20.04.2000: *Communicator: Gefahr durch JavaScript in Cookies* <http://www.heise.de/newsticker/data/nl-20.04.00-000>
- [HeiseD00] Heise Newsticker: *Doppelklick löscht Windows*, 01.03.2000
- [HeiseDA00] Heise Newsticker: *Datenschutz im Internet: Wunsch und Wirklichkeit*
- [HeiseF97] Weihrich, Thomas: *Filofax fürs Internet: Der Domain Name Service von TCP/IP*, c't, Heise Verlag, Hannover, 10/1997
- [HeiseF00] Heise Newsticker 12.02.2000: *Angeblich zigtausend Fehler in Windows 2000* <http://www.heise.de/newsticker/data/cp-12.02.00-000>
- [HeiseG00] Heise Newsticker, 26.08.2000: *Gefälschte Meldung führt zu Turbulenzen an US-Hightech-Börse*
<http://www.heise.de/newsticker/data/jk-26.08.00-000>
- [HeiseK00] Heise Newsticker, 26.01.2000: *Der gläserne Konsument nimmt Formen an* <http://www.heise.de/newsticker/data/hob-26.01.00-000>

- [HeiseIE99] Heise Newsticker, 28.09.1999: *Internet Explorer als Datenspion*
<http://www.heise.de/newsticker/data/nl-28.09.99-000>
- [HeiseILY00] Heise Newsticker, 05.05.2000: *Milliarden-Schaden durch „Liebesbrief“*
<http://www.heise.de/newsticker/data/cp-05.05.00-001>
- [HeiseL00] Heise Newsticker, 28.07.2000: *Umstrittenes britisches Lauschgesetz verabschiedet*
<http://www.heise.de/newsticker/data/fr-28.07.00-001>
- [HeiseM00] Heise Newsticker, 01.11.1999: *Multimedia-Player übertragen heimlich ID-Nummern*
<http://www.heise.de/newsticker/data/ju-01.11.99-000>
- [HeiseM99] Heise Newsticker, 11.11.1999: *Millionen-Klage gegen RealNetworks*,
<http://www.heise.de/newsticker/data/nl-11.11.99-000/>
- [HeiseN00] Heise Newsticker, 10.07.2000: *Netscapes Smartdownload belauscht Nutzer*,
<http://www.heise.de/newsticker/data/hob-10.07.00-001/>
- [HeiseP99] Heise Newsticker, 24.01.1999: *Pentium III - Ein Datenschutzrisiko?*,
<http://www.heise.de/newsticker/data/cp-24.01.99-004>
- [HeiseP00] Michael Wilde: *Pump & Dump: Manipulationen und Ungereimtheiten rund um die Börse*, Heise Verlag, Hannover, 19/2000
- [HeiseR99] Heise Newsticker, 09.11.1999: *RealNetworks: Kein Problem für TRUSTe*
<http://www.heise.de/newsticker/data/fr-09.11.99-000>
- [HeiseS00] Heise Newsticker, 13.01.2000: *Send It-Programmierer lesen jede E-Mail mit*
<http://www.heise.de/newsticker/data/nl-13.01.00-000>
- [HeiseSI00] Heise: *Sicherheitslücke bei Surf1*, c't, Heise Verlag, Hannover, 11/2000
- [HeiseGS00] Schnurer, Georg: *Freie Auswahl?*, c't, Heise Verlag, Hannover 25/2000
- [HeiseW00] Heise Newsticker, 07.07.2000: *US-Online-Werber wollen Privatsphäre besser schützen*
- [HeiseWM00] Heise Newsticker, 18.07.2000: *Windows Media Player 7 mit CD-Brenner und Sicherheitsproblemen*,
<http://www.heise.de/newsticker/data/axv-18.07.00-000/>

- [HeiseZ00] Heise Newsticker, 01.05.2000: *Briten bauen Zentrum für Internet-Überwachung auf*, <http://www.heise.de/newsticker/data/cp-01.05.00-000>
- [Heiß99] Heiß, Hans-Ulrich: *Sicherheit in Rechensystemen* Folienskript 1999
- [Hoax96] *Viren, die es eigentlich gar nicht gibt, oder etwa doch?*
<http://minerva.sozialwiss.uni-hamburg.de/majordomo/hoax.html>
- [HTML97] Graham, Ian S.: *HTML Sourcebook, A Complete Guide to HTML 3.2 and HTML Extensions* Wiley Verlag, New York, 3.Auflage 1997
- [HTTP00] Clinton Wong: *HTTP Pocket Reference*, Mai 2000, O'REILLY
- [Lauer98] Lauer, Thomas: *Internet, Kompendium Markt & Technik* Buch- und Softwareverlag, Haar bei München 1998
- [Luckh99] Luckhardt, Norbert: *Die Vettern aus Dingsda, Gefahr durch ungebetene Gäste im Windows-PC* Computerzeitschrift c't, Heise Verlag, Hannover, 17/99
- [Microsoft] Microsoft: *OFF97: How to Minimize Metadata in Microsoft Documents*
<http://support.microsoft.com/support/kb/articles/Q223/3/96.ASP>
- [Microsoft00] Microsoft: *Globally Unique Identifiers (GUIDs)*
<http://msdn.microsoft.com/library/books/inole/S10E8.HTM>
- [Münz98] Münz, Stefan: *SELFHTML V 7.0*
<http://www.teamone.de/selfhtml/>
- [Netscape] Netscape: *Persistent Client State HTTP Cookies*
http://www.netscape.com/newsref/std/cookie_spec.html
- [Raepple98] Raepple, Martin: *Sicherheitskonzepte für das Internet* dpunkt-Verlag für digitale Technologie, Heidelberg, 1.Auflage 1998
- [Rannenber99] Müller G., Rannenber K.(Hrsg.): *Multilateral Security, Volume 3: Technology, Infrastructure, Economy*, Addison-Wesley-Longmann Verlag, München-Reading/Massachusetts, 1999
- [RFC791] Network Working Group, 1981: *RFC 781, Internet Protocol, Darpa Internet Program Protocol Specification*
<http://www.faqs.org/rfcs/rfc781.html>
- [RFC821] Network Working Group, 1982: *RFC 821, Simple Mail Transfer Protocol* <http://www.faqs.org/rfcs/rfc821.html>

- [RFC822] Network Working Group, 1982: *RFC 822, Standard for the Format of Arpa Internet Text Messages* <http://www.faqs.org/rfcs/rfc822.html>
- [RFC881] Network Working Group, 1983: *RFC 881, The Domain Names Plan and Schedule*. <http://www.faqs.org/rfcs/rfc881.html>
- [RFC882] Network Working Group, 1983: *RFC 882, Domain Names - Concepts and Facilities*. <http://www.faqs.org/rfcs/rfc882.html>
- [RFC883] Network Working Group, 1983: *RFC 883, Domain Names - Implementations and Specification*. <http://www.faqs.org/rfcs/rfc883.html>
- [RFC1034] Network Working Group, 1987: *RFC 1034, Domain Names - Concepts and Facilities* <http://www.faqs.org/rfcs/rfc1034.html>
- [RFC1035] Network Working Group, 1987: *RFC 1035, Domain Names - Implementations and Specification*. <http://www.faqs.org/rfcs/rfc1035.html>
- [RFC1244] Network Working Group, 1991: *RFC 1244, Site Security Handbook* <http://www.faqs.org/rfcs/rfc1244>
- [RFC1918] Network Working Group, 1996: *RFC 1918, Address Allocation for Private Internets* <http://www.faqs.org/rfcs/rfc1918.html>
- [RFC1945] Network Working Group, 1996: *RFC 1945, Hypertext Transfer Protocol* <http://www.faqs.org/rfcs/rfc1945.html>
- [Rötzer99] Rötzer, Florian: *Microsoft und Privacy* 13.03.1999
<http://www.heise.de/tp/deutsch/inhalt/te/1962/1.html>
- [Rötzer00] Rötzer, Florian: *Alles unter Kontrolle: Verschwören und Spionieren sind tägliches Geschäft in Wirtschaft und Politik* 17.04.2000
<http://www.heise.de/tp/deutsch/inhalt/buch/8053/1.html>
- [Santifaller93] Santifaller, Michael : *TCP/IP und ONC/NFS in Theorie und Praxis*, Addison-Wesley, Bonn, 2. Auflage 1993
- [Siering99] Persson C., Siering P.: *Big Brother Bill, Microsofts heimliche ID-Nummern - angeblich eine Panne* Computerzeirung c't, Heise Verlag, Hannover, 6/99
- [Smith] Smith, Richard M.: *The Web Bug FAQ*
<http://www.privacyfoundation.org/education/webbug.html>
- [SmithS00] Smith, Richard M.: *List of WebBugs*
<http://users.rcn.com/rms2000/privacy/wbfind.htm>

- [Smith98] Smith, Richard E.: *Internet Kryptographie*, Addison-Wesley, Bonn 1998
- [SmithS99] Smith, Richard M.: *On Internet Privacy and Profiling Senate Commerce Committee* 11.11.1999
<http://www.tiac.net/users/smiths/privacy/wbfaq.html>
- [SmithRJB99] Smith, Richard M. : *The RealJukeBox monitoring system*, 31.10.1999, <http://users.rcn.com/rms2000/privacy/realjb.htm>
- [SpiegelC00] Spiegel online: *512-Bit-Code geknackt*, 12.10.2000
- [SpiegelCV00] Spiegel Online: *Computerviren, Mehr als drei Billionen Mark Schaden*, 08.07.00
<http://www.spiegel.de/netzwelt/ebusiness/0,1518,84429,00.html>
- [SpiegelC99] Spiegel online: *Cursor überwacht Surfverhalten*, 20.11.1999
<http://www.spiegel.de/netzwelt/politik/0,1518,54709,00.html>
- [SpiegelFS00] Spiegel online: *Panik auf dem Boulevard, Familienministerium öffnet Tür zu Sex-Sites*, 29.03.2000
<http://www.spiegel.de/politik/deutschland/0,1518,70967,00.html>
- [SpiegelT00] Spiegel online: *Tracking-System findet verurteilte Pädophile*, 05.01.2000
<http://www.spiegel.de/netzwelt/politik/o,1816,58867,00.html>
- [SpiegelV00] Spiegel Online: *Spielzeughändler wegen Verkauf von Kundendaten verklagt*, 11.07.2000
- [SpiegelW00] Spiegel Online: *Das Weiße Haus will keinen Durchblick*, 22.06.2000
- [StalderVi00] Stalder, Felix : *Internet-Viren: Monokulturen fördern Parasitentum* Computerzeitung c't, Heise Verlag, Hannover 2000
- [StevensI94] Stevens, W. Richard : *TCP/IP Illustrated, Volume 1, The Protocols* Addison-Wesley 1994
- [StevensII94] Stevens, W. Richard: *TCP/IP Illustrated, Volume 3, TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols* Addison-Wesley 1996
- [Stinson95] Stinson, Douglas R. : *Cryptography, Theory and Practice* CRC Press 1995
- [VIR] F-Secure: *Virus Description*, <http://www.europe.DataFellows.com/v-descs/>

[Weidner97] Mraz V., Weidner K.: *Falsch verbunden, Gefahr durch DNS-Spoofing* Computerzeitschrift c't, Heise Verlag, Hannover, 10/97

[Whalen] Whalen, David : *The Unofficial Cookie FAQ*
<http://www.cookiecentral.com/>

[Wojcicki91] Wojcicki, Marek: *Sichere Netze* Hanser Verlag 1991

Index

- aktive Elemente, 58
- aktuelle Situation, 2
- AltaVista, 28
- Angriffe, 1
- Angriffsformen
 - brute-force, 76
 - denial-of-service, 49, 76
 - gerichtete, 1
 - man-in-the-middle, 38
 - nicht-gerichtete, 1
- anon.pl, 100
- anonymizer, 73
- Authentisation, 74

- BackOrifice, 56
- BDSG, 5, 6
- BND, 57
- Bootsektoren, 46
- Browser, 65
- BSI, 50

- cache pollution, 39
- Cookie, 17, 26, 64

- Datensicherung, 63
- Datenspuren, 22
- DES, 95, 98
- DNS, 13, 18, 36
- dnslookup.pl, 100
- domain name lookup, 18, 37
- domain2ns.pl, 100
- DoubleClick, 23, 28

- EMail, 20, 35
- Europaparlament, 9
- Explorer, 67

- Firewall, 72

- Gesetzgebung, 5
- Good Time, 52
- GUID, 23, 31

- guid.cpp, 100

- Handshake, 87
- Header
 - HTTP, 17, 88
 - HTTP-Request, 88
 - HTTP-Response, 90
 - IP, 84
 - TCP, 86
- Hintertüren, 56
- Hoax, 51
- Homepage, 35
- HTML, 14, 15
- HTML Tag, 27
- HTTP, 15–17, 25, 88
- HTTP Methoden, 89
- HTTP-Status Code, 90

- IAF.net, 29
- IMG Tag, 27
- Infizierung, 49
- informationen.pl, 100
- informelle Selbstbestimmung, 6, 22
- Inhaltsdaten, 24
- Integrität, 22
- Internet
 - Aufbau, 14
 - Datenübertragung, 12
 - Schichten, 13
- Internet Explorer, 18
- IP, 13, 18
- IP-Adresse, 18, 25
- ip2name.pl, 100
- ISO, 83

- Klartext, 95

- laurin.html, 100
- Locationzeile, 41

- MAC, 18, 31
- Marketinggesellschaften, 30

- MBR, 46
- Media Player, 33
- Metadaten, 32, 71
- Microsoft, 31, 32
- MIME, 20
- MS-Excel, 31
- MS-OutLook, 31
- MS-Word, 31

- Nachricht, 12
- name2ip.pl, 100
- NetDeals.com, 29
- Netscape, 17, 33
- Network Information Center, 91
- News-Servern, 36
- NIC, 91
- NNTP, 35
- NSA, 23, 57, 77

- Office 97, 31
- One-Time Pad, 94
- Online Profil, 27
- Onlineagenturen, 30
- Onlineprofil, 29
- OSI, 83
- OSI-Modell, 83
- OSI-Schichten, 83

- Paket, 12
- Paketfilter, 72
- Persönlichkeitsprofil, 29
- PIN, 38
- POP3, 20
- Port, 86, 93
- Proxy Gateway, 72
- PPTP, 56
- Pretty Good Privacy, 77
- Programme, 100
- Protokolle, 12, 83
 - HTML, 15
 - HTTP, 15–17, 37
 - IP, 13, 18, 83
 - IPv4, 84
 - Kapselung, 14
 - MIME, 20
 - NNTP, 35
 - POP3, 20
 - PPTP, 56
 - SMTP, 20
 - TCP, 13, 84
 - UDP, 13, 84
- Public Key, 96

- Query-ID guess, 39

- RealJukebox, 33
- Registration Wizard, 32
- Registry, 69
- Remailer, 77
- Resource Records, 20, 76
- reverse dns lookup, 19, 76
- RR, 39, 76
- RSA, 97, 99

- Sandbox, 58
- Schutzmaßnahmen, 21
- SendIt, 33
- server-side resource processing, 15
- sichere Hafen, 10
- Sicherheitsmaßnahmen, 21
- SmartDownload, 33
- SMTP, 20
- socket.pl, 100
- Spoofing, 36
- Stammdaten, 24
- Statuszeile, 41
- StGB, 5

- Tag, 16
- TAN, 38
- Task Manager, 69
- TCP, 13
- TDDSG, 8
- TDG, 7
- time to live, 84
- TKG, 7
- top level domain, 19
- Toysmart, 23

- tracking, 23
- Trojaner, 30, 53, 68
 - AOL.Buddy, 54
 - Comet Cursor, 54
 - IRC-Hack, 54
 - Multimedia-Player, 54
 - SendIt, 54
- TRUSTe, 34
- ttl, 20, 39, 92
- ttl.pl, 100

- UDP, 13
- URL, 14, 15, 36
- URL Rewriting, 41
- Usenet, 35

- Verbindungsdaten, 24
- Verfügbarkeit, 22
- Verschlüsselung, 93
 - asymmetrisch, 96
 - symmetrisch, 95
- Vertraulichkeit, 22
- Viren, 45, 68
 - Additive, 46
 - CIH , 49
 - Ersetzende, 46
 - Formvirus, 48
 - I LOVE YOU, 43
 - Makroviren, 46
 - Melissa, 48
 - Michelangelo, 49
 - Programmviren, 46
 - Schalen, 46
 - Systemviren, 46
- Volkszählungsurteil, 5

- WebBug, 27
- WebSpoofing, 41
- well known port, 15, 93
- Werbeagentur, 30
- Windows 98, 31
- Word.Share.Fun, 44
- Wurm, 51
- WWW, 14

- Y2K, 56
- Zertifikat, 74