Politische und rechtliche Maßnahmen gegen unerwünschte Emails

Diplomarbeit

vorgelegt an der

Technischen Universität Berlin
Fakultät IV – Elektrotechnik und Informatik

Berlin, April 2006

Jan-Ole Beyer

eingereicht bei:
Prof. Dr. iur. Bernd Lutterbeck
Institut für Wirtschaftinformatik und Quantitative Methoden
Informatik und Gesellschaft
Franklinstr. 28/29
10587 Berlin

Eidesstattliche Erklärung

Die selbstständige und eigenhändige Anfertigung versichere ich an Eides Statt.

Berlin, 11. April 2006

Abstract

Die vorliegende Arbeit beschäftigt sich mit politischen, rechtlichen und technischen Strategien der Spam-Bekämpfung. Um einen umfassenden Überblick über diesen Themenbereich zu erhalten, wird zunächst eine Einführung in die technischen Grundlagen des Bereichs als auch in die derzeitige nationale und internationale Rechtslage gegeben. Ebenso wird auf bereits existierende nationale und internationale Projekte und Initiativen eingegangen. Darauf basierend werden mögliche Strategien ausgeführt, erörtert und bewertet, so dass abschließend umfassende Empfehlungen für Maßnahmen primär seitens der Bundesregierung, aber auch seitens der zu beteiligenden Unternehmen ausgesprochen werden können.

Danksagung

Ich möchte an dieser Stelle all denjenigen danken, die mir bei dem Verfassen dieser Diplomarbeit tatkräftig zur Seite standen. Insbesondere danke ich Prof. Bernd Lutterbeck und Frank Pallas für das mir entgegengebrachte Vertrauen und die Ermöglichung dieser Arbeit. Ebenso danke ich dem Bundesministerium des Innern, insbesondere Andreas Schmidt vom Referat IT3 sowie Dr. Joachim Sturm von der KBSt für ihre Unterstützung.

Des Weiteren danke ich meinen Freunden und Verwandten, allen voran meinen Eltern und meinen Großvater, die mich auf unterschiedlichste Weise unterstützt haben. Nicht zuletzt danke ich May-Britt für viele Monate der (nicht nur moralischen) Unterstützung und für die Korrektur von Rechtschreibfehlern und seltsamen Sätzen.

Inhaltsverzeichnis

Abkürzungsverzeichnis

ACMA	Australian Communications and Media Authority
APWG	Anti-Phishing Working Group
ARPANET	Advanced Research Projects Agency NETwork
ASEM	Asia-Europe Meeting
BATV	Bounce Adress Tag Validation
BMELV	Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz
BMWi	Bundesministerium für Wirtschaft und Technologie
BSA	Business Software Alliance
CNSA	Contact Network of Spam enforcing Authorities
DARPA	Defense Advanced Research Projects Agency
dDoS	distributed Denial of Service
DDV	Deutscher Direktmarketing Verband
DNS(1)	Domain Name System
DNS(2)	Delivery Status Notification
DNSBL	Domain-Name-System-Blacklist
EFF	Electronic Frontier Foundation
ESMTP	Extended Simple Mail TRansfer Protocol
FTC	Federal Trade Commission
GIAIS	Global Infrastructure Alliance for Internet Safety
http(s)	hypertext transfer protocol (secure)
iCAUCE	international Coalition Against unsolicited Commercial Email
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRC	Internet Relay Chat
ISC	Internet Society of China
ISP	Internet Service Provider
ITU	International Telecommunication Union
IX	Internet Exchange

KISA	Korean Information Security Agency
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
LAP	London Action Plan
MAAWG	Messaging Anti-Abuse Working Group
MLM	Multi-Level-Marketing
MMF	Make Money Fast
MMS	Multimedia Messaging Service
NASK	Naukowa i Akademicka Siec Komputerowa
NGO	Non-Governmental Organisation
OECD	Organisation for Economic Co-operation and Development
OFISP	Open Forum of the Internet Providers
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
PGP	Pretty Good Privacy
PIN	Persönliche Identifikationsnummer
POP3	Post Office Protocol version 3
RFC	Request For Comments
RHSBL	Right-Hand-Side-Blacklist
ROKSO	Register Of Known Spam Operations
S/MIME	Secure / Multipurpose Internet Mail Extensions
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPF	Sender Policy Framework
TAN	Transaktionsnummer
TCP	Transmission Control Protocol
TKG	Telekommunikationsgesetz
TLS	Transport Layer Security
UBE	Unsolicited Bulk Email
UCE	Unsolicited Commercial Email
URIDNSBL	Uniform-Resource-Identifier-Domain-Name-System-Blacklist
UWG	Gesetz gegen den unlauteren Wettbewerb
VoIP	Voice over IP
vzbv	Verbraucherzentrale Bundesverband
WBZ	Zentrale zur Bekämpfung des unlauteren Wettbewerbs
WSIS	World Summit on the Information Society

1 Einleitung

Emails, vor gerade einmal 15 Jahren noch eher eine Ausnahme, sind heutzutage nicht mehr wegzudenken aus der privaten und geschäftlichen Kommunikation. Der Siegeszug dieses Mediums in gerade einmal etwas mehr als einem Jahrzehnt ist beispielhaft. Noch sehr viel stärker als das Email-System selbst hat sich jedoch der Missbrauch desselben entwickelt. Während Mitte der neunziger Jahre die ersten Menschen begannen, Werbung in großer Anzahl per Email, aber auch im Usenet zu verschicken, steht das Email-System heute kurz vor dem Kollaps. Studien zufolge sind mittlerweile zwischen 60 und 90% des weltweiten Email-Aufkommens Spam. AOL, der weltweit größte Onlinedienst, filterte bereits 2003 nach eigenen Angaben täglich 2,3 Milliarden unerwünschte Emails.[1] Das Aussortieren kostet Privatanwender, vor allem aber auch Unternehmen Unsummen.

Ein komplettes Verhindern von Spam scheint jedoch – begründet vor allem in der (offenen) Struktur des Emails-Systems – nahezu unmöglich. Die radikalste Möglichkeit, die Neuschaffung des kompletten Systems, erscheint aufgrund der immensen Größe des Internets ebenso schwer umsetzbar. Um jedoch trotzdem Spam zumindest so weit wie möglich Einhalt zu gebieten, bedarf es der Arbeit auf verschiedenen Ebenen. Technische, regulatorische oder aufklärende Maßnahmen jeweils für sich genommen können nur wenig erreichen; zusammen bieten sie jedoch das schärfste Schwert, das derzeit im Kampf gegen Spam zur Verfügung steht.

Aus diesem Grund hat diese Arbeit zum Ziel, nicht nur technische, sondern vor allem auch rechtliche und politische Maßnahmen gegen Spam zu erarbeiten und bewerten. Ebenso soll sie einen Überblick bieten über die derzeitige (rechtliche und politische) Situation in Deutschland, aber auch in relevanten weiteren Staaten. Auf diese Weise kann die Arbeit einerseits als Einführung in die Problematik dienen – vor allem aus Sicht der Politik – als auch gleichzeitig mögliche Lösungen und Wege beschreiben.

Um dieses Ziel zu erreichen, bietet Kapitel 2 grundsätzliche Definitionen und Erläuterungen zu Spam und seinen verschiedenen Formen. Kapitel 3 beinhaltet technische Grundlagen bezüglich Spam. Neben einer kurzen Beschreibung des Internets selbst wird hierbei vor allem auf das Email-System eingegangen, um zu verdeutlichen, aus welchem Grund Spam funktioniert und wie Spammer vorgehen. Ebenso soll in diesem Kapitel auf mögliche technische

[1] Vgl. Schmidt (2003)

Ansätze der Spam-Bekämpfung eingegangen werden. Diese sollen jedoch im Rahmen dieser Arbeit nur einen kleinen Teil einnehmen; eine hervorragende Übersicht zu diesem Aspekt bietet z.B. BSI (2005).

Kapitel 4 beleuchtet einerseits die derzeitige Rechtslage in Deutschland bezüglich der verschiedenen, in der Einführung aufgeführten Arten von Spam. Ebenso werden die verschiedenen deutschen Akteure in der Spam-Bekämpfung – vor allem Behörden und Verbände – sowie deren Arbeit betrachtet. Um jedoch der Internationalität des Problems gerecht werden, werden auch weitere Staaten betrachtet, vor allem solche, die in vielen Studien als führende „Spam-Nationen" auftauchen. Des Weiteren werden internationale Projekte und Organisationen vorgestellt, die maßgeblich im multilateralen Bereich arbeiten.

Diese Kapitel vorausgeschickt, beinhaltet Kapitel 5 einen Überblick über mögliche Maßnahmen der Spam-Bekämpfung auf regulatorischer, aufklärender und technischer Ebene sowie durch internationale Kooperation und Selbstregulierung der Wirtschaft. Eine grundlegende Bewertung dieser Maßnahmen wird ebenfalls vorgenommen. Auf diesem Kapitel aufbauend beinhaltet Kapitel 6 dann Empfehlungen, welche Maßnahmen hinsichtlich einer effektiven nationalen Spam-Bekämpfungs-Strategie sinnvoll und umsetzbar sind. Dieser Katalog von Maßnahmen bietet auch für sich alleine einen Überblick über eine mögliche Strategie, nicht nur seitens der Bundesregierung, sondern auch seitens der zu beteiligenden Unternehmen und Verbände.

Aufgrund der schnellen Entwicklung im Bereich des Internets muss darauf hingewiesen werden, dass diese Arbeit den Stand von Anfang 2006 wiedergibt. Insbesondere Studien und Statistiken, aber auch die Techniken und Vorgehensweisen der Spammer verändern sich oftmals in sehr kurzer Zeit, so dass Details dieser Arbeit ebenso schnell nicht mehr aktuell sein mögen. Grundlegende Feststellungen dieser Arbeit betrifft dies jedoch nicht.

2 Einführung

Da die Bedeutung des Begriffes *Spam* nicht genau definiert ist, soll in diesem einführenden Kapitel eine innerhalb dieser Arbeit gültige Definition erarbeitet werden. Neben *Spam* selbst spielen jedoch auch noch andere Begriffe eine Rolle, die ebenfalls einführend erläutert werden sollen. Des Weiteren soll dargestellt werden, weswegen Spam zu einem immer größeren, vor allem auch wirtschaftlichen Problem wird.

2.1 Definition von Spam

Spam ist heutzutage in aller Munde. Jedoch wird der Begriff mittlerweile nahezu inflationär verwendet. Um die weitgehenden, umgangssprachlich oft verwendeten Bedeutungen für den Rahmen dieser Arbeit einzuschränken, wird in diesem Kapitel neben einem kurzen Blick auf die Herkunft des Begriffes eine klar abgrenzbare Definition festgelegt, auf der die folgende Arbeit beruht.

2.1.1 Herkunft des Begriffes *Spam*

Der Begriff *SPAM* bezeichnet in dieser Schreibweise und als Zusammenfassung aus *SPiced hAM* ursprünglich ein Dosen-Frühstücksfleisch der Firma Hormel Foods Inc.[2] Die Verwendung des Begriffs für unerwünschte Emails basiert vermutlich auf einem Sketch der britischen Komiker-Gruppe Monty Python.[3] Ursprünglich wurde der Begriff auf Werbung im Usenet angewandt und später dann auf Emails übertragen. Um Rechtsstreitigkeiten mit dem Hersteller des Frühstücksfleischs zu vermeiden, wurde sich darauf geeinigt, die unerwünschten Emails als Spam[4] zu bezeichnen.[5]

In der vorliegenden Arbeit wird nur das Medium *Email* behandelt. Andere Kommunikationsmittel, bei denen Spam vorkommt – z.B. Instant Messaging, aber auch Fax und Telefonie – werden in dieser Arbeit nicht betrachtet.

[2] online unter http://www.spam.com/ [18.02.2006]
[3] Der Sketch wurde im Rahmen der 25. Folge der Comedy-Serie *Monty Python's Flying Circus* aufgeführt
[4] Also nicht in Großbuchstaben geschrieben
[5] Vgl. *SPAM Corporate Info*: „SPAM and the Internet" (online unter: http://www.spam.com/ci/ci_in.htm [18.02.2006])

2.1.2 Definition von Spam

Basierend auf BSI (2005) verwendet diese Arbeit folgende Definition:

> Der Begriff *Spam* bezeichnet *unverlangt zugesandte Massen-Email*.
>
> *Unverlangt* ist eine Email dann, wenn das Einverständnis des Empfängers zum Empfang der Nachricht nicht vorliegt und nicht zu erwarten ist.
>
> *Massen-Email*, so genannte *bulk mail* bedeutet, dass der Empfänger die Nachricht nur als einer von vielen erhält.

Nur wenn beide oben genannte Kriterien auf eine Email zutreffen, so darf sie als Spam bezeichnet werden. Sowohl lediglich unverlangt empfangene Emails, z.B. eines aus den Augen verlorenen Freundes, als auch Massen-Emails z.B. in Form eines Newsletters, den der Empfänger freiwillig abonniert hat, sind also kein Spam.[6]

Im Allgemeinen werden so definierte Emails im Englischen als *unsolicited bulk emails* (Unverlangte Massen-Email, UBE) bezeichnet. Neben reiner kommerzieller Werbung[7] gehören hierzu ebenso per Email versandte Viren oder Würmer, Phishing-Emails oder Hoaxes[8]. Es ist an dieser Stelle zu beachten, dass im juristischen Bereich unter Spam im Normalfall lediglich unerwünschte Werbe-Emails, also UCE verstanden wird. Im Rahmen dieser Arbeit soll jedoch nicht nur dieser Bereich betrachtet, sondern es sollen Empfehlungen erarbeitet werden, die den gesamten Komplex *Spam* beinhalten.

Als Gegenbegriff zu Spam, also als Begriff für erwünschte Emails, hat sich *Ham* (englisch für „Schinken“) eingebürgert.

Obwohl die genannte Definition weitgehend anerkannt ist[9], ist die Einschätzung, ob es sich bei einer Email um Spam handelt, trotzdem immer abhängig von der Einstellung des Empfängers und somit kaum objektiv zu erfassen. Eine rein automatisierte Sortierung in Spam und Ham ist also nahezu undurchführbar. In diesem Zusammenhang kommt des Weiteren noch hinzu, dass z.B. eine inhaltliche Sortierung kaum fehlerfrei vorgenommen werden kann, da durchaus auch private Emails – zumindest für die Software – den Charakter von Spam haben können, andererseits aber auch Spam so geschickt „verpackt“ werden kann, dass er wie eine private Email aussieht.

Wie bereits am Beispiel des Newsletters weiter oben erläutert, gilt dasselbe für reine Massen-Emails. Der Charakter des massenhaften Versendens kann ein Indiz für Spam sein,

[6] Letzteres Beispiel wird natürlich genau dann zu Spam, wenn der Empfänger dem Absender mitgeteilt hat, dass er den Newsletter nicht weiter empfangen will, er ihn aber trotzdem erhält.

[7] Diese wird im Englischen als *unsolicited commercial email* (unverlangte kommerzielle Email, UCE) bezeichnet.

[8] Die vorangegangenen Begriffe werden im folgenden Abschnitt näher erläutert.

[9] Vgl. z.B. http://www.spamhaus.org/definition.html oder http://de.wikipedia.org/wiki/Spam. Eine ähnliche Definition findet sich bei http://www.mail-abuse.com/spam_def.html [18.02.2006].

ist aber keinesfalls hinreichend. Dasselbe gilt ebenso für die Frage, inwieweit Absender und Empfänger sich kennen. So versenden sich Viren z.B. häufig durch fehlerhafte Software auf Anwender-Rechnern und benutzen dabei Email-Adressen, die in Adressbüchern o.ä. auf dem befallenen Rechner gefunden wurden.[10] In diesem Fall ist es möglich, dass Absender und Empfänger sich kennen, aber die Email trotzdem als Spam klassifiziert werden kann.

2.2 Andere relevante Begriffserläuterungen

In diesem Abschnitt sollen, nachdem eine grundlegende Definition von Spam erarbeitet wurde, die bereits erwähnten einzelnen Formen des Email-Spams näher betrachtet werden. Teilweise handelt es sich dabei um Bereiche, die in ähnlicher Form auch in der „realen“ Welt existieren. Im Rahmen dieses Kapitel soll jedoch lediglich auf ihre Bedeutung innerhalb des Komplexes „Email und Spam“ eingegangen werden. Die folgenden Kategorisierungen basieren auf BSI (2005).

2.2.1 Kommerzielle Werbung

Mittels unverlangt zugesandter kommerzieller Werbung, meist als *unsolicited commercial email* (UCE) bezeichnet, wird versucht, den Empfänger zum Kauf des angepriesenen Produktes zu animieren. In der Regel ist der Versand von UCE mittlerweile in Deutschland wie auch in vielen anderen Staaten unzulässig; die juristische Definition von Spam beinhaltet nur diese Kategorie. Während, auch aufgrund des Verbots, seriöse Anbieter auf diese Art der Werbung nahezu verzichten, werden heutzutage primär pornografische Websites, potenzsteigernde Mittel, Diätpillen, aber auch Aktien u.ä. beworben. Zumeist wird die Werbung nicht direkt vom Betreiber einer Website bzw. dem Distributor eines Produktes, sondern als Dienstleistung durch (professionelle) Spammer versandt.

2.2.2 Nicht-kommerzielle Werbung

Neben der kommerziellen Werbung können auch Emails, die weltanschauliche, religiöse oder politische Positionen vertreten mit dem Zweck, die Empfänger zu beeinflussen, als Werbe-Spam bezeichnet werden. So wurden Anfang Mai 2005 eine Vielzahl an Emails mit rechtsextremistischem Inhalt mittels des Wurms *Sober.Q* versandt.[11]

[10] Vgl. z.B. http://www.bsi.bund.de/av/texte/wurm-meld.htm [18.02.2006]

[11] Vgl. z.B. Heise News vom 15.05.2005: „Neonazi-Propaganda überschwemmt Postfächer“ (online unter http://www.heise.de/newsticker/meldung/59562 [18.02.2006])

2.2.3 Malware

Neben Werbung wird i.A. auch so genannte *Malware*, zu deutsch Schadsoftware, als Spam bezeichnet. Hierunter versteht man Viren und Würmer, die sich über Schwachstellen im PC, aber auch per Email verbreiten, sowie Trojaner[12], also Software, die sich als eigentlich harmloses Programm tarnt. Des Weiteren zählt so genannte Spyware, die Benutzer- und Rechnerdaten ausspioniert, zu diesem Bereich. Im Rahmen dieser Arbeit soll die Bekämpfung von Malware lediglich am Rande betrachtet werden. Allerdings werden seit einiger Zeit so genannte *Botnets*[13] und auch Viren eingesetzt, um Spam über befallene Rechner zu verschicken. Dieser Aspekt wird in Kapitel 3.3.4 näher beschrieben.

2.2.4 Betrug und Phishing

Das bekannteste Beispiel für Betrug per Email ist sicherlich der so genannte *Nigeria-Scam*[14]. Hierbei gaukeln Emails mit Betreffzeilen wie z.B. „Confidential Business Proposal“ dem Empfänger vor, dass aus meist fadenscheinigen Gründen der Absender eine große Geldsumme ins Ausland transferieren muss und die Hilfe des Empfängers benötigt. Wenn man auf dieses Angebot eingeht, wird man zumeist nach kurzer Zeit gebeten, z.B. aufgrund von notwendigen Überweisungsgebühren o.ä. mit einer kleineren Summe in Vorleistung zu treten. Dieses Geld ist aber letztlich das Ziel der Betrüger, und so erhält man die versprochene riesige Geldsumme natürlich nicht. Mittlerweile gibt es eine Vielzahl an ähnlichen Versuchen, die in der Grundidee aber alle gleich aufgebaut sind.

Unter dem Begriff *Phishing*[15] versteht man den Versuch, das Opfer zur Preisgabe von sensiblen Daten wie Passwörtern, Kreditkartennummern, PINs oder TANs zu verleiten. Hierzu verschicken die Betrüger Emails, die denen von z.B. einem Webshop oder einer Bank gleichen. Hierin wird der Empfänger aufgefordert, z.B. sein Passwort bei dem entsprechenden Unternehmen zu ändern. Um es dem Empfänger einfach zu machen, beinhaltet die Email einen Link, der allerdings auf eine ebenfalls gefälschte Website führt, auf der er dann (ohne es zu bemerken) nicht sein Passwort ändert, sondern es den Betrügern übermittelt.[16]

Neben dieser grundlegenden Variante des Phishing steigt – vermutlich auch aufgrund der steigenden Bemühungen der Banken, „einfaches“ Phishing zu verhindern – die Anzahl ähnlicher Attacken. Das so genannte *Spear-Phishing* zielt dabei weniger auf Bankdaten, sondern

[12] Korrekt werden diese Programme als *Trojanische Pferde* (Vgl. Voß (1875, Zweiter Gesang, Vers 15ff)) bezeichnet. Im allgemeinen Sprachgebrauch hat sich aber die Kurzform durchgesetzt.

[13] Hierbei handelt es sich um eine große Anzahl von durch Trojaner befallenen Rechnern (häufig mehrere tausend bis über 100.000), die durch ihren Programmierer über das Internet gesteuert werden und quasi „auf Befehl“ Spam verschicken.

[14] Vgl. z.B. http://www.nigeria-connection.de/ [18.02.2006]

[15] Der Begriff wird hergeleitet von engl. *fishing*, also dem Fischen mit einem Köder

[16] Vgl. hierzu auch die Website der *Anti-Phishing Working Group*: http://www.anti-phishing.org/ [18.02.2006]

auf ausgesuchte Unternehmen. Hierzu sammeln die Phisher gezielt Informationen über dieses. Mit Hilfe dieser Daten wird eine Email erstellt und an Mitarbeiter des Unternehmens versendet, die den Anschein erweckt, als würde sie aus dem internen Firmennetzwerk stammen, und in der die Empfänger aufgefordert werden, z.B. Zugangsdaten zurückzusenden. Mit Hilfe dieser Zugangsdaten können die Phisher dann in das Firmennetzwerk eindringen und mit Hilfe von Spionage-Programmen interne Informationen abschöpfen, die dann an die Auftraggeber, oftmals Konkurrenten des Unternehmens, verkauft werden.[17]

Eine weitere Phishing-Variante ist das so genannte *Pharming*[18] . Phisher verschicken hierbei keine Emails, sondern ändern die DNS-Einträge der gängigen Banken, so dass z.B. bei Aufruf der Website der Deutschen Bank (http://www.deutsche-bank.de/) nicht mehr diese, sondern die Website der Phisher geöffnet wird. Zu diesem Zweck unterhalten sie große Serverfarmen, auf denen die entsprechenden Fälschungen angeboten werden. Von diesen Serverfarmen leitet sich der Begriff „Pharming“ ab. Um herbeizuführen, dass nicht mehr die echten Websites, sondern die Fälschungen aufgerufen werden, gibt es verschiedene Verfahren, die die Phisher anwenden. Beim so genannten *DNS-Cache-Poisoning* dringen die Phisher direkt in DNS-Server ein und ändern dort die Verweise von Domain auf IP-Adresse. Zumeist handelt es sich bei den betroffenen Servern um DNS-Server, die nahe am Client angesiedelt sind und die DNS-Anfragen zwischenspeichern. Daher sind auch nicht sämtliche Nutzer der entsprechenden Website, sondern lediglich die Nutzer eines korrumpierten DNS-Servers betroffen. Alternativ zum DNS-Cache-Poisoning werden die Clientrechner selbst durch Malware[19] so manipuliert, dass sie die Anfragen für die betroffenen Websites auf die Fälschungen umleiten. Hierzu bedient sich die Software der so genannten *hosts*-Datei des Rechners. Bei dieser handelt es sich im Grunde um eine Art lokaler DNS-Auflösung, die noch vor den eigentlichen DNS-Servern befragt wird. Durch dort eingefügte gezielte Einträge wird also erreicht, dass nicht die über das DNS-System korrekte IP-Adresse zu einer Website aufgerufen wird, sondern die der Phisher. Da es sich bei Pharming nicht um Spam handelt, soll im Folgenden hierauf jedoch nicht weiter eingegangen werden. Nichtsdestotrotz muss auch ein solches Phänomen bei der Erarbeitung einer umfassenden Internet-Sicherheitsstrategie bedacht werden.

2.2.5 Rufschädigung und ähnliches

Hierbei handelt es sich um eine eher indirekte Variante des Spams. Unter Ausnutzung der leichten Fälschbarkeit von Email-Absendern verschickt der Spammer seinen Spam in fremdem Namen, in diesem Fall aber in der Erwartung, dass sich die Empfänger beim vermeintlichen Absender oder dessen Firma oder Internet-Provider beschweren.

[17] Vgl. dazu z.B. Ziemann (2005)
[18] Vgl. z.B. http://de.wikipedia.org/wiki/Pharming [18.02.2006]
[19] Vgl. Kapitel 2.2.3

Während Spammer mittlerweile auch bei „echter“ Werbung beliebige, aber echte Email-Adressen verwenden, ist in diesem Fall nicht die Werbung das Ziel, sondern der Rücklauf durch Beschwerden. Insbesondere Anti-Spam-Aktivisten werden auf diese Weise von ihren Gegnern angegriffen.

Dieses gezielte Fälschen von Emails zur Rufschädigung wird i.A. als *Joe Job* bezeichnet. Der Begriff begründet sich auf dem Amerikaner Joe Doll, der 1997 Opfer eines solchen Angriffs wurde.[20] Nachdem er einen Spammer aus seinem System verbannt hatte, rächte sich dieser auf die beschriebene Weise, so dass durch Beschwerden und Fehlermeldungen, aber auch Gegenangriffe der Empfänger Dolls System zehn Tage nicht erreichbar war.

2.2.6 Hoaxes und Kettenbriefe

Hoaxes[21] und Kettenbriefe gehören zwar auch zum Oberbegriff *Spam*, unterscheiden sich aber insofern, als dass sie nicht von einem Spammer massenhaft an andere geschickt werden, sondern sich von einem Empfänger zu einigen weiteren etc. ausbreiten. Im Gegensatz zu allen anderen Kategorien verbreiten sich diese also über die Schwachstelle Mensch, nicht über Fehler im System.

Hoaxes kommen in vielen Formen vor und beinhalten z.B. den Hinweis auf eine Schwachstelle in einem bestimmten Betriebssystem, verbunden mit der Aufforderung, zur Behebung z.B. eine bestimmte Datei zu löschen sowie die Email an weitere Betroffene weiterzuleiten. In den meisten Fällen wird dadurch aber natürlich keine Schwachstelle behoben, sondern dem betroffenen System geschadet.

Kettenbriefe beinhalten häufig eine rührselige Geschichte, gerne über ein todkrankes Kind, das dringend eine Knochenmarkspende o.ä. benötigt. Auch nach dem Tsunami in Südostasien Ende 2004 gab es eine Welle von Kettenbriefen mit Fotos verletzter Kinder, die angeblich ihre Familie verloren haben. Diese Emails kursieren teilweise mehrere Jahre im Internet, so dass der eigentlich Anlass meist bereits vollkommen vergessen ist. Neben dieser Variante des Kettenbriefs sind auch die *Schneeball-* oder *Pyramidensysteme* weit verbreitet. Bei so genannten (illegalen) *Make Money Fast*-Systemen (MMF) werden die Empfänger in einem häufig verwirrenden und langen Text aufgefordert, an 5 oder 6 in der Email aufgeführte Personen einen kleinen Geldbetrag zu überweisen und den obersten Namen zu löschen. Daraufhin soll der eigene Name zu der Liste hinzugefügt werden und die Email an möglichst viele Personen weitergeleitet werden. Auf diese Weise, wird dem Empfänger vorgegaukelt, wird auch er in einiger Zeit oben auf der Liste stehen und viel Geld verdienen. Es kann jedoch nachgewiesen

[20] Vgl. den Bericht von Joe Doll (online unter http://www.joes.com/spammed.html [18.02.2006])

[21] Der englische Begriff *Hoax* bezeichnet eigentlich einen Scherz, kann in diesem Zusammenhang aber deutlicher als „Falschmeldung“ beschrieben werden.

werden, dass nur der Initiator – und u.U. sehr wenige Ebenen seiner Nachfolgerschaft – mit dieser Methode wirklich Geld verdienen können.[22]

Empfänger der oben genannten Email-Typen sollten diese keinesfalls weiterverbreiten, sondern sich auf einschlägigen Websites[23] über den Wahrheitsgehalt informieren.

Ähnlich zu MMF-Systemen verhalten sich Verkaufsstrategien wie das so genannte *Multi Level Marketing* (MLM). Hierbei stehen mehrere Verkäuferschichten übereinander; vor allem die unteren Strukturen pflegen den Kundenkontakt. Die Organisationsstruktur solcher Strategien besteht aus einer großen Anzahl von Beteiligten auf der untersten Ebene sowie sehr wenigen an der Spitze, was zu dem Begriff *Pyramidensystem* führte. Sie sind häufig auf den ersten Blick, z.B. in Anzeigen, nur schwer von Schneeballsystemen zu unterscheiden. Für eine solche Trennung ist entscheidend, ob tatsächlich Werbung und Verkauf eines Produktes oder die Werbung neuer Kunden im Vordergrund steht.

2.2.7 Kollateraler Spam

Kollateraler Spam unterscheidet sich dadurch von den bereits genannten Kategorien, dass es sich primär um per Email verschickte Fehlermeldungen (so genannte *bounces*) handelt, die durch den „eigentlichen" Spam verursacht wurden. So kommt es z.B. vor, dass der Empfänger einer Spam-Email nicht existiert oder dass die Email durch einen Virenscanner aufgehalten wird. Diese Systeme schicken dann zumeist eine Fehlermeldung an den Absender der Email. Da die meisten Spam-Emails allerdings gefälschte Absenderadressen tragen, erreicht dieser kollaterale Spam dann nicht die Verursacher selbst, sondern unschuldige Opfer.

2.3 Die Spam-Problematik

Zur Verdeutlichung der Probleme, die Spam in seiner Gesamtheit hervorruft, muss deutlich unterschieden werden zwischen den einzelnen, im vorhergehenden Kapitel beschriebenen Formen.

Auf nahezu alle Formen trifft die Belastung des weltweiten Email-Systems zu, die durch die hohe Anzahl an Spam-Nachrichten verursacht wird. Trotzdem der Anteil an Spam zu sinken scheint, sind Schätzungen zufolge immer noch deutlich über 60%[24] des weltweiten Email-Aufkommens unerwünschter Spam in jeglicher Variante. Dieser verursacht auf Seiten

[22] Vgl. z.B. Röß (1995, Kapitel 2.2.3)

[23] z.B. http://www.hoax-info.de/, http://www.hoaxbusters.de/ oder http://hoaxbusters.ciac.org/ [18.02.2006]

[24] Verschiedene Anbieter von Email-Filtern erstellen regelmäßige Statistiken über die bei ihren Kunden herausgefilterten Spam-Emails, so z.B. MessageLabs (http://www.messagelabs.com/emailthreats/ [18.02.2006]) und Postini (http://www.postini.com/stats/ [18.02.2006]).

der Mailprovider einen deutlich größeren Bedarf an Rechenleistung und Speicherplatz zur Verarbeitung der Emails als eigentlich notwendig wäre. Ebenso bedeutet das für den Anwender notwendige Aussortieren von Spam aus seinem Postfach einen Verlust an (Arbeits-)Zeit. Mag diese im Privatbereich noch vernachlässigbar sein, handelt es sich im Unternehmen um einen ernstzunehmenden Kostenfaktor – unabhängig davon, ob der Arbeitnehmer eigenständig Emails sortieren muss oder ob eine Filter-Software angeschafft und gewartet wird.

Obwohl der Anteil an reiner UCE einigen Studien[25] zufolge sinkt, stellt er dennoch den größten Teil des „Spamkuchens“ dar. Inwieweit und warum sich das Geschäft mit dieser Form der Werbung lohnt, soll anhand eines kurzen Beispiels erläutert werden.

Während Schäden durch Malware zumeist eindeutig und offensichtlich sind und der Betrug mittels Phishing eindeutig strafbar ist, stellt sich diese Situation bei UCE anders dar. So argumentieren Spammer häufig, dass ein einfaches Löschen ihres Spams durch den Empfänger nur wenig Zeit benötigt und keinerlei Schäden verursacht.

Ein wesentlicher Punkt für die Wirtschaftlichkeit von UCE ist der Kostenfaktor. Während normale, also gedruckte Werbung einerseits durch Druck- und Verteilungskosten teuer ist und andererseits im Normalfall relativ wenige Menschen erreicht, kostet Email-Spam nahezu nichts. So verschickte der im November 2004 verurteilte[26] Spammer Jeremy Jaynes nach eigenen Angaben bis zu 10 Millionen Spam-Emails pro Tag. Dazu nutzte er 16 Breitbandleitungen, für die er etwa 50.000 $ pro Monat zahlte. Trotz der geringen Rückmeldequote von nur 0,03‰ konnte Jaynes durch die immens hohe Anzahl an verschickten Emails so immer noch mehrere tausend Kunden erreichen, was zu einem Gewinn von bis zu 750.000 $ im Monat führte.[27]

Jaynes galt vor seiner Festnahme Ende 2004 nach einer Liste der Anti-Spam-Initiative Spamhaus[28] als einer der zehn aktivsten Spammer. Insgesamt zählt diese so genannte ROKSO[29]-Liste etwa 200 Spammer auf, die für 80% des weltweiten Spam-Aufkommens verantwortlich gemacht werden.

Ökonomisch betrachtet scheint das Geschäft mit der UCE also äußerst effizient. Im Gegensatz zu „traditionellen“ Werbetechniken wie z.B. Postwurfsendungen ist im Falle von UCE die Anzahl der angeschriebenen Personen nahezu irrelevant – die Grenzkosten dafür tendieren gegen Null. Neben den Kosten für die Internet-Verbindung[30] entstehen lediglich Kosten

[25] Vgl. Pressemitteilung von IBM vom 02.08.2005 (online unter http://www-5.ibm.com/de/pressroom/presseinfos/2005/8/02_1.html [18.02.2006]) oder Dietrich und Pohlmann (2005)
[26] Vgl. Heise News vom 04.11.2004: „Für jede Spam-Email eine halbe Stunde ins Gefängnis“ (online unter http://www.heise.de/newsticker/meldung/52887 [18.02.2006])
[27] Vgl. Barakat (2004)
[28] online unter http://www.spamhaus.org/rokso/ [18.02.2006]
[29] ROKSO steht für *Register Of Known Spam Operations*
[30] Diese sollte bei den wenigsten Spammern so hoch sein wie die von Jeremy Jaynes.

für die Erstellung der Email – da jedoch auf aufwändiges Layout, Repro, Druck etc. verzichtet werden kann, sind auch diese Fixkosten deutlich geringer als bei „analogen“ Werbemitteln. Der wesentliche Aspekt sind jedoch die nahezu fixen Gesamtkosten. Bei kaum einem anderen Medium ist es finanziell irrelevant, ob 20 oder 20.000 potentielle Kunden erreicht werden sollen.

Wie weiter oben bereits erwähnt, ist reine Email-Werbung offenbar jedoch im Rückzug. Während der IBM-Studie[31] zufolge im Januar 2005 die Anzahl von Werbe-Emails noch 83% betrug, sank die Rate im Juni 2005 auf 67%. Zu ähnlichen Ergebnissen kommen auch Dietrich und Pohlmann (2005). Gleichermaßen nahm die Anzahl virenverseuchter Emails im selben Zeitraum um 50% zu. Auch die Anzahl zielgerichteter Phishing-Attacken[32] u.ä. steigt deutlich.

Phishing und gezielte Viren-Attacken müssen also durchaus als die Spam-Variante angesehen werden, die in näherer Zukunft deutlich an Gefährlichkeit zunimmt. Gerade Phishing-Emails sind, inklusive der meist dazugehörenden gefälschten Websites, z.T. heute bereits selbst von Experten kaum mehr von denen der echten Unternehmen zu unterscheiden.[33] Es ist also unumgänglich, neben Email-Werbung gleichermaßen auch diese Probleme zu betrachten, wenn eine sinnvolle und längerfristige Strategie zur Verhinderung des Missbrauchs des Email-Systems erarbeitet werden soll.

[31] Vgl. Pressemitteilung von IBM vom 02.08.2005 (online unter http://www-5.ibm.com/de/pressroom/presseinfos/2005/8/02_1.html [18.02.2006])

[32] Für diese gelten ähnliche ökonomische Rahmenbedingungen wie die weiter oben für UCE beschriebenen

[33] Einen Online-Test, der das verdeutlicht, bietet z.B. das Anti-Spam-Unternehmen MailFrontier unter http://german.mailfrontier.com/survey/phishing_de.jsp [18.02.2006]

3 Technische Grundlagen

Um eine Auseinandersetzung mit der Frage zu führen, wie und weswegen Spam effektiv auf einer politischen und rechtlichen Ebene begegnet werden kann, ist es unumgänglich, die grundlegende Funktionsweise des Internets im Allgemeinen sowie des Email-Systems im Besonderen zu erläutern. Da im Rahmen dieser Arbeit nicht erschöpfend hierauf eingegangen werden kann, soll für eine tiefer gehende Einführung in die Materie auf die Literaturliste, insbesondere auf Wood (1999) und Johnson (1999) verwiesen werden.

3.1 Das Internet

Das Internet, eine Kurzform von engl. *Interconnected Networks* (also etwa „miteinander verbundene Netzwerke“) ist ein weltweites Netzwerk von voneinander unabhängigen kleineren Netzwerken, so z.B. Firmen-Netzwerke, Universitäts-Netzwerke oder Netzwerke von *Internet Service Providern* (ISPs). Diese verschiedenen Netzwerke sind an so genannten Internet-Knoten (*Internet Exchanges*, IX) über extrem leistungsstarke Verbindungen, den *Backbones*, miteinander verbunden.

Seinen Ursprung hat das Internet im US-amerikanischen ARPANET, einem Forschungsnetzwerk der heutigen *Defense Advanced Research Projects Agency* (DARPA), die dem Verteidigungsministerium zugeordnet ist.[34] In Zusammenarbeit mit dem Massachusetts Institute of Technology sollte in den 1960er Jahren ein Netzwerk entworfen werden, das die Computer der für das Verteidigungsministerium arbeitenden Labore und Universitäten miteinander verbindet. Da die Verbindungen über Telefonleitungen hergestellt wurden und somit recht unsicher waren, wurde zur Vergrößerung der Ausfallsicherheit ein vollkommen dezentrales Netzwerk konzeptuiert, das in der Lage war, bei ausgefallenenen Verbindungen auf andere zurückzugreifen.

Diese Denzentralität war damals revolutionär und legte die Grundlagen des heutigen Internets. Ebenso wie im damaligen ARPANET besitzt das Internet keinerlei zentralen Rechner

[34] Nähere Informationen zur Geschichte des Internets bietet z.B. Leiner u. a. (2003), Hafner und Lyon (2003) oder auch http://de.wikipedia.org/wiki/Geschichte_des_Internets

oder Ort, an dem sämtliche Verbindungen zusammenlaufen.[35] Da es sich um ein internationales Netzwerk handelt und sämtliche Verbindungen und Basis-Dienste wie das *Domain Name System* (DNS) redundant und international verfügbar sind, stoßen nationale Gesetze im Internet oftmals an ihre Grenzen.

Da dieses Kapitel lediglich einen kurzen und notwendigen Überblick über das Grundprinzip des Internets vermitteln soll, kann auf die einzelnen Techniken, die das Internet „antreiben", nicht weiter eingegangen werden.[36] Für Informationen über die verschiedenen Dienste und Protokolle, die über das Internet vermittelt werden, sei auf die einschlägige Literatur verwiesen.

3.2 Internet-Email

Neben dem *World Wide Web* ist das Email-System einer der wichtigsten – wenn nicht sogar der wichtigste – Dienst des Internets. Im Folgenden soll die Funktionsweise des Internet-Email-Systems erläutert werden, um eine Grundlage für die in den folgenden Kapiteln beschriebenen Arbeitsweisen von Spammern sowie Techniken gegen Spam zu schaffen.

3.2.1 Das Simple Mail Transfer Protocol (SMTP)

Da, wie oben erläutert, das Internet im Grunde ein Zusammenschluss aus vielen einzelnen Netzwerken ist, werden in diesen zum Teil auch verschiedene Systeme zum Email-Versand eingesetzt. Während jedoch Protokolle wie X.400 oder proprietäre Protokolle primär in lokalen oder anderen abgeschlossenen und unabhängigen Netzwerken verwendet werden, wird der Großteil der Internet-Email über das *Simple Mail Transfer Protocol* (SMTP)[37] transportiert.

Die ursprüngliche Version dieses Übertragungs-Protokolls wurde bereits Anfang der 1980er Jahre entwickelt – zu einer Zeit also, als es nur wenige Mailserver gab und diese sich vertrauen konnten. Über die Jahre wurde das Protokoll nur wenig verändert; heute kommt vermehrt die erweiterte Version ESMTP zum Einsatz, die einige zusätzliche (und optionale) Dienste anbietet. Da jene innerhalb dieser Arbeit jedoch keine Bedeutung haben, sei an dieser Stelle nur auf die entsprechenden RFCs[38] verwiesen.

[35] Trotz der Dezentralität gibt es mittlerweile dennoch neuralgische Punkte, an denen ein ernstzunehmender Angriff auf die Struktur des Internets möglich ist. Ein großes Problem ist offenbar die physische „Verkabelung" des Netzes. So konnte Sean Gorman in seiner Dissertation bereits 2003 nachweisen, dass in vielen Fällen die Zerstörung weniger Datenleitungen zu massiven Problemen des Datenverkehrs kommen kann (vgl. hierzu auch Traufetter (2003)).

[36] Eine Ausnahme bildet natürlich das Email-System, dessen Funktionsweise im Folgenden näher erläutert wird.

[37] Die genaue Definition des Protokolls findet sich in RFC821 (1982), der zukünftig durch RFC2821 (2001) ersetzt werden soll. Eine hervorragende Beschreibung (zu allen Bereichen des Email-Systems) bietet auch Wood

```
220 mail.empfaenger.de SMTP
HELO mail.sender.de
250 mail.empfaenger.de Hello mail.sender.de [192.168.1.66]
MAIL FROM: jan@sender.de
250 OK
RCPT TO: ole@empfaenger.de
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: jan@sender.de
To: ole@empfaenger.de
Subject: Eine kurze Mail per SMTP

Hallo, Ole,

dies ist eine kurze Mail, die im Gespräch mit
dem Mailserver verschickt wurde.

Ciao, Jan...
.
250 OK
QUIT
221 mail.empfaenger.de closing connection
```

Abbildung 3.1: Beispiel-Verbindung per SMTP

SMTP ist im wahrsten Sinne des Wortes *simpel* – so erlaubt es, mit einem einfachen Terminalprogramm zu einem entsprechenden SMTP-Server eine Verbindung aufzubauen und Emails zu verschicken. Anhand einer Beispiel-Verbindung (Abbildung 3.1) soll im Folgenden die Funktionsweise des Protokolls erläutert werden.

Die roten, mit einer Zahl beginnenden Zeilen sind jeweils Meldungen des kontaktierten Servers, die blauen sind Eingaben des Clients.[39] Zuerst meldet sich der SMTP-Server mit seinem Namen sowie dem verwendeten Protokoll.[40] Mit dem Befehl `HELO`[41], der als Argument den Namen des Clients erhält, „begrüßt“ dieser nun den Server. Als Antwort sendet der Server eine entsprechende Begrüßung. An dieser Stelle ist zu beachten, dass in der ursprünglichen Form des Protokolls der als Argument von `HELO` angegebene Domainname vom Server ohne Authentifizierung akzeptiert wurde, so dass es möglich war, gefälschte Fantasienamen an-

(1999).

[38] ESMTP selbst wird in RFC1869 (1995) beschrieben. Neben diesem gibt es aber noch eine große Anzahl anderer RFCs, die sich mit Erweiterungen beschäftigen. Auf diese soll im Rahmen dieser Arbeit jedoch nicht näher eingegangen werden.

[39] Die Verwendung der Begriffe „Client“ und „Server“ in diesem Zusammenhang kann zu Missverständnissen führen, da auch Mailserver untereinander auf diese Weise kommunizieren. Somit kann auch ein Mailserver ein „Client“ sein. Daher wird im Folgenden der Begriff „Client“ für den jeweils sendenden Kommunikationspartner benutzt, „Server“ dagegen für den empfangenden Partner.

[40] An dieser Stelle kann entsprechend statt *SMTP* auch *ESTMP* für die erweiterte Version stehen.

[41] Bei ESMTP-Servern kann auch `EHLO` verwendet werden. In diesem Fall gibt der Server als Antwort zusätzlich die von ihm unterstützten ESMTP-Kommandos zurück.

zugeben. Heutzutage ignorieren die meisten Mailserver diesen Domainnamen und ermitteln ihn stattdessen z.B. über die IP-Adresse des Clients.[42]

Nach der Begrüßung gibt der Client die Absender-Adresse (`MAIL FROM:`) sowie die Empfänger (`RCPT TO:`) der folgenden Email an. Um mehrere Empfänger zu erreichen, müssen lediglich mehrere `RCPT TO:`'s angegeben werden. Diese beiden Angaben bilden den *Envelope*, also den „Umschlag" der Email.

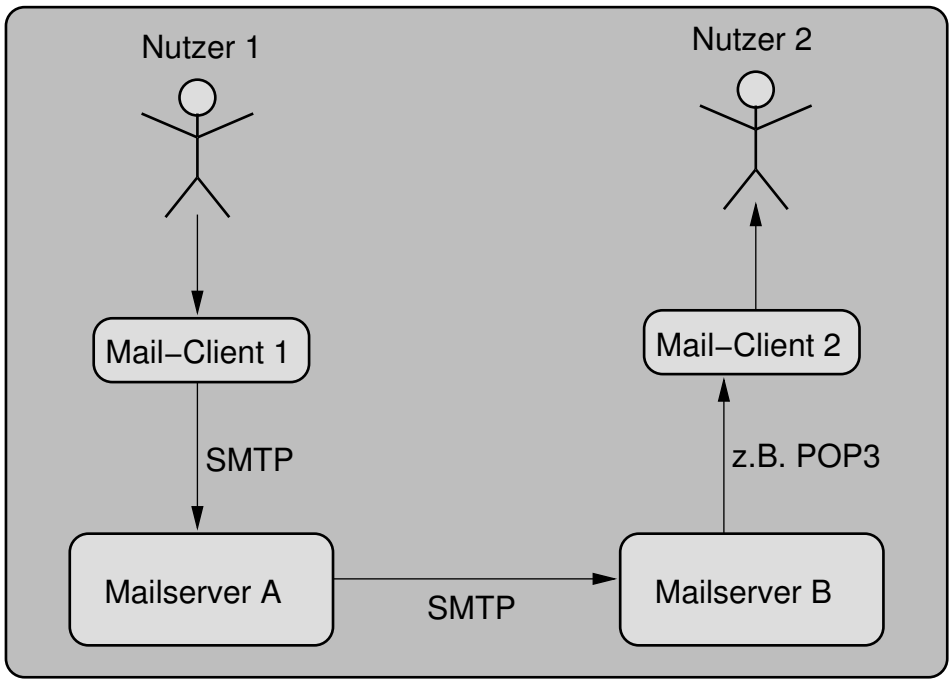

Abbildung 3.2: Symbolische Darstellung des Email-Systems

Wenn die Angabe aller Empfänger abgeschlossen ist, wird mit dem Befehl `DATA` der Beginn der eigentlichen Email eingeleitet. Hier steht neben üblichen und weniger üblichen Header-Zeilen[43] die Nachricht (der so genannte *Body*), die der Absender übermitteln will. Nachdem der Body mit einem einzelnen Punkt in einer Zeile abgeschlossen wurde, wird die Email vom Mailserver versendet. Ein `QUIT` beendet die Verbindung zum Server.

Um in den folgenden Kapiteln die verschiedenen Ansatzpunkte von Spammern und Anti-Spammern deutlich zu machen, zeigt Abbildung 3.2 (vereinfacht) den Weg, den eine Email vom Absender zum Empfänger nimmt. Im Allgemeinen schreibt der Absender mit einem Mailclient die Email und schickt sie an den Mailserver seines Providers. Von dort wird sie –

[42] Genauer gesagt, werden hierfür die Kopfzeilen der einzelnen IP-Pakete herangezogen. Eine Fälschung der dort angegebenen IP-Adresse ist relativ aufwändig, so dass davon ausgegangen werden kann, dass diese stimmt. Inwiefern diese Korrektheit von Wert ist, wird im Folgenden geklärt.

[43] Diese werden in Kapitel 3.2.2 beschrieben.

u.U. über verschiedene andere Mailserver – an den Mailserver des Empfängers verschickt, dessen Mailclient die Email dann z.B. mittels des POP3-Protokolls vom Mailserver abholt.

In den Anfangstagen der Internet-Email waren – entsprechend dem Standard – sämtliche Server so genannte *Open Relays*[44], die es ermöglichten, dass jede beliebige Person über sie Emails an eine beliebige andere Person verschicken konnte. SMTP unterstützt jedoch keinerlei Authentifizierungsmechanismen, was dazu führt, dass nahezu jede Angabe im „Gespräch“ mit dem SMTP-Server gefälscht werden kann – bis auf die IP-Adresse des Clients sowie die Empfänger-Adressen. Wie Spammer ersteres umgehen, wird in Kapitel 3.2.2 erläutert; letzteres stellt offensichtlich kein Problem für den Spammer dar. Aus diesen Gründen sind *Open Relays* größtenteils verschwunden und Mailserver akzeptieren lediglich Emails von oder an eigene Kunden. Trotzdem gibt es weiterhin *Open Relays*, und aufgrund der fehlenden Authentifizierungs-Möglichkeiten durch SMTP werden diese weiterhin missbraucht.

3.2.2 Envelope und Email-Header

Der *Envelope*, also der Umschlag der Email, wird während der SMTP-Verbindung[45] gebildet. Er besteht lediglich aus einem Absender sowie den Empfängern der Email. Allerdings beinhaltet SMTP keinerlei Authentifizierungs-Maßnahmen, so dass der Absender leicht gefälscht werden kann. Diese beiden Angaben sind die einzigen für den Transport der Email relevanten Daten – die Empfänger aus offensichtlichen Gründen, der Absender dagegen, da im Falle von Fehlern u.U. eine entsprechende Meldung an diesen geschickt wird.[46]

Zu beachten ist, dass die Daten des Umschlags im Normalfall nicht durch ein Email-Programm dargestellt werden. Die hier zumeist angezeigten Absender und Empfänger sind, genau wie die Betreffzeile, Teil des *Headers*[47], also des Kopfes der Email. Dieser ist, wie im Beispiel im vorangegangenen Kapitel zu erkennen, Teil der Nutzdaten der Email und kann durch den Absender beliebig gesetzt werden. Die Korrektheit dieser Daten ist also keinesfalls sichergestellt.

Neben den genannten drei Einträgen enthält der Header einer Email u.a.[48] auch so bezeichnete `Received`-Zeilen. Bei diesen handelt es sich im Grunde um „Poststempel“, die von jedem Mailserver, den die Email passiert, gesetzt werden und einen Zeitstempel sowie den empfangenden und den sendenden Server beinhalten. Mit Hilfe dieser Stempel kann der Weg einer Email vom Sender zum Empfänger nachvollzogen werden. Die Korrektheit sämtlicher

[44] Vgl. Kapitel 3.3.2
[45] Vgl. Abbildung 3.1
[46] Diese erreicht natürlich aus bereits genannten Gründen nicht zwangsläufig den echten Absender.
[47] Abbildung 3.3 zeigt einen Beispiel-Header.
[48] Der Header enthält noch deutlich mehr Daten, auf die hier nicht weiter eingegangen werden soll. Detailliertere Informationen bietet z.B. Wood (1999).

```
Received: from mail2.empfaenger.de (postfix@mail2.empfaenger.de
    [192.168.17.22])
    by mail.empfaenger.de (8.9.3p2/8.9.3) with ESMTP id LAA12571
    for <ole@empfaenger.de>; Wed, 20 Jul 2005 11:36:24 +0200 (MEST)
Received: from mail2.sender.net (pop.sender.net [192.168.3.112])
    by mail2.empfaenger.de (Postfix) with SMTP
    for <ole@empfaenger.de>; Wed, 20 Jul 2005 11:36:23 +0200 (MEST)
Received: from mail.sender.de (HELO [192.168.1.66])
    [192.168.1.66]
    by mail2.sender.net (Postfix) with SMTP; 20 Jul 2005 11:36:23 +0200
Message-ID: <42DE1B36.5080708@sender.de>
Date: Wed, 20 Jul 2005 11:36:54 +0200
From: jan@sender.de
User-Agent: Mozilla Thunderbird 1.0.2 (Windows/20050317)
X-Accept-Language: de-DE, de, en-us, en
MIME-Version: 1.0
To: ole@empfaenger.de
Subject: Test-Email
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 8bit

Hallo, Ole,
dies ist mal wieder eine Test-Email, um Mail-Header zu erläutern.
Gruß Jan
```

Abbildung 3.3: Beispiel-Header einer Email

Einträge ist jedoch nicht zwangsläufig gewährleistet. Während die einzelnen Mailserver, die die Email passiert, korrekte Zeitstempel setzen, steht es dem böswilligen Absender frei, bereits beim Versenden der Email in den Header falsche `Received`-Zeilen einzufügen. Stellt er sich hierbei geschickt an, kann ohne Mitarbeit der einzelnen Mailserver-Administratoren, deren Rechner die Email passiert, nicht erkannt werden, an welchem Server die Email wirklich eingeliefert wurde und welche Einträge lediglich gefälscht wurden.

3.2.3 Bounces und Fehlermeldungen

Sollte es zu Problemen bei der Zustellung einer Email kommen, gibt es zwei Varianten, wie der entsprechende Mailserver reagieren kann. Wird bereits während des SMTP-Dialoges zwischen Client und Server ein Fehler bemerkt, so meldet der Server diesen direkt. Eine Fehlermeldung kann der Server in jedem Schritt des Dialoges[49] abgeben – so z.B., falls der Empfänger nicht existiert oder falls der Absender nicht berechtigt ist, über den Server Emails zu verschicken.

Sollte der Mailserver erst später bemerkt haben, dass er die entsprechende Email nicht zustellen kann, generiert er eine *Delivery Status Notification* (DNS[50]) – einen so genannten *bounce*.[51] Eine solche Nachricht wird an die im Umschlag angegebene Adresse geschickt und enthält zumeist Informationen, die es dem ursprünglichen Absender ermöglichen, den Grund

[49] Vgl. Abbildung 3.1
[50] Nicht zu verwechseln mit dem *Domain Name System*, ebenfalls DNS abgekürzt.
[51] Näheres hierzu findet sich u.a. in RFC3461 (2003).

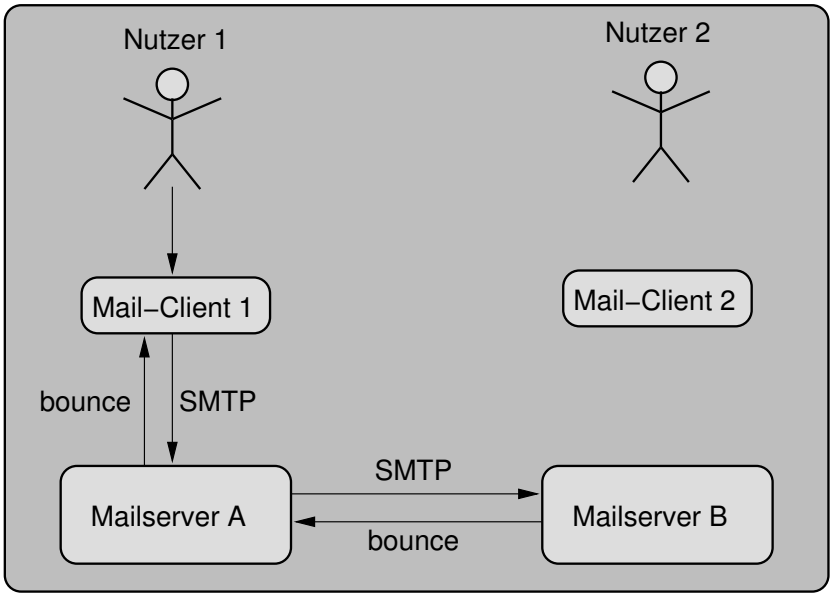

Abbildung 3.4: Symbolische Darstellung eines Email-Bounces

für die fehlgeschlagene Zustellung zu erkennen. Abbildung 3.4 zeigt symbolisch den Weg der ursprünglichen Email sowie der bounce-Nachricht.

Dieses eigentlich sinnvolle Werkzeug ist im Zuge der Viren- und Spam-Epidemien zunehmend in Verruf geraten. Da hierbei häufig Email-Adressen von unbeteiligten Dritten verwendet werden, werden diese häufig von einer großen Anzahl der entsprechenden bounces getroffen.

3.3 Spam-Versand

Im Laufe der Jahre, in denen Spammer bereits aktiv sind, wurden verschiedene Techniken angewandt, um Spam zu versenden. Die Spammer befinden sich dabei in einem fortdauernden Wettlauf mit Anti-Spam-Aktivisten, die versuchen, die Schlupflöcher, die die Spammer nutzen, zu schließen. Aus diesem Grund kann diese Arbeit nur den bisherigen und aktuellen Stand der Technik darstellen. Welche Maßnahmen Spammer ergreifen, wenn (und falls) die hier aufgeführten Varianten nicht mehr funktionieren, kann aus naheliegenden Gründen nicht erörtert werden.

Um die verschiedenen Möglichkeiten der Spammer zu verdeutlichen, wird Abbildung 3.2 Schritt für Schritt um eben diese ergänzt, so dass im Abschluss ein Überblick über aktuelle Spamming-Varianten erzeugt wird.

3.3.1 Spam-Server

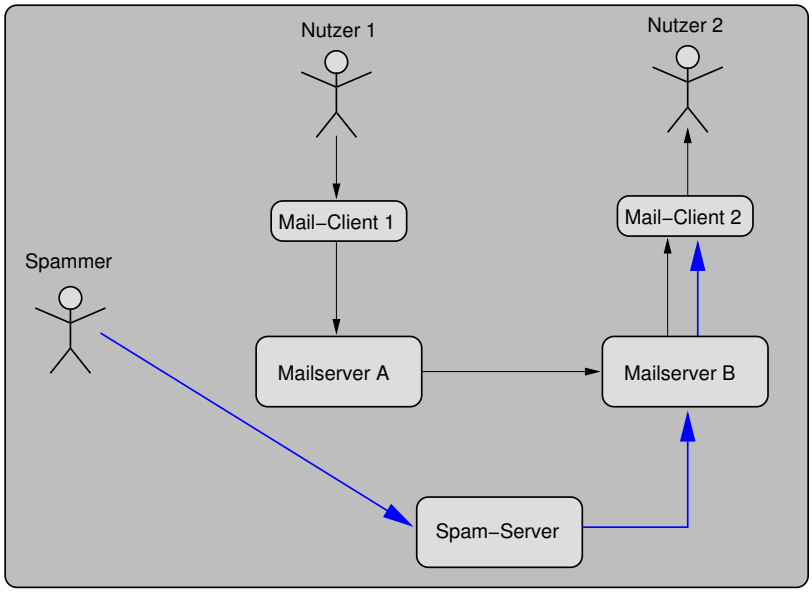

Abbildung 3.5: Verwendung eines eigenen Spam-Servers

Die naheliegendste und in der 1990er Jahren, also zu Beginn der Spam-Epidemie, meistgenutzte Variante bestand darin, den Spam über eigene Mailserver zu verschicken. Durch Filtertechniken wie *Blacklisting*[52], aber auch aufgrund der im Vergleich zu anderen Techniken hohen Kosten verwenden Spammer heute eher selten eigene Mailserver.

3.3.2 Open Relays

Wie bereits in Abschnitt 3.2 beschrieben, war es bis in die 1990er Jahre gängige Praxis, SMTP-Server als so genannte *Open Relays* zu konfigurieren. Über solche Server kann eine beliebige Person Emails an eine andere beliebige Person verschicken, ohne Kunde des Mailserver-Betreibers zu sein. Dies diente vor allem der Redundanz, so dass Nutzer bei Ausfall des eigenen Mail-Servers Emails auch über andere Server verschicken konnten – es bietet Spammern aber natürlich auch offensichtliche Missbrauchsmöglichkeiten.

Heutzutage gibt es aus diesem Grund so gut wie keine (absichtlichen) Open Relays mehr. Seit Mitte der 1990er Jahre ist die Konfiguration von Mail-Servern als Open Relay von 90% auf unter 1% gesunken.[53] Einer der wenigen, die weiterhin den Nutzen von Open Relay-Konfigurationen propagieren, ist der amerikanische Bürgerrechtler John Gilmore, einer der Gründer der *Electronic Frontier Foundation*. Gleichermaßen akzeptiert aber auch er, dass viele

[52] Vgl. Kapitel 3.4.1
[53] Vgl. *Wikipedia* unter http://en.wikipedia.org/wiki/Open_mail_relay [18.02.2006]

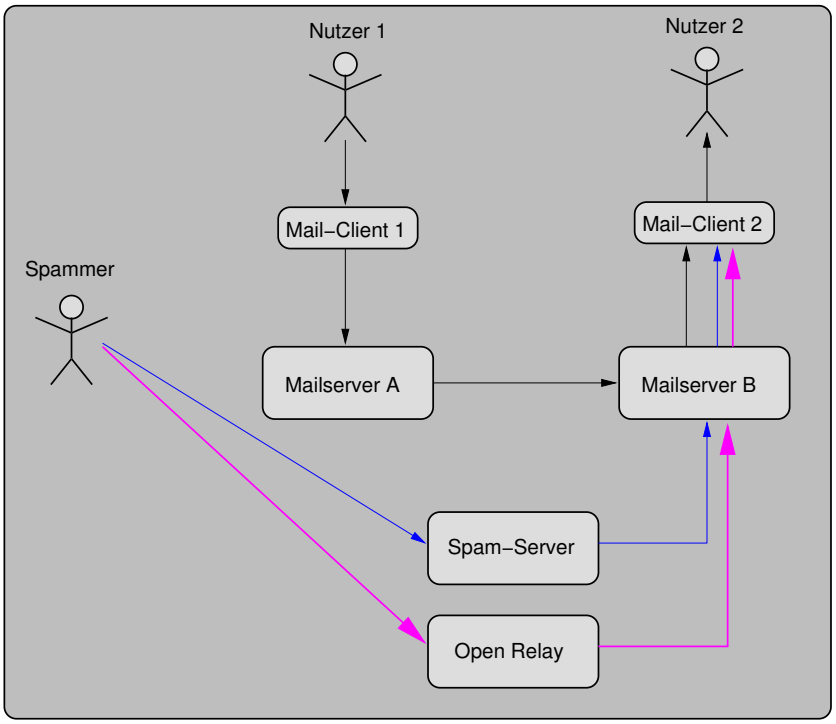

Abbildung 3.6: Verwendung eines Open Relays

Mailprovider Emails von seinem Server als Spam einstufen. Der weitaus größere Teil der aktuell vorhandenen Open Relays besteht aber aus fehlkonfigurierten Mail-Servern, deren Missbrauch dann ebenso meist relativ schnell dazu führt, dass sie auf gängigen schwarzen Listen[54] auftauchen und üblicherweise von Spamfiltern als Spam klassifiziert werden.

Um trotz SMTP, dass per se keine Authentifizierungs-Mechanismen bietet, legitime Benutzer von anderen zu trennen, werden verschiedene Mechanismen verwendet. Größtenteils erlauben Mailserver nur noch, Emails zu verschicken, die entweder an einen Benutzer des Mail-Server-Betreibers gerichtet sind oder die von einem solchen stammen. Ersteres lässt sich leicht an der Empfänger-Adresse überprüfen. Letzteres dagegen ist aufgrund der in Kapitel 3.2 genannten Einschränkungen des Protokolls nicht ohne weiteres möglich. Eher selten wird hierzu heutzutage die Ergänzung *SMTP-after-POP* genutzt, bei der der Nutzer, bevor er eigene Emails verschicken kann, sein Postfach über das POP3-Protokoll abrufen muss. Über einen Vergleich der IP-Adressen erlaubt es der Mail-Server dann für einen bestimmten Zeitraum, z.B. 10 Minuten, Emails zu verschicken. Weitaus häufiger dagegen wird *SMTP-Auth* (RFC2554 1999) genutzt, das eine Authentifizierung des Nutzers über ein Passwort erlaubt, bevor dieser Emails verschicken kann.

[54] Bekannte Listen dieser Art bieten z.B. *Spamhaus* (http://www.spamhaus.org/sbl/index.lasso) oder die *Open Relay Database* (http://www.ordb.org/).

3.3.3 Open Proxies

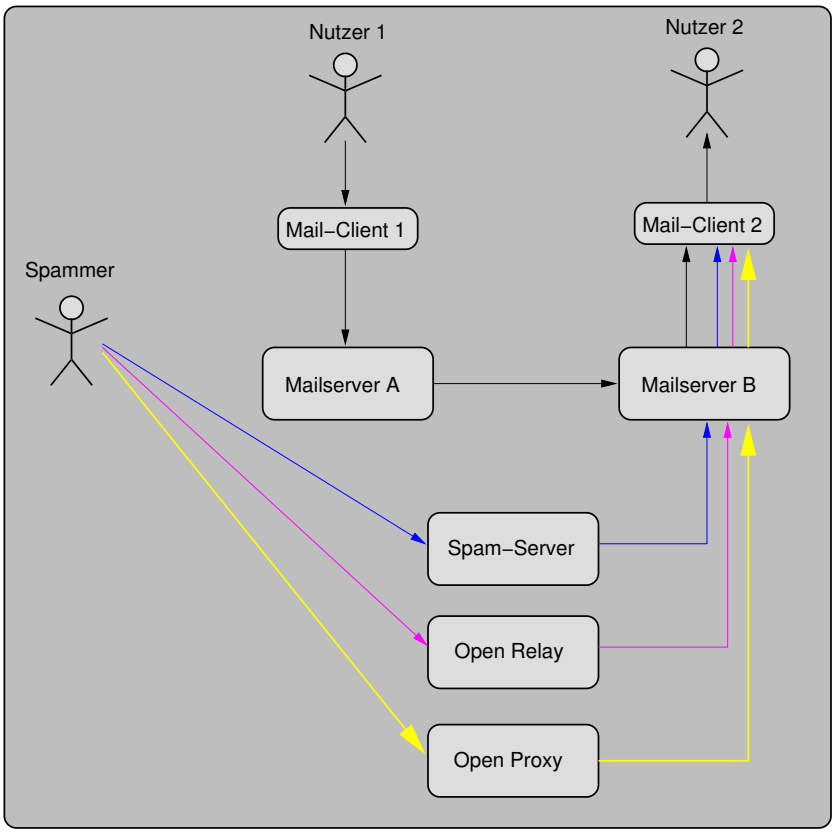

Abbildung 3.7: Verwendung eines Open Proxies

Proxy-Server, oder kurz *Proxies*, werden zumeist verwendet, um z.B. den kompletten www-, aber auch anderen Datenverkehr eines Firmen-Netzwerks über einen einzigen Server zu leiten. Einerseits dient dies dazu, um das durch eine Firewall geschützte Netzwerk nur für einen einzigen , den Proxy, und nicht für alle Rechner des Netzwerkes zu öffnen. Andererseits dienen Proxies aber auch häufig dazu, Datenverkehr zwischenzuspeichern, um z.B. bei erneutem Abruf einer Website nicht erneut kostenintensiv Daten über die Internet-Verbindung, z.B. eine Standleitung, abrufen zu müssen.

Fehlkonfigurationen solcher Proxies können dazu führen, dass diese nicht nur aus dem entsprechenden lokalen Netzwerk erreicht, sondern ebenso „aus dem Internet“ genutzt werden können. Dies nutzen Spammer aus, um sie zum Versand ihrer Werbung zu missbrauchen. Der große Vorteil dieser Variante ist, dass die so versendeten Emails in den `Received:`-Zeilen nur den Proxy, nicht aber die IP-Adresse des Spammers selbst enthalten. Somit kann der Spammer nicht über den Email-Header, sondern nur über die Log-Dateien des Proxies herausgefunden werden. Inwieweit solche Dateien aber auf einem derart konfigurierten Server existieren bzw.

ob man Zugriff auf sie erhält, ist in den meisten Fällen mehr als ungewiss. Um sich noch weiter abzusichern, können Spammer auch ganze Proxy-Ketten nutzen, so dass eine Entdeckung nahezu unmöglich ist.

3.3.4 Zombie-PCs und Botnets

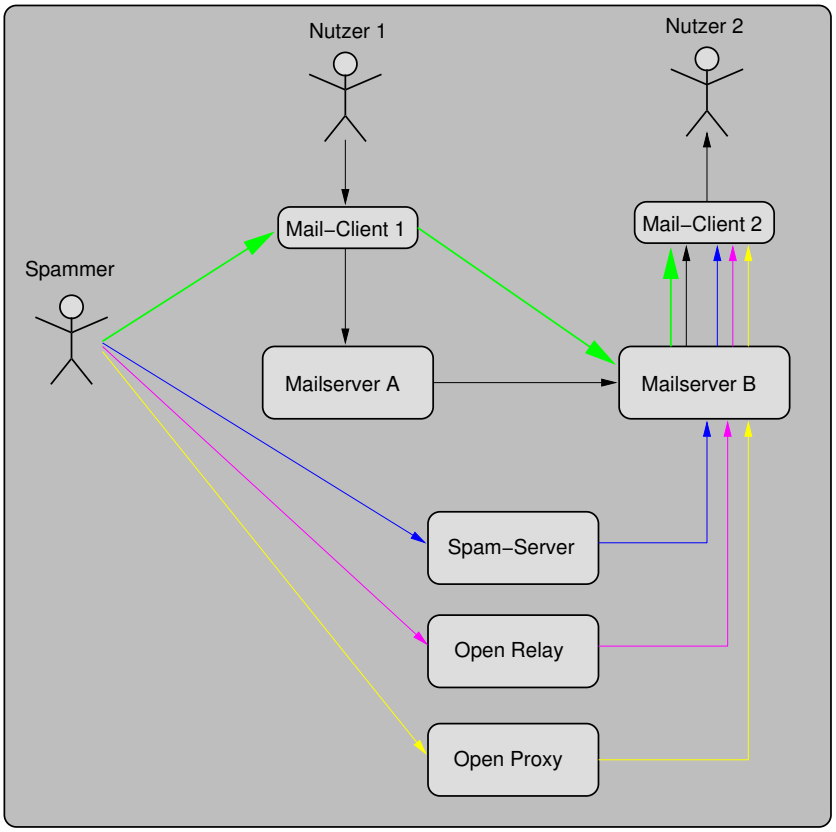

Abbildung 3.8: Verwendung eines Zombie-PCs aus einem Botnet

Aufgrund der beschriebenen großen Vorteile sind Open Proxies äußerst beliebt bei Spammern. Da es aber relativ aufwändig ist, immer neue Open Proxies zu auszumachen, sind Spammer (in Zusammenarbeit mit Virenprogrammierern) dazu übergegangen, eigene Open Proxies zu installieren oder installieren zu lassen. Diese werden über Würmer oder als Trojaner[55] auf PCs verteilt. Die einzelnen Zombie-PCs werden zu Netzwerken, so genannten *Botnets*, zusammengeschlossen, die über den *Internet Relay Chat* (IRC) von den Programmierern kontrolliert werden. Dem *Honeynet Project*[56] zufolge muss davon ausgegangen werden, dass es bis zu einer Million Zombie-PCs gibt. Bei Untersuchungen entdeckten die Forscher Bot-

[55] Vgl. Kapitel 2.2.3
[56] online unter http://www.honeynet.org/

nets, die aus bis zu 50.000 Rechnern bestanden;[57] es gibt jedoch auch Berichte über Botnets mit bis zu 400.000 Rechnern.[58]

Weltweit immer weiter verbreitete Breitband-Verbindungen und leistungsstarke Rechner erlauben den „Besitzern" solcher Botnets, unbemerkt und schwer entdeckbar ihren Machenschaften nachzugehen. Mittlerweile wird davon ausgegangen, dass die Kontrolle über solche Botnets immer weiter in den Bereich der organisierten Kriminalität abwandert, die ihre Netze u.a. dafür nutzt, zahlungskräftige Unternehmen mit dDoS-Angriffen auf deren Website zu erpressen.[59] Allerdings scheint auch die Vermietung solcher Botnets an Spammer immer weiter voranzuschreiten.[60]

3.3.5 Mailserver über Zombie-PCs

Während von den meisten Zombie-PCs die Emails direkt am Mailserver des Empfängers abgeliefert werden, nutzen sie offenbar immer häufiger auch die Mailserver der ISPs, über die der Zombie-PC seine Internetverbindung herstellt.[61] Auf diese Weise werden Echtzeit-Blacklists[62] – oder das Email-System selbst – nahezu unbrauchbar, da in vielen Fällen die Mailserver großer ISPs – über die in diesem Falle der Spam verschickt wird – in Blacklists aufgenommen werden müssten.

3.4 Technische Maßnahmen gegen Spam

In diesem Kapitel soll eine Übersicht über technische Maßnahmen gegeben werden, die an verschiedensten Stellen ansetzen, um Spam zu blockieren bzw. zu verhindern. Da der Hauptaspekt dieser Arbeit jedoch bei rechtlichen und politischen Maßnahmen liegt, handelt es sich lediglich um einen kurzen Überblick. Für tiefergehende Informationen sei auf die einschlägige Literatur verwiesen. Einen sehr guten Überblick bietet BSI (2005).

3.4.1 Filterung

Eine naheliegende und – je nach Verfahren – relativ leicht umsetzbare Möglichkeit, Postfächer von Spam zu befreien, ist das Filtern der Emails nach Spam und Ham, zumeist umgesetzt direkt in der Email-Software des Nutzers oder auf dessen Mailserver.

[57] Vgl. Honeynet (2005)
[58] Vgl. MessageLabs (2006, S.10)
[59] Vgl. Brauch (2004)
[60] Vgl. c't (2004) oder Pößneck (2005)
[61] Vgl. http://www.spamhaus.org/news.lasso?article=156 [18.02.2006]
[62] Vgl. Kapitel 3.4.1

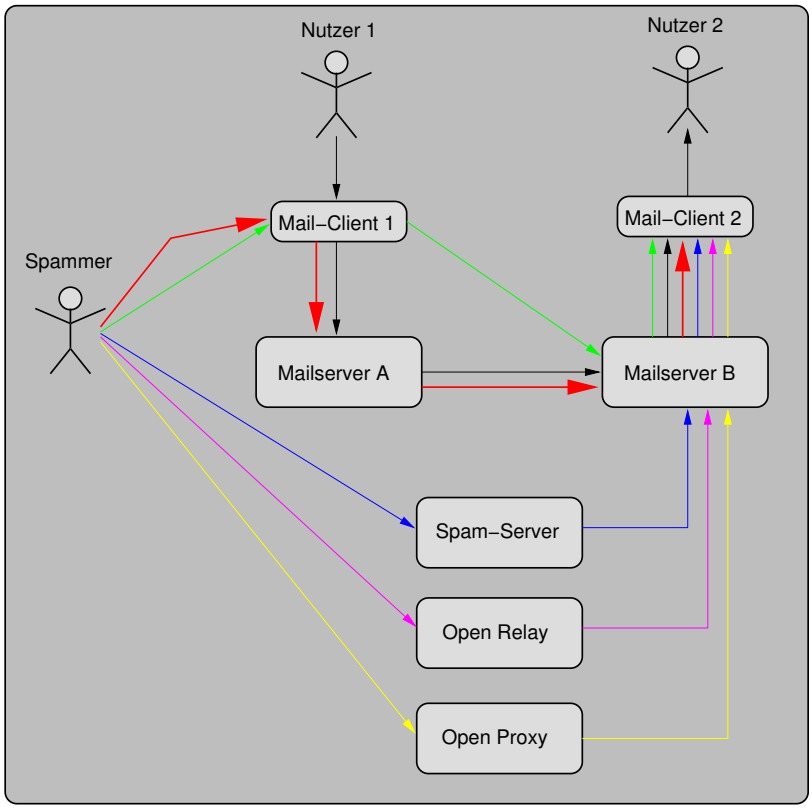

Abbildung 3.9: Verwendung eines Mailservers über einen Zombie-PC

Die einfachste Variante ist naheliegenderweise die *manuelle Filterung*.[63] Das manuelle Filtern durch Administratoren auf dem Mailserver ist datenschutzrechtlich bedenklich und sollte ohne schriftliche Erlaubnis der Betroffenen nicht eingesetzt werden. Zumeist ist diese Variante die letzte in einer Kette von Anti-Spam-Maßnahmen und wird durch den Nutzer selbst durchgeführt.

Eine grundlegende Form der Automatisierung bietet der Einsatz von manuell geführten so genannten *White-* oder *Blacklists*. Diese beinhalten z.B. IP-Adressen, Email-Adressen[64] oder Domainnamen. Whitelists beinhalten Datensätze von legitimen Absendern;[65] Blacklists dagegen enthalten Datensätze, von denen aus bereits einmal Spam gesendet wurde. White- und Blacklists können sowohl auf dem Mailserver als auch in der Email-Software eines Nutzers eingesetzt werden. Es ist zu beachten, dass eine ständige Aktualisierung für den effektiven Einsatz notwendig ist.

[63] Selbst bei anderen eingesetzten Verfahren ist ein manuelles Filtern nahezu immer notwendig, da kein Verfahren (inklusive diesem) perfekt arbeitet.

[64] Da mittlerweile nahezu sämtliche Spammer die Absender-Email-Adressen fälschen, ist eine Blacklist auf dieser Basis heute nicht mehr sinnvoll.

[65] Sie sind auch häufig bei Verwendung anderer Verfahren notwendig, um so genannten *false positives*, also fälschlich als Spam erkannte Emails, zu verhindern.

Zumeist auf Mailservern werden so genannte *DNS-basierte Blacklists* (DNSBLs) eingesetzt. Verschiedene solcher Listen werden durch diverse Unternehmen und Organisationen geführt und erlauben es dem Anwender, über eine bestimmte DNS-Abfrage zu ermitteln, ob eine in der Email vorhandene IP-Adresse schon einmal von Spammern missbraucht wurde.[66] DNSBLs sind, je nach Betreiber, mehr oder weniger effizient. Es ist zu beachten, dass sie durchaus unzuverlässig sein können, indem sie IP-Adressen Unschuldiger enthalten. Des Weiteren gilt die Verwendung solcher Listen z.Z. als juristisch zumindest bedenklich, da IP-Adressen i.A. als personenbezogene Daten gelten und somit nicht grundlos gespeichert werden dürfen. DNSBLs werden zumeist auf Mailservern eingesetzt, da sie eine ständige Internetverbindung benötigen.

Eine Variante der DNSBLs sind die *Right Hand Side Blacklists* (RHSBLs). Diese beinhalten keine IP-Adressen, sondern die Domain des Absenders – also die rechte Seite der Email-Adresse. Die Verwendung von RHSBLs ist mittlerweile nur noch sinnvoll, wenn eine Absender-Authentifizierung[67] stattfindet oder wenn sie lediglich bekannte Spammer-Domains beinhaltet, da ein Großteil der von Spammern verwendeten Email-Adressen (und somit auch -Domains) gefälscht ist.

Ebenfalls eine Variante von DNSBLs sind *URI-DNS-Blacklists* (URIDNSBLs). Sie beinhalten die IP-Adressen von Web- oder DNS-Servern, die von Spammer verwendet werden. Da die Herkunft einer Email-Adresse wesentlich leichter gefälscht werden kann als der Ort der beworbenen Website, werden bei diesem Verfahren die in einer Email vorkommenden URLs auf ihr Vorkommen in der URIDNSBL geprüft. Bei diesem Verfahren ist zu beachten, dass es zu Problemen z.B. mit Mailinglisten oder Freemail-Anbietern kommen kann, die bei jeder Email eine URL in der Fußnote ergänzen. Sowohl RHSBLs als auch URIDNSBLs werden wie auch DNSBLs primär auf Mailservern eingesetzt, da zur ständigen Aktualisierung eine dauerhafte Internetverbindung notwendig ist.

Ein wesentliches Merkmal von Spam ist das tausendfache Auftreten identischer oder nahezu identischer Emails. Diese Tatsache kann dazu verwendet werden, für eine neue Spam-Nachricht eine *Prüfsumme* zu erstellen, die aus body und header gebildet wird. Sollten weitere Emails dieselbe Prüfsumme ergeben, handelt es sich definitv um Spam. Dieses Verfahren wird durch Spammer umgangen, indem automatisiert Kleinigkeiten in jeder einzelnen Email verändert werden, so dass sich verschiedene Prüfsummen ergeben. Allerdings hat sich hiergegen mittlerweile der Einsatz so genannter *unscharfer Prüfsummen* bewährt, die auch bei leicht veränderten Emails funktionieren. Ebenso wie bei den oben genannten Listen gibt es verschiedene Anbieter solcher Prüfsummen-Listen. Da eine dauerhafte Internetverbindung notwendig ist, wird dieses Verfahren ebenfalls primär auf Mailservern eingesetzt.

[66] Klassische „Opfer“ solcher Listen sind z.B. offene Relays (vgl. Kapitel 3.3.2)
[67] Vgl. Kapitel 3.4.2

Um Spam schon während des *SMTP-Dialoges*, also vor Übertragung der eigentlichen Email zu erkennen, läßt sich die Absender-Adresse verwenden. Davon ausgehend, dass einige Spam-Emails gefälschte[68] Email-Adressen verwenden, kann die im SMTP-Dialog[69] angegebene Email-Adresse (bzw. die hier angebenene Domain) per DNS-Abfrage auf Existenz überprüft werden. Sollte die Domain nicht existieren, ist die Absender-Adresse sicher gefälscht – die Email kann abgewiesen werden. Alternativ (und etwas aufwändiger) kann auch die Echtheit der kompletten Email-Adresse überprüft werden. Hierzu wird parallel zum eigentlichen SMTP-Dialog ein weiterer in Gegenrichtung durch den empfangenden Mailserver initiiert, in dem vorgegeben wird, ebenfalls eine Email senden zu wollen. Ist der Mailserver des potentiellen Spam-Versenders nicht erreichbar oder kennt den ursprünglichen Absender nicht, so steigt die Möglichkeit, dass es sich bei der ursprünglichen Email um Spam handelt. Diese Variante bietet jedoch keine echte Sicherheit: Ebenso kann die Gegenstelle aus verschiedenen Gründen nicht erreichbar sein oder sendet erst später eine bounce message.

Neben den bereits erwähnten Filterungstechniken kann natürlich auch der Inhalt einer Email analysiert werden, um Spam zu erkennen. Bei der *Inhaltsanalyse* unterscheidet man *heuristische* und *statistische* Verfahren. Heuristische Verfahren benutzen ein festes Regelwerk, über das der body und der header einer Email geprüft werden. So können beispielsweise Betreffzeilen wie „Viagra“ o.ä. leicht erkannt werden. Wenn eine festzulegende Anzahl von Regeln auf Spam hindeutet, kann eine Email relativ sicher als Spam klassifiziert werden. Ebenso wie bei White- und Blacklists ist es auch hier notwendig, regelmäßig (in diesem Fall das Regelwerk) zu aktualisieren. Heuristische Verfahren werden zumeist auf Mailservern eingesetzt.

Statistische Verfahren nutzen fast immer das Prinzip der *naiven Bayes-Klassifizierung*. Hierbei werden sämtliche Zeichenketten einer Email auf ihre bisherige Signifikanz für Spam oder Ham untersucht. Als Ergebnis ergibt sich einer Wahrscheinlichkeit, ob es sich bei der aktuellen Email um Spam handelt. Um eine ausreichende Grundlage zur Bestimmung der Wahrscheinlichkeiten aufzubauen, muss ein solcher Filter mit einer möglichst großen Anzahl an Spam- und Ham-Emails trainiert werden. Ebenso muss er im Gebrauch weiterhin trainiert werden, um neue Muster zu erkennen. Da false positives nicht unwahrscheinlich sind und das Training mit Ham-Emails u.U. rechtlich bedenklich ist, werden statistische Filter selten auf Mailservern eingesetzt. Sinnvoller ist der Einsatz direkt in der Mail-Software der Nutzer als vorletztes Glied einer Filterkette direkt vor der manuellen Durchsicht.

Im Gegensatz zur reinen Filterung, die lediglich eine Markierung von Spam-Emails oder ein Aussortieren in einen gesonderten Ordner beinhaltet, wird beim *Blocking* die entsprechende Email direkt vom Mailserver abgewiesen. Dieses Verfahren wird oftmals im Falle von Viren-Emails, die zumeist eindeutig erkannt werden können, eingesetzt, um zu verhindern,

[68] In diesem Fall: nicht existente
[69] Vgl. Kapitel 3.2

dass ein Virus überhaupt in das Netzwerk eindringt. Ebenfalls können Emails u.U. schon auf dem ausgehenden Mailserver blockiert werden, so dass eine Belastung weiterer Server effektiv verhindert wird. In jedem Fall muss der Absender jedoch darauf aufmerksam gemacht werden, dass seine Email abgewiesen wurde.

Zu beachten bei sämtlichen in diesem Abschnitt aufgeführten Verfahren ist die Tatsache, dass es sich in jedem Fall nur um eine Symptom-Bekämpfung handelt. Die Kosten, die Spam auf dem Weg zu einem Postfach verursacht, werden hiervon nicht berührt. Trotzdem ist der Einsatz einer Kette von Filtern natürlich empfehlenswert, um zumindst den einzelnen Benutzer möglichst effektiv vor Spam zu schützen.

3.4.2 Authentifizierung

Neben der Symptom-Bekämpfung ist es natürlich auch sinnvoll zu versuchen, bereits das Verschicken von Spam zu erschweren oder zu verhindern. Eine Möglichkeit hierzu sind Versuche, an verschiedenen Stellen des Email-Systems Authentifizierungs-Maßnahmen einzusetzen.

Eine konsequente kryptographische Signierung der eigenen Emails mittels bekannter Verfahren wie *S/MIME* (RFC3850 2004; RFC3851 2004) oder *PGP* (RFC2440 1998) verhindert zwar keine Email-Werbung, schützt aber vor Joe Jobs und Phishing-Attacken.[70] Gerade letzteres wird für Unternehmen aktuellen Studien zufolge immer wichtiger, da derlei Attacken deutlich zunehmen. Ebenso ist heutzutage eine signierte oder verschlüsselte Email ein deutliches Zeichen, dass es sich höchstwahrscheinlich nicht um Spam handelt – wenn auch nur aufgrund der geringen Verbreitung dieser Verfahren.

Alternativ zur Signierung durch den Nutzer existieren Verfahren, um Emails durch den Mailserver signieren zu lassen. Hierzu zählt u.a. das *DomainKeys*-Verfahren, das u.a. von Google Mail und Yahoo eingesetzt wird.[71] In diesem Verfahren bildet der Mailserver aus seinem Zertifikat und der Email eine Signatur, die er in einem zusätzlichen Headerfeld der Email angibt. Der empfangende Mailserver kann nun mittels DNS das Zertifikat des sendenden Mailservers abrufen und die Gültigkeit der entsprechenden Signatur überprüfen. Da es sich um ein relativ neues Verfahren handelt, gibt es noch keine zuverlässigen Aussagen zur Sicherheit.

Mittels DomainKeys und ähnlichen Verfahren kann lediglich überprüft werden, ob eine Email tatsächlich von dem Mailserver stammt, der sie signiert hat. Weiter gehen Verfahren wie *Sender Policy Framework* (SPF) und *Caller ID*, die 2004 zum *Sender ID*-Verfahren vereinigt wurden. Durch zusätzliche Einträge im DNS kann festgelegt werden, für welche Domains

[70] Vgl. zu beidem Kapitel 2.2.4

[71] Vgl. Heise News vom 02.06.2005: „Gemeinsamer Vorschlag von Yahoo und Cisco zur Spam-Bekämpfung“ (online unter http://www.heise.de/newsticker/meldung/60185 [20.20.2006])

ein Mailserver Emails verschicken darf. Auf diesem Wege kann ein empfangender Mailserver nun beurteilen, ob der Mailserver des Absenders für die angegebene Domain tatsächlich zuständig ist. Das Verfahren schützt zwar vor falschen Absender-Adressen, hindert Spammer jedoch nicht daran, eine große Anzahl an „Wegwerf-Domains“ zu registrieren und passende DNS-Einträge zu erstellen. Eine Arbeitsgruppe der *Internet Engineering Task Force* (IETF) scheiterte bei der Standardisierung eines solchen Verfahrens u.a. aufgrund unklarer Patentansprüche.

3.4.3 Vergrößerung des Aufwand oder der Kosten

Einige Verfahren versuchen, durch die Vergrößerung des Aufwands oder der Kosten, eine Email zu versenden, die Vorteile des Spammens gegenüber herkömmlichen Werbemaßnahmen[72] zu verringern.

Token-basierte Verfahren erwarten bei ankommenden Emails bestimmete Zeichenketten in header, Empfänger-Adresse oder body. Sollte eine Email ein solches Token nicht beinhalten, wird die Email mit einem entsprechenden Hinweis zurückgeschickt. Alternativ dazu kann die Antwort auch aus dem Hinweis bestehen, zusätzlich z.B. per World Wide Web in Interaktion mit dem Empfänger zu treten – hierbei handelt es sich um ein typisches *Challenge-Response*-Verfahren. Trotzdem ein solches Verfahren Spam nahezu komplett blockieren könnte, spricht insbesondere die erschwerte Kommunikation für legitime Absender dagegen. Des Weiteren wird auf diese Weise auch der Versand von legitimen Massen-Emails wie Newsletters oder Mailinglisten verhindert.[73]

Das so genannte *Proof-Of-Work*-Konzept[74] erwartet vom Absender, dass er eine gewisse Menge an komplexen Berechnungen durchgeführt hat, bevor die Email versendet wurde. Die dazu notwendige CPU-Zeit verursacht höheren Aufwand und höhere Kosten pro Email. Um legitime Absender wenig zu belasten, muss parallel eine Whitelist geführt werden. Derartige Verfahren werden derzeit kaum genutzt – vor allem auch, da der Nutzen gegen Spammer mehr als unklar ist. Insbesondere bei der Verwendung von Botnets zum Versand des Spams wird der Aufwand auf die einzelnen Zombie-PCs abgewälzt und betrifft den Spammer nicht.

Seit längerer Zeit kursiert auch die Idee, mittels *virtueller Briefmarken*, mit denen jede Email „frankiert“ werden muss, Spam den Vorteil gegenüber konventioneller Post zu nehmen. Aufgrund des dazu notwendigen weltweiten und hochverfügbaren Micropayment-Systems ist der Aufbau eines solchen Systems aber als unrealistisch einzustufen. Abgesehen davon, dass es neben den Spammern auch sämtlichen legitimen Anwendern des Email-Systems die Vorteile desselben nähme, böte es auch enorme neue Missbrauchs- und Betrugsmöglichkeiten.

[72] Vgl. Kapitel 2.3

[73] Dieses Problem kann natürlich durch den parallelen Einsatz von Whitelists gelöst werden.

[74] z.B. das Hashcash-Verfahren; vgl. dazu http://www.hashcash.org/

Eine Variante eines solchen Systems wollen die Unternehmen Yahoo! und AOL nun trotzdem einsetzen. Sie wollen Unternehmen die Möglichkeit geben, durch eine geringe Gebühr pro Email ihre Seriösität zu beweisen, um Emails dieser Unternehmen dann nicht durch Spamfilter laufen zu lassen.[75] Beim Empfänger ankommender Spam wird auf diese Weise jedoch offensichtlich nicht behindert; es können lediglich Unternehmen sicherstellen, dass ihre Emails nicht versehentlich ausgefiltert werden. Das Projekt ist jedoch erwähnenswert, da hiermit erstmalig eine Art Porto auf Emails eingeführt wird.

Ein bereits eingesetztes Verfahren ist das so genannte *Greylisting*. Hierbei lehnt der Mailserver eine Spam-verdächtige Email während des SMTP-Dialoges temporär ab. Legitime Mailserver schicken bei solchen temporären Fehlern die Email im Normalfall nach einiger Zeit noch einmal; Spam-Software dagegen ist zumeist auf großen Durchsatz programmiert und unternimmt nur einen Zustellversuch. Dieses Verfahren bringt jedoch einige Probleme und Nachteile mit sich. So bindet es bei der (versehentlichen) Ablehnung von Ham zusätzliche Ressourcen, da die Email ein zweites Mal verschickt werden muss. Ebenso kann es vorkommen, dass bei einem großen Mailsystem die Email beim zweiten Zustellversuch nicht vom selben Mailserver versandt wird und somit wieder abgelehnt wird. Ebenso existieren legitime, aber nicht RFC-konforme Mailserver, die eine Email nicht ein zweites Mal verschicken.

Des Weiteren wird das Verfahren unwirksam, wenn Spammer (bzw. deren Zombie-PCs) die Mailserver der entsprechenden ISPs verwenden, die die Email dann weiterversenden. Sollte sich der Einsatz von Greylisting durchsetzen, werden Spammer vermutlich dazu übergehen, jede einzelne Email mehrmals zuzustellen, wodurch sich der Vorteil von Greylisting aufhebt und Nutzer, die kein Greylisting verwenden, doppelt belastet werden.

Keines der in diesem Abschnitt erwähnten Verfahren ist praktikabel. Während die ersten drei Verfahren den Aufwand nicht nur für Spammer, sondern insbesondere für legitime Benutzer enorm erhöhen, ist das letztgenannte Verfahren nur so lange wirksam, wie es von wenigen verwendet wird.

3.4.4 Sonstige Maßnahmen

Neben der Filterung von Emails, Authentifizierung auf verschiedenen Ebenen und der Aufwands- oder Kostenerhöhung beim Versand von Emails gibt es noch einige weitere Verfahren, die sich nicht weiter zuordnen lassen.

Eine grundlegende Technik vor allem zur Verhinderung des Spam-Versands über Botnets ist die *Sperrung des TCP-Ports 25*, der von SMTP verwendet wird, durch eine Firewall. Gerade in Unternehmen sollte die Arbeitsplatz-Rechner Emails nur über den firmeninternen Mailserver versenden dürfen. Ähnlich verfahren mitterweile einige ISPs insbesondere bei DSL-

[75] Vgl. Rötzer (2006)

oder Kabelmodem-Kunden, deren Rechner durch die relativ große Bandbreite als sehr effiziente Zombie-PCs verwendet werden können. Als Folge können betroffene Kunden Emails nur noch über den Mailserver ihres ISPs versenden oder müssen diesen um eine Ausnahmeregelung für ihren Mailserver bitten.

Ähnlich einer solchen Sperre funktioniert das *MTAMARK*-Verfahren. Hierbei legt der Besitzer einer IP-Adresse über einen Eintrag im DNS fest, ob von dieser IP-Adresse Emails versendet werden dürfen. Der empfangende Mailserver kann nun diesen Eintrag abfragen und darauf filtern. Der Vorteil der reinen Sperrung ist deutlich: Es wird dem Empfänger überlassen, ob er filtern möchte oder nicht. MTAMARK ist z.Z. kaum verbreitet. Es wird als Ersatz für Sender ID[76] und ähnliche Verfahren angesehen.

Auch eine *strengere Auslegung des SMTP-Protokolls* kann u.U. Spam zumindest zum Teil verhindern. Bei den folgenden Beispielen muss in jedem Fall aber parallel eine Whitelist für fehlkonfigurierte Mailserver oder -Software geführt werden.

Eine recht einfach zu implementierende Variante ist es, bereits während des SMTP-Dialoges[77] zu überprüfen, ob der vom Client angegebene Hostname dem eigenen oder einem localhost-Namen entspricht. In diesem Fall handelt es sich zumeist um Spam. Zu beachten ist, dass bei lokaler Zustellung „localhost“ offensichtlich ein legitimer Name ist und nicht gefiltert werden sollte.

Ebenfalls gängige Methode von Spammern ist es, aus Zeit- und Performancegründen nicht, wie vorgeschrieben, während des SMTP-Dialoges die Antwort des Servers abzuwarten, sondern sämtliche Kommandos auf einmal zu senden. In diesem Fall kann von Spam ausgegangen werden – allerdings muss beachtet werden, dass die PIPELINING-Erweiterung von ESTMP(RFC2920 2000), die dieses Vorgehen erlaubt, ausgeschaltet ist. In jedem Fall wartet ein korrekt implementierter, sendender Mailserver nach seinem `HELO`- bzw. `EHLO`- sowie nach dem `DATA`-Kommando.

Eine etwas aufwändigere Variante ist es, sendenden Mailservern die Verbindungs-Verschlüsselung mit TLS zu ermöglichen. Eine solche Verschlüsselung ist prinzipiell natürlich auch Spammern möglich, wird von diesen aus Performance-Gründen z.Z. aber nicht eingesetzt. Ein TLS nutzender Mailserver kann z.Z. also als Hinweis auf Ham genutzt werden.

Es gibt noch eine Reihe weitere Möglichkeiten, auf ähnliche Weise zumindest ein wenig Spam frühzeitig zu erkennen. Auf diese soll aber nicht weiter eingegangen werden. Einerseits sind die verschiedenen Ansätze zwar kostengünstig und juristisch unbedenklich umzusetzen, allerdings sind sie ebenso einfach zu umgehen. Ausserdem wird nur relativ wenig Spam erkannt, weswegen in jedem Fall weitere Maßnahmen, falls möglich, ergriffen werden sollten.

[76] Vgl. Kapitel 3.4.2
[77] Vgl. Kapitel 3.2

Neben dem eigentlichen Spam stellt, wie in Kapitel 2.2.7 erläutert, auch der kollaterale Spam, insbesondere bounce messages an unbeteiligte Dritte, ein Problem dar. Das Filtern solcher Nachrichten gestaltet sich schwierig, da sie nicht standardisiert sind und sich somit von Mailserver zu Mailserver unterscheiden. Lediglich das `Envelope From:` der ursprünglichen Email taucht in jeder bounce message zwangsläufig als `Envelope To:` wieder auf. Diese Tatsache macht sich die *Bounce Adress Tag Validation* (BATV) zunutze. Um überprüfen zu können, ob auf die Ursprungsnachrichten von auf dem eigenen Mailserver ankommenden bounce messages tatsächlich von diesem Server verschickt wurden, kodiert der Mailserver Tracking-Informationen im `Envelope From:`.[78] Bounce messages ohne oder mit gefälschten Tracking-Daten können zweifelsfrei als kollateraler Spam gefiltert werden. Derartige Systeme sind z.Z. nur testweise im Einsatz. Ein Problem bei diesem Konzept stellen Systeme dar, die das `Envelope From:` aus Authentifizierungszwecken interpretieren, z.B. Mailinglisten. Ebenso kollidiert BATV mit dem Greylisting-Verfahren.[79]

[78] Um Fälschungen zu verhindern, muss der Mailserver diese Informationen entweder kryptographisch sichern oder parallel in einer Datenbank sichern

[79] Vgl. Kapitel 3.4.3

4 Rechtslage und Initiativen

Um in den folgenden Kapiteln vor allem auf politischer Ebene mögliche und sinnvolle Maßnahmen gegen Spam entwickeln zu können, ist es unabdingbar, neben der derzeitigen Rechtslage und politischen Initiativen auch Aktivitäten auf der Ebene von Unternehmen und Non-Governmental Organisations (NGOs) zu untersuchen. Ausserdem soll aufgrund der Internationalität von Spam neben der deutschen auch die Gesetzeslage sowie Aktivitäten anderer Staaten betrachtet werden. Einen wesentlichen Teil nehmen hier auch bi- und multilaterale Vereinbarungen ein.

Zu beachten ist außerdem, dass sich die juristische Definition im Gegensatz zu der in dieser Arbeit verwendeten technischen Definition von Spam zumeist auf die Form der kommerziellen Werbung, also UCE, beschränkt. Spam ist also nicht mehr unverlangt zugesandte Massen-Email ohne Bedeutung des Inhalts, sondern lediglich unverlangt zugesandte Massen-Email mit kommerziellem Inhalt, die zudem zumeist auch noch ohne bestehenden geschäftlichen Kontakt zwischen Versender und Empfänger verschickt werden muss. Mittlerweile macht es jedoch nur noch wenig Sinn, Spam derart eingeschränkt zu betrachten. Die immer größer werdende Anzahl an Betrugsversuchen per Phishing[80], aber auch die steigende Verbreitung von Botnets[81] machen deutlich, dass eine umfassende Betrachtung auf Basis der einführend gegebenen, „technischen“ Definition von Spam notwendig ist, um zukunftsorientierte Strategien gegen den Missbrauch des Email-Systems zu erarbeiten.

Im Folgenden soll nun ein Überblick über diese verschiedenen Gebiete und Initiativen gegeben werden.

4.1 Rechtslage in Deutschland

Grundlegend zur Erarbeitung einer bundespolitischen Strategie gegen Spam ist sicherlich die derzeitige deutsche Rechtslage, die – wie in vielen Bereichen der (relativ neuen) Computertechnologie – teilweise noch unklar und umstritten ist. Viele vorhandene Gesetze stammen aus prä-Internet-Zeiten und sind für dieses Medium nur bedingt anwendbar bzw. in ihrer Anwendung umstritten.

[80] Vgl. Kapitel 2.2.4
[81] Vgl. Kapitel 3.3.4

Da sich die rechtliche Bewertung der verschiedenen Kategorien von Spam[82] unterscheidet, werden diese im Folgenden entsprechend Kapitel 2.2 getrennt untersucht.

4.1.1 Kommerzielle Werbung

Seit der im Juli 2004 veränderten Fassung des *Gesetzes gegen den unlauteren Wettbewerb* (UWG), die die EU-Richtlinie 2002/58/EG[83] umsetzt, ist kommerzielle Werbung per Email, also UCE, in Deutschland gesetzlich verboten. Bereits vor dieser Reform hatte sich jedoch eine weitgehend einheitliche Rechtssprechung entwickelt, die durch eine Grundsatzentscheidung[84] des Bundesgerichtshofs bestätigt wurde und die der durch das reformierte UWG vertretenen Ansicht in großen Teilen gleicht.

Wie in der EU-Richtlinie festgelegt, gilt in Deutschland das Opt-In-Prinzip. Des Weiteren legt §7 Abs. 2 UWG fest, dass der Empfänger jederzeit die Möglichkeit haben muss, einer zukünftigen Nutzung seiner Adresse zu widersprechen. Ebenso legt dieser Absatz fest, dass in jedem Fall eine gültige Adresse des Absenders bzw. Auftraggebers angegeben werden muss. Die Verschleierung oder Verheimlichung der Identität des Absenders ist verboten. Klagebefugt auf Basis des UWG sind jedoch nicht die Empfänger einer Spam-Email, sondern lediglich Mitbewerber, Handelskammern und Verbraucher- und Wettbewerbsverbände; im Rahmen der §§823, 1004 BGB („Schadensersatzpflicht“, „Beseitigungs- und Unterlassungsanspruch“) steht ersteren jedoch entsprechende Möglichkeiten zu.

Ein Vorgehen gegen UCE ist in Deutschland also rechtlich möglich; inwiefern sie sinnvoll ist, hängt vom Einzelfall ab. Gegen UCE, die entweder von einem deutschen Absender stammt oder die eine Website bewirbt, für die sich ein Deutscher rechtlich verantwortlich zeichnet, kann vorgegangen werden; rechtliche Ansprüche gegen Versender aus dem Ausland – die den größten Teil von Spam ausmachen – durchzusetzen ist dagegen insbesondere auch aufgrund des hohen finanziellen Risikos äußerst schwierig.

Strafrechtlich ist UCE in Deutschland z.Z. nicht verboten[85] – inwieweit ein entsprechendes Gesetz sinnvoll und zielführend wäre, ist umstritten. Im Zuge der Vorstellung des „Entwurfes eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes“ (DS 15/4835 2005) der rot-grünen Bundesregierung im Februar 2005 sowie des Antrages „Spam effektiv bekämpfen“ (DS 15/2655 2004) der CDU/CSU-Bundestagsfraktion vom März 2005 wurden mehrere Unternehmen, Verbände und Einzelsachverständige um eine Stellungnahme (DS 15 9) gebeten. Während ein Teil der Stellungnahmen einen Straftat-Bestand von Spam unterstützt, wird

[82] Vgl. Kapitel 2.2
[83] Vgl. Kapitel 4.3.1
[84] Urteil des I. Zivilsenats vom 11.3.2004, *I ZR 81/01* (online verfügbar unter http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&nr=28908 [22.02.2006])
[85] Vgl. Frank (2004) und DS 15/4835 (2005)

auch hier in anderen Texten eine weitere Rechtsregelung für unnötig befunden. Auf Argumente, die für eine Strafbarkeit von Spam sprechen, wird in Kapitel 5.1 näher eingegangen.

4.1.2 Nicht-kommerzielle Werbung

Werbung per Email, die gegen bereits geltende Gesetze verstößt[86], kann offensichtlich verfolgt werden. Des Weiteren gibt es im Falle von politischer Werbung mittlerweile eine Reihe von Urteilen, die diese Art Spam verbietet.[87] Im Allgemeinen wird nicht-kommerzielle Werbung bisher nicht im Rahmen von „Spam" betrachtet.[88] Vermutlich aufgrund der geringen Verbreitung dieser Art Spam gibt es in der juristischen Literatur und Rechtssprechung – ausgenommen die Urteile zu politischer Werbung – bisher keinerlei Beurteilung.

4.1.3 Malware

Insbesondere in Hinblick auf die immer weiter zunehmende Verbreitung von Spam über Botnets sowie auf die steigende Anzahl und vor allem auch Leistungsfähigkeit insbesondere von Trojanern spielt neben UCE auch Malware eine wesentliche Rolle.[89] Bei der Betrachtung dieses Aspektes muss unterschieden werden zwischen dem Hersteller, dem vorsätzlichen sowie dem versehentlichen Verbreiter der Software.

Der Hersteller von Malware ist, ebenso wie der vorsätzliche Verbreiter, juristisch unumstritten haftbar zu machen für den entstehenden Schaden. Abhängig von der Schadensroutine des Programms greifen hier §202 StGB („Ausspähen von Daten"), §263a StGB („Computerbetrug"), §303a StGB („Datenveränderung") oder §303b StGB („Computersabotage"). Ebenso bestehen zivilrechtliche Ansprüche mittels §826a BGB sowie anderen Vorschriften. Diese Rechtslage wird – wie in vielen Fällen von Spam – dadurch behindert, dass es oftmals schwierig ist, den eigentlichen Hersteller und ursächlichen Verbreiter zu finden; zumeist agiert dieser dann aus dem Ausland, was eine Verfolgung ebenfalls erschwert. Weiterhin ist der Nachweis eines Vorsatzes bei der Verbreitung von Malware meist nur schwer zu führen.

Weniger eindeutig sieht es im Falle der „versehentlichen" Verbreitung aus. Moderne Malware verbreitet sich mittlerweile vollkommen selbstständig und in großer Geschwindigkeit über das Internet, sobald sie erst einmal „in freie Wildbahn" entlassen wurde. Nicht nur das Unwissen der meisten Nutzer, sondern auch die derzeit vorhandene Betriebssystem-Monokultur durch Microsoft Windows spielt hier eine entscheidende Rolle. Unumstritten

[86] z.B. Massen-Emails rassistischen oder kinderpornographischen Inhalts

[87] OLG München v. 12.02.2004, 8 U 4224/03, http://www.jurpc.de/rechtspr/20040131.htm [18.02.2006]; AG Rostock v. 28.01.2003, 43 C 68/02, http://www.jurpc.de/rechtspr/20030083.htm [18.02.2006]; LG München I v. 05.11.2002, 33 O 17030/02, http://www.jurpc.de/rechtspr/20030008.htm [18.02.2006]

[88] Vgl. dazu die Einleitung dieses Kapitels.

[89] Vgl. dazu auch MessageLabs (2006)

ist in diesem Bereich lediglich die nicht existente Strafbarkeit mangels Vorsatz. Zivilrechtliche Haftungsfragen dagegen sind – auch da, soweit ersichtlich, bisher keinerlei gerichtlichen Entscheidungen zu diesem Themenkomplex vorliegen – umstritten.

Eine Haftungspflicht auch bei fahrlässigem Verhalten kann nur angenommen werden, wenn auch eine Verpflichtung zur Sicherung von Rechnern und Netzwerken gegen Malware existiert. Praktisch alle größeren Unternehmen werden z.B. durch das *Gesetz zur Kontrolle und Transparenz im Unternehmensbereich* (KonTraG) verpflichtet, ein IT-Risikomanagement und sichere Netzwerkinfrastrukturen zu schaffen. Ähnliche Verpflichtungen enthält auch §109 des *Telekommunikationsgesetzes* (TKG). Weiterhin verpflichten diverse Datenschutz-Vorschriften zum besonderen Schutze bei der Speicherung personenbezogener Daten. Wenn innerhalb des Unternehmens diesen Forderungen nachgekommen wird, kann dem Unternehmen keine Fahrlässigkeit nachgewiesen werden. In diesem Falle muss es auch nicht für entstandene Schäden haften. Weiterhin kann eine Haftung ausgeschlossen werden, sofern es sich um neu in den Umlauf gebrachte Malware handelt, für die seitens der Anti-Viren-Hersteller noch gar keine Erkennung existiert.[90]

Im Gegensatz zu Unternehmen gibt es für Privatpersonen keinerlei juristische Vorschriften zur Sicherung von Rechnern. Allenfalls in Ausnahmefällen kann also für Privatpersonen eine Haftung für die nicht vorsätzliche Verbreitung von Malware angenommen werden.[91]

4.1.4 Betrug und Phishing

Im Gegensatz zur sinkenden Anzahl an UCE steigt der Anteil an Phishing-Versuchen seit einiger Zeit deutlich.[92] Eine strafrechtliche Verfolgung dieser Betrugsversuche ist nach derzeitigem Recht jedoch nicht möglich, da es sich bei den Phishing-Emails lediglich um straflose Vorbereitungshandlungen handelt. Ebenso ist das „Ergaunern“ von PINs, TANs oder Passwörtern strafrechtlich nicht verfolgbar, da es sich bei diesen um „nicht besonders gesicherte“ Daten handelt. Nach herrschender Meinung können die Strafverfolgungsbehörden erst eingreifen, wenn die erbeuteten Daten tatsächlich für einen Betrug mit Vermögensschaden genutzt werden. Hier greift dann §263a StGB („Computerbetrug“) – gleichzeitig ist nun aber das erbeutete Geld zumeist verloren.

Ähnlich verhält es sich bei klassischen Betrugsversuchen wie dem *Nigeria-Scam*[93]. Zwar handelt es sich – wie beim Phishing – bei den massenhaft versandten Emails lediglich um straflose Vorbereitungshandlungen; sollte es jedoch zu einer Schädigung des Opfers kommen, so tritt §263 StGB in Kraft. Eine Verfolgung ist aber im Normalfall aufgrund der aus

[90] Vgl. BSI (2005, S.51f.)
[91] Vgl. ebd.
[92] MLabs:2005
[93] Vgl. Kapitel 2.2.4

dem Ausland operierenden Täter[94] nahezu unmöglich. Insbesondere die Verfolgung zivilrechtlicher Ansprüche ist so gut wie ausgeschlossen.[95]

Andere vorkommende Fälle wie angebliche Gewinnspiele, Glücksspiele o.ä. sind bereits hinlänglich juristisch geregelt; für die Verfolgung der Täter gilt aber offensichtlich dasselbe wie auch für die Verfolgung der „Nigeria-Scammer".

4.1.5 Rufschädigung und ähnliches

Im Falle einer Rufschädigung per Email gelten die bereits bestehenden rechtlichen Regularien. Strafrechtlich kommen die §§185ff. („Beleidigung", „Üble Nachrede" und „Verleumdung") in Betracht; zivilrechtlich können z.B. Abmahnungen, Unterlassungserklärungen und einstweilige Verfügungen als Mittel eingesetzt werden.

Unklarer ist die Situation bei den so genannten *Joe Jobs*[96]. Hier gibt es bisher noch keinerlei Beurteilung in der Rechtsprechung oder in der juristischen Literatur. Aus strafrechtlicher Sicht ist eine Verfolgung jedoch vermutlich schwierig, da es sich bei Emails nicht um Urkunden im rechtlichen Sinne handelt und somit auch der beim analogen Pendant „Brief" greifbare Sachverhalt der Urkundenfälschung nicht greift. Lediglich über den Umweg des Markenrechts ist es Unternehmen u.U. möglich, gegen die Verursacher vorzugehen. Den Geschädigten bleibt davon unabhängig der zivilrechtliche Weg auf Basis von z.B. §826 BGB („Sittenwidrige vorsätzliche Schädigung").[97]

4.1.6 Hoaxes und Kettenbriefe

Sowohl das Initiieren als auch die Teilnahme an so genannten *Make Money Fast*-Emails (MMF) – also profitorientierten Ketten-Email-Systemen – ist in Deutschland nach §16, Abs.2 UWG („Strafbare Werbung") unzulässig. So genanntes *Multi Level Marketing* (MLM) ist unter bestimmten Voraussetzungen[98] ebenfalls nach §16, Abs.2 UWG unzulässig.

„Normale" Kettenbriefe und Hoaxes dagegen sind sicherlich zumeist unerwünscht; rechtlich sind sie jedoch – genau wie ihre „analogen" Äquivalente – nicht zu verhindern.

[94] Neben dem namensgebenden Nigeria arbeiten die Täter teilweise auch aus dem europäischen Ausland (vgl. z.B. Roth (2004)).

[95] Vgl. z.B. die „Hinweise zum sogenannten Vorauszahlungsbetrug ‚Nigeria-Connection' (‚419-Connection')" des Auswärtigen Amtes (online unter http://www.auswaertiges-amt.de/www/de/laenderinfos/419_html [18.02.2006])

[96] Vgl. Kapitel 2.2.5

[97] Vgl. BSI (2005, S.50)

[98] Diese treten ein, sobald nicht mehr die Produktwerbung im Vordergrund steht, sondern vielmehr das Gewinnversprechen für den Fall, dass neue Verbraucher geworben werden. In diesem Fall handelt es sich im Grunde also eher um ein MMF-System unter dem „Deckmantel" des MLM.

4.1.7 Kollateraler Spam

Bei kollateralem Spam handelt es sich, wie bereits erörtert, um eigentlich sinnvolle Rückmeldungen des Email-Systems. Gerade in Fällen von Spam-Emails mit gefälschtem, aber existenten Absender können diese Rückläufer jedoch große Probleme bei dem eigentlichen Besitzer der Email-Adresse bzw. dessen Postfach verursachen. Diese werden aber nicht durch die Absender, sondern durch den ursprünglichen Spammer verschuldet, so dass für eine rechtliche Bewertung auf Abschnitt 4.1.1 bzw. 4.1.3 verwiesen werden kann.

Allerdings ist an dieser Stelle zu beachten, dass z.B. durch Virenfilter hervorgerufene *bounces* nur die für das Problem wesentlichen Daten übertragen sollten. Eine massive Werbung für das eigene Produkt auf diesem Wege kann juristisch u.U. als UCE eingeordnet werden.[99]

4.2 Sonstige Aktivitäten in Deutschland

Einen wesentlichen Punkt bei der Bekämpfung von Spam spielt nicht nur die Gesetzeslage, sondern ebenso auch die Arbeit von Behörden und anderen Organisationen, die auf politisch-strategischer, aber auch z.B. rechtsverfolgender oder aufklärender Ebene gegen Spam vorgehen. Oftmals bemängelt wird in diesem Bereich die fehlende bzw. nicht ausreichende Aktivität seitens der Bundesregierung.[100] Im Gegensatz zu einer Vielzahl anderer Länder besitzt die Bundesrepublik keine zentrale Anlaufstelle auf behördlicher Ebene.

Zur Zeit wird die Bundesrepublik in diesen wie auch in anderen Initiativen und Netzwerken durch den Verband der deutschen Internetwirtschaft *eco* vertreten. Mit der Gründung einer Anti-Spam Task Force im August 2003, der nach Eigenaussage mittlerweile ca. 80 Teilnehmer aller führenden Unternehmen der Internetbranche[101] angehören, sowie dem im September 2005 gestarteten SpotSpam-Projekt[102] ist der Verband z.Z. die wichtigste und aktivste deutsche Organisation, die sich mit Spam beschäftigt. Neben diesen Aktivitäten veranstaltet der eco regelmäßig seit 2003 den *Deutschen Anti-Spam-Kongress*, der sich einmal jährlich mit technischen, aber auch rechtlichen und politischen Maßnahmen und Strategien gegen Spam beschäftigt. Ebenso gründete der eco gemeinsam mit dem *Deutschen Direktmarketing Verband* (DDV) im September 2004 die so genannte *Certified Senders Alliance*, ein Positivlistenprojekt für seriöse Direktmarketing-Unternehmen. Des Weiteren ist der eco – neben der Bundesnetz-

[99] Vgl. BSI (2005, S.52)
[100] Vgl. Heise News vom 09.09.2005: „Mehr Anti-Spam-Klagen zu erwarten“ (online unter http://www.heise.de/newsticker/meldung/63743 [18.02.2006])
[101] Vgl. Mitteilung des eco vom Juli 2004: „Gesetz gegen den unlauteren Wettbewerb (UWG)“ (online unter http://www.eco.de/servlet/PB/menu/1350421/index.html [18.02.2006])
[102] Vgl. Kapitel 4.4.1

agentur – z.Z. der offizielle deutsche Ansprechpartner im europäischen *Kontaktnetz der Behörden zur Spambekämpfung* (contact network of spam enforcing authorities, CNSA)[103].

Neben dem *eco* setzen sich auch der *Verbraucherzentrale Bundesverband* (vzbv) und die *Zentrale zur Bekämpfung unlauteren Wettbewerbs* (WBZ) gegen Spam ein. Die drei Organisationen haben im März 2005 auf Initiative des *Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz* (BMELV) ein Aktionsbündnis gegründet und betreiben seit September desselben Jahres eine zentrale Spam-Beschwerdestelle[104]. Ersteres spielt auf Bundesebene insofern eine wichtige Rolle, als dass es dem eco erlaubt, über die Projektpartner Klagen gemäß UWG gegen UCE-Versender zu initiieren, die der Verband sonst nicht erheben dürfte.[105]

Neben den genannten Organisationen arbeiten auch das *BMELV*, das *Bundesministerium für Wirtschaft und Technologie* (BMWi) sowie die *Bundesnetzagentur* im Rahmen nationaler und internationaler Initiativen gegen Spam.

Als Teil des vom BMELV initiierten *Bündnisses gegen Spam* unterstützt das Ministerium weiterhin ein Kampagne zur Verbraucher-Aufklärung. Im März 2006 soll zu diesem Zweck durch den vzbv eine Website online gestellt werden, die Verbraucher und Internetnutzer für das Thema Spam sensibilisieren und informieren soll. Des Weiteren engagiert sich das BMELV u.a. in der *Task Force on Spam* der OECD sowie dem CNSA. Ebenso nahm das BMELV regelmäßig an den Treffen des *London Action Plans* teil, hat diese Vereinbarung jedoch noch nicht unterschrieben.[106]

Das BMWi engagiert sich stark im Bereich der internationalen Zusammenarbeit. Auf europäischer Ebene arbeitet das Ministerium im Rahmen des CNSA, auf weltweiter Ebene wie auch das BMELV in der *Task Force on Spam* der OECD, aber auch im Rahmen der ITU. Darüber hinaus arbeitet das BMWi auch mit der US-amerikanischen FTC bei der *Operation Spam Zombie*[107] zusammen.

Die Bundesnetzagentur, maßgeblich beteiligt an der Bekämpfung des Dialer-Problems, ist neben dem eco die für Deutschland benannte Stelle beim CNSA. Im Gegensatz zu diesem beschränkt sich die Arbeit der Bundesnetzagentur derzeit jedoch im Rahmen der Dialer-Bekämpfung auf Rufnummern-Spam. Im Falle von Email-Spam ist die Bundesnetzagentur nur unter der Voraussetzung zuständig, dass in der Email unmittelbar oder mittelbar Rufnummern beworben werden. Mittelbare Werbung beinhaltet in diesem Fall vor allem Emails,

[103] Vgl. Kapitel 4.4.1

[104] Vgl. Pressemitteilungen der vzbv vom 15.03.2005: „Spamming: Aktionsbündnis gegen Werbemüll im Internet“ (online unter http://www.vzbv.de/go/presse/512/ [18.02.2006]) sowie vom 22.09.2005: „Verbraucher gegen Spam: Spam-Beschwerdestelle beim Verbraucherzentrale Bundesverband“ (online unter http://www.vzbv.de/go/presse/608/ [18.02.2006]); die Beschwerdestelle ist online erreichbar unter http://www.wettbewerbszentrale.de/de/spam/formular.asp [18.02.2006].

[105] Vgl. dazu Kapitel 4.1.1

[106] Zu den genannten Initiativen finden sich weitere Informationen in Kapitel 4.4.1.

[107] Vgl. Kapitel 4.3.2

denen als Anhang z.B. ein Dialer angehängt ist oder die einen Link beinhaltet, der auf eine Website mit einem Dialer oder einer sonstigen Rufnummer führt.[108] Daneben arbeitet die Bundesnetzagentur im Rahmen des *London Actions Plans* neben dem BMELV und dem eco auf internationaler Ebene.

4.3 Rechtslage und Initiativen in anderen Staaten

Spam ist keineswegs lediglich ein deutsches, sondern ein internationales Phänomen. In der Struktur des Internets[109] begründet ist es Spammern möglich, z.B. aus den USA heraus Server in Asien zu missbrauchen, um Spam nach Deutschland zuzustellen. Einer Auflistung von Spamhaus zufolge kommt ein Großteil der Spammer aus den USA, gefolgt von China, Süd-Korea und Russland[110]. Die so genannte ROKSO-Liste[111], auch von Spamhaus erstellt, enthält ebenfalls größtenteils Amerikaner.[112] Um eine sinnvolle und weitreichende politische Strategie gegen Spam zu entwickeln, ist es also notwendig, nicht nur die Situation in der Bundesrepublik bzw. der EU zu untersuchen, sondern auch vor allem die Staaten zu betrachten, aus denen ein Großteil des weltweiten Spam-Aufkommens stammt.

Im Folgenden soll also neben der bereits vorhandenen EU-Richtlinie auch die Rechtslage in den Ländern, die in nahezu sämtlichen Statistiken führende Positionen beim Versand von Spam einnehmen: die USA, China, Süd-Korea sowie Russland. Ebenso soll die Arbeit der australischen Regierung, die als eine der erfolgreichsten gilt, untersucht werden.

4.3.1 Europäische Union

Bereits im Juli 2002 erließ die EU die Richtlinie 2002/58/EG über den Datenschutz in der elektronischen Kommunikation und übernahm damit eine Vorreiterrolle in Bezug auf die Erarbeitung multilateraler Richtlinien gegenüber Spam. Mit dieser Richtlinie – bzw. dem relevanten Artikel 13 („Unerbetene Nachrichten") – wurde EU-weit der Grundsatz der Opt-In-Regelung eingeführt. Direktwerbung – also u.a. auch Spam – ist nur noch zulässig entweder nach vorheriger Einwilligung der Teilnehmer oder bei einem bereits bestehenden Vertragsverhältnis, sofern der Kunde die Möglichkeit hat, der Werbung zu widersprechen.

[108] Die Informationen entstammen einem Emailkontakt zwischen dem Autor und Christoph Mayer vom *Referat für Grundsatzfragen der Verfolgung des Missbrauchs von Mehrwertdiensten* der Bundesnetzagentur zwischen Januar und Februar 2006. Die Emails können bei Bedarf beim Autor eingesehen werden.

[109] Vgl. Kapitel 3.1

[110] online verfügbar unter http://www.spamhaus.org/statistics/countries.lasso, Stand vom 8. Dezember 2005

[111] ROKSO steht für „Register of Known Spam Operations" und beinhaltet die 200 aktivsten Spam-Gruppen. Laut Eigenaussage gehen von diesen etwa 80% des weltweiten Spams aus. Die Liste findet sich unter http://www.spamhaus.org/rokso/index.lasso [18.02.2006].

[112] Stand: 22. Februar 2006

Ebenso verpflichtet Artikel 13 die Mitgliedsstaaten sicherzustellen, dass in anderen Fällen unerbetene Direktwerbung nicht gestattet ist. Es steht den Mitgliedsstaaten frei zu entscheiden, ob dieser Punkt für Teilnehmer gilt, die keine Einwilligung zur Werbung gegeben haben oder die sich explizit gegen solche Nachrichten entschieden haben. Weiterhin ist es verboten, bei der Versendung von Werbe-Emails die Identität des Absenders zu verschleiern oder zu verheimlichen. Absender sind verpflichtet, eine gültige Adresse anzugeben, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten richten kann.

Die Richtlinie 2002/58/EG sollte bis zum 30. Oktober 2003 in den Mitgliedsstaaten in Kraft gesetzt werden. Von den zu dem damaligen Zeitpunkt 15 EU-Mitgliedsstaaten hatten bis zu diesem Datum jedoch lediglich sechs die Richtlinie umgesetzt; gegen die neun weiteren Staaten[113] wurde seitens der EU ein Vertragsverletzungsverfahren eingeleitet. Mittlerweile haben sämtliche Staaten – inklusive der 2004 hinzugekommenen 10 Staaten – bis auf Griechenland die Richtlinie umgesetzt.[114]

Trotzdem gestaltet sich die grenzüberschreitende Verfolgung auf Basis der Richtlinie bzw. ihren Umsetzungen in nationales Recht mitunter schwierig. Sowohl die zivil- und strafrechtliche Bewertung als auch die Zumessung von Geldstrafen und Schadenersatzforderungen unterscheiden sich massiv zwischen den Mitgliedsstaaten. Ebenso gibt es massive Unterschiede bei den jeweils zuständigen nationalen Institutionen: Teilweise sind Verbraucherschutzbehörden, teilweise aber auch Datenschutzbehörden oder Telekommunikationsregulierer für die Spam-Bekämpfung zuständig.[115] Zur Behebung zumindest des letzteren Punktes wurde das (informelle) *Kontaktnetz der Behörden zur Spambekämpfung* (contact network of spam-enforcing authorities, CNSA)[116] aufgebaut.

Bis Mitte 2006 sollen die Berichte aller Mitgliedsstaaten zur Umsetzung der Richtlinie 2002/58/EG vorliegen, woraufhin gegebenenfalls Aktualisierungen vorgenommen werden sollen. Ebenfalls bis zu diesem Zeitpunkt wird eine Mitteilung der EU-Kommission erwartet, die ein besonderes Augenmerk auf Bedrohungen wie Phishing, Viren und Botnets legt.

[113] Belgien, Deutschland, Griechenland, Frankreich, Luxemburg, die Niederlande, Portugal, Schweden und Finnland

[114] Vgl. 5691/04 TELECOM 11 (2004) sowie KOM (2004). Weitere Informationen stammen aus einem Emailkontakt, den der Autor Anfang Januar 2006 mit Philippe Gérard von der *Generaldirektion Informationsgesellschaft* der EU-Kommission führte. Die Emails können bei Bedarf eingesehen werden.

[115] Vgl. Heise News vom 09.12.2004: „EU-Rat will mehr Koordination gegen Spam“ (online unter http://www.heise.de/newsticker/meldung/54106 [18.02.2006]) sowie Heise News vom 14.12.2004: „Langsame Fortschritte bei Anti-Spam-Politik der EU“ (online unter http://www.heise.de/newsticker/meldung/54214 [18.02.2006])

[116] Vgl. Kapitel 4.4.1

4.3.2 USA

In den Vereinigten Staaten wurde bereits im Dezember 2003 der so genannte *CAN-SPAM Act*[117] in Kraft gesetzt, mit dessen Hilfe Spam (bzw. UCE) bekämpft werden soll.

Der *CAN-SPAM Act* definiert Spam als „*any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)*“[118] – ausgenommen sind dabei ausdrücklich „*transactional or relationship messages*“[119]. Das Gesetz erlaubt es jedoch weiterhin, Emails mit werbendem Inhalt zu verschicken, wenn sie folgenden Ansprüchen genügen:

- Es existiert ein Opt-Out-Mechanismus.
- Die Betreffzeile und die Header-Informationen sind korrekt.
- Es wird eine rechtmäßige Postanschrift des Absenders angegeben.
- Im Falle von Inhalten, die nur Erwachsenen zugänglich gemacht werden dürfen, müssen diese gekennzeichnet werden.

Bei Verstößen gegen diese Vorschriften können von der US-Handelskommission *FTC*, den Staatsanwaltschaften, ISPs und ähnlichen Institutionen, nicht aber von Privatpersonen rechtliche Schritte eingeleitet werden.

Inwieweit der CAN-SPAM Act ein sinnvolles und effektives Mittel zur Bekämpfung von UCE ist, ist jedoch umstritten. Anti-Spam-Aktivisten bemängelten von Anfang an, dass das Gesetz nicht primär Spam verbietet, sondern – zumindest mit Einschränkungen – erlaubt.[120] Andererseits wurden auf Basis des *CAN-SPAM-Acts* bereits diverse Gerichtsverfahren eröffnet – vielfach gegen unbekannt. Zwei Jahre nach Inkrafttreten des Gesetzes gelten die USA jedoch immer noch als das Land mit der größten Anzahl an Spammern;[121] gleichermaßen kommen einige Studien aber zu dem Ergebnis, dass der Anteil der USA am weltweiten Spam-Aufkommen deutlich sinkt. So stehen die USA in einer Studie von *Sophos* von Anfang 2006[122] zwar weiterhin an erster Stelle der Spam-Verbreiter; gleichzeitig ist ihr Anteil aber im

[117] „CAN-SPAM“ steht für **C***ontrolling the* **A***ssault of* **N***on-***S***olicited* **P***ornography and* **M***arketing*. Das Gesetz ist online verfügbar unter http://www.spamlaws.com/federal/can-spam.shtml [18.02.2006]

[118] ebd.

[119] ebd.

[120] Vgl. Heise News vom 04.11.2003: „Scharfe Kritik am US-Gesetz gegen Spam“ (online unter http://www.heise.de/newsticker/meldung/41653 [18.02.2006])

[121] Vgl. z.B. die Statistiken von Spamhaus (http://www.spamhaus.org/statistics/countries.lasso [18.02.2006]) oder Ironport (http://www.ironport.com/toc/toc_spam.html [18.02.2006])

[122] Vgl. Pressemitteilung von Sophos vom 23.01.2006: „Bill Gates death-of-spam prediction flops, as ‚dirty dozen‘ spam countries revealed“ (online unter http://www.sophos.com/pressoffice/news/articles/2006/01/dirtdozjan05.html [22.02.2006])

Vergleich zum April 2005 von 41,5% auf 24,5% gesunken. Untersuchungen des Anti-Spam-Unternehmens *Commtouch* zufolge waren die USA Mitte 2005 zwar auf den dritten Platz nach China und Süd-Korea sowie auf einen prozentualen Anteil von etwa 15% abgerutscht, führen derzeit jedoch wieder mit 43,18%.[123] Experten gehen jedoch auch davon aus, dass viele US-amerikanische Spammer aufgrund des CAN-SPAM Acts nun aus dem Ausland operieren.[124] Die bereits erwähnte ROKSO-Liste des Spamhaus-Projektes[125] beinhaltet immer noch größtenteils US-Amerikaner, was diesen Schluss untermauert.[126] Eine endgültige Beurteilung der Statistiken ist schwierig, da die jeweiligen Unternehmen lediglich auf den durch ihre Kunden hervorgebrachten Datenbestand zugreifen können und diese Werte wiederum rein prozentual angegeben werden. Absolute Werte könnten – ebenso wie Informationen über die Datenbasis – hier die Vergleichbarkeit erhöhen, liegen jedoch nicht vor.

Neben dem *CAN-SPAM Act* gibt es auch auf Ebene der Bundesstaaten in vielen Fällen bereits vor dem Bundesgesetz verabschiedete und teilweise auch deutlich strengere Gesetze gegen UCE. Die Befürchtung der *CAN-SPAM Act*-Kritiker, dass diese Gesetze durch das Bundesgesetz, wie i.A. üblich, ausser Kraft gesetzt würden, wurde durch ein Urteil eines US-Bundesgerichts in Washington jedoch – zumindest für manche Fälle – widerlegt. Im Fall *Gordon v. Impulse Marketing Group Inc.*[127] stellte das Gericht fest, dass der *CAN-SPAM Act* eigene Gesetzesregelungen auf Ebene der Bundesstaaten durchaus zulässt – unter der Voraussetzung, dass diese sich mit gefälschten oder irreführenden Angaben in kommerziellen Emails befassen. Da dies im Falle des Washingtoner Anti-Spam-Gesetzes zutrifft, wurde dem Antragsteller rechtgegeben.[128]

Neben UCE nimmt seit einiger Zeit, wie bereits erörtert, vor allem das so genannte Phishing einen großen Teil des Gesamtaufkommens an Spam ein. Ähnlich wie in Deutschland sind Phisher in den USA z.Z. nur zu verfolgen, wenn bereits ein Schaden verursacht wurde. Wie in Deutschland ist das reine Versenden von Phishing-Emails sowie das Erstellen entsprechender Websites zumindest auf Bundesebene nicht strafbar.[129]

[123] Stand: Februar 2006; vgl. Pressemitteilung von Commtouch vom 11.08.2005: „Commtouch Reports July 2005 Spam Trends: 43% Volume Increase Over July 2004“ (online unter http://www.commtouch.com/Site/News_Events/pr_content.asp?news_id=433&cat_id=1 [18.02.2006]) sowie Pressemitteilung von Commtouch vom 15.02.2006: „January Virus and Spam Statistics: 2006 Starts with a Bang“ (online unter http://www.commtouch.com/Site/News_Events/pr_content.asp?news_id=602&cat_id=1 [22.02.2006])

[124] Vgl. Pressemitteilung von Sophos vom 13.10.2005: „Sophos reveals latest ‚dirty dozen‘ spamming countries“ (online unter http://www.sophos.com/pressoffice/news/articles/2005/10/pr_us_dirtydozoct05.html [18.02.2006])

[125] online unter http://www.spamhaus.org/rokso/index.lasso [18.02.2006]

[126] Vgl. hierzu auch die folgenden Kapitel

[127] Das Urteil ist online verfügbar unter http://www.steptoe.com/publications/365e.pdf [18.02.2006]

[128] Vgl. dazu auch *internetcases.com* (http://www.internetcases.com/archives/2005/07/leaving_a_thin.html [18.02.2006]) oder das Urteil selbst

[129] Vgl. Pressemitteilung von Senator Leahy vom 01.03.2005: „New Leahy Bill Targets Internet ‘PHISHING’ And ‘PHARMING’ That Steal Billions Of Dollars Annually From Consumers“ (online unter http://leahy.senate.gov/press/200503/030105.html [18.02.2006])

Bereits im Jahre 2004 brachte der demokratische Senator Patrick Leahy den so genannten *Anti-Phishing Act*[130] in den Senat ein, der im Oktober 2005 in leicht geänderter Form an den *Unterausschuss für Kriminalität, Terrorismus und Heimatschutz* des Kongresses verwiesen und dort noch nicht verabschiedet wurde.[131] Dieser Gesetzes-Entwurf beinhaltet in Form zweier neuer Straftaten oben genannte Tatbestände: Sowohl das Versenden von Phishing-Emails als auch das Erstellen entsprechender Website wird damit illegal – unabhängig von einem eventuell entstandenen Schaden. Kritiker weisen aber auch bei diesem Entwurf auf dieselben Punkte hin, die bereits beim *CAN-SPAM Act* genannt wurden: Oftmals arbeiten die Täter aus dem Ausland – insbesondere, sobald in ihrer aktuellen Operationsbasis die Gesetze geändert werden. Ebenso ist es oft schwierig bis unmöglich, die Täter überhaupt ausfindig zu machen. Wie bereits erwähnt, wird ein Großteil der auf dem *CAN-SPAM Act* basierenden Verfahren gegen unbekannt geführt; in diesem Punkt unterscheiden sich Phishing-Täter in keiner Weise von Spammern.[132]

Im Gegensatz zur Bundesebene sind einige Bundesstaaten hier schon weiter. Unter anderem Kalifornien, Washington, Texas und Arizona haben bereits Anti- Phishing-Gesetze verabschiedet. Deutliche Erfolge sind jedoch, wie im Vorfeld vermutet, noch nicht eingetreten.

Neben diesen vor allem rechtlichen Aspekten sind die USA bzw. die zuständige FTC bestrebt, auch durch internationale Zusammenarbeit gegen Spam vorzugehen. Neben verschiedenen bi- und trilateralen Memoranden – u.a. zwischen den USA und Spanien, den USA und Mexiko sowie den USA, dem Vereinigten Königreich und Australien – und der Mitarbeit im *London Action Plan*[133] war die FTC auch Initiator der 2004 gestarteten, so genannten *Operation Spam Zombie*[134], deren Ziel es ist, weltweit ISPs auf das Problem der Zombie-PCs aufmerksam zu machen und ihnen sinnvolle Lösungen anzubieten, und an der 35 Behörden[135] aus über 20 Staaten teilnahm. Ebenfalls durch die FTC initiiert wurde die *Operation Secure Your Server*[136], die Anfang 2004 gestartet wurde und an der 36 Behörden aus 26 Staaten teilnahmen. Ziel dieses Projekts war die Suche nach *Open Relays*[137] und *Open Proxies*[138], die oftmals zum Spam-Versand missbraucht werden. Wie auch bei der *Operation Spam Zombie* wurden die Betreiber dieser Server auf dieses Problem aufmerksam gemacht; durch praktische Lösungen wurde ihnen ebenfalls die Möglichkeit gegeben, das „Loch“ schnell zu schließen.

[130] online verfügbar unter http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.1099: [18.02.2006]
[131] Vgl. dazu auch die Datenbank der *Library of Congress* online unter http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.01099: [18.02.2006]; Stand: 01.02.2006
[132] Vgl. Stevenson (2005)
[133] Vgl. Kapitel 4.4.1
[134] Vgl. die Website der FTC zu dieser Operation: http://www.ftc.gov/bcp/conline/edcams/spam/zombie/
[135] u.a. auch das BMWi
[136] Vgl. die Website dazu: http://www.ftc.gov/secureyourserver/
[137] Vgl. Kapitel 3.3.2
[138] Vgl. Kapitel 3.3.3

4.3.3 China

Seit Inkrafttreten des US-amerikanischen *CAN-SPAM Acts* sinkt der Anteil der USA am weltweiten Spamaufkommen einigen Studien zufolge massiv.[139] Gleichzeitig ist der Anteil u.a. von China massiv gestiegen. Des Weiteren belegen Untersuchungen des Anti-Spam-Unternehmens *Commtouch*, dass im Juni 2004 über 70% aller Spamming-Websites in China gehostet wurden. Im August 2004 lag der Anteil bei 30%; aktuellere Daten sind leider nicht bekannt.

Aus diesen Gründen spielen die chinesischen Aktivitäten eine wichtige Rolle im weltweiten Kampf gegen Spam.[140] Bisher gibt es in China noch keinerlei Rechtsmittel gegen Spam in jeglicher Form. Einem Artikel der *Shanghai Daily*[141] vom 21. Februar 2006 zufolge soll jedoch am 30. März ein neues Gesetz in Kraft treten, das sich der Spam-Problematik mittels eines Opt-In-Verfahrens annimmt. Unabhängig davon hat die chinesische Regierung bereits seit 2004 ihre Bemühungen massiv vergrößert, durch Zusammenarbeit mit Unternehmen sowie anderen Staaten das Problem anzugehen.

Bereits im September 2004 wurde ein Memorandum zwischen der *Internet Society of China* (ISC) sowie den Unternehmen *AOL*, *eBay*, *Microsoft* und *Yahoo!* getroffen, um in Zukunft näher zusammenzuarbeiten und Informationen auszutauschen im Kampf gegen Spam.[142] Im Juli 2005 schloss sich China dem *London Action Plan*[143] an, um auch in internationaler Zusammenarbeit Anti-Spam-Maßnahmen, u.a. z.B. direkte Ermittlungen gegen die Verursacher, ergreifen zu können.[144] Des Weiteren arbeitet China auch im Rahmen der während der eCommerce-Konferenz 2005 der *Asian European Meetings* (ASEM) getroffenen Vereinbarungen mit den 38 europäischen und asiatischen Mitgliedsländern zusammen.[145]

Neben dem Spam-Versand zählt jedoch auch das Hosting von Websites, die in UCE beworben, aber auch zum Phishing gebraucht werden, zu Chinas Problemen. Auch auf diesem

[139] Vgl. z.B. Pressemitteilung von Sophos vom 13.11.2005: „Sophos reveals latest ‚dirty dozen' spamming countries" (online unter http://www.sophos.com/pressoffice/news/articles/2005/10/pr_us_dirtydozoct05.html [18.02.2006]) sowie im Vergleich auch Pressemitteilung von Sophos vom 23.01.2006: „Bill Gates death-of-spam prediction flops, as ‚dirty dozen' spam countries revealed" (online unter http://www.sophos.com/pressoffice/news/articles/2006/01/dirtdozjan05.html [22.02.2006])

[140] Nicht ausser Acht gelassen werden sollte natürlich die Tatsache, dass im Falle eine rigorosen Bekämpfung von Spam seitens der chinesischen Regierung Spammer vermutlich in ein weiteres Land „weiterzögen". Ähnliches ist, wie bereits erläutert, nach dem Inkrafttreten des *CAN-SPAM Acts* in den USA geschehen.

[141] Li (2006)

[142] Das Memorandum ist online einzusehen z.B. unter http://www.itu.int/osg/spu/spam/legislation/china-mou-en.html [18.02.2006]

[143] Vgl. Kapitel 4.4.1

[144] Vgl. http://www.londonactionplan.com/news/?p=14 [18.02.2006]

[145] Vgl. Kapitel 4.4.1

Gebiet, war China 2004 in den weltweiten Top3.[146] Einem Bericht der *Asia Times*[147] zufolge spricht aus Sicht der Spammer neben den z.Z. fehlenden Rechtsmitteln und hohen möglichen Bandbreiten vor allem auch das bisherige Desinteresse chinesischer ISPs am Problem „Spam" für China. Ebenso führten Sprachprobleme oftmals nicht zu der Reaktion der ISPs, die sich ausländische Aktivisten wünschten. Dem Leiter des Spamhaus-Projektes Steve Lindon zufolge[148], steht Spamhaus mittlerweile jedoch mit nahezu allen chinesischen ISPs in Kontakt, so dass hier mit einer zukünftig deutlich besseren Zusammenarbeit gerechnet werden kann.

Inwieweit die weiteren bisher getroffenen Maßnahmen erfolgreich sind, kann zum derzeitigen Zeitpunkt noch nicht gesagt werden. Insbesondere das Schaffen klarer Rechtsmittel ist aber sicherlich unumgänglich.

4.3.4 Süd-Korea

Den bereits erwähnten Untersuchungen von Sophos zufolge ist der Anteil von südkoreanischem Spam von Mitte 2004 bis Mitte 2005 zwar massiv gestiegen, bis Anfang 2006 jedoch auch wieder gesunken, so dass Süd-Korea derzeit den dritten Platz in Sophos' Statistik einnimmt.[149] Im Unterschied zu China[150] besitzt Süd-Korea jedoch bereits seit langem ein Anti-UCE-Gesetz, das letztmalig im Januar 2003 überarbeitet wurde.[151] Das Gesetz verbietet es, Email-Nutzern Werbung zukommen zu lassen, die sich explizit dagegen ausgesprochen haben (Opt-Out). Außerdem verpflichtet es den Versender, u.a. Namen und Anschrift anzugeben sowie dem Absender die Möglichkeit zu geben, sich für die Zukunft gegen weitere Emails auszusprechen. In der z.Z. gültigen Fassung verbietet das Gesetz außerdem das automatische Generieren von Email-Adressen, das Sammeln von Email-Adressen von Websites sowie technische Möglichkeiten zur Umgehung von Spam-Filtern.[152] Ebenso muss UCE in der Betreffzeile gekennzeichnet werden, um dem Empfänger das Filtern zu erleichtern.

Inwiefern das Gesetz jedoch erfolgreich ist, kann nicht mit Bestimmtheit gesagt werden. Einem Bericht der *Korea Times* zufolge[153] hält sich der Erfolg jedoch in Grenzen. Das Gesetz

[146] Vgl. Pressemitteilung von Commtouch vom 11.10.2004: „Commtouch Reports September Spam Trends: The Return of China, Phishing" (online unter http://www.commtouch.com/Site/News_Events/pr_content.asp?news_id=34&cat_id=1) aktuellere Zahlen liegen nicht vor.

[147] Galloway (2004)

[148] Vgl. Linford (2005)

[149] Vgl. Pressemitteilung von Sophos vom 13.10.2005: „Sophos reveals latest ‚dirty dozen' spamming countries" (online unter http://www.sophos.com/pressoffice/news/articles/2005/10/pr_us_dirtydozoct05.html [18.02.2006]) sowie Pressemitteilung von Sophos vom 23.01.2006: „Bill Gates death-of-spam prediction flops, as ‚dirty dozen' spam countries revealed" (online unter http://www.sophos.com/pressoffice/news/articles/2006/01/dirtdozjan05.html [22.02.2006])

[150] Vgl. Kapitel 4.3.3

[151] Vgl. Artikel der *Korea Infromation Security Agency* (online unter http://www.kisa.or.kr/kisae/ksrc/jsp/ksrc_06_01.jsp [18.02.2006])

[152] Vgl. Williams (2003)

[153] Kim (2005)

erlaubt es zwar seit der Überarbeitung, Spammer mit einer Strafe von bis zu 30 Mio. Won (etwa 25.000€) zu belegen; bisher wurde jedoch kein Spammer zu mehr als 10 Mio. Won (etwa 8.000€) Strafe verurteilt – der Großteil musste unter 3 Mio Won (etwa 2.500€) Strafe zahlen. Gleichzeitig ist Süd-Korea mittlerweile bei nahezu allen Studien in die Top3 der Spamversendenden Länder gekommen.[154]

Neben der Arbeit auf nationaler Ebene arbeitet Süd-Korea auch in internationalen Initiativen zur Bekämpfung von Spam, so z.B. dem *London Action Plan*.[155] Ebenso kooperiert Süd-Korea im Rahmen der Vereinbarungen durch die *Asian European Meetings* (ASEM) mit den 38 europäischen und asiatischen Mitgliedsländern.[156] Ein 2003 mit Australien vereinbartes Memorandum zum Informationsaustausch über Anti-UCE-Politik und -Strategien sowie die Rechtsverfolgung von Spammern, der *Seoul-Melbourne Act*[157], wurde 2005 zum *Seoul-Melbourne Anti-Spam Agreement*[158], dem zehn weitere Organisationen aus sieben asiapazifischen Staaten[159] angehören, erweitert.

4.3.5 Russland

Neben den USA und China spielt Russland derzeit eine wesentliche Rolle im weltweiten „Spam Business". Während China meist vor allem als sicherer Hafen für Websites genutzt wird, beinhaltet die ROKSO-Liste der Top10-Spammer[160] weltweit mittlerweile vier russische Individuen und Gruppen.[161] Diese arbeiten – im Gegensatz zu den meisten amerikanischen Spammern – mittlerweile im Bereich der organisierten Kriminalität. Neben dem eigentlichen Spamming sind sie nach Aussage des Leiters von Spamhaus, Steve Linford, vor allem aktiv in der Programmierung von Viren und Trojanern und dem Aufbau von Botnets, die dann auch an US-amerikanische Spammer vermietet werden.[162]

Zur Zeit gibt es keinerlei rechtliche Regulierung hinsichtlich Spam in Russland. Entgegen einer Aussage des russischen Kommunikationsministers Leonid Reiman von Anfang 2005[163]

[154] Vgl. z.B. Sophos (s.o.) oder Commtouch (http://www.commtouch.com/Site/ResearchLab/statistics.asp; Stand: 19.01.2006
[155] Vgl. Kapitel 4.4.1
[156] Vgl. ebd.
[157] Vgl. das Memorandum zwischen Australien und Süd-Korea vom 20.10.2003 im Wortlaut (online unter http://www.acma.gov.au/acmainterwr/consumer_info/spam/spam_mou.rtf [18.02.2006])
[158] Vgl. *Seoul Melbourne multilateral Memorandun of Understanding on cooperation in countering spam* vom 27.04.2005 (online unter http://www.acma.gov.au/acmainterwr/consumer_info/spam/spam%20-%20multilateral%20mou%20seoul.melbourne%20-%20final%20web%20version.rtf [18.02.2006])
[159] namentlich China, Hongkong, die Philippinen, Malaysia, Japan, Thailand und Neuseeland.
[160] Die Liste ist online verfügbar unter http://www.spamhaus.org/statistics/spammers.lasso [12.02.2006], Stand: 12.01.06
[161] Vgl. auch McWilliams (2005)
[162] Vgl. Warden (2004)
[163] Vgl. aunty-spam.com (2005)

gibt es jedoch in Russland durchaus Bestrebungen, ein solches Gesetz einzuführen. So befinden sich z.Z. Änderungsanträge zur derzeitigen Gesetzeslage in der Duma, dem russischen Parlament, in der Diskussion. Nach Aussage des Koordinators des Anti-Spam-Projektes des UNESCO „Information for All"-Programms Russland, Eugene Altovsky, ist dieses jedoch wenig hilfreich. Aus diesem Grund erarbeitete sein Projekt eigene Änderungen und hofft, diese 2006 im Parlament einbringen zu können.[164] Bereits jetzt ist Spamming durch einen „Code of Conduct" des Verbandes der russischen ISPs, dem *Open Forum of the Internet Providers* (OFISP) und den daraus resultierenden Vertragsbestimmungen der ISPs im Grunde verboten.[165]

Derzeit gibt es keine offizielle russische Unterstützung internationaler Kooperationen. Das bereits erwähnte Anti-Spam-Projekt arbeitet jedoch bereits seit längerem in den entsprechenden Initiativen der ITU und der OECD.[166] Ebenso wurden auf dieser Basis Vereinbarungen im Rahmen des *London Action Plans*[167] getroffen, um eine Teilnahme Russlands an dieser Kooperation zu ermöglichen. Das Anti-Spam-Projekt hofft, dass auch offizielle russische Vertreter im Laufe des Jahres 2006 das Abkommen unterzeichnen.

In Bezug auf Phishing und auch Botnets gibt es in Russland keine spezielle Gesetzgebung. Jedoch sind diese Aktivitäten bereits jetzt durch die russische Strafgesetzgebung verboten. Ebenso arbeitet Russland in Form der dem Innenministerium zugeordneten CyberCrime-Abteilung mit ausländischen Behörden und Interpol bei der internationalen Verfolgung derartiger Straftaten zusammen.

4.3.6 Australien

Im Gegensatz zu den bisher genannten Staaten gilt Australien als vorbildlich in der Bekämpfung von Spam, zumindest in der Form von UCE. Die weltweit strengste UCE-Gesetzgebung sowie die aktive Durchsetzung der Gesetze durch die *Australian Communications and Media Authority* (ACMA) und eine forcierte internationale Vernetzung führte zu einem starken Rückgang der Aktivitäten inländischer Spammer.[168]

Der australische *Spam Act 2003*[169] verbietet den Versand von UCE bei möglichen Strafen bis zu über 680.000€ und erlaubt lediglich den Versand an nach dem Opt-In-Prinzip legitimierte Email-Adressen. Die Email muss außerdem Informationen über den korrekten Absender bzw. Auftraggeber enthalten und muss jedem Empfänger die Möglichkeit geben, sich aus der

[164] Diese und folgende Aussagen basieren, wenn nicht anders gekennzeichnet, auf einem Email-Verkehr zwischen dem Autor und Eugene Altovsky im Januar 2006. Bei Bedarf können die Emails zur Verfügung gestellt werden.
[165] Vgl. dazu Altovsky (2005)
[166] Vgl. zu beiden Kapitel 4.4.1
[167] Vgl. ebd.
[168] Vgl. dazu Linford (2005) oder Spamhaus (2004)
[169] online verfügbar unter http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm [18.02.2006]

Empfängerliste auszutragen. Des Weiteren verbietet das Gesetz den Gebrauch von automatisierten Adresssammlern bzw. den von diesen gesammelten Adressen.

Insbesondere die hohen möglichen Strafen sowie die strenge Verfolgung durch die ACMA führten nach Aussage von Spamhaus dazu, dass *„das australische Anti-Spam-Gesetz funktioniert“* (Spamhaus 2004).

Neben der Bekämpfung inländischer Spammer hat die australische Regierung jedoch auch schon frühzeitig begonnen, auf internationaler Ebene durch Memoranden und ähnliche Vereinbarungen Netzwerke zur Verringerung des weltweiten Spam-Aufkommens aufzubauen. Neben der Zusammenarbeit mit der OECD, der ITU sowie im *London Action Plan*[170] zählt hierzu für die australische Regierung auch die weltweite Zusammenarbeit mit ISPs und Herstellern von Anti-Virus- und Anti-Spam-Software. Des Weiteren wurde eine gemeinsame Erklärung zu Telekommunikation und IT mit der thailändischen Regierung veröffentlicht, die u.a. auch den Informationsaustausch über Anti-UCE-Politik und -Strategien vereinbart.[171]

Ebenso wurde ein Memorandum zwischen Australien, Großbritannien und den USA verabschiedet, das seinen Schwerpunkt in der Zusammenarbeit in der Rechtsverfolgung von Spammern, auch auch in der Nutzer-Aufklärung hat.[172] Bereits 2003 wurde ein Memorandum zwischen Australien und Süd-Korea zum Informationsaustausch über Anti-UCE-Politik und -Strategien sowie die Rechtsverfolgung von Spammern, der *Seoul-Melbourne Act*, vereinbart.[173] Dieses Memorandum wurde im April 2005 ausgeweitet zum *Seoul-Melbourne Anti-Spam Agreement*[174], dem zehn weitere Organisationen aus sieben asia-pazifischen Staaten[175] beigetreten sind.

4.3.7 Überblick

Die umfangreichen politischen und legislativen Maßnahmen verschiedener relevanter Staaten wurden in den vorhergehenden Abschnitten erläutert. Die folgende Tabelle soll nun als Zusammenfassung und schneller Überblick über diese Maßnahmen dienen. Die Tabelle betrachtet dabei lediglich die untersuchten Nationalstaaten. Aus diesem Grunde und da sie in der Spam- Bekämpfung vorwiegend integrierende Funktionen besitzt, wird die Europäische

[170] Vgl. hierzu Kapitel 4.4.1

[171] Vgl. Joint Statement zwischen Australien und Thailand vom 05.07.2004 (online unter: http://www.acma.gov.au/acmainterwr/consumer_info/spam/aust_thailand_joint_statement.rtf [18.02.2006])

[172] Vgl. Memorandum zwischen den USA, Australien und dem Vereinigtem Königreich von 2004 (online unter http://www.acma.gov.au/acmainterwr/consumer_info/spam/spam_mou-aus_uk_usa.pdf [18.02.2006])

[173] Vgl. das Memorandum zwischen Australien und Süd-Korea vom 20.10.2003 im Wortlaut (online unter http://www.acma.gov.au/acmainterwr/consumer_info/spam/spam_mou.rtf [18.02.2006])

[174] Vgl. *Seoul Melbourne multilateral Memorandun of Understanding on cooperation in countering spam* vom 27.04.2005 (online unter http://www.acma.gov.au/acmainterwr/consumer_info/spam/spam%20-%20multilateral%20mou%20seoul.melbourne%20-%20final%20web%20version.rtf [18.02.2006])

[175] namentlich China, Hongkong, die Philippinen, Malaysia, Japan, Thailand und Neuseeland

	Gesetzgebung			Internationale Kooperationen	Behörden und Organisationen[a]
	Spam	Phishing	Viren		
Deutschland	✓	(✓)[b]	✓[c]	CNSA[d], LAP[e], ITU, OECD, SpotSpam, ASEM[f]	eco, BMWi, BMELV, BNA; auch vzbv und WBZ
USA	✓	(✓)[b]	✓[c]	LAP, MoUs, ITU, OECD	FTC; auch DoJ, DoC, DoHS
China	✓	k.A.	k.A.	LAP, MoU mit mehreren Unternehmen, ASEM[f], ITU	ISC, MII
Süd-Korea	✓	k.A.	k.A.	ITU, ASEM[f], LAP, MoUs	KISA, KCPB, KFTC
Russland	—	(✓)[b]	✓[c]	ITU[g], OECD[g], LAP[g]	Anti-Spam-Projekt von Unesco IFAP; auch MITC
Australien	✓	(✓)[b]	✓[c]	MoUs, z.B. Seoul-Melbourne Agreement, LAP, ITU, OECD	ACMA, ACCC; auch DCITA, AHTCC

Legende: (nicht aufgeführte Abkürzungen wurden in den vorangehenden Kapiteln bereits erläutert)
ACCC: Australian Competition and Consumer Commission
ACMA: Australian Communications and Media Authority
AHTCC: Australian High Tech Crime Centre
BNA: Bundesnetzagentur
DCITA: Department of Communications, Information Technology and the Arts
DoC: Department of Commerce
DoHS: Department of Homeland Security
DoJ: Department of Justice
KCPB: Korea Consumer Protection Board
KFTC: Korea Fair Trade Commission
MII: Ministry of Information Industry
MITC: Ministry of Information Technologies and Communications
MoU: Memorandum of Understanding

[a] Es werden nicht alle Einrichtungen der einzelnen Staaten aufgeführt, sondern nur die für die internationale Betrachtung relevanten.
[b] Die Betrugshandlung selbst kann verfolgt werden, nicht jedoch das Verschicken von Phishing-Emails.
[c] im Rahmen allgemeiner Rechtsbestimmungen bzgl. Computerkriminalität
[d] rein europäisches Netzwerk
[e] noch nicht unterzeichnet
[f] nur europäische und asiatische Teilnehmer
[g] derzeit noch keine behördliche Beteiligung

Tabelle 4.1: Übersicht über Rechtslage und Aktivitäten der betrachteten Staaten

Union nicht aufgeführt. Stattdessen wurde die Bundesrepublik aufgenommen, um so einen Vergleich der deutschen Maßnahmen mit denen anderer Staaten zu ermöglichen.

4.4 Internationale Kooperationen

Wie dargelegt wurde, ist Spam kein nationales Problem – und somit auch nicht national zu bekämpfen. Aus diesem Grund spielen internationale Kooperationen eine wesentliche Rolle. Neben bi- und multilateralen Vereinbarungen zählen hierzu auch Initiativen internationaler Organisationen wie der *Organisation für wirtschaftliche Zusammenarbeit und Entwicklung*[176] (OECD) oder der *Internationalen Fernmeldeunion*[177] (ITU). Im Bereich der multilateralen Bemühungen sind insbesondere die Arbeit der Europäischen Union[178] sowie der *London Action Plan* hervorzuheben.

4.4.1 Bi- und multilaterale Vereinbarungen

Um dem internationalen Charakter von Spam gerecht zu werden, haben viele Staaten begonnen, durch bi- und multilaterale Vereinbarungen vor allem den Austausch von Informationen über Spam und damit zusammenhängende Phänomene voranzutreiben. Aufgrund der rasch voranschreitenden weiteren internationalen Vernetzung können an dieser Stelle nicht alle Vereinbarungen angeführt werden. Daher sollen nur einige für die Bundesrepublik wesentliche Abkommen erläutert werden.[179]

Wie bereits in Kapitel 4.3.1 erläutert, wurde vom Europäischen Parlament bereits Mitte 2002 die Richtlinie 2002/58/EG (2002) verabschiedet, die sich unter anderen mit dem Schutz vor Spam beschäftigt. Während die Umsetzung in nationales Recht mittlerweile nahezu abgeschlossen ist,[180] wurden auch rein praktische Anstrengungen unternommen, um das Problem zu bekämpfen. Ein wesentlicher Schritt war hierbei die Gründung des *Kontaktnetzes der Behörden zur Spambekämpfung* (contact network of spam-enforcing authorities, CNSA) Anfang 2004. Das CNSA, dem bisher 19 Behörden und Organisationen aus 16 EU-Ländern[181] angeschlos-

[176] Informationen zur Arbeit der OECD in diesem Bereich finden sich online unter http://www.oecd.org/department/0,2688,en_2649_22555297_1_1_1_1_1,00.html [18.02.2006]

[177] Informationen zur Arbeit der ITU finden sich online unter http://www.itu.int/osg/spu/spam/index.phtml [18.02.2006]

[178] Vgl. Kapitel 4.3.1

[179] Einen mehr oder weniger aktuellen und umfassenden Überblick bietet z.B. die OECD unter http://www.itu.int/osg/spu/spam/intcoop.html [18.02.2006].

[180] Vgl. KOM (2004)

[181] Die deutschen Kontaktstellen sind derzeit der eco sowie für Rufnummern-Spam die Bundesnetzagentur; das BMWi beteiligt sich ebenfalls an dieser Initiative (Vgl. Website des BMWi unter http://www.bmwi.de/BMWi/Navigation/Technologie-und-Innovation/Informationsgesellschaft/spam,did=72988.html [18.02.2006]).

sen sind, soll die Zusammenarbeit und den Informationsaustausch[182] zwischen den nationalen Anti-Spam- Einrichtungen verbessern.[183] Auf diese Weise soll ein europaweites Vorgehen gegen innerhalb der EU operierende Spammer gestärkt werden. In näherer Zukunft sollen die derzeitigen Ergebnisse durch eine gemeinsam mit dem *London Action Plan*[184] erarbeitete Vereinbarung über den grenzüberschreitenden Informationsaustausch und gerichtliche Verfolgung ergänzt werden.[185] Die genannte Vereinbarung wurde bereits durch mehrere EU-Mitgliedsstaaten und die USA eingesetzt.

Einen ähnlichen Ansatz verfolgt das von der EU-Kommission im Rahmen des *Safety Internet Action Plans* unterstützte und im September 2005 gestartete SpotSpam[186]-Projekt. In Form einer europäischen Spambox sollen Beschwerden über Spammer aus verschiedenen Ländern zentral gesammelt werden – wobei Daten nationaler Spambox-Projekte und Hotlines auf diese Weise auf europäischer Ebene zusammengeführt werden sollen.[187] SpotSpam wird durch den Verband der deutschen Internetwirtschaft *eco* koordiniert. Die *Naukowa i Akademicka Siec Komputerowa* (NASK), die Registrierungsstelle für die polnische Länderdomain .pl, betreut die technische Umsetzung. Neben der Europäischen Union wird das Projekt durch Microsoft gefördert. Des Weiteren ist z.Z. die Teilnahme des französische Spambox-Projektes *Signal-Spam*[188] sowie der britischen *Anti-Spam Working Group* des *Department of Trade and Industry* geplant.[189] Das Projekt befindet sich noch in der Vorbereitungsphase; es werden Entwürfe der geplanten Memoranden sowie weitere Vorgehensweisen bezüglich der Spam-Datenbank erarbeitet.

Im Gegensatz zu den auf die EU beschränkten genannten Initiativen arbeiten im im Oktober 2004 gestarteten *London Action Plan* (LAP) mittlerweile über 30 öffentliche und private Institutionen zusammen, u.a. auch die *Korean Information Security Agency* (KISA) und die *Internet Society of China* (ISC). Deutschland wird auf den Treffen neben dem eco meist durch die Bundesnetzagentur und das Verbraucherministerium (BMELV) vertreten; diese oder andere deutsche Behörden haben den LAP im Gegensatz zum eco jedoch noch nicht unterzeichnet.

[182] Hierzu zählt vor allem auch der Austausch von Beschwerden über Spam, die bei den entsprechenden nationalen Stellen eingehen.

[183] Vgl. CNSA (2004) sowie Pressemitteilung der Europäischen Kommission vom 07.02.2005: „Europäische Länder wollen Spam gemeinsam bekämpfen“ (online unter http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/146&language=DE [18.02.2006]).

[184] Vgl. weiter hinten in diesem Kapitel

[185] Soweit nicht anderes gekennzeichnet, entstammen die hier und im Folgenden getroffenen Aussagen über die CNSA einer Email von Wout de Natris, dem derzeitigen Koordinator des CNSA. Die Email ist bei Bedarf beim Autor einzusehen.

[186] SpotSpam steht für *Selfregulatory Plan on Tackling Spam* und findet sich im Internet unter http://www.spotspam.net/ [18.02.2006]

[187] Vgl. http://europa.eu.int/information_society/activities/sip/projects/self_regulation/SpotSpam/index_en.htm [18.02.2006]

[188] online unter http://www.signal-spam.fr/ [18.02.2006]

[189] Die genannten Informationen stammen aus einem Telefonat des Autors mit Sven Karge, dem Projektmanager der Anti-Spam Task Force des eco, am 16.01.2006.

Ebenso wie die CNSA auf europäischer Basis soll der LAP die internationale Kommunikation bei der Bekämpfung von Spam – ausdrücklich nicht beschränkt auf UCE – stärken. Neben der Kommunikation der verschiedenen nationalen Behörden zählt der LAP hierzu jedoch auch explizit die Zusammenarbeit mit Repräsentanten der Privatwirtschaft. Ebenso sollen legislative und exekutive Anti-Spam-Maßnahmen der mitarbeitenden Staaten diskutiert und unterstützt werden.[190]

Eine weitere Zusammenarbeit wurde Anfang 2005 auch im Rahmen der eCommerce-Konferenz der *Asian European Meetings* (ASEM) vereinbart. In einer gemeinsamen Erklärung kamen die 25 europäischen und 13 asiatischen ASEM-Mitgliedsländer überein, in Zukunft verstärkt bei der Bekämpfung von Spam zusammenzuarbeiten. Hierzu zählen neben legislativen und exekutiven Maßnahmen auch technische Maßnahmen, Unterstützung von Selbstregulierung durch die Industrie sowie Partnerschaften zwischen den Regierungen und der Internet-Gemeinschaft. Neben der Bekämpfung von Spam auf nationaler Ebene wurde der internationalen Arbeit, insbesondere auch zwischen ASEM und anderen Organisationen wie der EU oder der OECD Spam Task Force[191], ein besonderer Stellenwert eingeräumt.[192]

4.4.2 Aktivitäten der OECD

Neben den genannten Abkommen und Vereinbarungen arbeiten auch andere internationale Organisationen aktiv im Bereich der Spam-Bekämpfung. Die Anti-Spam Task Force der *Organisation für wirtschaftliche Zusammenarbeit und Entwicklung* (OECD) bietet seit Ende September 2004 mit dem *Anti-Spam Toolkit*[193] eine Sammlung von Ressourcen und Informationen zu Anti-Spam-Aktivitäten und -Lösungen auf internationaler Ebene. Es befindet sich in andauernder Entwicklung und besteht aus den folgenden acht Bausteinen[194]:

1. Anti-Spam Regulierung
2. Internationale Durchsetzung und Kooperation
3. Industrie-getriebene Lösungen gegen Spam
4. Anti-Spam Technologien
5. Aufklärung und Steigerung des Problembewusstseins
6. Kooperative Partnerschaften gegen Spam
7. Spam-Messung
8. Kontakt zu Nicht-OECD-Staaten

[190] Vgl. *The London Action Plan On International Spam Enforcement Cooperation* vom Oktober 2004 (online unter http://www.londonactionplan.org/?q=node/1 [18.02.2006])
[191] Vgl. Kapitel 4.4.2
[192] Vgl. Pressemitteilung der ASEM vom 01.03.2005: „Asian and European countries agree to work together to defeat the spam criminals at ASEM London conference“ (online unter http://www.asemec-london.org/media/march2/AsianEurope.doc [18.02.2006])
[193] online verfügbar unter http://www.oecd.org/sti/spam/ bzw. http://www.oecd-antispam.org/ [18.02.2006]
[194] Vgl. OECD (2005)

Teil 1 bietet ein Hilfsmittel für die Entwicklung und Überprüfung von Strategien von Anti-Spam-Gesetzen und -Vorschriften. Insbesondere bei der Entwicklung soll dieser Teil durch die Hervorhebung eines „best practices"-Ansatzes den interessierten Staaten ermöglichen, aus den Erfahrungen anderer einen Nutzen zu ziehen. Ebenso bietet er auch Ländern ein wichtiges Mittel zur Verbesserung bzw. zum Aufbau grenzüberschreitender Rahmenbedingungen. Der zweite Teil beinhaltet primär Kontaktinformationen und eine Momentaufnahme der rechtlichen Rahmenbedingungen in Bezug auf Spam sowohl von OECD- als auch von Nicht-OECD-Staaten. Weiterhin bietet der dritte Teil eine Bestandsaufnahme von von der Wirtschaft ausgehenden Lösungen und Partnerschaften gegen Spam, während der vierte Teil einen Überblick über derzeit aktuelle technologische Maßnahmen gegen Spam und verwandte Phänomene wie Viren und Spyware beinhaltet.

Teil 5 ist gedacht als Sammlung von Publikationen in einer Vielzahl von Sprachen, die sich mit der Weiterbildung sowie der Steigerung des Problembewusstseins von Konsumenten, ISPs, Regierungsorganisationen sowie der Wirtschaft beschäftigen. Im sechsten Teil sollen effiziente Modelle und Methodiken für kooperative Abmachungen vor allem zwischen Regierungen und Wirtschaft herausgearbeitet werden. Neben diesen wesentlichen Teilen spielt ebenso die Messung des Spam-Aufkommens und damit die Möglichkeit der Beobachtung der Spam-Evolution (Teil 7) sowie die Kontaktaufnahme und Zusammenarbeit mit Nicht-OECD-Staaten eine Rolle. Für letzteres wird vor allem auf die entsprechenden Stellen der ITU[195] als Schlüsselstellen hingewiesen.

Von deutscher Seite arbeitet der eco, das BMWI und das BMELV in diesem Bereich mit der OECD zusammen. Neben dem Anti-Spam Toolkit arbeitet die OECD und ihre Mitgliedsländer z.Z. des Weiteren an Empfehlungen für die grenzüberschreitende Verfolgung von Spammern. Ebenso befindet sich ein Überblick über den derzeitigen technischen Status Quo in Arbeit. Neben der Kooperation auf staatlicher Ebene beschäftigt sich die OECD in Zusammenarbeit mit Unternehmen und Unternehmensinitiativen mit der Erstellung von „best practices"-Richtlinien für ISPs, die ebenfalls in Kürze[196] veröffentlicht werden sollen. Mit diesen Richtlinien versucht die OECD, die durch eine große Anzahl verschiedener Organisationen erstellten „best practices" zu vereinen.

Während das Anti-Spam Toolkit sich anfangs lediglich mit UCE beschäftigen sollte, wurde im Laufe der Arbeit die Bedrohung durch mobilen Spam per SMS oder MMS, aber auch durch Phishing und Viren, immer relevanter. Aus diesem Grund ist eine Erweiterung des Toolkits inklusive der „best practices" für ISPs auf die Bereiche „Phishing", „Malware" sowie „allgemeine Sicherheitsprobleme" bereits vorgesehen. [197]

[195] Vgl. Kapitel 4.4.3

[196] Stand: 17.01.2006

[197] Vorangegangene Informationen stammen aus einem Telefonat des Autors mit Claudia Sarrocco (Abteilung für Informations-, Computer- und Kommunikationspolitik, OECD) am 18.01.2006.

4.4.3 Aktivitäten der ITU

Wie im vorangegangenen Kapitel angedeutet, beschäftigt sich auch die *Internationale Fernmeldeunion* (International Telecommunication Union, ITU) mit dem Thema „Spam“. Ähnlich dem Anti-Spam Toolkit der OECD bietet sie einen umfassenden öffentlich zugänglichen Überblick über sämtliche Aspekte der Spam-Bekämpfung auf ihrer Website[198]. Neben dieser Informationssammlung unterstützt die ITU Maßnahmen zur internationalen Kooperation, zur Bildung von harmonisierten internationalen Rahmenbedingungen und zum Austausch von Informationen und „best practices“. Im Rahmen ihrer Informationssammlung führt die ITU eine regelmäßig aktualisierte Bestandsaufnahme der Anti-Spam-Gesetzgebung auf weltweiter Ebene durch.

Des Weiteren veranstaltete die ITU – neben weiteren virtuellen und echten Konferenzen – im Rahmen des *world summit on the information society* (WSIS) im Sommer 2004 eine Konferenz zum Thema „Spam-Bekämpfung“[199] sowie im Sommer 2005 zum Thema „Cybersecurity“[200]. Letztere beschäftigte sich ebenfalls mit dem Thema „Spam“. Neben diesen Aktivitäten arbeitet die ITU an einen informellen Netzwerk von Behörden und politischen Entscheidungsträgern, die im Bereich „Anti-Spam“ arbeiten.

4.5 NGOs und ähnliche Initiativen

Ein Großteil der im Anti-Spam-Bereich aktiven Non-Governmental Organisations (NGOs) ist im besonderen in der technischen Bekämpfung von Spam – z.B. durch das Erstellen und Warten von Blacklists[201] – involviert. Ein Teil der Initiativen ist jedoch auch oder primär auf einer politischen Ebene aktiv gegen Spam. Hierzu zählen insbesondere die *International Coalition Against Unsolicited Commercial Email* (iCAUCE) mit ihren regionalen Unterorganisationen sowie *Spamhaus*.

Spamhaus betreibt und erstellt verschiedene Blacklists sowie das bereits erwähnte *Register of Known Spam Operations* (ROKSO), eine Auflistung der weltweit aktivsten bekannten Spammer und Spam-Gruppen. Des Weiteren arbeitet Spamhaus lobbyistisch in verschiedenen Staaten und Gremien für eine effiziente Anti-Spam-Gesetzgebung.

iCAUCE entstand aus der US-amerikanischen CAUCE und ist die Dachorganisation der verschiedenen regionalen CAUCE-Gruppen. Diese bieten keine technischen Maßnah-

[198] http://www.itu.int/osg/spu/spam/ [18.02.2006]
[199] Informationen dazu finden sich online unter http://www.itu.int/osg/spu/spam/background.html [18.02.2006]
[200] Informationen dazu finden sich online unter http://www.itu.int/osg/spu/cybersecurity/index.phtml [18.02.2006]
[201] Vgl. Kapitel 3.4.1

men gegen Spam an, sondern verstehen sich als Lobbyisten für eine effiziente Anti-UCE-Gesetzgebung in ihrem jeweiligen „Zuständigkeitsbereich“. Mittlerweile besteht iCAUCE aus fünf Mitgliedsorganisationen[202] sowie einer Vielzahl regionaler Kommitees in über zwanzig Staaten. Ein wesentlicher Punkt, für den sich iCAUCE einsetzt, ist das Opt-In-Verfahren. Nach Ansicht der Organisation ist ein Anti-Spam-Gesetz nur dann sinnvoll, wenn es dieses Marketing-Verfahren als einzig gültiges zulässt. Sowohl die australische als auch die europäische Gruppe hat massiv auf die seit 2002 in Europa[203] bzw. 2003 in Australien[204] geltenden Anti-UCE-Richtlinien hingearbeitet.

Im Gegensatz zu diesen Initiativen, die sich primär mit UCE auseinandersetzen, beschäftigt sich die *Anti-Phishing Working Group* (APWG) vor allem mit Betrug und Identitätsdiebstahl in Zusammenhang mit Phishing, Pharming und ähnlichen Phänomenen. Die APWG besteht aus mittlerweile über 2000 Mitgliedern, von den über 1300 Unternehmen und Behörden, insbesondere auch Strafverfolgungsbehörden, aus aller Welt sind. Sie versteht sich vor allem als Forum „*to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs, and share information and best practices for eliminating the problem*“[205].

4.6 Initiativen der Wirtschaft

Neben politischen Organisationen und NGOs spielt auch die Wirtschaft eine wesentliche Rolle bei der Bekämpfung von Spam – einerseits im Falle von Mailprovidern durch die Umsetzung technischer Maßnahmen wie Filter o.ä., andererseits aber auch durch die Unterstützung politischer und legislativer Initiativen. Ebenso wichtig ist die Arbeit der Mailprovider als Betroffene bei der rechtlichen Verfolgung von Spammern.

Eine aktive Rolle in diesem Bereich spielt bereits seit mehreren Jahren die Firma *Microsoft*, die neben der Software-Entwicklung auch mit *Hotmail* als Mailprovider aktiv ist. Neben der permanenten Verbesserung der technischen Maßnahmen für ihre Kunden arbeitet Microsoft dabei auch in internationalen Initiativen und Organisationen mit.

Das Unternehmen engagiert sich ebenso bei der Ermittlung und rechtlichen Verfolgung von Spammern. Neben einer dreistelligen Anzahl an eröffneten Verfahren in den USA – teilweise gegen ermittelte Spammer, großteils jedoch auch gegen „John Doe“, also unbekannt – wurden zwischen 2003 und 2005 dreizehn[206] Verfahren unter Verantwortung von Microsoft EMEA[207]

[202] Diese arbeiten in den USA, in der Europäischen Union, Australien, Indien und Kanada.
[203] Vgl. Kapitel 4.3.1
[204] Vgl. Kapitel 4.3.6
[205] Auszug aus http://www.antiphishing.org/membership.html [18.02.2006]
[206] Vgl. Le Toquin (2005)
[207] EMEA steht für „Europe, Middle East, Africa“. Microsoft EMEA ist der für diese Gebiete zuständige Zweig des Unternehmens.

geführt. Auch in Deutschland hat das Unternehmen bereits mehrere Verfahren gegen deutsche Spammer geführt.[208]

Im diesem Rahmen arbeitet Microsoft auf deutscher Ebene mit der Anti-Spam Task Force des eco zusammen. Ebenfalls zusammen mit dem eco wurde das europäische SpotSpam-Projekt gestartet, das die europaweite Rechtsverfolgung von Spammern vereinfachen soll.[209]

Darüber hinaus war Microsoft eines des führenden Gründungsmitglieder der *Global Infrastructure Alliance for Internet Safety* (GIAIS)[210], einer Allianz von Internet-Providern[211] mit dem Ziel der verbesserten Sicherheit ihrer Kunden im Internet. Das wesentliche Arbeitsgebiet der Allianz ist die Erarbeitung und Diskussion technischer Maßnahmen gegen sowie die Nutzer-Information über Malware, Spam und Phishing. So entwickelte die Allianz bereits kurz nach der Gründung Anfang 2004 Programme zur Entfernung der damals aktuellen Viren „MyDoom“ und „W32.Blaster“.[212]

Andere Großunternehmen aus der IT-Branche beschäftigen sich ebenfalls im internationalen Rahmen mit der Spam-Bekämpfung. *AOL* und *Yahoo!* kooperieren bereits seit 2003 mit Microsoft, um auf technischem, rechtsverfolgendem und nutzer-aufklärendem Wege Spam Einhalt zu gebieten.[213]

Ebenso gehören die genannten Unternehmen (neben weiteren) der *Anti-Spam Technical Alliance* an, die 2004 einen umfangreichen Vorschlag zu technischen Maßnahmen gegen Spam[214] vorstellte.

Microsoft, AOL, Yahoo! und eBay verfassten des Weiteren 2004 zusammen mit der *Internet Society of China* (ISC) ein Memorandum[215], das eine nähere Zusammenarbeit bei der Bekämpfung von Spam vereinbart.

Viele weitere Unternehmen arbeiten indirekt über die Aktivitäten ihrer jeweiligen Verbandsorganisationen bzw. vor allem im Falle von Mailprovidern und ähnlichen Unternehmen

[208] Vgl. z.B. Pressemitteilungen von Microsoft vom 26.06.2005: „Unterlassungs- und Schadenersatzklage gegen Urheber von Spam-Emails “ (online unter http://www.microsoft.com/germany/presseservice/detail.mspx?id=531390 [18.02.2006]) sowie vom 01.03.2004: „Microsoft geht gerichtlich gegen Spammer vor“ (online unter http://www.microsoft.com/germany/presseservice/detail.mspx?id=531054 [18.02.2006])

[209] Vgl. zu SpotSpam auch Kapitel 4.4.1

[210] Informationen zur GIAIS finden sich online unter http://www.microsoft.com/serviceproviders/giais/ [18.02.2006]

[211] namentlich British Telecom, Chunghwa Telecom, Cox Communications, EarthLink, Korea Telecom, MSN, NTT Communications, Planet Internet, Shaw Communications, TDC, T-Online, TeliaSonera, Tiscali, United Online, Wanadoo und Telecom New Zealand

[212] Vgl. Heise News vom 25.02.2004: „Microsoft geht Sicherheitsallianz mit Providern ein“ (online unter http://www.heise.de/newsticker/meldung/44981 [18.02.2006])

[213] Vgl. Pressemitteilung von Microsoft vom 05.05.2003: „AOL, Microsoft und Yahoo! kooperieren im Kampf gegen Spam-Emails“ (online unter http://www.microsoft.com/germany/presseservice/detail.mspx?id=530899 [18.02.2006])

[214] ASTA (2004)

[215] online verfügbar unter http://www.itu.int/osg/spu/spam/legislation/china-mou-en.html [18.02.2006]

auf technischem Wege daran, Spam zu verringern. So gibt es bereits in vielen Ländern von Seiten von ISPs bzw. deren Verbänden *Codes of Conduct*, die neben anderen Verhaltensrichtlinien auch solche zum Verhalten gegenüber Spam festlegen.[216]

Eine weitere unternehmensbasierte Initiative ist die *Message Anti-Abuse Working Group* (MAAWG), die durch das US-amerikanische Unternehmen *OpenWave* Anfang 2004 initiiert wurde und mittlerweile von einer Vielzahl internationaler IT-Unternehmen getragen wird. Die MAAWG versteht sich nach Eigenaussage als globale Organisation mit dem Anspruch, den Missbrauch von Messaging-Systemen ganzheitlich zu betrachten. Hierzu zählt nicht nur Spam per Email, sondern ebenso Spam per SMS, MMS, Instant Messaging genauso wie Phishing und Viren. Die Arbeit der MAAWG betrifft drei Gebiete: Ein wesentlicher Teil ist die Zusammenarbeit der Mitglieder beim Austausch von „best practices“, der Entwicklung von Verhaltensrichtlinien für ISPs und der Entwicklung eines vertrauenswürdigen Netzwerkes zwischen diesen. Neben diesem Aspekt der Zusammenarbeit beschäftigt sich die MAAWG mit den technologischen Aspekten des Problems und der Diskussion über grundlegende technologische Rahmenbedingungen[217]. Als drittes Arbeitsgebiet der MAAWG wird die Zusammenarbeit mit politischen Entscheidungsträgern genannt.

Bezüglich Phishing ist die bereits im vorgehenden Kapitel erläuterte *Anti-Phishing Working Group* die weltweit derzeit größte und aktivste primär von wirtschaftlicher Seite getragene Organisation.

4.7 Zusammenfassung

Dieses Kapitel bietet ein Überblick über die Anti-Spam-Maßnahmen der Bundesrepublik sowie weiterer Staaten, aus denen große Teile des weltweiten Spams verschickt werden oder die – im Falle von Australien – beispielhaft versuchen, Spam einzudämmen. Hierzu wurden die derzeitigen rechtlichen Gegebenheiten der Länder, aber auch deren internationale Kooperationen betrachtet. Des weiteren wurden einige, vor allem auf politischer Ebene aktive NGOs und Unternehmen vorgestellt. Anhand zweier Schaubilder sollen die verschiedenen Verbindungen zwischen Staaten, Initiativen und Vereinbarungen – einerseits auf internationaler, andererseits aber auch deutscher Ebene – verdeutlicht werden. Hierbei soll es sich nicht um einen umfassenden Überblick handeln. Es werden lediglich die im vorangegangenen Kapitel untersuchten Organisationen und Staaten behandelt.

Auf internationaler Ebene wurden die Europäische Union, Süd-Korea, China, die USA, Australien und Russland betrachtet. In Abbildung 4.1 wurde jedoch auf die Aufnahme der

[216] Einige (europäische) Beispiele finden sich unter http://www.euroispa.org/25.htm [18.02.2006]
[217] z.B. Sender ID oder SPF (vgl. hierzu Kapitel 3.4.2)

EU verzichtet, da diese zwar an einigen Initiativen partizipiert und diese teilweise auch initiiert, ihre Mitgliedsstaaten jedoch in vielen Fällen natürlich auch unabhängig agieren. Für die im Folgenden zu erarbeitende deutsche Strategie gegen Spam ist es daher sinnvoller, Deutschlands Einbettung in die verschiedenen weltweiten Kooperationen zu betrachten.

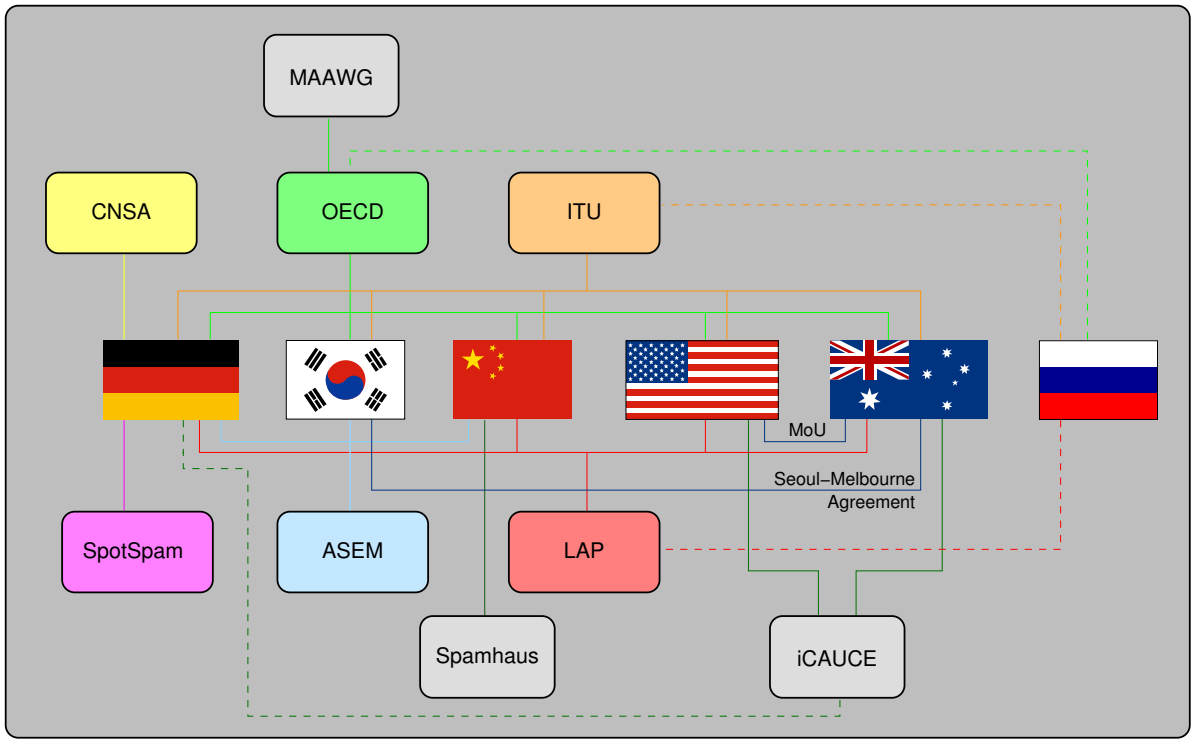

Abbildung 4.1: Überblick über internationale Kooperationen

Das *Kontaktnetz der Behörden zur Spambekämpfung* (contact network of spam enforcing authorities, CNSA) und SpotSpam[218] sind zwei rein europäische Projekte, die daher auch keine Verbindungen zu den anderen genannten Staaten aufweisen. Ähnlich verhält es sich mit den Vereinbarungen im Rahmen der *Asian European Meetings* (ASEM)[219], an denen lediglich asiatische und europäische Staaten teilnehmen. Der *London Action Plan*[220] dagegen ist eine weltweite internationale Kooperation, an der sämtliche betrachtete Staaten teilnehmen. OECD[221] und ITU[222] sind internationale Organisationen, an deren Anti-Spam-Bemühungen, ähnlich dem LAP, viele Staaten partizipieren. In den drei letztgenannten Kooperationen bildet Russland einen Sonderfall, da derzeit[223] noch keine russische Behörde diese unterstützt. Lediglich

[218] Vgl. für beide Kapitel 4.4.1
[219] Vgl. ebd.
[220] Vgl. ebd.
[221] Vgl. Kapitel 4.4.2
[222] Vgl. Kapitel 4.4.3
[223] Stand: Januar 2006

das Anti-Spam-Projekt des Unesco „Information for All"-Programmes nimmt sowohl an den Initiativen von ITU und OECD als auch bei den Treffen des LAP teil.[224]

Neben diesen wichtigen Zusammenschlüssen gibt es noch eine Vielzahl von bi-, aber auch multilateralen Memoranden. Hierzu zählen in Zusammenhang mit den vorgestellten Staaten ein Memorandum zwischen den USA, Großbritannien und Australien sowie das Seoul-Melbourne Agreement, das ursprünglich zwischen Australien und Süd-Korea geschlossen und mittlerweile auf weitere Staaten der Region ausgedehnt wurde.

Weiterhin sind verschiedene NGOs[225], aber auch Unternehmens-Gruppierungen[226] in den genannten Kooperationen aktiv. Auf NGO-Ebene sind hier vor allem Spamhaus und iCAUCE zu nennen, während auf Unternehmens-Ebene die *Messaging Anti-Abuse Working Group* (MAAWG) eine wesentliche Rolle in der technischen, aber auch politischen Anti-Spam-Arbeit spielt. Spamhaus betreibt eine Unterorganisation in China, die sich für eine Verbesserung des chinesischen „Spam-Problems" einsetzt. iCAUCE besteht aus fünf Mitgliedern, darunter dem europäischen Ableger EuroCAUCE, der auch ein regionales Kommittee in Deutschland besitzt.

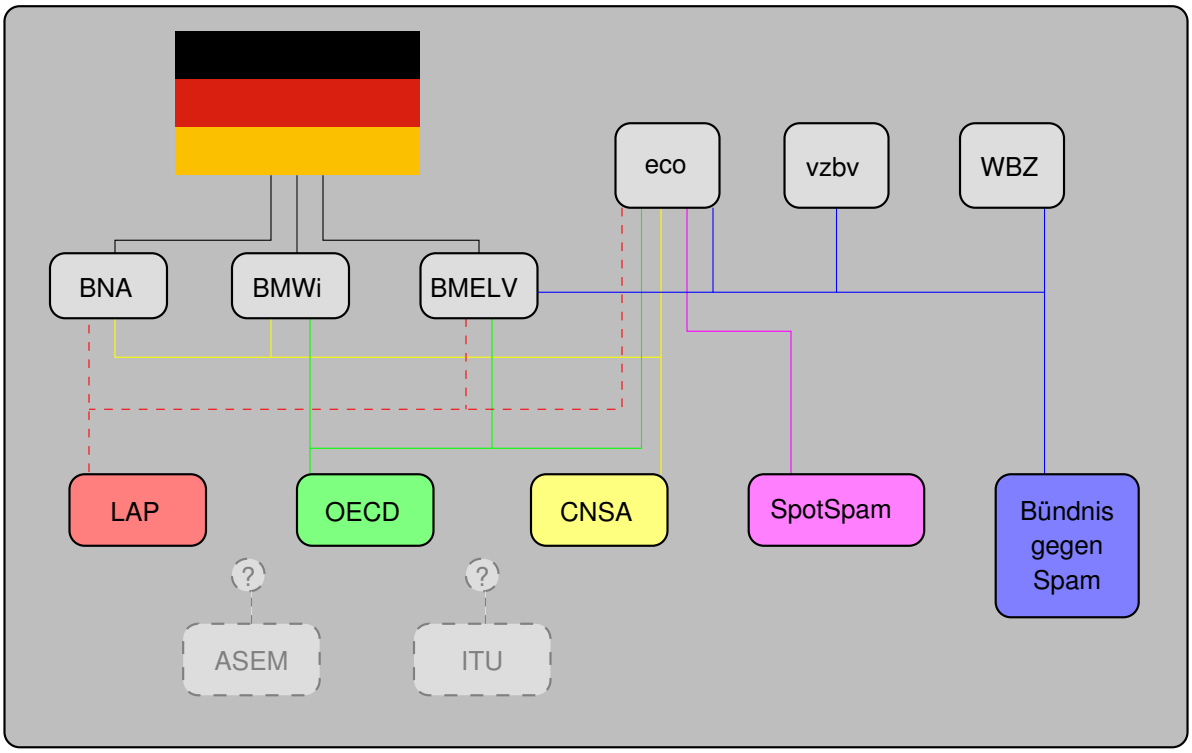

Abbildung 4.2: Überblick über die Kooperationen deutscher Organisationen und Behörden

[224] Vgl. Kapitel 4.3.5
[225] Vgl. zu näheren Informationen Kapitel 4.5
[226] Vgl. zu näheren Informationen Kapitel 4.6

Auf deutscher Ebene[227] gibt es eine große Anzahl an Behörden und Institutionen, die sich sowohl national als auch international mit dem Problem „Spam“ beschäftigen. Eine wesentliche Rolle spielt der eco, der an nahezu allen genannten Initiativen beteiligt ist und auf europäischer Ebene das Spambox-Projekt *SpotSpam* initiiert hat. Initiiert durch das BMELV und getragen von diesem, dem eco, dem vzbv und der WBZ, ist das *Bündnis gegen Spam* die größte nationale Initiative gegen Spam.[228] Neben diesem Projekt nimmmt das BMELV auf internationaler Ebene an den Treffen der OECD und des LAPs[229] teil.

Neben dem BMELV sind weiterhin das BMWi sowie die Bundesnetzagentur in die Anti-Spam-Arbeit der Bundesrepublik involviert. Beide Behörden engagieren sich im CNSA. Weiterhin vertritt das BMWI – neben dem BMELV – die Bundesrepublik in der *Task Force on Spam* der OECD. Die Bundesnetzagentur nimmt, neben eco und BMELV an den Treffen des LAPs teil – hat diesen jedoch, wie bereits erwähnt, ebenfalls noch nicht offiziell signiert. An den entsprechenden Treffen der ASEM sowie der ITU teilnehmende Institutionen konnten nicht recherchiert werden.

[227] Vgl. Abbildung 4.2
[228] Vgl. Kapitel 4.2
[229] Dieser wurde jedoch bisher weder vom BMELV noch von einer anderen deutschen Behörde signiert.

5 Erläuterung und Bewertung möglicher Maßnahmen

In den vorangehenden Kapiteln wurde ein Überblick über mögliche technische Maßnahmen, aber auch über die derzeitige Rechtslage sowie politische Strategien der Bundesrepublik und weiterer Staaten und Organisationen vermittelt. In diesem Kapitel sollen nun diese Voraussetzungen genutzt werden, um mögliche Maßnahmen und Strategien zu erarbeiten. In diesem Rahmen sollen dabei gleichberechtigt auch bereits umgesetzte Maßnahmen (z.B. die Aktivitäten des *Bündnisses gegen Spam*[230]) behandelt werden.

Technische Maßnahmen sollen dabei nur in Teilen betrachtet werden, da diese, sofern sie grundlegende Änderungen am derzeitigen Email-System beinhalten, nicht in einem nationalen Alleingang umgesetzt werden können. Stattdessen sind hier andere Organisationen wie die *Internet Engineering Task Force* (IETF), die ITU o.ä. gefordert. Neben möglichen regulatorischen Maßnahmen spielen auf nationaler Ebene vor allem auch die Verfolgung, die Aufklärung der Betroffenen sowie die internationale Kooperation eine wesentliche Rolle und sollen hier im Gegensatz zu technischen Maßnahmen vertieft behandelt werden.

5.1 Regulierung

Trotz des bereits bestehenden Verbotes von UCE auf Basis des UWG gibt es weiterhin Empfehlungen, diese, aber auch Spam i.A., durch weitere regulatorische Maßnahmen zu bekämpfen. Der im Februar 2005 vorgestellte Entwurf eines Anti-Spam-Gesetzes (DS 15/4835 2005) durch die rot-grüne Koalition, der vom März 2005 stammende Antrag „Spam effektiv bekämpfen“ (DS 15/2655 2004) der CDU/CSU-Fraktion sowie die im Zuge der Diskussion eingeholten Expertenmeinungen[231] machten deutlich, dass hier noch erheblicher Diskussionsbedarf besteht – insbesondere hinsichtlich der Frage der Strafbarkeit der einzelnen Arten von Spam, vornehmlich UCE und Phishing-Emails. Diese Diskussion muss jedoch unter Juristen geführt werden. Daher soll im Folgenden lediglich auf einige grundsätzliche Fragen eingegangen werden, ohne ins (juristische) Detail zu gehen.

[230] Vgl. Kapitel 4.2

[231] u.a. vom eco, von AOL, T-Online und dem vzbv; vgl. DS 15 (9) und Protokoll 15/89 (2005)

Hervorzuheben ist, dass es im Bereich des Phishing offensichtlich weiterer regulatorischer Maßnahmen bedarf. Zur Zeit ist nach herrschender Meinung das Versenden von Phishing-Emails als reine Vorbereitungshandlung straflos. Lediglich Einzelmeinungen[232] halten Phishing bereits jetzt für strafbar. Die Verfolgung von Phishern ist also offenbar erst nach einem Vermögensverlust nach §263a StGB („Computerbetrug") möglich; aufgrund der häufig aus dem Ausland und nahezu anonym arbeitenden Phisher ist das verlorene Geld nun aber meist unwiederbringlich verloren.[233] Das eindeutige Verbot von Phishing-Emails und dem Erstellen gefälschter Unternehmens-Websites[234] könnte – zumindest bei deutschen bzw. europäischen Tätern – die Arbeit der Strafverfolgungsbehörden vereinfachen und einem finanziellen Schaden der Opfer wirksam vorbeugen.

Wesentlich umstrittener ist die Frage, inwiefern eine weitere rechtliche Regulierung – auf ordnungs- oder strafrechtlicher Ebene – zur Bekämpfung von UCE sinnvoll ist. Die derzeitige Rechtslage[235] erlaubt es bereits jetzt u.a. Wettbewerbern und Verbraucherschutzorganisationen, gegen diese Form von Spam auf Basis des UWG vorzugehen. Kritiker bemängeln jedoch die durch dieses Gesetz bedingte Einschränkung der Klageberechtigten auf wenige Beteiligte.[236] Die unmittelbar Betroffenen – Unternehmen, Verbraucher und Provider – können derzeit nicht eigenständig gegen Spam vorgehen, sondern müssen sich an die entsprechenden Verbände wenden. Eine Umsetzung mit einem eigenen Klagerecht für die Betroffenen könnte hier Abhilfe schaffen.

Auch angesichts der immer weiter voranschreitenden Professionalisierung der Spammer ist es zudem überlegenswert, diese nicht nur zivilrechtlich durch das UWG, sondern mit den Mitteln des Ordnungswidrigkeiten- oder Strafrechts zu verfolgen. Nach derzeitigem Stand sind in ersterem Fall – also bei der Einordnung als Ordnungswidrigkeit – die Ordnungsbehörden der Städte und Gemeinden zuständig für die Verfolgung. Aufgrund mangelnder Kompetenz und Personals könnten sie diese Aufgabe jedoch kaum bewältigen. Auch aus diesem Grunde wäre die Schaffung einer zentralen Einrichtung, deren Verantwortlichkeit gesetzlich festgelegt wird und die über eine hohe technische Kompetenz und Sanktionsmöglichkeiten[237] verfügt, angeraten. Für eine Einordnung im Strafrecht sprechen – neben der bereits erwähnten fortschreitenden Professionalisierung der Täter – vor allem auch der daraus folgende Zugriff auf die durch den Versand entstehenden Nutzdaten, vor allem der IP-Adressen, da dieser nach geltender Rechtslage auf Straftaten beschränkt ist. Ebenfalls ermöglicht das Strafrecht bei ausländischen Spammern (insbesondere im Nicht-EU-Ausland) internationale Rechtshil-

[232] z.B. Weber (2004)
[233] Vgl. zu Phishing auch Kapitel 4.1.4
[234] ohne den Umweg über z.B. das Markenrecht
[235] Vgl. Kapitel 4.1.1
[236] Vgl. z.B. Stellungnahme des Heise Zeitschriften Verlages zum Entwurf des Anti-Spam-Gesetzes der rot-grünen Koalition (DS 15-9-1864 2005)
[237] Vgl. Kapitel 5.4

fe. Eine zentrale Verfolgungsstelle ist auch in diesem Fall notwendig, um eine effektive Arbeit zu ermöglichen.

Ein weiterer in die Diskussion eingebrachter Ansatz ist die Ausweitung des UWG bzw. einer zu erarbeitenden Straftat oder Ordnungswidrigkeit auf die Beworbenen, die Nutznießer der Werbung. Diese sind gleichzeitig natürlich auch diejenigen, die den finanziellen Anreiz zum Spamming geben. Insbesondere aufgrund der dadurch eröffneten Missbrauchsmöglichkeiten[238] scheint dieser Ansatz jedoch wenig praktikabel.

Für ISPs und andere Betreiber von Mailservern, deren Infrastruktur massiv durch Spam herausgefordert wird, aber auch für Unternehmen ist das direkte Blockieren von Spam- und Viren-Emails, bevor sie in das eigene Netz eingeliefert werden, eine der effizientesten Möglichkeiten, um die durch Spam verursachten Kosten zu minimieren. Gleichzeitig ist dieses Verfahren jedoch rechtlich nicht unumstritten. Neben dem Blockieren ist das Filtern, also z.B. das Markieren einer Email mit dem Hinweis „Achtung Spam!“, ebenso beliebt wie strittig. Nach herrschender Meinung ist das Blockieren von eindeutigen Viren-Emails rechtlich unproblematisch, da in diesem Fall das Interesse am Erhalt der IT-Infrastruktur Vorrang vor dem Interesse des Nutzers an der Zustellung der Email hat. Im Falle des Blockierens oder Filterns von Spam sprechen jedoch datenschutz- und telekommunikations-, aber vor allem auch strafrechtliche Vorschriften[239] für ein Verbot dieser Maßnahmen. Es ist für Unternehmen und ISPs zwar bereits heute vergleichsweise einfach, durch vorab eingeholte Einwilligungen der Nutzer diese Maßnahmen zu legitimieren. Nichtsdestotrotz wäre hier eine gesetzgeberische Klarstellung für die pauschale Einwilligung über AGBs und Betriebsvereinbarungen wünschenswert.

In einigen Staaten ist im Rahmen des jeweiligen Anti-Spam-Gesetzes vorgeschrieben, dass UCE mit einem Label in der Betreffzeile beschriftet werden muss, z.B. mit einem vorangestellten „ADV:“[240]. Dies ermöglicht den Nutzern, unerwünschte Werbung leicht zu filtern. Obwohl die Grundidee auf den ersten Blick sinnvoll erscheint, ist sie genauer betrachtet kontraproduktiv. Offensichtlich ließe sich Werbung auf diese Weise leicht filtern. Es ist jedoch zu beachten, welche Art der Werbung dies betrifft. Ein Spammer, der trotz bereits bestehender Verbote seine Emails verschickt, wird kaum ein solches *Label* verwenden. Im Gegensatz dazu werden seriöse Direktwerber, die sich bereits an geltende Gesetze wie z.B. das Opt-In-Gebot in Deutschland halten, massiv behindert. Eine derartige Vorschrift schadet also diesen Anbietern, ohne auch nur ansatzweise die illegitime Form der Werbung bzw. deren Verursacher zu bekämpfen.

[238] So könnten Unternehmen oder Personen Spam-Emails verschicken, die z.B. einen missliebigen Konkurrenten „bewerben“ und diesen dann danach anzeigen.

[239] §88 TKG „Fernmeldegeheimnis“, §206 StGB „Verletzung des Post- oder Fernmeldegeheimnisses“, §303a StGB „Datenveränderung“

[240] als Abkürzung für das englische *advertisement* (zu deutsch *Werbung*)

In jedem Falle einer Gesetzes-Überarbeitung oder -Neuschaffung in diesem Bereich muss jedoch beachtet werden, dass sich Spam heutzutage mitnichten auf Emails beschränkt. Neben Spamming in Weblogs, Gästebüchern und dem so genannten *Spamdexing*[241] muss hier vor allem auch Spam über SMS/MMS, Instant Messenger wie ICQ sowie – insbesondere in Hinblick auf die steigende Verbreitung der Internet-Telefonie – *Voice over IP*[242] beachtet werden. Eine zukunftsweisende Anti-Spam-Gesetzgebung muss diese Phänomene integrieren. Wie bereits in der Einführung angedeutet, übersteigt eine solche umfassende Betrachtung jedoch den Rahmen dieser Arbeit, so dass sie hier – trotz ihrer Relevanz – nicht detaillierter betrachtet werden sollen.

5.2 Aufklärung

Die bereits erwähnte Aufklärung und Steigerung des Problembewusstseins seitens der Nutzer, aber auch der Direktwerber und Unternehmen, ist ein weiterer äußerst wichtiger Schritt im Rahmen einer umfassenden Strategie zur Bekämpfung von Spam. Letztere benötigen klare Informationen, in welcher Weise sie gesetzeskonform werben dürfen. Hierzu zählen auch Informationen zur rechtmäßigen Sammlung persönlicher Daten wie Email-Adressen o.ä..

Vor allem aber Nutzer müssen – insbesondere bei einer steigenden Verbreitung von Phishing-Attacken[243] und Botnets/Zombie-PCs – informiert werden über Gefahren und Risiken des Internets sowie über sinnvolle Schutzmaßnahmen. Eine solche Aufklärungskampagne, die im Rahmen einer Website Verbraucher für das Thema sensibilisieren und informieren will, wird derzeit – durch das BMELV finanziert – vom vzbv entwickelt und soll im März 2006 online gehen. Eine enge Zusammenarbeit bzw. ein konzentriertes Vorgehen mit Unternehmen, insbesondere ISPs, Mailprovidern und Betriebssystem-Entwicklern, aber auch mit Verbraucherschutzverbänden kann in diesem Zusammenhang zu einer weiten Verbreitung der Informationen führen und ist daher ratsam. Neben der Aufklärung über die Gefahren des Internets zählt zu einer solchen Kampagne auch die Aufklärung über Rechte der Nutzer in Bezug auf Werbung. Hierunter fallen vor allem auch praktische Schritte des Nutzers bei der Konfrontation mit Spam – z.B. die vorhandenen Beschwerdestellen, Spamboxes etc.

Eine zentrale Internet-Anlaufstelle für den Nutzer, die über Spam, Viren, aber auch z.B. über Rechte gegenüber Spammern informiert, ist zu fördern. In der Praxis bietet sich hierfür neben dem BMELV vor allem das BSI an, das mit seiner Website „BSI für Bürger“[244] bereits

[241] Darunter versteht man Suchmaschinen-Spamming, also die Manipulation von Suchmaschinen, damit eigene, mit dem vom Nutzer gesuchten Begriff nicht in Zusammenhang stehende Informationen auf den vordersten Plätzen erscheinen.

[242] so genannter *Spit* (Spam over Internet- Telephony)

[243] die zudem immer professioneller und spezialisierter werden.

[244] online unter http://www.bsi-fuer-buerger.de/ [18.02.2006]

erfolgreich in diesem Gebiet arbeitet. Ebenso ist die geplante Kampagne des BMELV[245] zu unterstützen. Um Doppelarbeit zu vermeiden und für den Nutzer eindeutige Ansprechpartner zu vermitteln, wäre in diesem Bereich eine engere Zusammenarbeit im Rahmen eines gemeinsamen Projektes ratsam. Ebenfalls ratsam ist es, nicht nur im Rahmen eines Internet-Angebotes, sondern auch offline, z.B. in Zusammenarbeit mit den Verbraucherschutzverbänden sowie der Wirtschaft, zu arbeiten.

Neben der reinen Aufklärung über Spam, Viren etc. kann auch die Stärkung von digitalen Signaturen und Verschlüsselung ein weiteres Mittel sein. Insbesondere die Verwendung digitaler Signaturen z.B. bei der Kommunikation zwischen Bank und Kunde kann maßgeblich dazu beitragen, Phishing zu erschweren. Ebenso kann die verstärkte Aufklärung über Sinn, Zweck und Funktion von verschlüsselten Verbindungen im Internet[246] das Problembewusstsein des Nutzer stärken. Viele der betroffenen Unternehmen, vor allem Banken, aber auch Webmailprovider und Firmen wie eBay, bieten zu diesem Thema bereits ausführliche Informationen auf ihren Websites. Auch hier könnte eine zentrale Anlaufstelle im Internet jedoch helfen, die Nutzer für dieses Thema zu sensibilisieren.

Im Gegensatz zu verschlüsselten Internetverbindungen hat sich die digitale Signatur derzeit noch nicht durchgesetzt. Hier besteht massiver Aufklärungs- und Förderungsbedarf. Trotz der Vertrauensstärkung, die derartige Signaturen gerade in der Kommunikation von Unternehmen mit ihren Kunden bietet, muss aber auch erwähnt werden, dass es sich hierbei mitnichten um ein Allheilmittel gegen Phisher handelt. Diese können problemlos auch eigene Zertifikate erstellen, die auf den ersten Blick nicht als Fälschung zu entlarven sind.[247]

Ebenfalls sinnvoll ist die Aufklärung der Nutzer über Möglichkeiten zur Vermeidung von Spam – z.B. durch Verwendung spezieller Email-Adressen bei Anmeldung in Foren o.ä. – sowie über Produkte und Dienste, die diesem Zweck dienen. Hierunter sind vor allem Filtersoftware, Antiviren-Programme und Anti-Spyware-Programme zu verstehen.

5.3 Selbstregulierung

Nicht nur die Politik, sondern natürlich auch die Wirtschaft selbst spielt eine entscheidende Rolle bei der Bekämpfung von Spam. Neben den bereits genannten Aktivitäten wie z.B. den Projekten des eco gibt es verschiedene Ansätze, um auf dieser Ebene zu arbeiten. Ein wesentlicher Aspekt ist die Selbstregulierung der verschiedenen „Player“. Hierzu zählen vor allem ISPs und Mailprovider, aber genauso auch seriöse Direktwerber.

[245] s.o.
[246] z.B. die verschlüsselte Verbindung zu den Online-Banking-Seiten einer Bank
[247] Vgl. hierzu auch Kapitel 5.5

„Codes of Conduct“, also Verhaltensrichtlinien, die auf der jeweiligen Verbandsebene erarbeitet werden, vereinbaren dabei für die Mitglieds-Unternehmen eindeutige Regeln in Bezug auf Spam. Bei ISPs z.B. kann es sich hierbei um Regeln handeln, wie mit ein- oder ausgehendem Spam umgegangen wird. Insbesondere bei ausgehendem Spam – auch durch Open Proxies[248] oder Open Relays[249] – können hier Maßnahmen wie die Aufforderung des Kunden zur sofortigen Problembehebung bis hin zur Sperrung des entsprechenden Kunden vereinbart werden.

Direktwerber können durch solche Verhaltensrichtlinien eine Selbstverpflichtung vereinbaren, sich – unabhängig von der Rechtslage – an seriöse Werbemaßnahmen zu halten. Hierunter kann z.B. die Verpflichtung zu Double-Opt-In o.ä. gehören. In diesem Rahmen können auch Gütesiegel vergeben werden, die für den Nutzer als Beleg für die Seriösität des werbenden Unternehmens dienen können. Ein solches Projekt ist die 2004 gestartete *Certified Senders Alliance*[250] des *Deutschen Direktmarketing Verbandes* und des eco. Dieses Projekt verpflichtet teilnehmende Direktwerber zur Erfüllung verschiedener Kriterien, um ein seriöses Marketing zu gewährleisten. Gleichzeitig werden sie in eine zentrale Positivliste aufgenommen, die eine Filterung der zulässigen Werbe-Emails seitens der ISPs verhindert.

Direkt für den Nutzer ersichtlich arbeiten Unternehmen und Organisationen, die „echte“ Gütesiegel vergeben.[251] Sie geben ihren Kunden die Möglichkeit, auf Websites oder in Emails ein Siegel in Form einer Grafik zu verwenden, dass belegt, dass sie sich an die Bestimmungen des Anbieters halten. Ebenso sind die teilnehmenden Unternehmen auf der Website des Gütesiegel-Anbieters zu finden. Es bleibt jedoch dem Nutzer überlassen, ob er dem jeweiligen Gütesiegel vertraut – bei der großen Anzahl der Anbieter ist diese Entscheidung oftmals nicht leicht. Aus diesem Grunde haben sich unter der Federführung der *Initiative D21*[252] mehrere deutsche Anbieter von Gütesiegeln zusammengefunden, um einheitliche Standards zu definieren.[253] Dem Monitoring Board, das die Einhaltung der Siegel und Richtlinien überprüft, gehören u.a. Mitarbeiter des vzbv, des BMELV und des BfD an.

Ähnliche Formen der Selbstregulierung wie bei ISPs und Direktwerbern wäre in Hinsicht auf das Phishing auch in anderen Bereichen wünschenswert. So könnte eine Vereinbarung unter Banken oder eCommerce-Anbietern, in der diese sich zum Einsatz von signierten Emails

[248] Vgl. Kapitel 3.3.3
[249] Vgl. Kapitel 3.3.2
[250] online unter http://www.eco.de/servlet/PB/menu/1446034_l1/index.html [18.02.2006]
[251] z.B. das deutsche Unternehmen *Trusted Shops* (online unter http://www.trustedshops.de/ [18.02.2006]) oder die US-amerikanische Organisation *TRUSTe* (online unter http://www.truste.org/ [18.02.2006])
[252] Die *Initiative D21* ist eine public-private-partnership, deren Ziel nach Eigenaussage die Stimulierung des wirtschaftlichen Wachstums Deutschlands vor allem in Bezug auf die Informations- und Kommunikationstechnologien ist; die Initiative ist online erreichbar unter http://www.initiatived21.de/ [18.02.2006].
[253] Die jeweiligen Gütesiegel sind dabei nicht auf Spam beschränkt, sondern betreffen auch andere Gebiete wie z.B. Datenschutz etc.; die Initiative ist online zu erreichen unter http://www.internet-guetesiegel.de [18.02.2006].

u.ä. verpflichten, helfen, Phishing zumindest zu erschweren. Der Einsatz der Wirtschaft kann hier als noch wichtiger als im Falle von UCE betrachtet werden, da sie durchaus auch als Opfer dieser Attacken gelten muss. Verringertes Vertrauen der Nutzer in eCommerce und Online-Banking kann durch Phishing wesentlich stärker hervorgerufen werden als durch beispielsweise UCE.

5.4 Vollstreckung und internationale Zusammenarbeit

Spam ist kein nationales Phänomen. Neben einem effektiven Vorgehen auf nationaler Ebene sind daher internationale Kooperationen unabdingbar. Bereits heute arbeiten verschiedene deutsche Behörden und Verbände, allen voran der eco, in verschiedenen internationalen Organisationen und Projekten, darunter der OECD, der ITU und dem London Action Plan.[254] Im Vergleich zu anderen Staaten, z.B. Australien[255] und den USA[256], aber auch Großbritannien, kann diese Arbeit jedoch noch deutlich intensiviert werden. So wurde z.B. der London Action Plan trotz der regen Teilnahme deutscher Behörden bisher lediglich vom eco unterzeichnet.

Bi- und multilaterale Vereinbarungen und Memoranden können ebenfalls helfen, mit ausgewählten Staaten enger zusammenzuarbeiten, um einen direkteren Informationsaustausch zu gewährleisten. Des Weiteren kann auf diesem Wege nicht nur die effektive Gesetzgebung anderer Staaten gefördert werden, sondern vor allem auch deren Durchsetzung mittels polizeilicher und gerichtlicher Zusammenarbeit.

Wie bereits erläutert, beschäftigen sich die meisten Initiativen jedoch primär mit UCE. Phishing und seine Derivate kommen nur langsam in den Fokus der bestehenden Organisationen. Gleichwohl ist abzusehen, dass sich – im Zuge der fortschreitenden weltweiten Kriminalisierung und Verfolgung von UCE sowie der zunehmenden Professionalisierung der Täter – diese lukrative (und z.Z. relativ sichere) Art von Spam deutlich weiter verbreiten und verbessern wird. Bereits heute sind manche Phishing-Emails und -Websites nicht mehr von den Originalen zu unterscheiden. Gerade in diesem Bereich könnte die Bundesrepublik derzeit durch den Aufbau internationaler Netzwerke mit einem Fokus auf Phishing eine Vorreiter-Rolle spielen. Ein jetzt beginnendes rigoroses Vorgehen gegen Phisher kann u.U. verhindern, dass sich dieses Problem weiter ausbreitet und den Rang von UCE erreicht.

Wie bereits in Kapitel 4.2 erläutert, gibt es auf nationaler Ebene verschiedene Behörden und Organisationen, die sich mit dem Thema „Spam“ beschäftigen. Im wesentlichen sind dies das BMELV, das BMWi, die Bundesnetzagentur sowie der eco. Letzterer ist als Mitbegründer des

[254] Vgl. zu diesen Projekten Kapitel 4.4.1
[255] Vgl. Kapitel 4.3.6
[256] Vgl. Kapitel 4.3.2

deutschen *Bündnisses gegen Spam*, als Initiator des europäischen Spambox-Projektes, als Teilnehmer an sämtlichen wichtigen internationalen Projekten z.Z. einer der aktivsten Akteure im Kampf gegen Spam.[257]

Die Tatsache, dass es sich beim eco „lediglich" um einen privatwirtschaftlichen Verband und nicht um eine öffentliche Behörde handelt, führt trotz der großen Bemühungen und des Einsatzes desselben u.U. jedoch zu Problemen. So ist im Rahmen des CNSA[258] ein Austausch vertraulicher Informationen z.B. mit der niederländischen Regulierungsbehörde *OPTA* schwierig bis unmöglich, da das niederländische OPTA-Gesetz einen Austausch mit Organisationen des privaten Sektors nicht erlaubt.[259]

Eine zentrale Anlaufstelle auf Bundesebene kann helfen, diese möglichen Probleme zu beheben. Zur Zeit beschäftigen sich sowohl auf nationaler als auch auf internationaler Ebene diverse Behörden mit der Spam-Bekämpfung. Eine Zentralisierung an dieser Stelle kann Kräfte bündeln und Doppelarbeit verhindern. Wie Abbildung 4.2 auf Seite 59 zu entnehmen ist, arbeiten sowohl das BMELV als auch das BMWi und die Bundesnetzagentur im Bereich „Spam". Dazu kommen für bestimmte Teilbereiche das *Bundeskriminalamt* (BKA), das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) und weitere.

Als zentrale Kontrollinstanz käme vor allem die Bundesnetzagentur, aber auch das BSI in Frage. Ebenso wäre die Einrichtung einer Schwerpunktstaatsanwaltschaft möglich. Die Bundesnetzagentur hat ihre Handlungsfähigkeit und Effizienz bereits bei der Bekämpfung des Dialer-Problems gezeigt. Um eine durch die ausgebauten Verantwortlichkeiten entstehende „Superbehörde" zu vermeiden, wäre jedoch – aufgrund des verfügbaren technischen Sachverstands – ebenso das BSI zu empfehlen. Im Gegensatz zu einer Schwerpunktstaatsanwaltschaft haben beide Behörden den Vorteil, dass sie nicht nur auf der gerichtlichen Ebene, sondern vor allem auch auf technischer, aufklärender und internationaler Ebene Erfahrung und Kompetenzen besitzen. In jedem Fall müssen die bereits existierenden Initiativen, allen voran die Spam-Beschwerdestelle von eco und vzbv[260], in die Arbeit eingebunden werden. Eine erfolgreiche Arbeit einer neu geschaffenen Behörde ist auch abhängig von der engen Zusammenarbeit mit und Einbindung von diesen u.a. durch die Wirtschaft bereits eingeleiteten Projekten, da hier bereits maßgebliche Erfahrungen in der Bekämpfung von Spam gesammelt werden konnten.

Neben den genannten Maßnahmen spielt die rigorose polizeiliche und gerichtliche Verfolgung der Spammer eine wesentliche, wenn nicht sogar ausschlaggebende Rolle bei der Bekämpfung von Spam. Um diese zu ermöglichen, müssen verschiedene Rahmenbedingungen

[257] Vgl. dazu auch Abbildung 4.2 auf Seite 59.
[258] Vgl. Kapitel 4.4.1
[259] Diese Aussage basiert auf Emails zwischen dem Autor und Wout de Natris, dem CNSA-Koordinator der OPTA, vom Januar 2006. Die Emails können bei Interesse beim Autor eingesehen werden.
[260] Vgl. Kapitel 4.2

erfüllt werden. Hierzu zählt neben rechtlichen Aspekten vor allem die Schaffung einer schlagkräftigen Organisation sowie eine starke Zusammenarbeit zwischen dieser, den betroffenen Unternehmen und innerhalb internationaler Kooperationen.

In Deutschland spielen derzeit – abgesehen von den beteiligten Behörden – eco, vzbv und WBZ im Rahmen des Bündnisses gegen Spam eine entscheidende Rolle. Ersterer arbeitet zudem massiv in internationalen Kooperationen sowie maßgeblich am europäischen Spambox-Projekt SpotSpam. Derzeit dürfte damit der eco der wichtigste Partner in der aktiven Spam-Bekämpfung in der Bundesrepublik sein. Im Rahmen der Beschwerdestelle gegen Spam, einem Teilprojekt des Bündnisses gegen Spam, wurden nach Eigenaussagen bereits eine Vielzahl an strafbewehrten Unterlassungserklärungen an identifizierte deutsche Spammer gesandt, die zumeist unterzeichnet wurden. In jedem Fall traten über die identifizierten Spammer – auch bei Nicht-Unterzeichnung – keine Beschwerden mehr auf.[261]

Eine Verfolgung ausländischer Spammer – die den größten Teil deutschen Spams ausmachen – ist jedoch ungleich schwieriger. Während europäische Spammer im Rahmen von europäischen Projekten wie z.B. der CNSA durch die entsprechenden Staaten weiter verfolgt werden können, ist die Verfolgung von Spammern aus Nicht-EU-Ländern derzeit kaum möglich – unabhängig davon, ob diese sich durch deutsche Unterlassungserklärungen beeindrucken ließen.

Eine Verschärfung des Verbotes von Spam z.B. durch das Strafrecht, aber auch die Einrichtung einer zentralen staatlichen Behörde zur Spam- Bekämpfung können hier helfen. Insbesondere die Verstärkung der internationalen, vor allem auch bilateralen Vereinbarungen durch die Bundesrepublik sind jedoch unabdingbar.

Neben den genannten spielen weitere Aspekte eine entscheidende Rolle bei der erfolgreichen Bekämpfung von Spam. Hierzu zählt zum Beispiel die Einrichtung von „Spamboxes“, also zentralen Spam-Datenbanken, an die betroffene Nutzer die erhaltenen Spam-Nachrichten weiterleiten können. Der eco hat für diesen Zweck das europaweite SpotSpam-Projekt[262] gestartet, das eine solche Spambox aufbaut und pflegt. Eine zentrale Sammlung von aktuellen Spam-Nachrichten hat vielerlei Nutzen. Zuerst einmal erlaubt sie es – ausreichende Nutzung vorausgesetzt –, einen Überblick über aktuelle Trends und Arten von Spam zu erlangen. Auf diese Weise wird es ermöglicht, gezielt und frühzeitig Spam einzuordnen und Prioritäten für die weitere Verfolgung zuzuweisen. Ein Überblick darüber, welche Arten von Spam weniger und welche mehr werden, ist immanent wichtig, um gegebenenfalls weitere legislative und exekutive Maßnahmen zu erarbeiten und die Effektivität der aktuellen Maßnahmen zu überprüfen. Eine europaweite Spambox, wie von SpotSpam geplant, ist hierbei einer nationalen Lösung vorzuziehen.

[261] Vgl. Ermert (2005)
[262] Vgl. Kapitel 4.4.1

Des Weiteren vereinfacht der Aufbau einer solchen (multilateralen) Datenbank auch die internationale Zusammenarbeit bei der Verfolgung der Täter. Durch die gesammelten Daten können wesentlich leichter maßgebliche Spammer – oder zumindest die auffälligsten Spam-Wellen – identifiziert und weiter verfolgt werden. Ebenfalls können die aus den Daten erarbeiteten Informationen dazu dienen, im Rahmen von an Nutzer, aber auch an Direktwerber gerichtete Aufklärungsmaßnahmen zielgerichteter informieren zu können. Nebenbei erlauben Spamboxes es den Nutzern selbst, einen aktiven Schritt zur Bekämpfung von Spam zu tun und damit die Durchsetzung der existenten Rechtsvorschriften zu erleichtern.

5.5 Technik

Eine wesentliche Rolle bei der Spam-Bekämpfung spielt neben regulatorischen Aspekten auch das Email-System[263] selbst. Eine grundsätzliche Änderung des derzeitigen, auf SMTP basierenden Email-Systems ist auf nationaler Ebene jedoch aufgrund der Internationalität des Internets nicht möglich. Eine solche Lösung, die „das Übel an der Wurzel packt", muss auf internationaler Ebene, z.B. durch die *Internet Engineering Task Force* (IETF) erarbeitet werden. Auf diese Aspekte soll daher – aufgrund der nationalen Ausrichtung dieser Arbeit – im Folgenden nicht eingegangen werden.

Nichtsdestotrotz können auch auf nationaler Ebene technische Maßnahmen ergriffen werden, die die Verbreitung von Spam verhindern bzw. die Belästigung des Nutzers minimieren. Eine in jedem Fall sinnvolle Maßnahme ist das Filtern von Emails. Nutzer, aber auch ISPs und Mailprovider können auf diese Weise relativ wirksam und automatisiert oftmals einen Großteil der Spam-Emails aussortieren.[264]

Es ist an dieser Stelle jedoch anzumerken, dass die Filterung durch Provider, insbesondere aber auch durch Unternehmen, rechtlich nicht unumstritten ist.[265] Neben dem Einsatz von Filtern auf eingehende Emails sollten diese grundsätzlich – im Falle von Providern und Unternehmen – auch ausgehende Emails „durchsehen", um bereits frühzeitig Spammer im eigenen Netzwerk erkennen zu können.

Das Blockieren unterscheidet sich insofern vom Filtern, als dass bei letzterem die Emails zwar gegebenenfalls mit einem Hinweis auf Spam markiert oder in einen gesonderten Ordner einsortiert werden. Trotzdem werden die Emails jedoch in jedem Fall zugestellt, so dass letztlich der Empfänger die Möglichkeit hat, auf *false positives* zu reagieren. Beim Blockieren

[263] Vgl. dazu Kapitel 3

[264] So filtert die Software des Mailproviders GMX nach Aussage des Unternehmens bis zu 98% des Spams aus; für Bayes-Filter (vgl. Kapitel 3.4.1) werden ähnliche Zahlen in der Literatur genannt.

[265] Vgl. Kapitel 5.1

hingegen wird die Email direkt am Mailserver – also vor Eingang in die Mailbox des Empfängers – abgewiesen und nicht zugestellt. Vorteilig ist diese Maßnahme vor allem bei eindeutig erkannten Viren-Emails o.ä., da so ohne Gefahr eines *false positives*[266] verhindert wird, dass der Nutzer die Email öffnet und so den enthaltenen Virus weiterverbreitet. UCE hingegen ist oftmals nicht eindeutig und fehlerfrei zu erkennen, so dass hier Filter das Mittel der Wahl ist. Das Blockieren von erkannten Spam-Emails ist, ebenso wie das Filtern, rechtlich nicht unumstritten. Gleichermaßen ist es aber – zumindest bei Einsatz für ausgehende Emails – deutlich effektiver, da die Spam-Email noch vor ihrem „Eintritt" ins Internet gestoppt wird und somit keine weiteren Mailserver belastet. In diesem Fall ist es ratsam, dem Absender eine Meldung über den Vorfall zukommen zu lassen. Auf diese Weise kann er entweder auf sein Fehlverhalten oder – im Falle eines Zombie-PCs – auf Sicherheitsprobleme seines Rechners aufmerksam gemacht werden. Filter werden mittlerweile von den meisten Mailprovidern angeboten.[267]

Authentifizierungs-Maßnahmen können an verschiedenen Punkten ansetzen. Direkt auf dem Mailserver setzen Verfahren wie Domainkeys, SPF oder SenderID[268] an. Auf diesem Wege lassen sich zumindest gefälschte Absender-Adressen verhindern. Die Standardisierung solcher Verfahren durch die IETF ist jedoch – u.a. aufgrund unklarer Patentansprüche – bisher gescheitert. Davon abgesehen ist weiterhin unbekannt, inwieweit diese Verfahren effektiv Spam verhindern, da Spammer sie auf verschiedene Weise (mehr oder weniger) leicht umgehen können.

Sinnvoller – und vor allem auch einfacher umsetzbar – ist die Verschlüsselung und/oder Signierung von Emails durch den Nutzer selbst. Mittels Verfahren wie S/MIME oder PGP[269] kann der Nutzer sowohl Emails verschlüsseln, so dass nur der Empfänger sie lesen kann, als auch – und das ist im Rahmen der Spam-Bekämpfung entscheidend – signieren, so dass der Empfänger die Identität des Absenders verifizieren kann. Insbesondere in Bezug auf Phishing können Unternehmen wie Banken etc. durch konsequente Signierung ihrer Emails das allzu leichte Fälschen durch Phisher erschweren. Es ist jedoch zu beachten, dass auch die Signierung kein „Allheilmittel" ist. Phisher können z.B. eigene Zertifikate erstellen, die – bei oberflächlicher Betrachtung – wie legitime Zertifikate wirken.

Verschlüsselung kann – sofern der Einsatz weit genug verbreitet ist – indirekt als Anti-Spam-Maßnahme verstanden werden. Insbesondere im Privatbereich kann die Verschlüsselung (bzw. Nicht-Verschlüsselung) bei konsequenter Verbreitung z.B. im Freundeskreis als deutliches Kriterium zur Spam-Filterung dienen. Bei einer weiteren Verbreitung erschwert Verschlüsselung in diesem Zusammenhang auch das Versenden von Spam-Emails, da der Spammer seine Emails nicht mehr an beliebige Empfänger verschicken kann, sondern zu-

[266] Legitime Emails, die fälschlicherweise als Spam deklariert werden
[267] Vgl. z.B. die Angebote von AOL, Yahoo!, Hotmail, Lycos, web.de, GMX und anderen
[268] Vgl. zu allen Kapitel 3.4.2
[269] Vgl. zu beiden Kapitel 3.4.2

sätzlich den jeweiligen Schlüssel des Empfängers benötigt. Es ist jedoch zu beachten, dass bei Betrachtung der vergangenen Spam-Bekämpfungs-Ansätze Spammer oftmals schnell reagiert haben, um die entsprechenden Maßnahmen zu umgehen. So ist es in diesem Falle möglich und wahrscheinlich, dass die Adress-Datenbanken der Spammer zusätzlich die (öffentlichen verfügbaren) Schlüssel der jeweiligen Empfänger enthalten, so dass – insbesondere bei Verwendung von Zombie-PCs – dieser Aspekt ins Leere läuft. Ebenso ist es ungewiss, inwieweit Durchschnitts-Nutzer überhaupt vom Einsatz von kryptographischer Software zu überzeugen sind.

Es bleibt zu sagen, dass die hier aufgeführten technischen Maßnahmen zwar helfen können, auf individueller Ebene mit dem existierenden Spam umzugehen, dass sie aber nicht an der Wurzel ansetzen. So haben die immer weiter entwickelten Filter bisher nicht etwa zu weniger Spam geführt, sondern zu mehr und vor allem trickreicherem, da Spammer versuchen, die durch Filter verbuchten Verluste durch eine größere Anzahl an Nachrichten oder kaschierte Inhalte[270] auszugleichen. Ein technischer Ansatz, der direkt an SMTP selbst ansetzt, ist somit langfristig unerlässlich.

5.6 zusammenfassender Überblick

Die Tabellen 5.1 und 5.2 fassen die vorangegangenen möglichen Maßnahmen noch einmal übersichtlich zusammen. Detailliertere Informationen sind den Kapiteln 5.1 bis 5.5 zu entnehmen. Um die jeweiligen Maßnahmen leicht einordnen zu können, beinhalten die Tabellen neben der entsprechenden Maßnahme die für diese sinnvoller- oder gezwungenerweise zuständige Behörde/Organisation sowie Vor- und Nachteile. Es ist zu beachten, dass den Tabellen aus Übersichtsgründen keine Wertung zu entnehmen ist. Diese wurde in den vorangehenden Abschnitten beschrieben. Des Weiteren werden die als sinnvoll erachteten Maßnahmen im folgenden Kapitel noch einmal erläutert.

[270] So schreiben viele Spammer mittlerweile z.B. nicht mehr „Viagra“, sondern beispielsweise „V*1*a*G*r*A“. Auf diese Weise können sehr viele Varianten gefunden werden, die ein menschlicher Leser leicht erkennen kann, eine Maschine jedoch nicht. Ebenso wird häufig die eigentliche Werbung in Form einer Grafik verschickt; der Email-Text besteht dann aus einer unverfänglichen Nachricht, die kein Filter als Spam deklariert.

	Maßnahme	zuständig	pro	contra
Regulierung	Verbot von Phishing-Emails und -Websites	Parlament	Verfolgung der Täter bereits auf Basis der Emails/Websites	—
	Verbot von UCE durch Ordnungswidrigkeiten- oder Strafrecht	Parlament	Ausweitung der Klageberechtigten auf alle Betroffenen[a]; Reaktion auf zunehmende Professionalisierung der Spammer; Strafrecht: Auswertung der Nutzdaten[b] möglich, internationale Rechtshilfe möglich; vor allem bei Aufbau einer zentralen Anti-Spam-Behörde sinnvoll	Verbot besteht bereits auf Basis des UWG; Ordnungswidrigkeitenrecht: grundsätzlich zuerst kommunale Ordnungsbehörden zuständig
	Ausweitung des UCE-Verbotes auf die Beworbenen/Nutznießer	Parlament	verantwortlich durch finanziellen Anreiz; u.U. durch verlinkte Websites leichter zu identifizieren	Missbrauch leicht möglich
	rechtliche Verfolgung von Zombie-PCs	Parlament	Verringerung des Zombie-Problems auf zumindest nationaler Ebene	kaum umsetzbar aufgrund der Menge; Kriminalisierung unbedarfter Nutzer; evtl. Verringerung des privaten Einsatzes von IT und somit widersprüchlich zur Förderung desselben; stattdessen Aufklärung der Nutzer über Gefahren
	Gebot zur Verwendung von Labels („ADV:“) bei kommerziellen Emails	Parlament	Erleichterung der Filterung von Email-Werbung	nur seriöse Werber sind betroffen, Spammer werden Labels nicht benutzen
	Rechtliche Klarstellung zu Filterung und Blocking durch Provider und Unternehmen	Parlament	Vereinfachung der Einverständniserklärung der Nutzer[c]	keine Notwendigkeit, da Einsatz bereits nach Bestätigung des Nutzers möglich
Aufklärung	Aufklärung der Direktwerber und Unternehmen	zuständige Behörde[d], Unternehmen, Verbände	Verringerung von „unbeabsichtigtem“ Spam	—
	Aufklärung der Nutzer	zuständige Behörde[d], Unternehmen, Verbände	unabdingbar in Bezug auf Gefahren des Internets; zentrale Anlaufstelle gewährleistet, dass Nutzer alle relevanten Informationen finden; Erweiterung des Problembewusstseins der Nutzer	—
	Unterstützung von Verschlüsselung und Signierung	zuständige Behörde[d], Unternehmen, Verbände	Vertrauenssteigerung der Nutzer in das Email-System; Erschwerung von Phishing	Akzeptanz zumindest von Verschlüsselung durch Nutzer ungewiß
	Aufklärung über die Verwendung von Schutz-Software	zuständige Behörde[d], Verbände, Unternehmen	Nicht nur Spam-relevant; zu geringe Verbreitung solcher Software derzeit	—
Selbstregulierung	Erarbeitung von Verhaltensrichtlinien durch ISPs	Provider, Verbände (eco)	einheitliche Richtlinien für zumindest deutsche und verbandsgebundene ISPs; sinnvoll aufgrund der nationalen Beschränkung nur für Maßnahmen gegen Spam-Emails, nicht gegen das Problem an sich	—
	Erarbeitung von Verhaltensrichtlinien durch Direktwerber	Direktwerber, Verbände (DDV)	Verminderung der Fälle von versehentlich verschicktem Spam; klare Richtlinien für seriöse Anbieter	unseriöse Direktwerber werden naturgemäß nicht angesprochen; nur deutsche Unternehmen sind angesprochen
	Vergabe von Gütesiegeln o.ä. an seriöse Direktwerber	zuständige Behörde[d], Verbände, Unternehmen	Steigerung des Vertrauens in Unternehmen durch Nutzer;	derzeit Verwirrung durch Vielzahl der Anbieter[e]

[a] v.a. auch internationale Unternehmen, die weltweit gerichtlich gegen Spam vorgehen
[b] z.B. IP-Adressen
[c] z.B. durch AGB oder allgemeine Betriebsbestimmungen
[d] sofern diese eingerichtet wird; ansonsten wie bisher BMELV, BMWi, BSI
[e] Diesem Problem wird bereits durch die *Initiative D21* entgegengewirkt.

Tabelle 5.1: Übersicht über mögliche Strategien zur Spam-Bekämpfung (Teil 1)

	Maßnahme	zuständig	pro	contra
Vollstreckung und internationale Zusammenarbeit	Einrichtung einer zentralen Behörde zur Spam-Bekämpfung[a]	Parlament	internationaler Informationsaustausch wird vereinfacht oder u.U. erst ermöglicht; zentraler Ansprechpartner für Nutzer und internationale Partner; Verhinderung von Doppelarbeit	derzeitige Arbeit des eco und der verschiedenen Behörden[b] ist effizient
	Einrichtung von Spamboxes	zuständige Behörde[d], eco	erlaubt Überblick über Spam-Trends; notwendig zur effektiven Verfolgung der Spammer; aktive Teilnahme der Nutzer/Betroffenen	relativ aufwändig zu pflegen
	Enge Zusammenarbeit mit der Wirtschaft	zuständige Behörde[d]	notwendig und unabdingbar für effektives Handeln, insbesondere aufgrund der starken Aktivität deutscher Unternehmen und Verbände wie dem eco	—
	Verstärkung der Arbeit in internationalen Kooperationen	zuständige Behörde[d]	Spam ist international; derzeit im Vergleich noch keine ausreichende Aktivität der Bundesverwaltung;	—
	Aufbau von bilateralen Abkommen	zuständige Behörde[d]	direkt und enge Zusammenarbeit mit ausgewählten, auch weniger weit entwickelten Staaten möglich	keine Vorteile gegenüber multilateralen Kooperationen
Technik	grundlegende Änderung der Email-Systems	IETF o.ä. Organisationen	sehr wirksam	national nicht umsetzbar; international mindestens langwierig, wenn nicht unmöglich
	Einführung von SPF o.ä.	IETF o.ä. Organisationen	Verhinderung gefälschter Absenderadressen	große Effektivität nur bei weltweiter Umsetzung; derzeit: offene Patentfragen; Umgehung durch Spammer leicht möglich; kein wirklicher Spam-Schutz
	Filterung von Spam-Emails	Provider, Nutzer	Verringerung der Belästigung des einzelnen Nutzers; derzeit nahezu alternativlos; mittlerweile unproblematische Umsetzung;	keine Verringerung der Mailserver-Belastung; Einsatz durch Provider nur mit Zustimmung des Empfängers
	Blocking von Spam-Emails	Provider	bei ausgehenden Emails: schnelles Erkennen von Spam-Wellen; keine Belastung weiterer Mailserver; bei eingehenden Emails: keine Belästigung des Nutzers	nur möglich bei z.B. Gefahr für das eigene Netz durch Viren o.ä., ansonsten Pflicht der Zustellung; nur einzusetzen bei Einverständnis des Empfängers
	Verschlüsselung von Emails (PGP, S/MIME)	Nutzer	Vertrauenssteigerung; Verschlüsselung derzeit für Spammer vermutlich zu aufwändig	keine „echte“Anti-Spam-Maßnahme[c]; derzeit zwei konkurrierende Systeme[d]; Akzeptanz durch Nutzer ungewiss
	Signierung von Emails (PGP, S/MIME)	Nutzer, Unternehmen	Vertrauenssteigerung in eCommerce und Online-Banking	Täuschung durch Erstellung eigener Zertifikate der Phisher möglich; derzeit zwei konkurrierende Systeme[e]

[a] Bundesnetzagentur oder BSI
[b] BMWi, BMELV, BSI, Bundesnetzagentur
[c] Voraussetzung: Der Empfang von legitimen unverschlüsselten Emails ist ausgeschlossen
[d] S/MIME und PGP
[e] S/MIME und PGP

Tabelle 5.2: Übersicht über mögliche Strategien zur Spam-Bekämpfung (Teil 2)

6 Empfohlene Maßnahmen

Wie bereits erläutert, kann eine effektive Strategie gegen Spam nur dann funktionieren, wenn von verschiedenen Ebenen aus gearbeitet wird. Im vorangegangenen Kapitel wurden verschiedene Maßnahmen erläutert und bewertet, so dass in diesem Kapitel nun eine umfassende Strategie gegen Spam erarbeitet werden kann. Hierbei ist unabdingbar, dass die verschiedenen Ebenen miteinander verknüpft werden, da die zu treffenden Maßnahmen nur im Zusammenspiel mit den jeweils anderen Maßnahmen ihre volle Wirkung entfalten können. So ist eine eine wirksame Verfolgung nur bei einer entsprechenden Gesetzeslage möglich. Gleichermaßen nutzt eine strenge Gesetzeslage jedoch ebenso wenig ohne die entsprechende Verfolgung. Es soll unterteilt werden in regulatorische, vor allem gesetzgeberische Maßnahmen, in ausführende bzw. vollstreckende Maßnahmen, in die Aufklärung der verschiedenen Akteure sowie in technische Maßnahmen, sofern sich diese auf nationaler Ebene umsetzen lassen.

Es ist des Weiteren unabdingbar, Spam nicht nur, wie gerade im juristischen Bereich oftmals geschehen, auf die Form der kommerziellen Werbe-Emails zu beschränken, sondern stattdessen sämtliche Formen von Spam zu betrachten. Insbesondere Phishing wird deutlich professioneller und tritt deutlich häufiger auf. Trotzdem wird dieser Bereich jedoch auch innerhalb der internationalen Initiativen bisher oftmals vernachlässigt. Hier kann Deutschland durch schnelle und effektive Maßnahmen sowie durch den Aufbau spezialisierter internationaler Initiativen eine Vorreiterrolle spielen.

Neben den hier – vor allem in Kapitel 2.2 – angeführten verschiedenen Arten von Email-Spam müssen jedoch auch die nicht per Email übertragenen Formen von Spam betrachtet werden. Durch die steigende Verbreitung von u.a. Instant Messaging Programmen, Internet-Telefonie und SMS/MMS bilden sich hier mittlerweile andere für Spammer interessante Tätigkeitsfelder aus. Eine zukunftsträchtige Strategie muss ebenso wie den Email-Spam auch diese Technologien beachten. Auf diese Weise, also durch ein frühzeitiges Problembewusstsein, kann u.U. verhindert werden, dass diese neueren Technologien dermaßen durch Spammer missbraucht werden, wie es das (nahezu zusammenbrechende) Email-System z.Z. erfährt. Im Rahmen dieser Arbeit kann jedoch nicht im Detail auf die anderen Technologien eingegangen werden. In vielen Fällen – vor allem in den nicht-technischen – können jedoch die hier betrachteten Maßnahmen relativ leicht auf diese abgebildet werden.

6.1 Regulierung

Mit der Umsetzung der EU-Richtlinie 2002/58/EG im UWG hat die Bundesrepublik bezüglich Spam einen Schritt nach vorn gemacht. Diese Richtlinie – und damit auch die UWG-Ergänzungen – beschäftigen sich jedoch lediglich mit UCE. Andere relevante Gebiete wie z.B. Viren werden zwar schon anderweitig verfolgt; insbesondere für den Bereich „Phishing“ ist die derzeitige Gesetzeslage jedoch nach herrschender Meinung nicht ausreichend.

Empfehlung 1: Bereits das Versenden von Phishing-Emails und das Erstellen von Phishing-Websites muss rechtlich eindeutig geregelt werden.

Phishing – ein (Computer-)Betrugsdelikt – ist bisher erst nach einem Vermögensverlust des Opfers verfolgbar. Das reine Versenden von Phishing-Emails sowie das Erstellen der entsprechenden Websites kann bisher – entgegen Einzelmeinungen — nicht bzw. nur auf Umwegen[271] verfolgt werden. Ein Verbot dieser Vorbereitungshandlungen kann massiv dabei helfen, insbesondere innerhalb Deutschlands agierende Phisher[272] zu verfolgen. Da bei Betrachtung der Entwicklung der Phishing-Techniken davon ausgegangen werden muss, dass diese Form des Betruges massiv zunimmt und vor allem in relativ kurzer Zeit deutlich schwerwiegender werden wird, ist ein schnelles Handeln vonnöten. Im Gegensatz zu UCE führt die Zunahme von Phishing zu einer massiven Verunsicherung der Nutzer in Bezug auf Online-Banking, eCommerce u.ä. Ein zeitnahes und rigoroses Verbot dieses Tatbestands ist demnach auch aus ökonomischen Gründen anzuraten.

Empfehlung 2: UCE sollte nicht nur durch das UWG, sondern auch auf Ebene des Ordnungswidrikeiten- oder Strafrechts sanktioniert werden.

Ähnliches gilt auch für UCE. Trotz des Verbotes unerwünschter kommerzieller Emails auf Basis des UWG kann eine Ausweitung in den Bereich des Ordnungswidrigkeiten- oder Strafrechts empfohlen werden. Hierfür sprechen mehrere Gründe. Derzeit besteht für Provider und andere betroffene Unternehmen kein eigenes Klagerecht gegen Spammer.[273] Die Unternehmen sind, wie auch die privaten Nutzer, gezwungen, über die entsprechenden klageberechtigten Verbände wie vzbv oder WBZ bzw. im Rahmen der von ihnen und dem eco getragenen Spam-Beschwerdestelle gegen Spammer vorzugehen. Ein eigenes Klagerecht gerade für große internationale Unternehmen wie Microsoft oder AOL, die weltweit aktiv

[271] Hierzu zählt z.B. die Verfolgung auf Basis des Markenrechts bei illegitimer Verwendung von Namen und Symbolen der betroffenen Unternehmen.

[272] Diese sind jedoch Studien nach deutlich in der Minderheit gegenüber Tätern aus anderen, vor allem auch Nicht-EU-Ländern.

[273] Es sei denn, das betroffene Unternehmen steht in einer Wettbewerbssituation zum Spammer, was bei den gängigen per Spam vermarkteten Produkten die Ausnahme sein dürfte.

gerichtlich gegen Spammer vorgehen, könnte hier für eine effektivere Verfolgung der Spammer sorgen.

Des Weiteren ist der internationale Austausch relevanter Informationen sowie die Rechtshilfe durch andere Staaten auf Basis des Zivilrechts oftmals nicht durchzusetzen. Bei einem weltweiten Blick auf die Spam-Gesetzgebung anderer Staaten wird deutlich, dass sich die Einordnung von UCE im Strafrecht mit hohen Geld- oder sogar Gefängnisstrafen durchsetzt. Spammer sind heutzutage nicht mehr – oder nur selten – Einzeltäter, sondern vielmehr professionelle Gruppierungen, die oftmals der organisierten Kriminalität zuzuordnen sind. Auf zivilrechtlichem Wege ist gegen diese Tätergruppen zumeist – auch aufgrund ihrer internationalen Ausrichtung – kaum vorzugehen, so dass eine Einordnung im Strafrecht empfehlenswert und angebracht erscheint.

Empfehlung 3: Die Erlaubnis von Filter- und Blockingmaßnahmen seitens Unternehmen und Providern muss rechtlich klargestellt werden.

Nur indirekt mit der Bekämpfung von Spam hängt die Frage der Legitimität von Filter- und Blocking-Maßnahmen seitens der Provider und Unternehmen zusammen. Zwar ist sich die Literatur mittlerweile weitgehend einig, dass insbesondere Filter bei entsprechender Zustimmung des Kunden oder Arbeitnehmers zulässig sind; gleichermaßen könnte hier aber eine rechtliche Klarstellung helfen. So ist derzeit nach herrschender Meinung das Filtern nur bei expliziter Zustimmung des einzelnen Nutzers erlaubt; per AGB oder allgemeiner Betriebsbestimmungen pauschal getroffene Vereinbarungen sind angesichts der datenschutzrechtlichen Relevanz gleichwohl nicht ausreichend.

6.2 Aufklärung

Aufklärung, vor allem eine Steigerung des Bewusstseins der Email-Nutzer – seien es Privatnutzer, Firmen oder Direktwerber – über die Gefahren des Internets, spielt eine wesentliche Rolle bei der Bekämpfung von Spam. Zu diesem Zweck sollte auf verschiedenen Ebenen gearbeitet werden.

Empfehlung 4: Direktwerbende Unternehmen müssen weiter über die geltende Rechtslage informiert werden.

Direktwerber müssen darüber informiert werden, was nach geltender Rechtslage legal ist und was nicht. Ein sinnvoller Ansatz für diesen Bereich ist das Positivlistenprojekt von eco und DDV, die *Certified Senders Alliance*. Hierin verpflichten sich Direktwerber, entscheidende „Spielregeln“ einzuhalten. Dies vorausgesetzt, werden sie auf eine Positivliste aufgenom-

men, die von ISPs genutzt wird, um seriöse Direktwerber zu erkennen und im Rahmen von Filterungs-Maßnahmen nicht auszufiltern. Ein solches Projekt ist jedoch nicht ausreichend. Noch immer gibt es deutsche Unternehmen, die Spam verschicken, ohne über die Rechtslage aufgeklärt zu sein. Nach Aussage von eco unterschreiben die meisten der im Rahmen der Spam-Beschwerdestelle zur Unterlassung aufgeforderten Unternehmen und Personen unverzüglich eine Unterlassungserklärung und treten in Zukunft nicht weiter in Erscheinung. Es muss davon ausgegangen werden, dass diese zumindest zum Teil unwissentlich unzulässige Werbung verschickt haben. Eine weitreichendere Aufklärung kann dabei helfen, diese Fälle zu minimieren.

Empfehlung 5: Email- und Internetnutzer müssen noch besser über die Gefahren des Internets aufgeklärt werden.

Nichtsdestotrotz spielt die Aufklärung der Email-Nutzer[274] eine noch entscheidendere Rolle. Ein Großteil der Spam-Emails werden nicht aus Deutschland bzw. von Deutschen verschickt. Eine Aufklärungskampagne, die an die Absender gerichtet ist, erreicht diese also nur zu einem geringen Teil – ganz abgesehen davon, dass ein Großteil sich der Illegalität ihres Handelns oftmals bewusst ist. Die Aufklärung der Nutzer hingegen, also der Leidtragenden von Spam, ermöglicht u.U. deutliche Fortschritte hinsichtlich der Spam-Bekämpfung und -Minimierung.

Die Gefahren des Internets – seien es Phishing-Angriffe, Pharming oder Trojaner – sind vielen Nutzern bisher noch nicht ausreichend bekannt. Ebenso wenig bekannt sind ihnen dementsprechend auch mögliche Abwehrmaßnahmen. Eine von *Forrester Custom Consumer Research* im Auftrag der *Business Software Alliance* (BSA) durchhgeführte internationale Studie[275] von Oktober/November 2005 ergab, dass deutsche Nutzer zwar besorgt über die Sicherheit im Internet sind, gleichwohl aber im internationalen Vergleich wenig für diese Sicherheit tun; so setzten nur 6% der deutschen Befragten die überprüften Arten von Sicherheitsprodukten wie z.B. Anti-Viren-Software, Firewalls oder Spam-Filter ein. Der Durchschnitt der untersuchten Länder lag dagegen bei 19%. Hier besteht also offenbar – auch für den Bereich Spam – deutlicher Bedarf an weiteren Aufklärungsmaßnahmen – insbesondere auch, da ein Großteil der Befragten nach Aussagen der Studie durchaus an Informationen zur Computersicherheit interessiert ist.

[274] im Sinne von Empfängern

[275] Vgl. Pressemitteilung der BSA vom 22.11.2005: „Internetnutzer in Deutschland verwenden im internationalen Vergleich weniger Security-Produkte"(online unter http://www.bsa.org/germany/presse/newsreleases/BS115-18.cfm [18.02.2006]); die Studie selbst kann unter http://www.bsa.org/germany/piraterie/forrester.cfm [18.02.2006] heruntergeladen werden.

Empfehlung 6: Ein zentrales Nutzerportal zu Spam, aber auch anderen Gefahren des Internets, kann bei der Aufklärung der Nutzer vorteilig sein.

Ein zentrales Nutzerportal im Internet ist ein Schritt zu einer verbesserten Aufklärung. Hier kann das BSI mit der Website „BSI für Bürger“[276] bereits ein ansprechendes Projekt vorweisen. Ebenso plant der vzbv in Zusammenarbeit mit dem BMELV z.Z. eine speziell auf Anti-Spam-Maßnahmen zugeschnittene Website, die im März 2006 online gehen soll. Ein Bündeln der Kräfte zur Erstellung eines zentralen Portals könnte hier jedoch aus Sicht des Nutzers von Vorteil sein. Ebenso kann auf diese Weise Doppelarbeit verhindert werden. Eine engere Zusammenarbeit zwischen den einzelnen aktiven Behörden, aber auch mit der Wirtschaft ist hier empfehlenswert. Informationen dürfen nicht nur in einem Medium – in diesem Fall dem Internet – bereit gestellt werden; stattdessen müssen auch andere Medien zur Aufklärung eingesetzt werden. Auch hier kann Zusammenarbeit mit der Wirtschaft, vor allem aber auch – wie in oben genannten Projekt des vzbv und des BMELV – den Verbraucherverbänden in diesem Zusammenhang empfohlen werden.

Empfehlung 7: Die Unterstützung von Verschlüsselungs- und Signierungstechnologien stärkt die Sicherheit und das Vertrauen in den eCommerce.

Des Weiteren kann die Steigerung von Akzeptanz und Anwendung von digitalen Signaturen und Email-Verschlüsselung[277] indirekt zu einem gestärkten Vertrauen in das Kommunikationsmedium „Email“ beitragen. Diese Verfahren verhindern zwar nicht direkt Spam; trotzdem kann ein verbreiteter Einsatz von signierten Emails – vor allem in der Kommunikation zwischen Unternehmen und Kunden – zu deutlich mehr Sicherheit führen. Inwieweit sich jedoch der Einsatz von vor allem Verschlüsselungstechnologien durch Aufklärung und ähnliche Maßnahmen vergrößern lässt, ist ungewiss; sinnvoll ist der Versuch jedoch in jedem Fall

6.3 Selbstregulierung

Selbstregulierung durch die Wirtschaft ist ebenfalls ein empfehlenswertes Mittel zur Spam-Bekämpfung. Neben technischen Maßnahmen[278] zählt hierzu vor allem die Erarbeitung von Verhaltensrichtlinien z.B. durch die entsprechenden Verbände. Insbesondere betrifft diese Maßnahme ISPs bzw. Mailprovider und (seriöse) Direktwerber.

[276] zu finden unter http://www.bsi-fuer-buerger.de/ [18.02.2006]
[277] Vgl. zu beiden Kapitel 6.5
[278] Vgl. Kapitel 6.5

Empfehlung 8: Verhaltensrichtlinien durch ISPs bzw. deren Verband eco stellen deutlich heraus, auf welche Weise mit Spam umgegangen werden soll.

„Codes of Conduct“ sollten auf Seiten der ISPs und Mailprovider festlegen, wie verbandsweit mit Spam umgegangen wird. So kann z.B. festgelegt werden, welche Maßnahmen ergriffen werden, wenn ein Kunde versucht, Spam zu versenden. Solche Maßnahmen können bei der Benachrichtigung des Kunden über sein Fehlverhalten beginnen und bis zur Sperrung des entsprechenden Nutzers führen. Derzeit hat der eco als zuständiger Verband zwar noch keinen derartigen auf die ISPs und Spam zugeschnittenen „Code of Conduct“ erarbeitet. Aufgrund der aber bereits sehr aktiven Arbeit des Verbandes und auch seiner Mitglieder wäre ein solcher vor allem aber auch ein weiteres Zeichen für die eigenen Bemühungen denn ein echter praktischer Fortschritt.

Empfehlung 9: Verhaltensrichtlinien der Direktwerber, die u.U. auch strengere als die gesetzlich geforderten Anforderungen stellen, können eine Akzeptanzsteigerung dieser Werbeform hervorrufen und dienen einer deutlichen Abgrenzung gegenüber unseriösen Spammern.

Die Erarbeitung von Verhaltensrichtlinien auf Seiten der Direktwerber kann einer Akzeptanzsteigerung und vor allem einer Abgrenzung zu Spam dienen. Durch die Vereinbarung von über den Gesetzesrahmen hinausgehenden Verpflichtungen wie z.B. Double-Opt-In kann sichergestellt werden, dass nur interessierte Nutzer die entsprechende Werbung bekommen. Ein solcher „Code of Conduct“ wurde vom DDV und dem eco erarbeitet und ist Teil des so genannten Positivlistenprojektes der Verbände. Unterzeichner dieser Vereinbarung bekommen in diesem Projekt die Möglichkeit, auf Positivlisten aufgenommen zu werden, so dass sie durch ISPs nicht mehr gefiltert werden. Im weiteren Sinne kann hierbei von einer Art „Gütesiegel“ gesprochen werden.

Empfehlung 10: Gütesiegel können das Vertrauen in den eCommerce deutlich steigern.

„Echte“ Gütesiegel, die seriösen Direktwerbern verliehen werden, werden mittlerweile von einer Vielzahl von Unternehmen angeboten. Sie belegen, dass das werbende Unternehmen sich an die Bestimmungen des Anbieters des entsprechenden Gütesiegels hält. Oftmals werden die Siegel in Form einer Grafik auf der Website oder in Emails eingebunden. Des Weiteren sind die Kunden eines Anbieters von Gütesiegeln zumeist in einer Datenbank auf dessen Website aufgeführt. Aufgrund der Vielzahl an Anbietern ist es jedoch für den Nutzer oftmals nicht leicht zu entscheiden, inwieweit er einem Gütesiegel vertrauen kann. Aus diesem Grund und um einheitliche Standards zu gewährleisten, wurde unter Federführung der *Initiative D21* ein Bündnis mit verschiedenen Anbietern gegründet, das deren

Gütesiegel sowie die Einhaltung der erarbeiteten Standards überprüft. Insbesondere so „zertifizierte“ Gütesiegel können, bei entsprechender Verbreitung und Bekanntheit bei den Nutzern, eine wesentliche Rolle spielen, um das durch Spam beinträchtigte Vertrauen dieser zurückzugewinnen.

6.4 Vollstreckung und internationale Zusammenarbeit

Neben einer straffen Gesetzgebung als Grundlage weiterer staatlicher Maßnahmen spielen internationale Kooperationen eine wesentliche Rolle bei der Bekämpfung von Spam. Solches internationales Handeln setzt gleichwohl aber auch eine durchdachte nationale Anti-Spam-Politik voraus. Die aktiv am Anti-Spam-Kampf teilnehmenden Staaten müssen – auch wenn sich die inländischen Spammer in Grenzen halten – vorbildlich gegenüber weniger weit entwickelten Staaten agieren können; das ist nur bei einer effektiven nationalen Anti-Spam-Politik gegeben, die insbesondere auch eine aktive Verfolgung von Spammern im In-, aber auch im Ausland beinhaltet.

Empfehlung 11: Internationale Kooperationen sind entscheidend in der Spam-Bekämpfung und können seitens der Bundesregierung weiter ausgebaut werden.

Es gibt mittlerweile eine Vielzahl von Initiativen, Gruppierungen und Kooperationen, die sich auf internationaler Ebene mit dem Kampf gegen Spam beschäftigen.[279] An einem Großteil davon ist die Bundesrepublik beteiligt, meist durch den eco, oft aber auch durch das BMELV und BMWi.

In diesem Bereich besteht jedoch noch Verbesserungsbedarf. So nehmen deutsche Behörden zwar oftmals teil an internationalen Treffen; es wäre jedoch wünschenswert, wenn diese Arbeit noch weiter verstärkt würde. So hat bisher z.B. noch keine deutsche Behörde – trotz reger Teilnahme – den London Action Plan (LAP) unterschrieben – eine Initiative, die durch Teilnehmer wie China, Süd-Korea und den USA[280] als sehr chancenreich angesehen werden muss. Bisher wurde der LAP von deutscher Seite nur durch den eco unterschrieben. Eine – vor allem auch formal – stärkere Teilnahme deutscher Behörden an dieser und anderen Initiativen würde verdeutlichen, dass Spam auf Bundesebene als äußerst ernst zu nehmendes Phänomen betrachtet wird und die internationale Zusammenarbeit einen verdienten Stellenwert als Grundlage für effektives nationales Handeln einnimmt.

Wenngleich (vor allem deutsche) Spammer bereits aktiv im Rahmen der Spam-Beschwerdestelle verfolgt werden, besteht auf internationaler Ebene noch erheblicher Ver-

[279] Vgl. dazu Kapitel 4.4.1
[280] also Staaten, aus denen ein Großteil des weltweiten Spams stammt

besserungsbedarf. Die europäische CNSA ist ein Schritt in die richtige Richtung; jedoch kann die Einrichtung einer zentralen Behörde im Zusammenhang mit internationaler Rechtshilfe und Informationsaustausch die Erfolge weiter verbessern.[281] Insbesondere im Bereich des Phishing, das im Gegensatz zu UCE noch wenig im Rahmen internationaler Kooperationen behandelt wird, kann die Bundesrepublik durch die Schaffung von bilateralen Abkommen und multilateralen Arbeitsgruppen eine führende Rolle in der internationalen Zusammenarbeit einnehmen.

Empfehlung 12: Bilaterale Abkommen können helfen, in Bezug auf Spam weniger entwickelte Staaten zu unterstützen und eine engere Zusammenarbeit bei der Verfolgung von Spammern zu vereinbaren.

Ebenso wurden von deutscher Seite bisher noch keinerlei zusätzliche bilaterale Abkommen vereinbart, die es erlauben, in Bezug auf Spam weniger weit entwickelte Länder im Gesetzgebungsprozess zu unterstützen; vor allem kann im Rahmen solcher Abkommen jedoch auch eine engere Zusammenarbeit bei der Verfolgung von Spammern vereinbart werden.

Empfehlung 13: Eine zentral für die Spam-Bekämpfung zuständige Bundesbehörde hilft, Kräfte zu bündeln und Doppelarbeit zu verhindern.

Im Zuge dieser Überlegungen ist der Aufbau einer zentralen Bundesbehörde zur Spam-Bekämpfung nahe liegend, so dass nicht wie bisher verschiedene Behörden in verschiedenen Initiativen aktiv[282] wären. Doppelarbeit kann auf diese Weise ebenso vermieden werden wie auch für alle ausländischen Partner ein konkreter Ansprechpartner zur Verfügung steht. Bisher ist dies oftmals der eco. Da es sich bei diesem jedoch um einen privatwirtschaftlichen Verband handelt, ist der internationale Informationsaustausch u.U. eingeschränkt. Eine zentral zuständige Behörde hätte dieses Problem nicht. Aufgrund der positiven Erfahrungen im Rahmen der Dialer-Bekämpfung kann die Bundesnetzagentur, ebenso aber auch das BSI für diese Aufgabe empfohlen werden.

Empfehlung 14: Spamboxes sind entscheidend zur Verfolgung und Bewertung von Spammern und Spam-Trends.

Ein wirksames Mittel bei der Verfolgung kann die Einrichtung so genannter „Spamboxes“ sein. Bei diesen handelt es sich um Datenbanken, in denen auftretende Spam-Emails zentral gesammelt werden – z.B. durch die Einrichtung von Spam-Traps[283] oder durch

[281] Vgl. Empfehlung 13

[282] Vgl. dazu auch Abbildung 4.2 auf Seite 59

[283] Hier handelt es sich um Email-Adressen, die speziell eingerichtet wurden, um Spam zu empfangen.

die Zusendung durch betroffene Nutzer. Die so gesammelten Informationen können für eine weitere Verfolgung der Spammer, aber auch zur Erkennung aktueller Spam-Trends genutzt werden. Eine solche Spambox wird z.Z. auf europäischer Ebene unter dem Namen *SpotSpam*[284] u.a. durch den eco aufgebaut.

Empfehlung 15: Eine enge Zusammenarbeit mit der Wirtschaft, insbesondere dem in diesem Gebiet ausserordentlich aktiven eco, ist notwendig.

Eine weiterhin enge Zusammenarbeit mit der Privatwirtschaft, insbesondere dem eco, ist anzuraten. Wenngleich in manchen Fällen der Einsatz einer Bundesbehörde sinnvoll ist, spielt die Wirtschaft dennoch eine entscheidende Rolle. Neben dem eco, insbesondere dessen Spam-Beschwerdestelle sowie dem SpotSpam-Projekt[285], müssen ISPs und Mailprovider aktiv im Rahmen von Aufklärungskampagnen, aber auch in der Diskussion über technische Maßnahmen beteiligt werden.

6.5 Technik

Technische Maßnahmen, die das Problem „Spam“ an der Wurzel bekämpfen, sind aufgrund der Internationalität des Internets nahezu unmöglich national umzusetzen. Sie müssen bereits auf Ebene des zugrunde liegenden SMTP durchgeführt werden, so dass ein nationaler Alleingang hier nur wenig erfolgsversprechend ist. Dennoch gibt es einige technische Maßnahmen, die zumindest helfen können, die Belästigung der Nutzer durch Spam einzudämmen sowie die Belastung der Provider zu verringern.

Empfehlung 16: Email-Filter auf Provider- und Nutzerseite sind vor allem bei geschäftlichem Einsatz von Emails derzeit unumgänglich.

So können ständig aktualisierte Email-Filter auf Provider- oder Nutzerseite bereits massiv dazu beitragen, dass Spam nicht mehr das eigentliche Postfach des Nutzers überfüllt, sondern stattdessen bereits automatisch erkannt und in einem gesonderten Ordner gespeichert wird. Dieses Zwischenspeichern ist in den meisten Fällen vonnöten, da aktuelle Filter u.U. auch legitime Emails als Spam deklarieren.[286] Für solche Fälle muss das System dem Nutzer erlauben, die Email trotzdem finden und lesen zu können, weswegen bei der Spamfilterung dieses nicht sofort gelöscht, sondern nur verschoben wird. Es ist zu beachten, dass der Verwendung von Filtern auf Provider- bzw. Unternehmensbasis z.Z. aus rechtlichen

[284] Vgl. Kapitel 4.4.1
[285] Vgl. ebd.
[286] so genannte *false positives*

Gründen vom Nutzer zugestimmt werden muss. Eine pauschale Zustimmung über AGB oder allgemeine Betriebsbestimmungen reicht dazu nach herrschender Meinung aufgrund der datenschutzrechtlichen Relevanz nicht aus.

Empfehlung 17: Das Blockieren von Spam auf ausgehender Seite verhindert die Belastung weiterer Server deutlich. Auf eingehender Seite kann das Blockieren im Falle von Malware das Eindringen in lokale Netze effektiv verhindern.

Filter sind derzeit für den professionellen Email-Nutzer unverzichtbar; sie helfen jedoch nicht dabei, die Überlastung des Email-Systems selbst, also der Mailserver, zu verhindern, da aus genannten Gründen die Emails in jedem Falle zugestellt werden müssen. Anders verhält es sich mit Blocking-Maßnahmen. Hierunter versteht man das Abweisen einer Email bereits auf Ebene des (versendenden oder empfangenden) Mailservers. In beiden Fällen kann ein Provider durch geeignete Software bereits während des Absendens durch einen Kunden u.U. erkennen, dass es sich bei der Email um Spam handelt. Zu diesem Zwecke können z.B. Virenscanner eingesetzt werden, die ausgehende Emails auf Viren untersuchen; der Provider kann aber ebenso, wenn ein Nutzer unerwarteterweise sehr viele Emails auf einmal verschickt, diese blockieren. In jedem Fall ist es notwendig, den Absender (z.B. per Email) auf das Blockieren aufmerksam zu machen. In diesem Zusammenhang sollte er ebenso auf mögliche Ursachen hingewiesen werden. Der Einsatz derartiger Blocking-Verfahren bietet sich vor allem auf Seiten des ausgehenden Mailservers an, da auf diese Weise effektiv verhindert werden kann, dass die Spam-Emails andere Server belasten bzw. das Postfach des Empfängers erreichen.

Filter- und Blocking-Verfahren werden mittlerweile von einem Großteil der Mailprovider angeboten. Gerade auf dieser Ebene können durch die deutlich höhere Anzahl an Emails als beim Kunden selbst effektive Filter trainiert[287] werden, so dass bei Mitarbeit[288] der Kunden nur wenig Spam unerkannt bleibt.

Empfehlung 18: Der Einsatz von digitalen Signaturen kann zumindest Phishing erschweren, wenn auch nicht verhindern.
Empfehlung 19: Der Einsatz von Verschlüsselung kann indirekt auch zum Spamschutz gebraucht werden. Unabhängig davon kann der Einsatz von Verschlüsselung in jedem Falle empfohlen werden.

Auf nationaler bzw. individueller Ebene lassen sich des Weiteren verschiedene Verfahren der kryptographischen Sicherung einsetzen, die – zumeist indirekt – helfen, Spam zu

[287] Vgl. zur Funktionsweise von Filtern Kapitel 3.4.1

[288] Um die Filter zu verfeinern, ist es in den meisten Fällen notwendig, dass der Kunde Emails z.B. im Falle von Webmail markiert, so dass der Filter des Providers diese Email in seine Datenbank aufnehmen kann.

erkennen bzw. zu vermeiden. Hierunter sind vor allem die Verschlüsselung sowie das Signieren von Emails zu verstehen. Mit Hilfe der führenden Verfahren S/MIME und PGP ist es möglich sicherzustellen, dass nur der Empfänger selbst die Email lesen kann (Verschlüsselung) und dass der Absender derjenige ist, für den er sich ausgibt (Signieren). PGP und S/MIME sind jedoch nicht kompatibel zueinander; ebenso ist der Anteil der Nutzer, die entsprechende Software einsetzen, nur gering.

Digitale Signaturen, eingesetzt durch Banken und andere betroffene Unternehmen, können verhindern, dass durch einfache Kopien des entsprechenden Layouts Phisher in die Lage versetzt werden, nahezu unerkennbare Fälschungen zu erstellen. Durch die Signatur kann der Empfänger sicherstellen, dass eine Email wirklich von seine Bank gesendet wurde. Phishern ist es natürlich möglich, eigene Signaturen zu erstellen, die auf den ersten Blick legitim erscheinen. Über diese Risiken muss der Nutzer aufgeklärt werden. Trotz Vorhandenseins eines Signaturgesetzes, das bestimmte Signaturen Unterschriften gleichstellt, sowie der entsprechenden Angebote für Signaturkarten werden digitale Signaturen jedoch von Privatanwendern und auch Unternehmen kaum eingesetzt.

Ähnliches gilt für die Verschlüsselung von Emails. Diese kann – wenn auch nur auf sehr indirektem Wege – ebenfalls zum Spamschutz gebraucht werden. So können unter der Prämisse, dass ein Nutzer prinzipiell oder größtenteils nur noch verschlüsselte Emails empfängt, (unverschlüsselte) Spam-Emails leicht ausgefiltert werden. Ebenfalls gestaltet es sich derzeit für Spammer schwierig, ihre Spam-Emails mit dem jeweiligen Schlüssel des Empfängers zu verschlüsseln. Erfahrungen in der Vergangenheit zeigen jedoch, dass Spammer zumeist sehr schnell auf neue Gegebenheiten reagieren. In diesem Zusammenhang wäre es denkbar, dass Adress-Datenbanken mit den jeweiligen öffentlichen Schlüsseln verkauft werden, so dass – insbesondere bei Verwendung von Botnets – kaum ein Mehraufwand für Spammer durch die Verschlüsselung entsteht. Neben dem also nur in Maßen vorhandenen Anti-Spam-Effekt von Verschlüsselung kann diese jedoch – ebenso wie die Verschlüsselung von Websites bzw. den Verbindungen per *https* – das Vertrauen in das und die Datensicherheit des Email-Systems deutlich stärken.

6.6 zusammenfassender Überblick

Um den Überblick über die empfehlenswerten Maßnahmen zu wahren, fasst Tabelle 6.1 die vorangegangenen Abschnitte noch einmal präzise zusammen. Detaillierte Informationen zu den einzelnen Punkten finden sich in den Kapiteln 6.1 bis 6.5. Einen Überblick über alle vorgestellten Maßnahmen bietet Kapitel 5.6.

Im Rahmen dieser Zusammenfassung ist zu beachten, dass es unumgänglich für eine zukunftsorientierte Strategie ist, den Begriff *Spam* weiter als oftmals bisher zu formulieren.

Spam ist nicht nur kommerzielle Werbung per Email, sondern umfasst auch Phänomene wie Phishing, per Email verschickte Trojaner etc. Des Weiteren lässt sich Spam mittlerweile nicht mehr auf Emails alleine reduzieren. Verschiedene Formen von Spam werden auch per Instant Messenger, SMS/MMS oder Internet-Telefonie übertragen. Eine zukunftsorientierte Strategie muss auch diese Technologien beinhalten.[289]

	Maßnahme	**zuständig**	**umgesetzt**[a]
Regulierung	Verbot von Phishing-Emails und -Websites	Parlament	nein
	Verbot von UCE durch Ordnungswidrigkeiten- oder Strafrecht	Parlament	nein
	Rechtliche Klarstellung zu Filterung und Blocking durch Provider/Unternehmen	Parlament	nein[b]
Aufklärung	Aufklärung der Direktwerber und Unternehmen	zuständige Behörde[c,d], Verbände	nein
	Aufklärung der Nutzer	zuständige Behörde[c,d], Verbände, Wirtschaft	ja[e]
	neinrichtung eines zentralen Internet-Portals	zuständige Behörde[c,d], Verbände, Wirtschaft	(ja)[f]
	Unterstützung von Verschlüsselung und Signierung	zuständige Behörde[c]	nein

[a] Stand: 27.02.2006
[b] beide Verfahren sollten per AGB oder allgemeiner Betriebsbestimmungen durchsetzbar sein
[c] sofern diese eingerichtet wird; ansonsten je nach Aufgabe wie bisher BMELV, BMWi, BSI, Bundesnetzagentur
[d] in Zusammenarbeit mit Wirtschaft und Verbraucherverbändern
[e] Im Rahmen des „BSI für Bürger“ sowie durch das BMELV und den vzbv (ab März 2006)
[f] Das „BSI für Bürger“ ist ein solches Portal, wird aber nur durch das BSI geführt; das BMELV und der vzbv z.B. erarbeiten ein weiteres Portal

Tabelle 6.1: Übersicht über empfohlene Strategien zur Spam-Bekämpfung (Teil 1)

[289] Diese Arbeit beschränkt jedoch auf Spam per Email. Viele der angesprochenen Maßnahmen lassen sich jedoch auch leicht auf die anderen Technologien abbilden.

	Maßnahme	zuständig	umgesetzt[a]
Selbst-regulierung	Erarbeitung von Verhaltensrichtlinien durch ISPs	Verbände[b]	nein
	Erarbeitung von Verhaltensrichtlinen durch Direktwerber	Verbände[c]	ja[d]
	Vergabe von Gütesiegeln o.ä. an seriöse Direktwerber	zuständige Behörde[c], Verbände[e], Unternehmen	ja
Vollstreckung und internationale Zusammenarbeit	Teilnahme an internationalen Kooperationen	zuständige Behörde[f]	ja[g]
	Aufbau von bilateralen Vereinbarungen	zuständige Behörde[f]	nein
	Einrichtung einer zentralen Behörde zur Spam-Bekämpfung	Parlament	nein
	Einrichtung von Spamboxes	zuständige Behörde[f], eco	ja[h]
	Enge Zusammenarbeit mit der Wirtschaft, insb. dem eco	zuständige Behörde[f]	ja
Technik	Email-Filterung	Nutzer, Provider	ja
	Blocking von Spam-Emails	Provider	ja
	Signierung von Emails (PGP, S/MIME)	Nutzer	(ja)[i]
	Verschlüsselung von Emails (PGP, S/MIME)	Nutzer	(ja)[i]

[a] Stand: 27.02.2006
[b] z.B. eco
[c] z.B. DDV
[d] im Rahmen des Positivlistenprojekts von eco und DDV
[e] eco, DDV, vzbv
[f] sofern diese eingerichtet wird; ansonsten wie bisher BMELV, BMWi, Bundesnetzagentur
[g] kann noch intensiviert werden
[h] auf europ. Ebene durch den eco: SpotSpam
[i] Verbreitung sowohl auf privater als auch geschäftlicher Ebene derzeit gering

Tabelle 6.2: Übersicht über empfohlene Strategien zur Spam-Bekämpfung (Teil 2)

7 Schluss

Die im Rahmen der vorliegenden Arbeit ausgeführten Empfehlungen bieten eine sinnvolle Kombination von Maßnahmen der Spam-Bekämpfung. Eine solche auf mehreren Ebenen angreifende Strategie muss derzeit als unabdingbar im Kampf gegen Spam angesehen werden. Es hat sich jedoch in der Zusammenfassung von Kapitel 6 gezeigt, dass die Bundesregierung, aber auch die anderen beteiligten Organisationen bereits viele der empfohlenen Maßnahmen getroffen haben. Nichtsdestotrotz besteht an verschiedenen Punkten, worauf ebenfalls in diesem Kapitel eingegangen wurde, noch Verbesserungsbedarf.

Neben der Erarbeitung der genannten Empfehlungen wurde im Rahmen dieser Arbeit jedoch auch ein Überblick über die nationale und internationale Rechtslage sowie die führenden nationalen und multilateralen Initiativen gegeben. Einerseits aus Gründen des Umfangs, aber auch aufgrund der sich stetig ändernden Situation in den verschiedenen Ländern wurde hierbei nur auf einige wenige Staaten eingegangen, die entweder in vielen Studien als führende „Spam-Nationen“ auftauchen oder die, im Falle von Australien, erfolgreich auf rechtlichem Wege und im Rahmen internationaler Kooperationen Spam bekämpfen. Einen umfassenderen Überblick über die geltende Rechtslage und die Aktivitäten einer Vielzahl von Staaten bietet vor allem das *Anti-Spam Toolkit* der OECD[290] sowie die ITU[291].

Es bleibt zu bemerken, dass ein aktives Vorgehen gegen Spam auch seitens der Bundesregierung unerlässlich ist, um das mittlerweile unverzichtbar gewordene Email-System vor einem Kollaps zu bewahren. Ein rigoroses Vorgehen gegen den Missbrauch kann – vor allem auf nationaler Ebene – das Problem zwar nicht gänzlich lösen, jedoch kann es dieses u.U. zumindest soweit einschränken, dass die Vorteile der Email-Kommunikation weiterhin erhalten bleiben.

[290] online unter http://www.oecd-antispam.org/ [27.02.2006]
[291] online unter http://www.itu.int/osg/spu/spam/index.phtml [27.02.2006]

Glossar

Anti-Spam Toolkit Das *Anti-Spam Toolkit* der OECD ist eine Sammlung von Informationen bezüglich Spam. Insbesondere beinhaltet es auch eine Datenbank der in den verschiedenen Staaten zuständigen Stellen sowie der Gesetzeslage, aber auch eine Vielzahl weiterer Informationen. Es ist online verfügbar unter http://www.oecd-antispam.org/.

ARPANET Das *Advanced Research Projects Agency NETwork* war ein in den 1960er Jahren ursprünglich im Auftrag der US-Luftwaffe entwickeltes Computernetzwerk und gilt als Vorläufer des heutigen Internets. Vgl. hierzu auch Kapitel 3.1.

Backbone *Backbone* bezeichnet einen zentralen Bereich eine Computernetzwerkes mit sehr hohen Bandbreiten, der zumeist durch Dopplung seiner Komponenten gegen Ausfälle geschützt ist. Im Internet bezeichnet *Backbone* vor allem die Verbindungspunkte der einzelnen Netzwerke.

BATV *Bounce Adress Tag Validation* ist ein Verfahren zur Feststellung, ob eine *bounce*-Nachricht auf einer Nachricht beruht, die tatsächlich vom eigenen Server verschickt wurde. Vgl. für weiter Details Kapitel 3.4.4.

Bayes-Klassifizierung Die *naive Bayes-Klassifizierung* wird u.a. in statistischen Spamfiltern zur Spam-Erkennung eingesetzt. Es handelt sich um ein statistisches Verfahren, bei dem (bei diesem Verwendungszweck) durch die Auswerung charakteristischer Wörter in einer Email entschieden wird, ob es sich um Spam oder Ham handelt. Für eine vernünftige Trefferquote müssen diese Filter mit einer ausreichenden Anzahl von legitimen und illegitimen Emails trainiert werden. Vgl. Kapitel 3.4.1.

Blacklist Eine *Blacklist* beinhaltet in Zusammenhang mit Spam und Emails Daten von bekannten Spam-Emails, aufgrund derer Emails gefiltert werden. Man unterscheidet verschiedene Arten von Blacklists, z.B. DNSBLs, RHSBLs oder URIDNSBLs. Vgl. hierzu auch Kapitel 3.4.1.

Botnet Unter einem *Botnet* versteht man ein fernsteuerbares Netzwerk von so genannten Zombie-PCs, die ohne Wissen ihrer Benutzer zumeist durch Viren oder Trojaner in dasselbe eingebunden wurden. Durch die mittlerweile aus bis zu mehreren 100.000 Einzelrechnern, so genannten *Bots* bestehenden Netze können effizienze dDoS-Attacken gestartet oder Spam verbreitet werden. Vgl. auch Kapitel 3.3.4.

bounce s. DNS(2).

Caller ID *Caller ID* ist ein Verfahren zur Sicherstellung der Authentizität von Email-Absendern mittels zusätzlicher DNS-Einträge. Es wurde 2004 zusammen mit dem SPF zu Sender ID vereinigt. Vgl. Kapitel 3.4.2.

CAN-SPAM-Act Der *CAN-SPAM-Act* ist ein US-amerikanische Gesetz zur Bekämpfung von Spam. Vgl. hierzu Kapitel 4.3.2.

Challenge-Response *Challenge-Response*-Verfahren dienen der Authentifizierung. So kann sich Person A durch das Stellen einer Aufgabe , z.B. der Frage nach einem Passwort, und die folgende Lösung dieser Aufgabe durch Person B vergewissern, ob er wirklich mit Person B kommuniziert. Da die Übermittlung des Passwortes in diesem Fall dasselbe kompromittieren wurde, muss Person B bei den meisten *challenge-Response*-Verfahren lediglich beweisen, dass er das Passwort kennt.

Client *Client* bezeichnet eine Anwendung, die den Dienst eines Servers in Anspruch nimmt. Beispiele sind Mailclients oder Webbrowser. Umgangssprachlich bezeichnet *Client* auch einen Rechner, der in einem Netzwerk primär Client-Anwendungen ausführt.

dDoS Eine *distributed Denial of Service*-Attacke bezeichnet einen Angriff auf einen Server mit dem Ziel, diesen arbeitsunfähig zu machen, in der Regel durch Überlastung. Im Gegensatz zu einer normalen *DoS*-Attacke wird bei einem *dDoS*-Angriff eine große Anzahl von Systemen eingesetzt, um den Zielserver so durch die deutlich größere Bandbreite schneller oder überhaupt lahmlegen zu können.

Dialer *Dialer* sind Programme, mit denen über eine Telefonleitung eine Verbindung zum Internet oder einem anderen NEtzwerk aufgebaut werden kann. Umgangssprachlich versteht man unter *Dialern* jedoch vor allem solche, die ohne ausdrückliche oder nur unzureichende Zustimmung des Nutzers Verbindungen aufbauen, um auf diesem Wege überzogene Gebühren abzurechnen. Derartige *Dialer* werden oftmals über Trojaner oder Viren verteilt.

DNS(1) Das *Domain Name System* ist eine verteilte Datenbank, die primär dazu dient, Domainnamen, z.B. www.bmi.bund.de in die dazugehörige IP-Adresse (in diesem Fall 194.95.178.105) umzuwandeln. Es zählt zu den grundlegenden Diensten des Internets.

DNS(2) Neben dem Domain Name System bezeichnet 'DNS' ebenfalls eine so genannte *Delivery Status Notification*. Eine solche Nachricht wird durch Mailserver generiert, wenn eine Email nicht zugestellt werden kann. DNS ist ein Synonym zu *bounce message*.

DNSBL So genannte *Domain-Name-System-Blacklists* sind Listen von IP-Adressen, die es erlauben, über eine bestimmte DNS-Abfrage festzustellen, ob eine in einer Email vorkommende IP-Adresse bereits einmal von Spammern missbraucht wurde. Vgl. hierzu auch Kapitel 3.4.1.

Domain Eine *Domain* ist ein zusammenhängender Teilbereich im DNS. Es wird unterschieden in Top-, Second-, Third-Level-Domains etc. Top-Level-Domains sind die Domains höchster Ebene (z.B. .de oder .com), Second-Level-Domains die darunter liegende Ebene wie z.B. google.com.

DomainKeys Das *DomainKeys*-Verfahren ist ein Verfahren zur Sicherstellung der Authentizität von Email-Absendern. Vgl. Kapitel 3.4.2.

Double Opt-In *Double Opt-In* bezeichnet ein bstimmtes Opt-In-Verfahren, bei dem dem Erhalt von regelmäßigen Nachrichten oder Werbung zweifach zugestimmt werden muss. Im Email-Bereich geschieht dies zumeist durch ein Eintragen der eigenen Email-Adresse z.B. in einem Webformular und einer dann folgenden Bestätigung einer an diese Adresse geschickten Nachricht.

Email-Body Der *Email-Body* bezeichnet die eigentliche Nachricht einer Email.

Email-Header Der *Email-Header* enthält die Kopfzeilen einer Email wie u.a. Absender, Empfänger, Betreff, Datum und Route. Vgl. Kapitel 3.2.2.

ESMTP Das *Extended Simple Mail Transfer Protocol* ist eine Weiterentwicklung von SMTP, die über ein modulares Konzept die Einbindung zusätzlicher Befehle erlaubt, z.B. Authentifizierungsmaßnahmen. Vgl. für eine ausführlichere Darstellung Kapitel 3.2.

false positive Als *false positives* werden Emails bezeichnet, die ein Spamfilter fälschlicherweise als Spam deklariert hat. Im Gegensatz dazu bezeichnet *false negative* Spam, der nicht als solcher erkannt wurde.

Greylisting *Greylisting* bezeichnet ein Verfahren der Spam-Bekämpfung, bei dem Emails vom Mailserver temporär abgelehnt werden. Das Verfahren beruht auf der Tatsache, dass reguläre Mailserver in einem solchen Fall die Email nach einiger Zeit ein weiteres Mal zuzustellen versuchen, Spam-Server jedoch oftmals aus Performance-Gründen nur einen einzigen Zustellversuch unternehmen. Aufgrund diverser Probleme gilt das Verfahren nicht als praktikabel. Vgl. Kapitel 3.4.3.

Ham *Ham* bezeichnet das Gegenteil von Spam, nämlich legitime Emails.

Hoax Als *Hoaxes* wird im Deutschen eine z.B. per Email verbreitete Falschmeldung bezeichnet. Vgl. dazu auch Kapitel 2.2.6 und 4.1.6.

Host Ein *Host* ist ein Rechner, der in einem Netzwerk Server-Dienste anbietet.

Hostname Der *Hostname* eines Rechners ist der Name, der ihn in einem Netzwerk eindeutig kennzeichnet. Bei Rechnern, die an das Internet angebunden sind, setzt er sich aus dem Domainnamen sowie dem lokalen Rechnernamen zusammen. Ein Beispiel hierfür wäre der Rechner 'Kunigunde', der im Internet als 'kunigunde.example.com'angesprochen wird.

hosts-Datei Die hosts-Datei ist eine lokal auf einem Rechner liegende Textdatei, die eine Zuordnung von Hostnamen zu IP-Adressen enthält. Muss auf einem System z.B. beim Internet-Surfen ein Hostname in eine IP-Adresse aufgelöst werden, wird zumeist erst die hosts-Datei nach einem passenden Eintrag durchsucht, bevor weitergehende Dienste wie DNS eingesetz werden.

HTTP(s) Das *Hypertext Transfer Protocol* ist ein Protokoll zur Übertragung von Daten über ein Netzwerk. Hauptsächlich wird HTTP derzeit zur Übertragung von Webseiten und ähnlicher Daten im Internet verwendet. *HTTPs* – das 's' steht für *secure* – bezeichnet eine mittels TLS verschlüsselte Variante des Protokolls.

Instant Messaging *Instant Messaging* bezeichnet einen Dienst, mit dessen Hilfe über ein Programm, den Instant Messenger, mit anderen Teilnehmern in Echtzeit kommuniziert werden kann. Neben dem IRC gehören hierzu auch kommerzielle Dienste wie ICQ, AIM oder MSN.

IP Das *Internet Protocol* ist eines der grundlegenden Protokolle des Internets. Als IP-Adresse bezeichnet die logische Adresse eines Gerätes in einem Computer- bzw. besser IP-Netzwerk wie z.B. dem Internet.

IRC *Internet Relay Chat* ist ein textbasiertes Chat-System im Internet. Es existiert bereits seit 1988 und kann damit als Vorgänger von Instant Messaging-Programmen wie ICQ angesehen werden, ist heutzutage jedoch weiterhin sehr stark genutzt.

ISP *Internet Service Provider* sind Unternehmen, die ihren Kunden verschiedene technische, für die Nutzung oder den Betrieb von Internet-Diensten notwendige Leistungen an. Insbesondere zählen hierzu Anbieter, die Internetzugänge anbieten sowie solche, die das Hosting, also u.a. die Vermietung von Webservern, übernehmen. Oftmals werden ISPs auch einfach als *Provider* bezeichnet.

IX *Internet Exchanges* sind die zentralen Netzknoten des Internets und dienen dazu, die einzelnen Teilnetze im Rahmen des Internets zu verbinden. Der größte deutsche Knoten ist der DE-CIX in Frankfurt/Main, der durch den eco betrieben wird.

Joe Job Als *Joe Jobs* werden gefälschte Emails bezeichnet, deren Absender auf eine Person oder Institution verweist, die auf diese Weise diskreditiert werden soll. Namensgebend ist der US-Amerikaner Joe Doll, der 1997 Opfer einer solchen Rufschädigungskampagne wurde. Vgl. auch Kapitel 2.2.5 und 4.1.5.

Log-Datei Eine Log-Datei beinhaltet ein automatisch erstelltes Protokoll von allen oder bestimmten Aktionen eines Programms oder eines Nutzers. Auf diese Weise kann der Administrator des Rechners z.B. im Falle einer Fehlfunktion oder eines Einbruchsversuches, aber auch zum Aufbau von Statistiken (z.B. im Falle von Webservern) die Arbeit der Software nachvollziehen.

Mailclient Ein *Mailclient* ist ein Programm, mit dem Emails geschrieben, gelesen, empfangen und versendet werden können.

Mailprovider Ein *Mailprovider* ist ein ISP, der Email-Adressen und -Postfächer anbietet. Bekannte deutsche Mailprovider sind *web.de* oder *GMX*.

Malware *Malware* bezeichnet Programme, die eine offene oder verdeckte Schadfunktion aufweisen und mit dem Ziel entwickelt werden, Schaden anzurichten oder z.B. gegen den Willen des Nutzers Daten auszuwerten. Vgl. dazu auc Kapitel 2.2.3 und 4.1.3.

MLM *Multi-Level-Marketing* ist eine Marketing-Methode, die auf einer pyramidenförmig Hierarchie von Verkäufern beruht, wobei lediglich die unterste Schicht Kundenkontakt hält. Oftmals sind derartige Systeme nur schwer von MMF- oder Schneeballsystemen zu unterscheiden. Vgl. auch Kapitel 2.2.6 und 4.1.6.

MMF So genannte *Make Money Fast*-Systeme bezeichnen heutzutage zumeist im Internet kursierende Schneeballsysteme, bei denen der Empfänger einer im Brief angegebenen Liste von Menschen einen geringen Geldbetrag zuzusenden, die erste Person auf der Liste zu entfernen und den eigenen Namen hinzuzufügen. Danach muss der Brief an möglichst viele Menschen weitergeleitet werden; es wird suggeriert, dass, sobald man selbst im oberen Bereich der Liste angekommen ist, eine große Geldsumme verdienen kann. Derartige System funktionieren nachgewiesenermaßen jedoch nicht. Vgl. auch Kapitel 2.2.6 und 4.1.6.

MMS Der *Multimedia Messaging Service* ist ein Nachfolger von SMS. Er erlaubt es, neben SMS-typischen kurzen Textnachrichten auch Multimedia-Daten wie Bilder oder Filme in GSM-Mobilfunknetzen zu versenden.

MTAMARK *MTAMARK* ist ein ähnliches Verfahren wie Sender ID. Der Besitzer einer IP-Adresse legt hierbei im DNS fest, ob von diese Emails verschickt werden dürfen. Der empfangende Mailserver kann auf diesen Eintrag filtern. Derzeit ist das Verfahren kaum verbreitet.

NGO *Non-Governmental Organisations* sind nicht gewinnorientierte, nicht von staatlichen Stellen organisierte oder abhängige und auf freiwilliger Basis aktive Organisationen. Klassische Beispiele sind Greenpeace oder amnesty international.

Nigeria-Scam *Nigeria-Scam* bezeichnet eine besondere Form des Betruges, der ursprünglich per Brief, mittlerweile jedoch zumeist per Massen-Email umgesetzt wird. Die Absender behaupten, eine große Geldsumme unbemerkt ins Ausland transferieren zu müssen und dazu die Hilfe des Empfängers zu benötigen, der für diese einen Teil der Summe erhält. Bei Einstieg in dieses 'Geschäft' wird das Opfer jedoch gebeten, nach und nach vorgebliche Gebühren etc. vorstrecken zu müssen. Der Name dieser Art von Betrug stammt von den zumeist nigerianischen Banden, die seit Mitte der 1980er Jahre sehr aktiv in diesem Bereich arbeiten. Vgl. auch Kapitel 2.2.4 und 4.1.4.

Open Proxy *Open Proxies* sind fehlkonfigurierte Proxy-Server, die auch den Zugriff von ausserhalb ermöglichen, so dass der Server z.B. zum Spamversand missbraucht werden kann. Vgl. Kapitel 3.3.3.

Open Relay *Open Relay* bezeichnet Mailserver, die von jedem beliebigen Rechner Emails annehmen und an beliebige Dritte weiterleiten, obwohl sie für eine solche Email eigentlich nicht zuständig sind. Vgl. Kapitel 3.3.2.

Opt-In *Opt-In* ist ein Marketing-Verfahren, bei dem dem Empfang von Werbung oder regelmäßigen Nachrichten wie Newsletters im Gegensatz zu Opt-Out explizit zugestimmt werden muss, z.B. durch das Eintragen in eine Verteilerliste.

Opt-Out *Opt-Out* ist ein Marketing-Verfahren, bei dem der Empfänger erst bei Zusendung von Werbung die Möglichkeit erhält, sich aus dem Verteiler des Anbieters auszutragen. Auf eine aktive Zustimmung zum Empfang von WErbung wird im Gegensatz zu Opt-In verzichtet.

PGP *Pretty Good Privacy* ist ein Softwareprodukt zur Verschlüsselung von Daten wie z.B. Emails. Im Gegensatz zu S/MIME basiert es nicht auf Zertifikaten, sondern auf Schlüsseln, die von anderen Teilnehmern beglaubigt werden und so ein so genanntes *Web of Trust*, also ein Netzwerk vertrauenswürdiger Personen bzw. Schlüssel aufbaut. Mittlerweile gibt es eine Vielzahl von Produkten, die auf dem Grundprinzip von PGP beruhen und zu diesem kompatibel sind.

Phishing *Phishing* bezeichnet eine Form des Trickbetrugs im Internet, bei der dem Opfer in offiziell wirkende Emails, z.B. von Banken, gebeten wird, vertrauliche Informationen auf einer verlinkten Website preiszugeben. Diese Website ist ebenso wie die Email selbst gefälscht, so dass die Täter die entsprechenden Daten erhalten. Vgl. auch Kapitel 2.2.4 und 4.1.4.

PIN Die *Personliche Identifikationsnummer* oder *Geheimzahl* ist eine nur einer oder wenigen Personen bekannte Zahl, mit der diese sich gegenüber einer Maschine, z.B. beim Onlinebanking authentifizieren können.

PIPELINING *PIPELINING* ist eine Erweiterung von ESTMP, das es erlaubt, sämtliche Kommandos eines SMTP-Dialoges (vgl. Kapitel 3.2) auf einmal und ohne die Antwort des Servers abzuwarten zu senden.

POP3 Das *Post Office Protocol version 3* ist ein Protokoll zur Übertragung von Emails von einem Server zum Client. Es wird in RFC1939 bechrieben.

Prüfsumme Eine *Prüfsumme* dient einer Gewährleistung der Integrität von Daten. Mittels verschiedener Verfahren werden solche Summen aus den grundlegenden Daten berechnet, die ein Empfänger der Daten nutzen kann um festzustellen, ob die Daten verändert wurden. Ein einfaches Beispiel ist die Bildung der Quersumme einer Zahl. Sogenannte *unscharfe Prüfsummen*, die häufig in Spamfiltern eingesetzt werden, funktionieren auch bei leicht veränderten Daten. Vgl. Kapitel 3.4.1.

Proof-of-work-Konzept Das *Proof-of-work-Konzept* ist ein Ansatz zur Spamverhinderung. Bei Einsatz dieses Verfahrens erwartet der empfangende Mailserver vom Absender eine gewisse Menge an komplexen Berechnungen und damit Zeit. Auf diese Weise soll das massenhafte Versenden von Emails verhindert werden. Die Praktikabilität, aber auch der Nutzen gegen Spammer von solchen Verfahren ist jedoch mehr als zweifelhaft, so dass sie derzeit nur testweise eingesetzt werden. Vgl. auch Kapitel 3.4.3.

Provider s. ISP.

Proxy-Server Ein Proxy dient i.A. dazu, den Datenverkehr eines lokalen Netzes aus Sicherheits- und Kostengründen zentral über einen einzigen Server – den Proxy-Server – ins Internet zu leiten.

RFC Die so genannten *Request For Comments* sind eine Reihe von technischen und organisatorischen Dokumenten, die ursprünglich zwar im wörtlichen Sinne zur Diskussion gestellt wurden, mittlerweile jedoch auch grundlegende Standards des Internets beinhalten. Sämtliche RFCs können online unter http://www.rfc-editor.org/ abgerufen werden.

RHSBL *Right-Hand-Side-Blacklists* beinhalten Domainnamen von Spammern und dienen dazu, anhand dieser Spam durch Filter auszusortieren. Da mittlerweile die Absenderadressen von Spammern zumeist gefälscht sind, ist ein Einsatz von RHSBLs nur noch bedingt zu empfehlen. Vgl. hierzu auch Kapitel 3.4.1.

ROKSO Das *Register Of Known Spam Operations* ist eine von Spamhaus geführte Datenbank der weltweit aktivsten Spammer. Es werden öffentlich zugängliche Informationen über Gruppen und Individueen gesammelt und online unter http://www.spamhaus.org/rokso/index.lasso zur Verfügung gestellt. Nach Spamhaus-Angaben sind die etwa 200 auf der Liste stehenden Spammer für 80% des weltweiten Spamaufkommens verantwortlich.

S/MIME *Secure / Multipurpose Internet Mail Extensions* ist ein auf digitalen Zertifikaten aufbauendes System zur Verschlüsselung von z.B. Emails.

Sender ID *Sender ID* ist die Vereinigung von Caller ID und SPF, zweier Verfahren zur Sicherstellung der Authentizität von Email-Absendern mittels des DNS. Durch zusätzliche Einträge im DNS wird festgelegt, für welche Domains ein Mailserver Emails verschicken darf, so dass festgestellt werden kann, ob es sich um eine legitime Email handelt oder nicht. Die Wirksamkeit des Verfahrens gegen Spam und Phishing ist jedoch umstritten. Vgl. Kapitel 3.4.2.

Server Ein *server* ist ein Programm, das Clients zumeist in einem Netzwerk eine bestimmte Dienstleistung zur Verfügung stellt. So dient ein Mailserver zum Verschicken von Emails und ein Webserver stellt Webseiten für den Browser bereit. Umgangssprachlich wird auch der Rechner, der Server-Anwendungen anbietet, als *Server* bezeichnet. Korrekt wäre hier jedoch der Begriff *Host*.

Serverfarm Eine *Serverfarm* ist eine Gruppe von gleichartigen, vernetzten Servern, welche zu einem logischen System verbunden sind. Solche Farmen werden insbesondere bei lastintensiven Internet-Angeboten eingesetzt, um die Leistungsfähigkeit zu erhöhen.

SMS Der *Short Message Service* ist ein Telekommunikationsdienst zur Übertragung kurzer Textnachrichten. Ursprünglich für den Mobilfunk entwickelt, ist SMS mittlerweile auch im Festnetz verfügbar.

SMTP Das *Simple Mail Transfer Protocol* ist das meist verbreitete Internet-Protokoll zum Austausch von Emails in Computernetzwerken. Da es bereits 1982 entwickelt wurde – einem Zeitpunkt mit nur wenigen Internet-Teilnehmern –, beinhaltet es keinerlei

Authentifizierungs- o.ä. Maßnahmen. Diese Einfachheit des Protokolls ist einer der wesentlichen Gründe für das derzeitige Problem mit Spam und verwandten Attacken. Vgl. für eine ausführlichere Darstellung auch Kapitel 3.2.

SMTP-after-POP *SMTP-after-POP* bezeichnet ein Verfahren, das verwendet wurde, um die im Standard-SMTP-Protokoll fehlende Authentifizierung zu erreichen. Hirzu muss der Anwender sein Postfach per POP3 abrufen, bevor er für in einem bestimmten Zeitfenster, z.B. zehn Minuten, Emails verschicken kann.

SMTP-Auth *SMTP-Auth* ist eine Erweiterung von ESMTP, das die Authentifizierung des Nutzers über ein Passwort ermöglicht.

Spam *Spam* bezeichnet unverlangt zugesandte Massen-Emails. Vgl. zu dieser Definition Kapitel 2.1.2.

Spam-Trap *Spam-Traps* sind Email-Adressen, die nur eingerichtet und veröffentlicht wurden, um Spam zu empfangen. Sie dienen oftmals Forschungszwecken, aber auch z.B. um Spam zur weiteren Verfolgungsund Auswertung zu sammeln.

Spambox Als *Spambox* wird ein Email-Postfach oder eine Datenbank bezeichnet, in der Spam zur weiteren Auswertung, z.B. durch statistische Filter, aber auch Strafverfolgungsbehörden gesammelt wird. Ein europäisches Spambox-Projekt ist SpotSpam.

Spamdexing Unter *Spamdexing*, auch *Suchmaschinen-Spamming* genannt, versteht man sämtliche Verfahren, dass eine Internet-Suchmaschine auf eine Stichworteingabe hin auf den vordersten Plätzen Webseiten ausgibt, die keine für den Surfer relevanten oder dem Suchbegriff entsprechenden Informationen, sondern lediglich Spam enthalten.

SPF Das *Sender Policy Framework* ist eine Technik, die das Fälschen von Email-Adressen erschweren soll. Dazu wird im DNS-Eintrag einer Domain festgelegt, welche Server Emails mit der Absenderadresse dieser Domain verschicken dürfen. SPF wurde 2004 zusammen mit dem *Caller ID*-Verfahren zum *Sender ID*-Verfahren vereinigt.

Spyware *Spyware* bezeichnet Programme, die ohne Wissen des Nutzers persönliche Daten von ihm oder seinem Rechner an den Hersteller oder an Dritte versendet. Vgl. auch Malware.

TAN Die *Transaktionsnummer* ist ein Einmalpasswort, dass zur Absicherung von Onlinebanking verwendet wird. Der Nutzer erhält hierzu von der Bank eine Liste von TANs und muss bei jedem Buchungsvorgang eine davon eingegeben, um die Transaktion zusätzlich zur PIN weiter abzusichern.

TCP Das *Transmission Control Protocol* ist eines der grundlegenden Protokolle des Internets und legt fest, auf welche Art und Weise Daten zwischen Computern übertragen werden. So genannten *TCP-Ports* bezeichnen Adresskomponenten, um Datenpakete dem richtigen Dienst bzw. Protokoll zuordnen zu können.

Terminalprogramm Ein *Terminalprogramm*, genauer ein *Terminal-Emulator*, ist ein Programm zur Herstellung einer Verbindung mit einem anderen Computersystem.

TLS *Transport Layer Security* ist ein Verschlüsselungsprotokoll für Datenübertragungen im Internet. TLS wurde früher auch als *Secure_Sockets_Layer* (SSL) bezeichnet.

Trojaner *Trojaner*, eigentlich *Trojanische Pferde*, sind im IT-Bereich Programme, die neben ihrer offensichtlichen und gewünschten Funktion ohne Wissen des Anwenders noch eine versteckte Funktion erfüllen. So können sie z.B. Eingaben des Nutzers mitschneiden oder den Webbrowser des Nutzers auf unerwünschte Websites umleiten. Vgl. auch Malware.

UBE *Unsolicited Bulk Email* bezeichnet unerwünschte, massenhaft versendete Emails. Im Gegensatz zu UCE müssen diese ncht zwangsläufig kommerziellen Inhaltes sein. Vgl. zu UBE auch Kapitel 2.1.2.

UCE *Unsolicited Commercial Email* bezeichnet unerwünschte Emails kommerziellen Inhalts. Obwohl UCE nicht zwangsläufig massenhaft versendet werden muss, gilt sie zumeist als Untermenge von UBE. Vgl. zu UCE auch Kapitel 2.1.2.

URIDNSBL *Uniform Resource Identifier Domain Name System Blacklists* beinhalten die IP-Adressen von Web- oder DNS-Servern, die von Spammer verwendet werden, zum Zwecke der Filterung von Spam-Emails. Vgl. hierzu auch Kapitel 3.4.1.

Virus Ein *Computervirus* ist ein Programm, das sich selbst in andere Programme einschleust und auf diese Weise reproduziert. Oftmals wird der Begriff auch für andere Arten von Malware wie z.B. Würmer verwendet. Im Gegensatz zu Würmern verbreitet sichein Virus jedoch nicht selbstständig auf andere Rechner. Vgl. auch Malware.

VoIP *Voice over IP*, auch Internet-Telefonie genannt, bezeichnet das Telefonieren über ein Computernetzwerk auf der Basis des Internetprotokolls (IP).

Weblog Ein *Weblog*, oft auch nur kurz *Blog* genannt, ist eine Website mit regelmäßig aktualisierten Einträgen, wobei der jeweils neueste Eintrag an oberster Stelle steht und ältere Artikel in umgekehrt chronologischer Reihenfolge folgen.

Whitelist Eine *Whitelist* in Zusammenhang mit Emails und Spam ist eine Liste von vertrauenswürdigen, legitimen Absendern, IP-Adressen o.ä. *whitelists* werden eingesetzt, um das versehentliche Filtern von Emails durch z.B. Blacklists zu vermeiden.

Wurm Ein *Computerwurm* ist ein Programm, dass sich über Netzwerke, z.B. über Sicherheitslücken, selbstständig verbreitet. Vgl. auch Malware.

Zombie-PC Ein *Zombie-PC* ist ein an das Internet angeschlossener Rechner, der durch Viren, Trojaner oder ähnlicher Programme unter die Kontrolle eines Dritten gebracht wurde. Zombie-PCs werden oftmals in Botnets zusammengefasst, um z.B. Spam zu verbreiten oder dDoS-Attacken zu starten. Vgl. Kapitel 3.3.4.

Verzeichnis der aufgeführten Organisationen

ACMA Die *Australian Communications and Media Authority* ist die australische Regulierungsbehörde im Bereich TV, Radio und Telekommunikation sowie dem Internet. Weitere Informationen bietet die Behörde unter http://www.acma.gov.au/.

AOL *AOL*, ehemals ausgeschrieben *America Online*, ist der weltweit größten ISPs mit mehr als 30 Millionen Kunden. Online findet sich AOL unter http://www.aol.com/.

APWG Die *Anti-Phishing Working Group* ist ein Interessensverband der Internetwirtschaft zur Bekämpfung von Identitätsdiebstahl und Betrug durch Phishing und ähnliche Attacken mit mittlerweile weit über 2000 Mitgliedern, darunter Banken, ISPs und Behörden. Die APWG findet sich online unter http://www.antiphishing.org/.

ASEM Das *Asia-Europe Meeting* ist ein informelles Dialogforum zwischen europäischen und asiatischen Staaten mit derzeit 39 Teilnehmern, das sich mit der Zusammenarbeit in Wirtschaft, Politik, Bildung und Kultur beschäftigt. Weitere Informationen finden sich unter http://www.aseminfoboard.org/.

BMELV Das *Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz* ist online zu finden unter http://www.bmelv.de/.

BMWi Das *Bundesministerium für Wirtschaft und Technologie* ist online zu finden unter http://www.bmwi.de/.

BSA Die *Business Software Alliance* ist ein internationaler Interessenverband von Softwareanbietern und deren Hardware-Partnern. Nähere Informationen finden sich unter http://www.bsa.org/.

Bundesnetzagentur Die *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* hat die Aufgabe, durch Liberalisierung und Deregulierung eine weitere Entwicklung des Elektrizitäts-, Gas-, Telekommunikations-, Post- und Eisenbahninfrastrukturmarktes zu unterstützen. Sie findet sich online unter http://www.bundesnetzagentur.de/.

Certified Senders Alliance Die *Certified Senders Alliance* ist ein durch den eco und den DDV initiiertes Positivlistenprojekt, das seriöse Direktwerber auf eine Whitelist aufnimmt, so dass diese von den Spamfiltern teilnehmender Mailprovider nicht ausgefiltert werden. Weitere Informationen bietet http://csa.eco.de/.

CNSA Das *Contact Network of Spam enforcing Agencies* ist ein EU-weites, informelles Netzwerk der nationalen Institutionen, die sich mit der Bekämpfung von Spam beschäftigen. Deutsche Kontaktstellen sind derzeit der eco sowie die Bundesnetzagentur; das BMWi beteiligt sich ebenfalls an dieser Initiative.

Commtouch *Commtouch* ist ein Hersteller von Anti-Viren- und Anti-Spam-Software für den Unternehmensbereich. Im Rahmen seiner Arbeit stellt das Unternehmen auf seiner Website (http://www.commtouch.com/) in Echtzeit aktualisierte Daten über Spam, Viren etc. bereit.

DARPA Die *Defense Advanced Reasearch Project Agency* ist die Agentur des US-Verteidigungsministeriums, die Hightech-Projekte für das US-Militär durchführt. Unter anderem wurde von ihr das ARPANET entwickelt, aus dem das Internet hervorging. Die DARPA findet sich online unter http://www.darpa.mil/.

DDV Der *Deutsche Direktmarketing Verband* ist die Interessenvertretung der deutschen Direktwerber. Online erreichbar ist der DDV unter http://www.ddv.de.

eBay *eBay* ist der weltweit größte Anbieter von Internetauktionen und online zu finden unter http://www.ebay.com/.

eco Der *Verband der deutschen Internetwirtschaft* ist die Interessenvertretung der deutschen Internetwirtschaft mit z.Z. etwa 300 Mitgliedern. Online ist der eco erreichbar unter http://www.eco.de/.

EFF Die *Electronic Frontier Foundation* ist eine in den USA gegründete NGO, die sich mit den Bürgerrechten im Cyberspace beschäftigt. Sie ist online zu finden unter http://www.eff.org/.

Forrester Custom Consumer Research *Forrester* ist ein weltweit tätiges Technologie- und Marktforschungsunternehmen. Weitere Informationen zum Unternehmen finden sich auf der Unternehmenswebsite unter http://www.forrester.com/.

FTC Die *Federal Trade Commission*, die US-amerikanische Handelskommission ist als Wettbewerbsbehörde zuständig für die Zusammenschlusskontrolle, aber auch für den Verbraucherschutz. Weitere Informationen finden sich auf der Website der FTC unter http://www.ftc.gov/.

GIAIS Die *Global Infrastructure Alliance for Internet Safety* ist eine von Microsoft unterstützte Arbeitsgruppe der großen ISPs zur Steigerung der Sicherheit im Internet und zur Bekämpfung des Missbrauchs. Weitere Informationen finden sich unter http://www.microsoft.com/serviceproviders/resources/securitygiais.mspx.

iCAUCE die *international Coalition Against Unsolicited Commercial Email* ist die Dachorganisation mehrerer NGOs, die sich in den jeweiligen Regionen und Staaten gegen Spam und vor allem für die Erarbeitung gestzlicher Verbote gegen sowohl UCE als auch UBE einsetzt. Einen wesentlichen Aspekt nimmt hierbei die Verbreitung sogenannter Opt-In-Regelungen ein. Die Organisation findet sich online unter http://www.international.cauce.org/.

IETF Die *Internet Engineering Task Force* beschäftigt sich mit der Erarbeitung und Förderung von Internet-Standards und RFCs. Online ist die IETF unter http://www.ietf.org/ zu finden

Initiative D21 Die *Initiative D21* ist nach eigener Aussage Europas größte Public-Private-Partnership, bestehend aus 200 Mitgliedunternehmen und -organisationen. Ziel des geminnützigen Vereins ist die Stimulierung wirtschaftlichen Wachstums durch Förderung von Bildung, Qualifikation und Innovationsfähigkeit. In Zusammenarbeit mit dem BMWi betreibt die Initiative D21 das Projekt *Internet Gütesiegel* zur Erarbeitung von Qualitätskriterien von insbesondere im eCommerce eingesetzen Gütesiegeln. Weitere Informationen zu den anderen Projekten der Initiative finden sich unter http://www.initiatived21.de/.

ISC Die *Internet Society of China*, deren Mitglieder sich aus Unternehmen, Forschungsinstituten, Universitäten etc. zusammensetzen, beschäftigt sich mit der Weiterentwicklung des Internets in China. Die ISC betreibt eine englischsprachige Website unter http://www.isc.org.cn/English/.

ITU Die *International Telecommunication Union* beschäftigt sich als einzige Organisation offiziell und weltweit mit technischen Aspekten der Telekommunikation mit dem Ziel der Abstimmung und Förderung der internationalen Zusammenarbeit im Nachrichtenwesen. Sie ist eine Teilorganisation der Vereinten Nationen mit derzeit 190 Mitgliedsländern. Online ist die ITU unter http://www.itu.int/ zu finden.

KISA Die *Korean Information Security Agency* ist zuständig für die Bekämpfung des Missbrauchs dess Internets in Südkorea. Die Organisation bietet eine englischsprachige Website unter http://www.kisa.or.kr/maine.jsp an.

LAP Der *London Action Plan* ist ein internationales Forum von Behörden, die sich mit der Bekämpfung von Spam beschäftigen, zur Stärkung der internationalen Zusammenarbeit in diesem Bereich. Nähere Informationen finden sich unter http://www.londonactionplan.org/.

MAAWG Die *Messaging Anti-Abuse Working Group* ist eine Gruppe von Telekommunikationsunternehmen mit dem Ziel der Bekämpfung von Spam, Phishing und ähnlichem Missbrauch, die von dem US-amerikanischen Unternehmen OpenWave initiiert wurde. Informationen zur MAAWG finden sich unter www.maawg.org/.

Microsoft *Microsoft* ist der weltweit größte Anbieter und Hersteller von Software, u.a. das Betriebssystem Windows und das Office-Paket. *Microsoft EMEA* ist der für Europa, den Mittleren Osten sowie Afrika zuständige Teil des Unternehmens. Online findet sich Microsoft unter http://www.microsoft.com/.

NASK *Naukowa i Akademicka Siec Komputerowa*, zu deutsch 'Forschungs- und akademisches Computernetzwerk', ist u.a. Registrar der polnischen Länderdomain *.pl*. Zusammen mit dem eco arbeitet NASK am SpotSpam-Projekt. Die Organisation bietet eine englischsprachige Website unte http://www.nask.pl/.

OECD Die *Organisation for Economic Co-operation and Development* ist eine internationale, strikt intergovernmentale Organisation mit derzeit 30 Mitgliedern, die sich mit der Steigerung des Wirtschaftwachstums und des Lebensstandards in Mitglieds- und Entwicklungsländern sowie der Ausweitung des Welthandels beschäftigt. Weitere Informationen können unter http://www.oecd.org/ abgerufen werden.

OFISP Das *Open Forum of the Internet Providers* ist ein Zusammenschluss russischer ISPs und anderer Mitglieder der russischen Internet-Gemeinschaft und sieht sich als Dialog- und Diskussionsforum und Interessensvertretung seiner Mitglieder. Eine englischsprachige WEbsite ist verfügbar unter http://www.ofisp.org/engl/.

OpenWave *OpenWave* ist ein US-amerikanisches Telekommunikationsunternehmen und Gründer der MAAWG. Die Website des Unternehmens findet sich unter http://www.openwave.com/.

OPTA Die *Onafhankelijke Post en Telecommunicatie Autoriteit* ist die niederländische Post- und Telekommunikations-Regulierungsbehörde. Derzeit leitet sie u.a. die CNSA. Online ist die OPTA erreichbar unter http://www.opta.nl/.

Sophos *Sophos* ist ein US-amerikanischer, weltweit aktiver Hersteller von Anti-Viren- und Anti-Spam-Produkten. Die Website des Unternehmens findet sich unter http://www.sophos.com/.

Spamhaus Das *Spamhaus*-Projekt ist eine größtenteils aus Freiwilligen bestehende Organisation, die sich zum Ziel gesetzt hat, Email-Spammer und Spam-Aktivitäten zu verfolgen. Hierzu betreibt das Projekt zwei von vielen ISPs eingesetzte Blacklists sowie die ROKSO-Liste, einer Datenbank der weltweit aktivsten Spammer. Die Blacklists sowie die ROKSO-Liste sind verfügbar auf der Website des Projekts unter http://www.spamhaus.org/.

SpotSpam *SpotSpam* ist ein durch den eco und die NASK initiiertes, von der EU gefördertes Projekt einer EU-weiten Spambox, in der Spam-Emails gesammelt und ausgewertet werden sollen. Weitere Informationen finden sich auf der Projekt-Website unter http://www.spotspam.org/.

vzbv Der *Verbraucherzentrale Bundesverband* ist die Dachorganisation der Verbraucherzentralen der Bundesländer sowie von diversen verbraucherpolitischorientierten Verbänden. Er vertritt die Interessen der Verbraucher gegenüber Politik, Wirtschaft und Zivilgesellschaft. Online ist der vzbv unter http://www.vzbv.de/ zu finden.

WBZ Die *Zentrale zur Bekämpfung des unlauteren Wettbewerbs* ist ein branchenübergreifender Zusammenschluss von Unternehmen und Wirtschaftsorganisationen und beschäftigt sich u.a. mit dem Erhalt des Wettbewerbs sowie der Verfolgung vpn Wettbewerbsverstößen. Die WBZ ist online erreichbar unter http://www.wettbewerbszentrale.de/.

WSIS Der *World Summit on the Information Society* ist ein von den Vereinten Nationen gesponsorter und durch die ITU durchgeführter Weltgipfel zu den Themen Information und Kommunikation, der im Dezember 2003 in Genf sowie im November 2005 in Tunis stattfand und auf dem vielfätige Themen dieses Bereiches diskutiert wurden. WEitere Informationen bietet die Website unter http://www.itu.int/wsis/.

Yahoo *Yahoo* ist eines der weltweit größten Internetportale und Anbieter von diversen Dienstleistungen wie Email-Accounts u.ä. *Yahoo* ist online zu finden unter http://www.yahoo.com/.

Tabellen und Abbildungen

Tabellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

2002/58/EG EU-PARLAMENT UND -RAT (Hrsg.): *Richtlinie 2002/58/EG*. Juli 2002. – URL http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:DE:PDF. – Zugriffsdatum: 08.02.2006

5691/04 TELECOM 11 EU-PRÄSIDENTSCHAFT (Hrsg.): *Unsolicited communications for direct marketing purposes or spam – Presidency Paper. 5691/04 TELECOM 11*. November 2004. – URL http://register.consilium.eu.int/pdf/en/04/st15/st15148.en04.pdf. – Zugriffsdatum: 08.02.2006

Altovsky 2005 ALTOVSKY, Eugene: *Legal status of spam in Russia*. April 2005. – URL http://ifap.ru/eng/projects/as01.doc. – Zugriffsdatum: 08.02.2006

ASTA 2004 ASTA (Hrsg.): *Anti-Spam Technical Alliance Technology and Policy Proposal*. Juni 2004. – URL http://docs.yahoo.com/docs/pr/pdf/asta_soi.pdf. – Zugriffsdatum: 08.02.2006

aunty-spam.com 2005 AUNTY-SPAM.COM (Hrsg.): *Russia says „Nyet" to Anti-Spam Laws*. März 2005. – URL http://www.aunty-spam.com/russia-says-nyet-to-anti-spam-laws/. – Zugriffsdatum: 08.02.2006

Barakat 2004 BARAKAT, Mathew: "Man findet genug Idioten". In: *stern online* (2004), November. – URL http://www.stern.de/computer-technik/internet/?id=532963. – Zugriffsdatum: 08.02.2006

Brauch 2004 BRAUCH, Patrick: Geld oder Netz! In: *c't* (2004), Nr. 14, S. 48. – URL http://www.heise.de/ct/04/14/048/. – Zugriffsdatum: 08.02.2006

BSI 2005 BSI (Hrsg.): *Anti-Spam-Strategien*. Bonn : Bundesamt für Sicherheit in der Informationstechnik, 2005

CNSA 2004 CNSA (Hrsg.): *Cooperation procedure concerning the transmission of complaint information and intelligence relevant to the enforcement of article 13 of the privacy and electronic communication directive 2002/58/EC, or any other applicable national law*

pertaining to the use of unsolicited electronic communications. Dezember 2004. – URL http://europa.eu.int/information_society/policy/ecomm/doc/todays_framework/privacy_protection/spam/cooperation_procedure_cnsa_final_version_20041201.pdf. – Zugriffsdatum: 08.02.2006

c't 2004 N.N.: Ferngesteuerte Spam-Armeen. In: *c't* (2004), Nr. 5, S. 18–22. – URL http://www.heise.de/kiosk/archiv/ct/2004/5/18. – Zugriffsdatum: 08.02.2006. – kostenpflichtige Online-Version

Dietrich und Pohlmann 2005 DIETRICH, Christian J. ; POHLMANN, Norbert: Spam auf dem Rückmarsch? In: *IT-Sicherheit* (2005), Nr. 4, S. 32, 33

DS 15(9)1864 BUNDESTAG, Deutscher (Hrsg.): *Schriftliche Stellungnahme zur öffentlichen Anhörung am 18. April 2005, Heise Zeitschriften Verlag GmbH & Co. KG. Bundestags-Drucksache 15(9)1864*. April 2005

DS 15/2655 KROGMANN, Martina u. a.: *Spam effektiv bekämpfen (Antrag). Bundestags-Drucksache 15/2655*. März 2004. – URL http://dip.bundestag.de/btd/15/026/1502655.pdf

DS 15/4835 FRAKTIONEN SPD UND BÜNDNIS 90/DIE GRÜNEN: *Entwurf eines Zweiten Gesetzes zur Änderung des Teledienstegesetzes (Anti-Spam-Gesetz). Bundestags-Drucksache 15/4835*. Februar 2005. – URL http://dip.bundestag.de/btd/15/048/1504835.pdf

DS 15(9)1848 BUNDESTAG, Deutscher (Hrsg.): *Materialien zur öffentlichen Anhörung am 18. April 2005, Zusammenstellung der schriftlichen Stellungnahmen. Bundestags-Drucksache 15(9)1848*. April 2005. – URL http://www.bundestag.de/ausschuesse/archiv15/a09/eanhoerungen/oantispam/bmaterialien.pdf. – Zugriffsdatum: 08.02.2005

Ermert 2005 ERMERT, Monika: Die Spam-Jäger. In: *Die Zeit* (2005), Nr. 42. – URL http://www.zeit.de/2005/42/Spam-J_8ager. – Zugriffsdatum: 08.02.2006

Frank 2004 FRANK, Thomas: *Zur strafrechtlichen Bewältigung des Spamming*. Berlin : Logos Verlag, 2004

Galloway 2004 GALLOWAY, Colin: Spammers hide behind the Great Wall. In: *Asia Times online* (2004), Dezember. – URL http://atimes.com/atimes/China/FL14Ad02.html. – Zugriffsdatum: 08.02.2006

Hafner und Lyon 2003 HAFNER, Katie ; LYON, Matthew: *Where wizards stay up late*. London [u.a.] : Pocket Books, 2003

Honeynet 2005 HONEYNET PROJECT (Hrsg.): *Know your Enemy: Tracking Botnets*. März 2005. – URL http://www.honeynet.org/papers/bots/. – Zugriffsdatum: 08.02.2006

Johnson 1999 JOHNSON, Kevin: *Internet Email Protocols. A Developer's Guide*. Reading [u.a.] : Addison-Wesley, 1999

Kim 2005 KIM, Tae-gyu: Weak Anti-Spam Measures Invite Criticism. In: *The Korea Times* (2005), Januar. – URL http://times.hankooki.com/lpage/200501/kt2005011916321653460.htm. – Zugriffsdatum: 21.02.2006

KOM(2004)759 EU-KOMMISSION (Hrsg.): *Europäische Vorschriften zur elektronischen Kommunikation und Märkte 2004. KOM(2004) 759 endgültig*. Dezember 2004. – URL http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0759:DE:HTML. – Zugriffsdatum: 08.02.2006

Le Toquin 2005 LE TOQUIN, Jean C.: *European Spam Project „SpotSpam"*. September 2005. – URL http://www.eco.de/servlet/PB/show/1653610/1_%20jc%20letoquin.ppt. – Zugriffsdatum: 07.02.2006. – Präsentation im Rahmen des 3. deutschen Anti-Spam-Kongresses in Köln

Leiner u. a. 2003 LEINER, Barry M. u. a.: *A Brief History of the Internet*. Dezember 2003. – URL http://www.isoc.org/internet/history/brief.shtml. – Zugriffsdatum: 08.02.2006

Li 2006 LI, Xinran: China declares its war on spam. In: *Shanghai Daily online* (2006), Februar. – URL http://www.shanghaidaily.com/art/2006/02/21/243441/China_declares_its_war_on_spam.htm. – Zugriffsdatum: 21.02.2006

Linford 2005 LINFORD, Steve: Keynote Speech at ITU WSIS Thematic Meeting on Cybersecurity. (2005), Juni. – URL www.itu.int/osg/spu/cybersecurity/presentations/keynote-linford-spamhaus.pdf. – Zugriffsdatum: 08.02.2006

McWilliams 2005 MCWILLIAMS, Brian: Russians, not Ralsky, now rule the spam world. In: *Spam Kings Weblog* (2005), November. – URL http://spamkings.oreilly.com/archives/2005/11/russians_not_ralsky_now_rule_t.html. – Zugriffsdatum: 08.02.2006

MessageLabs 2006 MESSAGELABS (Hrsg.): *MessageLabs Intelligence 2005 Annual Security Report*. Januar 2006. – URL http://www.messagelabs.com/portal/server.pt/gateway/PTARGS_0_0_389_594_-594_43/http%3B/0120-0176-CTC1%3B8080/publishedcontent/publish/_dotcom_libraries_en/files/monthly_reports/2005_annual_report_5.pdf. – Zugriffsdatum: 22.02.2006

OECD 2005 OECD TASK FORCE ON SPAM (Hrsg.): *Outline for the OECD Anti-Spam toolkit (work plan). DSTI/CP/ICCP/SPAM(2004)1/FINAL*. Mai 2005. – URL http://www.oecd.org/dataoecd/22/21/34874504.pdf. – Zugriffsdatum: 08.02.2006

Pößneck 2005 PÖSSNECK, Lutz: Die kriminelle Parallelwelt der Botnets. In: *silicon.de* (2005), Juni. – URL http://www.silicon.de/cpo/ts-antivirus/detail.php?nr=21675. – Zugriffsdatum: 08.02.2006

Protokoll 15/89 BUNDESTAG, Deutscher (Hrsg.): *Wortprotokoll 89. Sitzung, Ausschuss für Wirtschaft und Arbeit. Ausschussprotokoll 15/89*. April 2005. – URL http://www.bundestag.de/ausschuesse/archiv15/a09/eanhoerungen/oantispam/cprotokoll.pdf. – Zugriffsdatum: 08.02.2006

RFC1869 KLENSIN, John u. a.: *RFC 1869: SMTP Service Extensions*. November 1995. – URL http://www.ietf.org/rfc/rfc1869.txt. – Zugriffsdatum: 08.02.2006

RFC2440 CALLAS, Jon u. a.: *RFC 2440: OpenPGP Message Format*. November 1998. – URL http://www.ietf.org/rfc/rfc2440.txt. – Zugriffsdatum: 08.02.2006

RFC2554 MYERS, John G.: *RFC 2554: SMTP Service Extension for Authentication*. März 1999. – URL http://www.ietf.org/rfc/rfc2554.txt. – Zugriffsdatum: 08.02.2006

RFC2821 KLENSIN, John: *RFC 821: Simple Mail Transfer Protocol*. April 2001. – URL http://www.ietf.org/rfc/rfc2821.txt. – Zugriffsdatum: 08.02.2006

RFC2920 FREED, Ned: *RFC 2920: SMTP Service Extension for Command Pipelining*. September 2000. – URL http://www.ietf.org/rfc/rfc2920.txt. – Zugriffsdatum: 08.02.2006

RFC3461 MOORE, Keith: *RFC 3461: Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)*. Januar 2003. – URL http://www.ietf.org/rfc/rfc3461.txt. – Zugriffsdatum: 08.02.2006

RFC3850 RAMSDELL, Blake: *RFC 3850: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling*. Juli 2004. – URL http://www.ietf.org/rfc/rfc3850.txt. – Zugriffsdatum: 08.02.2006

RFC3851 RAMSDELL, Blake: *RFC 3851: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification*. Juli 2004. – URL http://www.ietf.org/rfc/rfc3851.txt. – Zugriffsdatum: 08.02.2006

RFC821 POSTEL, Jonathan B.: *RFC 821: Simple Mail Transfer Protocol*. August 1982. – URL http://www.ietf.org/rfc/rfc821.txt. – Zugriffsdatum: 08.02.2006

Röß 1995 RÖSS, Dieter: *Zinsen und Betrügerische Spiele*. Dezember 1995. – URL http://www.tu-berlin.de/www/software/hoax/amuesant/index.html. – Zugriffsdatum: 20.02.2006

Roth 2004 ROTH, Wolf-Dieter: Spam, Betrug und Drogen. In: *Telepolis* (2004), Februar. – URL http://www.heise.de/tp/r4/artikel/16/16665/1.html. – Zugriffsdatum: 08.02.2006

Rötzer 2006 RÖTZER, Florian: Porto für Emails. In: *Telepolis* (2006), Februar. – URL http://www.heise.de/tp/r4/artikel/21/21964/1.html. – Zugriffsdatum: 08.02.2006

Schmidt 2003 SCHMIDT, Holger: Milliarden von Spam-Mails bedrohen das Internet. (2003), Mai. – URL http://www.faz.net/s/RubE2C6E0BCC2F04DD787CDC274993E94C1/Doc~EC1A853D786954C2CAC7E49104FF8A62F~ATpl~Ecommon~Scontent.html. – Zugriffsdatum: 28.02.2006

Spamhaus 2004 SPAMHAUS (Hrsg.): *Follow Australia!* Juli 2004. – URL http://www.spamhaus.org/news.lasso?article=154. – Zugriffsdatum: 08.02.2006

Stevenson 2005 STEVENSON, Robert Louis B.: Plugging the „phishing“ hole: legislations versus technology. In: *Duke Law & Technology Review* (2005), Nr. 6. – URL http://www.law.duke.edu/journals/dltr/articles/2005dltr0006.html. – Zugriffsdatum: 08.02.2006

Traufetter 2003 TRAUFETTER, Gerald: Schatzkarte für Terroristen. In: *Der Spiegel* (2003), Nr. 32, S. 128, 129. – URL http://www.spiegel.de/spiegel/0,1518,259739,00.html. – Zugriffsdatum: 08.02.2006. – kostenpflichtige Online-Version

Voß 1875 VOSS, Johann H. ; GÜTHLING, Otto (Hrsg.): *Vergilis Äneide*. Philipp Reclam jun., 1875. – URL http://gutenberg.spiegel.de/vergil/aeneis/aeneis.htm. – Zugriffsdatum: 18.02.2006

Warden 2004 WARDEN, Graeme: *Russia and China 'behind current spam deluge'*. Juni 2004. – URL http://www.zdnet.com.au/insight/toolkit/security/systems/0,39023913,39150051,00.htm. – Zugriffsdatum: 08.02.2006

Weber 2004 WEBER, Roman G.: Phishing: Brauchen wir einen Sondertatbestand zur Verfolgung des Internetphishings? In: *HRR-Strafrecht* (2004), Nr. 12, S. 406–410. – URL http://hrr-strafrecht.de/hrr/archiv/04-12/index.php3?seite=6. – Zugriffsdatum: 08.02.2006

Williams 2003 WILLIAMS, Martyn: Spam falls after South Korea strengthens e-mail law. In: *Computerworld* (2003), September. – URL http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,84963,00.html?from=imutopicheads. – Zugriffsdatum: 08.02.2006

Wood 1999 WOOD, David: *Programming Internet Email*. Beijing [u.a.] : O'Reilly, 1999

Ziemann 2005 ZIEMANN, Frank: Spear Phishing auf dem Vormarsch. In: *PC-Welt* (2005), Oktober. – URL http://www.pcwelt.de/news/sicherheit/122964/index.html. – Zugriffsdatum: 08.02.2006