JUSTUS-LIEBIG-UNIVERSITÄT GIESSEN
PROFESSUR BWL – WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Bodenbender, Renè; Schick, Lukas; Schwickert, Axel;
Patzak, Maxilmilian

Client- und Server-seitige Maßnahmen gegen E-Mail-Spam

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 7 / 2019
ISSN 1613-6667

Arbeitspapiere WI Nr. 7 / 2019

Autoren: Bodenbender, René; Schick, Lukas; Schwickert, Axel; Patzak, Maximilian

Titel: Client- und Server-seitige Maßnahmen gegen E-Mail-Spam

Zitation: Bodenbender, René; Schick, Lukas; Schwickert, Axel; Patzak, Maximilian: Client- und Server-seitige Maßnahmen gegen E-Mail-Spam, in: Arbeitspapiere WI, Nr. 7/2019, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2019, 37 Seiten, ISSN 1613-6667.

Kurzfassung: Im vorliegenden Arbeitspapier WI „Client- und Server-seitige Maßnahmen gegen E-Mail-Spam“ wird erläutert, was unter E-Mail-Spam zu verstehen ist und mithilfe welcher Technik bzw. mithilfe welchen Vorgehens dieser versandt wird. Dabei wird zwischen der Beschaffung von E-Mail-Adressen, den technischen Maßnahmen zum Versand von E-Mail-Spam und den Arten des E-Mail-Spams unterschieden und aufgezeigt, welche Sicherheitsrisiken E-Mail-Spam verursachen kann. Des Weiteren wird dargestellt, was der Unterschied zwischen Client- und Server-seitigen Maßnahmen zur Abwehr von E-Mail-Spam ist. Basierend auf diesen Maßnahmen zur Abwehr von E-Mail-Spam werden Konfigurationsbeispiele von E-Mail-Clients und E-Mail-Servern beschrieben, um die Anwendungsorientierung zu verdeutlichen. Im vorliegenden Arbeitspapier wird gezeigt, wie E-Mail-Spam „funktioniert“ und wie sich Anwender und Administratoren in alltäglichen Situationen gegen E-Mail-Spam wehren können.

Schlüsselwörter: Electronic Mail, Spam, Client, Server, Open Relays, E-Mail, E-Mail-Filter, Spamihilator, SpamSieve, Outlook, Thunderbird, Webmail, Apple Mail, Anwender, Administratoren

Inhaltsverzeichnis

Abbildungsverzeichnis

Seite

1 Problemstellung, Ziel und Aufbau der Arbeit

Der geschätzte relative Anteil an weltweitem E-Mail-Spam ist in den vergangenen vier Jahren zwar um etwa 18 Prozentpunkte gesunken,[1] in absoluten Zahlen jedoch gestiegen. So berichtet der E-Mail-Dienst „Web.de“ 2015 beispielsweise von pro Tag etwa 205,6 Milliarden versendeten und empfangenen E-Mails.[2] Im gleichen Jahr schätzt das Statistik-Portal „statista“ den Anteil von E-Mail-Spam auf ungefähr 53 Prozent.[3] Dies entspricht in etwa 109 Milliarden Spam-E-Mails pro Tag im Jahr 2015. Im Jahr 2018 schätzt das Statistik-Portal „statista“ den E-Mail-Verkehr pro Tag auf rund 281 Milliarden E-Mails.[4] Dahingegen hat sich laut Schätzungen der Anteil der Spam-E-Mails auf rund 48 Prozent verringert.[5] Daraus lässt sich schließen, dass die absolute Anzahl an Spam-E-Mails pro Tag seit 2015 um 26 Milliarden auf ungefähr 135 Milliarden pro Tag im Jahr 2018 gestiegen ist. Zukünftig ist mit einem weiteren Anstieg des gesamten E-Mail-Verkehrs zu rechnen, wodurch das Problem des E-Mail-Spam weiterhin zunehmen wird.[6]

Diese hohe Anzahl an Spam-E-Mails verursacht weltweit jährlich wirtschaftliche Schäden in Höhe von etwa 38 Milliarden Euro. Neben den monetären Kosten von E-Mail-Spam entstehen aber auch Opportunitätskosten und Produktivitätsverluste für Unternehmen, die mit etwa 1500 Euro pro Mitarbeiter pro Jahr beziffert werden können.[7] Diese Bewertung der Opportunitätskosten resultiert aus der Arbeitszeit, die die Mitarbeiter beim manuellen Ausfiltern der Spam-E-Mails aus dem E-Mail-Postfach und dem Sichten des E-Mail-Spam-Ordners aufwenden müssen.

E-Mail-Spam findet jedoch auch den Weg in die Postfächer privater Nutzer. Der an dieser Stelle entstehende Schaden ist schwer zu beziffern, da es sich meist um verlorene Freizeit und eine Strapazierung der Nerven beim Filtern des E-Mail-Postfachs handelt. Werden Spam-E-Mails

1 Vgl. Wagner, Patrick: Spamfilter haben immer weniger zu tun, Online im Internet: https://de.statista.com/infografik/14912/anteil-von-spam-am-weltweiten-mailverkehr/, 30.07.2018.

2 Vgl. Kramp, Linda: E-Mail-Aufkommen nimmt weltweit weiter zu, Online im Internet: https://newsroom.web.de/2015/05/19/e-mail-aufkommen-nimmt-weltweit-weiter-zu/, 19.05.2015.

3 Vgl. Wagner, Patrick: Spamfilter haben immer weniger zu tun, a. a. O.

4 Vgl. o. V.: Prognose zur Anzahl der täglich versendeten und empfangenen E-Mails weltweit von 2018 bis 2022 (in Milliarden), Online im Internet: https://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/, 03.11.2018.

5 Vgl. Wagner, Patrick: Spamfilter haben immer weniger zu tun, a. a. O.

6 Vgl. o. V.: Prognose zur Anzahl der täglich versendeten und empfangenen E-Mails weltweit von 2018 bis 2022 (in Milliarden), a. a. O.

7 Vgl. Pempel, Kacper: Spam verursacht jährlich einen Schaden von 38 Mrd. Euro, Online im Internet: https://diepresse.com/home/techscience/internet/sicherheit/1430918/Spam-verursacht-jaehrlich-Schaden-von-38-Mrd-Euro-, 16.07.2013 & Rao, Justin; Reiley, David: The Economics of Spam, Online im Internet: https://www.aeaweb.org/articles?id=10.1257/jep.26.3.87, 03.11.2018.

nicht gelöscht, kann es dazu führen, dass die Kapazität des E-Mail-Postfaches nicht mehr ausreichend ist, um weitere gewünschte E-Mails empfangen zu können. Außerdem können gewünschte E-Mails in der Flut von E-Mail-Spam leicht übersehen werden.[8]

Neben der Vergeudung von Freizeit und dem Verlust von Informationen kann es aber auch zu finanziellen Schäden kommen. So kann E-Mail-Spam zum Beispiel nicht nur unerwünschte Werbung enthalten, sondern auch Viren und Malware. Außerdem wird über Spam-E-Mails das sog. „Phishing" betrieben. Beim „Phishing" handelt es sich um das Ausspähen von benutzerspezifischen Zugangsdaten, die beispielsweise für das Online-Banking nötig sind und für kriminelle Zwecke missbraucht werden können.[9]

Das Phänomen „E-Mail-Spam" ist also für jegliche Nutzer des Kommunikationsmediums E-Mail sowohl im privaten als auch im geschäftlichen Bereich ein großes Problem.

Ziel dieser Arbeit ist es, das Problem E-Mail-Spam auf der Versender- und der Empfängerseite zu analysieren und Lösungskonzepte zur Abwehr von E-Mail-Spam zu erarbeiten. Zu diesem Zweck werden in Kapitel 2 die Begriffe „E-Mail" und „Spam" definiert und voneinander abgegrenzt. In Kapitel 2.2 wird der Begriff „E-Mail" auf Basis technischer Grundlagen definiert. Kapitel 2.3 liefert eine allgemeine Definition des Begriffes „Spam", unabhängig vom Begriff „E-Mail" sowie eine Zusammenführung der beiden Begriffe. In Kapitel 2.4 erfolgt eine Abgrenzung des Begriffes „E-Mail-Spam" von ähnlichen Begriffen aus diesem Kontext. Die in Kapitel 2 erarbeiteten Definitionen und Abgrenzungen der für die Arbeit wichtigen Begriffe dienen als Grundlage für das Verständnis von Kapitel 3 und 4.

In Kapitel 3 wird die Versenderseite des E-Mail-Spam betrachtet. Die in Kapitel 3 erarbeiteten Ergebnisse dienen als Grundlage für Kapitel 4, in welchem Abwehrmaßnahmen gegen E-Mail-Spam auf der Empfängerseite erarbeitet werden. Dabei wird explizit auf die in Kapitel 3 erarbeiteten Vorgehensweisen Bezug genommen.

Im ersten Schritt werden in Kapitel 3.2 die Beschaffungswege von E-Mail-Adressen dargelegt und in Kapitel 3.3 die technischen Grundlagen für den Versand von E-Mail-Spam erläutert. In Kapitel 3.4 werden dann die in Kapitel 2.4 erarbeiteten Unterscheidungen noch einmal aufgegriffen und detaillierter erläutert.

In weiterer Folge wird in Kapitel 4.2 der Fokus auf Client-seitige Maßnahmen auf der Empfängerseite gelegt, wobei in Kapitel 4.2.1 präventive Maßnahmen erläutert und in Kapitel 4.2.2 allgemein die Filteroptionen der E-Mail-Clients dargestellt und diskutiert werden. In Kapitel 4.2.3 werden darauf folgend spezielle Tools und Systeme vorgestellt, die es dem Anwender ermöglichen, gegen E-Mail-Spam vorzugehen. Anschließend werden in Kapitel 4.3.1 Server-

8 Vgl. Schneider, Markus; Winter, Christian; Yannikos, York: Untersuchung von Spam-Eigenschaften kostenfreier Email-Dienste, 2010, S. 14.

9 Vgl. o. V.: verbraucherzentrale.de: Spam: E-Mail-Müll im Internet, Online im Internet: https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/spam-emailmuell-im-internet-10757, 03.05.2018.

seitige Maßnahmen zur Konfiguration eines E-Mail-Servers beschrieben. In Kapitel 4.3.2 folgt eine Bewertung der zuvor erarbeiteten Maßnahmen unter den Gesichtspunkten der Effektivität und rechtlicher Vorgaben.

Kapitel 5 gibt abschließend einen Ausblick auf die Entwicklung und Bedeutung des Kommunikationsmediums E-Mail und der damit verbundenen Problematik des E-Mail-Spam.

2 Begriffsdefinitionen und -abgrenzungen

2.1 Systematisierung der Begriffsdefinitionen

Wie bereits in Kapitel 1 erwähnt, erfolgt in Kapitel 2 die Definition und Abgrenzung der für diese Arbeit relevanten Begriffe. Dazu werden zunächst in Kapitel 2.2 die Grundlagen des Begriffes „E-Mail“ erarbeitet. Ferner wird das technische Konzept erläutert, auf dem das Kommunikationsmedium E-Mail beruht. Darunter werden die sogenannten „Protokolle“ erläutert, die beim Versenden und Empfangen von E-Mails zum Einsatz kommen. Außerdem wird der Aufbau der Infrastruktur dargestellt, die beim E-Mail-Verkehr zum Einsatz kommt.

Neben dem Begriff „E-Mail“ wird in Kapitel 2.3 weiterhin der Begriff „Spam“ erläutert. Hierzu wird auf den Ursprung und die Verwendung des Begriffes „Spam“ in unterschiedlichen Kontexten eingegangen. Letztendlich soll daraus der Begriff „E-Mail-Spam“ abgeleitet werden, wobei ein Aspekt dieses Begriffs gezielt herausgearbeitet wird, der für die in der Arbeit behandelten Inhalte besonders relevant ist.

Abschließend werden in Kapitel 2.4 Phänomene beschrieben, die dem in Kapitel 2.3 definierten Begriff „E-Mail-Spam“ ähnlich sind und in der Praxis eine hohe Relevanz besitzen. Zu diesen Phänomenen zählen „Phishing“, „Spoofing“, kommerzielle Werbung und der Versand von Malware und Viren.

Ziel dieses Kapitels ist es, die Grundlagen zum Verständnis der nachfolgenden Kapitel 3 und 4 zu erarbeiten.

2.2 Zum Begriff „E-Mail“

Der Begriff „E-Mail“ ist die Abkürzung für Electronic Mail und stellt neben dem World Wide Web einen der meistgenutzten Dienste im Internet dar. Mit Hilfe von Electronic Mail können Nachrichten, darunter Text oder auch Multimediadaten, an einen oder mehrere bestimmte Empfänger gesendet werden.[10] Der Dienst „E-Mail“ ist zusammen mit dem Internet gewachsen. So wurde die erste E-Mail 1984 in Deutschland empfangen.

10 Vgl. Sjurts, Insa: Gabler Wirtschaftslexikon: E-Mail Definition, Online im Internet: https://wirtschaftslexikon.gabler.de/definition/e-mail-33576, 6.11.2018.

Weltweit wird die E-Mail heute von etwa 50 Prozent der Bevölkerung genutzt, während es in Deutschland sogar ungefähr 84 Prozent sind. Deutschlandweit ist die Nutzung von E-Mail seit 2002 um etwa 40 Prozentpunkte gestiegen.[11]

Eine E-Mail besteht immer aus einem Kopfteil und einem Nachrichtenteil. Der Kopfteil, auch als „Header" bezeichnet, beinhaltet die Informationen, die für den Versand und die Zustellung einer E-Mail notwendig sind. Diese Informationen bestehen aus den E-Mail-Adressen des Senders und des Empfängers bzw. der Empfänger. Der Weg, den die E-Mail vom Sender zum Empfänger zurückgelegt hat und die IP-Adresse des Absenders sind ebenfalls enthalten.[12] Der Header einer E-Mail kann also mit dem Adressfeld einer Postkarte verglichen werden, welches ebenfalls die zum Versand und zur Zustellung relevanten Informationen enthält.

Der Nachrichtenteil ist jener Teil der E-Mail, der die für den Empfänger eigentlich interessanten Informationen enthält und ist mit dem Text bzw. mit dem Bild auf der Postkarte zu vergleichen. Wie die Postkarte ist auch eine E-Mail beim Versand nicht vor der Einsicht Dritter geschützt. So kann eine E-Mail beim Transfer zum Empfänger von Dritten gelesen und sogar manipuliert werden. Dies ist zumindest bei einem unverschlüsseltem Versand von E-Mails möglich. Es sind aber nicht nur die Informationen im Nachrichtenteil unverschlüsselt. Auch Header-Informationen können manipuliert werden, sodass eine E-Mail den Eindruck vermittelt, als wäre ihr Absender eine andere Person.[13]

Die Versendung einer E-Mail erfolgt über das Simple Mail Transfer Protocol (SMTP). Bei der Übertragung per SMTP wird die E-Mail auf dem Weg zum Empfänger über Zwischenknoten weitergeleitet und dort temporär gespeichert. Diese Vorgehensweise nennt man „Store-and-forward-Prinzip". SMTP war ursprünglich dazu gedacht, Textnachrichten mit amerikanischem Zeichensatz zu übertragen. Damit aber auch Multimediadaten, Binärdaten und internationale Zeichensätze übertragen werden können, wurde SMTP um das Mailpurpose Internet Mail Extension Protokoll (MIME) erweitert.[14]

Der Weg einer E-Mail vom Sender zum Empfänger soll anhand von Abbildung 1 erläutert werden. Auf dem Weg vom Client des Senders zum Client des Empfängers passiert die E-Mail einige Interaktionspunkte. Will der Sender eine Nachricht per E-Mail versenden, muss er diese zunächst in einem E-Mail-Client (erster Interaktionspunkt) erstellen. Dazu zählen lokale E-

11 Vgl. o. V.: Deutsches Institut für Vertrauen und Sicherheit im Internet: 30 Jahre E-Mail: wichtigstes Kommunikationsmedium der älteren Generation?, Online im Internet: https://www.divsi.de/30-jahre-e-mail-wichtigstes-kommunikationsmedium-der-aelteren-generation/, 12.08.2014.

12 Vgl. Eckert, Claudia: IT-Sicherheit - Konzepte - Verfahren – Protokolle, München, Wien: Oldenbourg Verlag 2005, S. 63 ff. & o. V.: verbraucherzentrale.de: So lesen Sie den Mail-Header, Online im Internet: https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/so-lesen-sie-den-mailheader-6077, 6.11.2018.

13 Vgl. Eckert, Claudia: IT-Sicherheit - Konzepte - Verfahren – Protokolle, a. a. O., S. 64.

14 Vgl. Dent, Kyle: Postfix - Ein sicherer und leicht zu verwaltender MTA für Unix, 2. Auflage, Köln: O'Reilly 2005, S. 3 ff. & Eckert, Claudia: IT-Sicherheit - Konzepte - Verfahren – Protokolle, a. a. O., S. 64.

Mail-Clients, wie z. B. Microsoft Outlook, Apple Mail oder Mozilla Thunderbird und Web-Clients, wie z. B. Roundcube, Zimbra oder RainLoop. Diese Software wird unter dem Begriff „Mail User Agent“ (MUA, nachfolgend als E-Mail-Client bezeichnet) zusammengefasst.[15]

Wurde die Nachricht erstellt, weist der Sender seinen E-Mail-Client an, die E-Mail an den Empfänger zu senden. Dazu muss der E-Mail-Client zunächst eine Verbindung zum E-Mail-Server des Senders (zweiter Interaktionspunkt) herstellen und anschließend die Nachricht per SMTP an den Mail-Server des Senders übermitteln. Der Mail-Server des Senders wird allgemein auch als „Mail Transfer Agent (Sender)“ (MTA_S) bezeichnet.

Im Anschluss muss der E-Mail-Server des Senders (MTA_S) den E-Mail-Server des Empfängers („Mail Transfer Agent (Recipient)“, MTA_R) kontaktieren, um die E-Mail weiterleiten zu können. Dafür muss der MTA_S herausfinden, welchen E-Mail-Server der Empfänger nutzt. Diese Information stellt ein DNS-Server[16] (dritter Interaktionspunkt) bereit. Der MTA_S fragt dementsprechend die Adresse des MTA_R (vierter Interaktionspunkt) bei dem DNS-Server an und sendet anschließend die E-Mail an den E-Mail-Server des Empfängers.

Dort angelangt, wird die E-Mail an den „Mail Delivery Agent“ (MDA, fünfter Interaktionspunkt) des Empfängers weitergeleitet. Der MDA ist für den Empfang von E-Mails zuständig. Der E-Mail-Server des Empfängers wird in den meisten Fällen von vielen weiteren Personen genutzt, wohingegen der MDA nur dem jeweiligen Benutzer zur Verfügung steht. Der MDA legt die empfangene E-Mail im Nachrichtenspeicher (sechster Interaktionspunkt) des Nutzers ab. Dort wartet die E-Mail mit u. U. einigen weiteren E-Mails auf Abholung durch den Nutzer. Die Nachricht kann hier jedoch noch nicht gelesen werden, da sie immer noch auf dem E-Mail-Server liegt. Um die E-Mail über den lokalen oder den Web Client lesen zu können, kommen noch zwei weitere Protokolle zum Einsatz. Für die Bereitstellung der E-Mail auf dem Client wird das „Post Office Protocol“ (POP) und/oder das „Internet Mail Application Protocol“ (IMAP) benötigt. Diese Protokolle erlauben es dem Nutzer, die E-Mails vom E-Mail-Server (POP- oder IMAP-Server, siebter Interaktionspunkt) auf den Client herunterzuladen (achter Interaktionspunkt).[17]

Bei der Verwendung von POP wird die E-Mail nur einmal aus dem Nachrichtenspeicher heruntergeladen und auf dem E-Mail-Server gelöscht. Dies impliziert auch, dass bei der Nutzung von POP eine E-Mail nur von einem (1) Client abgefragt werden kann. Wurde die Nachricht bspw. vom POP-Server nach Microsoft Outlook heruntergeladen, kann sie nicht erneut in Apple Mail heruntergeladen werden. Die Nachrichten sind durch den Download auf den Client auch

15 Vgl. Dent, Kyle: Postfix - Ein sicherer und leicht zu verwaltender MTA für Unix, a. a. O., S. 3 ff.

16 Ein DNS (Domain Name System)-Server, auch Nameserver genannt, kann bspw. einer Web Site die richtige IP-Adresse zuweisen. Ein DNS-Server hält also Domains bzw. URLs und die dazugehörigen IP-Adressen vor und kann diese auf Anfrage zuordnen.

17 Vgl. Dent, Kyle: Postfix - Ein sicherer und leicht zu verwaltender MTA für Unix, a. a. O., S. 3 ff.

ohne Verbindung zum Internet jederzeit lesbar. Werden jedoch mehrere E-Mail-Clients genutzt, sollte IMAP verwendet werden. Bei der Verwendung von IMAP kann eine E-Mail beliebig oft vom E-Mail-Server heruntergeladen werden und wird nicht nach einem Download direkt gelöscht. Gleichzeitig können die Clients über den E-Mail-Server miteinander synchronisiert werden. Das heißt, wenn eine E-Mail von einem Client gelöscht wird, wird sie gleichzeitig auf dem E-Mail-Server und von allen anderen Clients gelöscht. Anders als bei POP werden bei IMAP die heruntergeladenen Nachrichten standardmäßig nur im Cache des Clients gespeichert. Das bedeutet, dass zum wiederholten aufrufen der E-Mail wieder eine Verbindung zum Internet bestehen muss.[18]

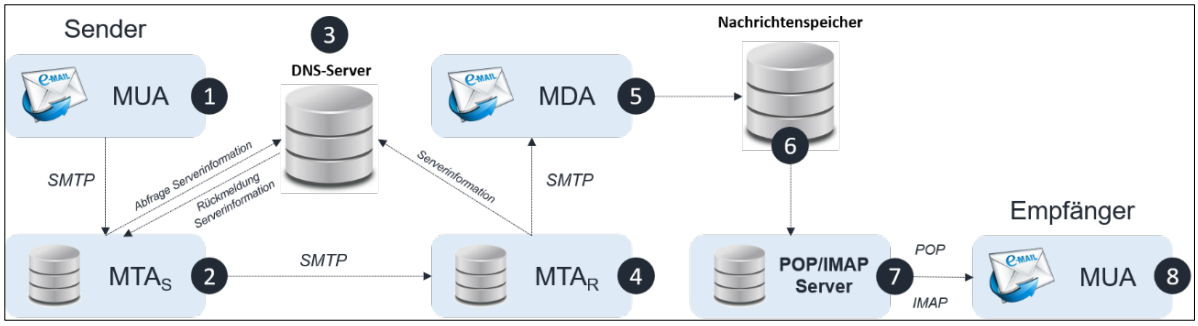

Abb. 1: Einfacher Nachrichtenfluss im Internet[19]

2.3 Zum Begriff „Spam“

Der Begriff „Spam“, wie er heute meist in Verbindung mit Kommunikationsmedien im Internet gebraucht wird, stammt aus einem Sketch der britischen Komiker-Gruppe „Monthy Python“ aus dem Jahr 1970. In diesem Sketch fragt eine ältere Dame in einem Frühstückscafé nach den Gerichten, die sie bestellen könne. Die Kellnerin liest ihr daraufhin die Speisekarte vor, in der in jedem Gericht „Spam“ kurz für „spiced ham“, also gewürzter Schinken, enthalten ist. Die Dame fragt daraufhin, ob sie auch Gerichte ohne Spam bestellen könne, da sie Spam nicht mag. Jedoch gibt es nur Gerichte mit Spam und sie müsse sich damit begnügen.[20]

Genau dieser Umstand der Unerwünschtheit von Inhalten ist es, den der Begriff „Spam“ heute noch beschreibt. Spam kann in allen Kommunikationsformen zum Problem werden, wenn der

18 Vgl. Eckert, Claudia: IT-Sicherheit - Konzepte - Verfahren – Protokolle, a. a. O., S. 63 & Dent, Kyle: Postfix - Ein sicherer und leicht zu verwaltender MTA für Unix, a. a. O., S. 5, 88 ff.

19 In Anlehnung an Dent, Kyle: Postfix - Ein sicherer und leicht zu verwaltender MTA für Unix, a. a. O., S. 4.

20 Vgl. Kreitling, Holger: Wie Monty Python das Wort „Spam“ erfanden, Online im Internet: https://www.welt.de/ kultur/article3078427/Wie-Monty-Python-das-Wort-Spam-erfanden.html, 25.01.2009.

Mehrheit der Benutzer Nachrichten und andere Inhalte unerwünscht mitgeteilt werden.[21] So kann beispielsweise ein persönlich geführtes Gespräch ohne den Einsatz jeglicher Technik zum Opfer von Spam werden. Dies ist dann der Fall, wenn sich eine oder mehrere Personen unerwünscht in das Gespräch einbringen oder in näherer Umgebung so laut unterhalten, dass das eigene Gespräch übertönt wird.

Der für diese Arbeit relevante Begriff „E-Mail-Spam“ ist eine Verallgemeinerung für den Begriff „Unsolicited Bulk E-Mail“ bzw. „Unsolicited Commercial E-Mail“. Diese Begriffe beschreiben den Umstand, dass ein Sender eine Nachricht an viele Empfänger sendet, zu denen er zuvor keinen Kontakt hatte, ohne dass diese solche E-Mails angefordert haben. Auch hier zeigt sich das Hauptmerkmal von Spam, nämlich die Unerwünschtheit der Nachricht. Der Versand von E-Mail-Spam kostet den Sender fast nichts und die Grenzkosten für die Aufnahme einiger hundert oder tausend weiterer Empfänger sind nahezu Null. Da die Grenzkosten geringer sind als die Grenzerträge, ist es für die Versender von E-Mail-Spam vorteilhaft, ihre Nachrichten an so viele E-Mail-Adressen wie möglich zu versenden.[22]

Den extrem geringen Kosten für den Versand von E-Mail-Spam steht ein nicht zu vernachlässigender Schaden auf Seiten der Empfänger gegenüber. Während der Versand von einer Millionen E-Mails gerade einmal circa 100 Euro kostet, verursacht das Bearbeiten der E-Mails bei den Empfängern einen erheblichen Zeitaufwand und somit ein Vielfaches an Kosten.[23]

Ein Beispiel: Wenn zum Sichten, unmittelbaren Identifizieren und Löschen einer Spam-E-Mail 30 Sekunden benötigt werden, müssen 500.000 Minuten aufgewendet werden, um 1 Mio. E-Mails zu bearbeiten. 500.000 Minuten entsprechen in etwa 8.333 Stunden. Selbst wenn zum Bearbeiten einer E-Mail Arbeitskräfte zum Mindestlohn beschäftigt würden, kostete dies bereits 70.830 Euro. Auf der anderen Seite haben lediglich circa 0,01% der Spam-E-Mails Erfolg und verleiten den Empfänger z. B. zum Kauf eines Produkts. Angenommen eine Bestellung bringt dem Auftraggeber des E-Mail-Spams im Durchschnitt einen Umsatz von 50 Euro, dann hat dieser einen Gesamtumsatz von 5.000 Euro erzielt. Davon zahlt er circa 30% Provision an die Person oder Organisation, die die Spam-E-Mails versenden. Es sind also insgesamt 4.900 Euro (5.000 Euro - 100 Euro) umgesetzt worden, gleichzeitig aber Kosten in Höhe von 75.830 Euro (70.830 Euro + 5.000 Euro) entstanden. Dies entspricht im aufgezeigten „Best Case“ einen Wohlfahrtsverlust von 70.930 Euro.[24]

Neben den finanziellen Schäden wird durch E-Mail-Spam auch Bandbreite und Festplattenkapazität des Empfängers verschwendet bzw. blockiert. Gleichzeitig wird auch die Bandbreite

21 Vgl. Schneider, Markus; et al: Untersuchung von Spam-Eigenschaften kostenfreier Email-Dienste, a. a. O., S. 13 f. & Topf, Jochen; Etrich, Matthias; Heidrich, Jörg; Romeo, Leslie; Thorbrügge, Marco; Ungerer, Bert: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, 2005, S. 12 ff.

22 Vgl. Dent, Kyle: Postfix - Ein sicherer und leicht zu verwaltender MTA für Unix, a. a. O., S. 133.

23 Vgl. Topf, J. et al: Antispam - Strategien – Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 17.

24 Vgl. Topf, J. et al: Antispam - Strategien – Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 16 ff.

anderer Nutzer blockiert, da sich viele Nutzer eines E-Mail-Dienstes die gleichen E-Mail-Server teilen. Während die zu versendende Spam-E-Mail lediglich einige wenige hundert Kilobyte groß ist, belegt sie durch millionenfache Versendung einige hundert Gigabyte an Festplattenplatz bei den Empfängern. Je nachdem, wie groß der den Empfängern gewährte Speicherplatz ist, wird dieser früher oder später mit E-Mail-Spam gefüllt sein. Dies kann bei unbeobachtetem Umgang mit dem E-Mail-Postfach dazu führen, dass keine weiteren E-Mails mehr empfangen werden können.[25]

E-Mail-Spam ist also ein grundlegendes Problem, mit dem sich jeder Teilnehmer am E-Mail-Verkehr mehr oder weniger zwingend auseinandersetzen muss. In den folgenden Kapiteln wird auf dieses Problem näher eingegangen und es werden Lösungskonzepte zur Abwehr von E-Mail-Spam erarbeitet, um die oben dargestellten Probleme zu reduzieren.

2.4 Abgrenzung von E-Mail-Spam zu ähnlichen Phänomenen

In Kapitel 2.3 wurde der Begriff E-Mail-Spam grundlegend definiert und auf die Versendung von Massen-E-Mails in Form von kommerzieller Werbung eingeschränkt. Nachfolgend werden ähnliche Phänomene aus dem gleichen Kontext aber mit anderen Hintergründen vorgestellt.

Neben der kommerziellen Werbung, bei der Empfänger dazu veranlasst werden sollen, Produkte oder Dienstleistungen zu erwerben, kann E-Mail-Spam auch nicht-kommerzielle Werbung beinhalten. Nicht-kommerzielle Werbung enthält dabei häufig z. B. religiöse Propaganda oder die Bewerbung politischer Kandidaten während Wahlperioden.[26] Diese Form des E-Mail-Spam erzeugt durch fehlende monetäre Gewinne einen noch höheren Wohlfahrtsverlust als kommerzielle Werbung. Eine weitere Form des E-Mail-Spam ist der Versand von sogenannten „Phishing“- oder „Spoofing“-Mails. Der Begriff „Phishing“ entsteht aus der Kombination der Begriffe „Password“ und „Fishing“. Die Versender verfolgen also die Absicht, Passwörter der Empfänger herauszufinden und zu missbrauchen.[27] Der Begriff „Spoofing“ beschreibt eine betrügerische Masche, bei der sich der Sender der Nachricht beispielsweise als eine wohlhabende Person aus dem Ausland ausgibt, der wertvolle Waren ins Inland transportieren möchte und dazu eine Person braucht, die ihren Namen zur Verfügung stellen und bspw. den Zoll bezahlen soll. Dafür soll der Empfänger der Nachricht, also das „Opfer“, zu einem späteren Zeitpunkt einen Anteil am Verkaufserlös der Waren erhalten. Dadurch wird das „Opfer“ dazu verleitet, dem Sender Geld zu überweisen, das er zumeist nie wieder sehen wird.[28]

25 Vgl. Dent, Kyle: Postfix - Ein sicherer und leicht zu verwaltender MTA für Unix, a. a. O., S. 133 ff.

26 Vgl. Topf, Jochen; et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 14 f.

27 Vgl. Speichert, Horst: Praxis des IT-Rechts - Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, 2. Auflage, Wiesbaden: Vieweg 2007, S. 303 f., 309 f.

28 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 15.

Zwei weitere E-Mail-Spam-ähnliche Phänomene beruhen auf der bereits beschriebenen leichten Fälschbarkeit der im E-Mail-Header befindlichen Informationen zur Identität des Absenders bzw. der Rücksendeadresse. Dies führt zu folgenden Problemen:

Zum einen kann eine Spam-E-Mail in fremdem Namen verschickt werden, mit der Absicht, möglichst provokant auf den Empfänger zu wirken. Ziel ist es hierbei, den Empfänger zu verärgern, um eine möglichst aggressive Reaktion gegenüber dem vermeintlichen Absender der E-Mail zu provozieren. Ziel ist die systematische Rufschädigung des scheinbaren Versenders. Zum anderen kann im Header die „reply to"-Zeile so manipuliert werden, dass der Sender einen unbeteiligten Dritten als Empfänger einer möglichen Antwort einsetzt. Dies ist besonders interessant für Versender von Viren und Malware, welche nicht als Absender identifiziert werden wollen.[29] Eine weitere mögliche Antwort an den o. g. Unbeteiligten kann im Falle dessen, dass die E-Mail dem Empfänger nicht zugestellt werden kann, so aussehen, dass Fehlermeldungen, die bspw. bei Nicht-Existenz der adressierten E-Mail-Adresse entstehen (und den Absender über die Nichtzustellbarkeit der E-Mail informieren sollen), an den angegebenen Absender zurückgesendet werden. Daher würde der Unbeteiligte diese sog. „bounces" als Spam in sein E-Mail-Postfach zugestellt bekommen. Diese Form des E-Mail-Spam nennt man „kollateralen Spam".[30]

E-Mail-Spam kann jedoch nicht nur kollateraler Natur sein oder zur Beeinflussung des Nutzers eingesetzt werden, sondern auch zur Schädigung von Systemen oder zur Ausnutzung von Sicherheitslücken in Systemen führen. So kann eine E-Mail bspw. eine Reihe unterschiedlicher Schadsoftware enthalten, die das System angreifen oder ausspähen kann. Die daraus entstehenden Schäden sind weit höher als die des „gewöhnlichen" E-Mail-Spams. Allerdings kann nicht nur die Technik des Empfängers missbraucht bzw. ausgenutzt werden, sondern auch der Anwender selbst. Dies ist beispielsweise bei Kettenbriefen oder sog. „Hoaxes" (Falschmeldungen) der Fall. Dabei wird die Gutgläubigkeit des Empfängers zur Verbreitung von Spam ausgenutzt, sodass Spam nicht mehr nur von einer Person, sondern von vielen Personen gleichzeitig verbreitet wird. Dies führt zu einer exponentiellen Ausbreitung des E-Mail-Spams.[31]

Diese E-Mail-Spam ähnlichen Phänomene treten allerdings nicht nur getrennt voneinander auf, sondern auch in den verschiedensten Kombinationen. Ein detaillierter Einblick in die Arten des E-Mail-Spams mit einigen Beispielen wird in Kapitel 3.4 gegeben.

29 Vgl. o. V.: wisu - das wirtschaftsstudium: IT-Security – wohl nur ein Traum, 04.2017, S. 352 ff.

30 Vgl. Dent, Kyle: Postfix - Ein sicherer und leicht zu verwaltender MTA für Unix, a. a. O., S. 133 ff. & Topf, Jochen; et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 16.

31 Vgl. Topf, Jochen; et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 16 f. & o. V.: wisu - das wirtschaftsstudium: IT-Security – wohl nur ein Traum, 04.2017, S. 352 ff.

3 Grundlagen zur Versendung von E-Mail-Spam

3.1 Systematisierung der Vorgehensweisen

Nachdem in Kapitel 2 eine Definition und Abgrenzung der für die Arbeit wesentlichen Begriffe „E-Mail“ und „Spam“ bzw. „E-Mail-Spam“ erfolgt ist, soll nun in Kapitel 3 aufbauend darauf die Versenderseite des E-Mail-Spam dargestellt werden. Dazu wird die Vorgehensweise der Spam-Versender erläutert, dementsprechend stellt Kapitel 3 eine Seite (Versenderseite) des E-Mail-Spams dar und bildet neben Kapitel 2 die Grundlage für Hauptkapitel 4, in dem die Empfängerseite des E-Mail-Spam erläutert werden soll. Ziel von Kapitel 3 ist es, die „Angriffsmöglichkeiten“ der E-Mail-Spam-Versender aufzuzeigen, um in weiterer Folge in Kapitel 4 Maßnahmen gegen genau diese „Angriffe“ erarbeiten zu können.

Zunächst wird dazu in Kapitel 3.2 die Beschaffung der für den Versand von E-Mail-Spam notwendigen E-Mail-Adressen beschrieben.

In Kapitel 3.3 wird der infrastrukturelle Hintergrund zur Versendung des E-Mail-Spams dargestellt. Hierbei wird implizit auf das in Kapitel 2.2 erarbeite technische Konzept Bezug genommen, auf dem der E-Mail-Verkehr beruht.

In Kapitel 3.4 werden die in Kapitel 2.4 genannten E-Mail-Spam-ähnlichen Phänomene genauer betrachtet. Insbesondere sollen Intentionen und Unterschiede, die diese Arten des E-Mail-Spam ausmachen, diskutiert werden. Weiterhin werden rechtliche Hintergründe erläutert.

3.2 Beschaffung von E-Mail-Adressen

Als Grundlage für die Versendung von E-Mail-Spam muss der E-Mail-Spam-Versender über eine große Anzahl an E-Mail-Adressen verfügen. Der „E-Mail-Spam-Versender“ selbst wird zu Beginn des E-Mail-Verkehrs in fast jedem Fall als Sender auftreten, da er keine E-Mail-Adressen aus zuvor erhaltenen E-Mails verwenden kann. Daher stellt sich nun die Frage, woher der Versender des E-Mail-Spams die benötigten E-Mail-Adressen beziehen bzw. über welche Kanäle oder Vorgehensweisen er an die für ihn bis dahin unbekannte E-Mail-Adressen gelangen kann. Dazu kann er sich verschiedener Quellen oder Techniken bedienen.[32] Hinsichtlich der Datenquellen und Akquirierungstechniken lässt sich folgende Systematisierung treffen:

- Datensammlung aus bestätigt existierenden E-Mail-Adressen
  - Netzwerk aus E-Mail-Spam-Versendern
  - Beschaffung von Offline-Medien, die E-Mail-Adressen beinhalten
  - Analyse von Website-Impressen

32 Vgl. zu den folgenden Ausführungen zu den Datenquellen und Akquirierungstechniken der E-Mail-Spam-Versender Topf, Jochen; et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 26 ff.

  - Whois-Datenbanken
  - Missbrauch von „gehackten“ Adressbüchern
- Akquirierung neuer E-Mail-Adressen durch Erraten
  - Erraten von E-Mail-Adressen
  - Versand von Test-E-Mails an „erratene“ E-Mail-Adressen zur Verifizierung

Netzwerk aus E-Mail-Spam-Versendern: Ein etablierter E-Mail-Spam-Versender kann bei der Beschaffung neuer und aktueller E-Mail-Adressen auf ein Netzwerk zurückgreifen, bestehend aus vielen weiteren E-Mail-Spam-Versendern. So schließen sich die E-Mail-Spam-Versender bspw. in Online-Newsgruppen zusammen und tauschen die gesammelten und als aktuell geltenden E-Mail-Adressen unter Umständen auch gegen Bezahlung untereinander aus. Denn für den Versand von E-Mail-Spam ist es von entscheidender Bedeutung, dass die E-Mail-Adressen der Empfänger auch genutzt werden. Es ist trotz der bereits erwähnten geringen Grenzkosten für die Aufnahme einer weiteren E-Mail-Adresse in den E-Mail-Verteiler der „E-Mail-Spam-Versender“ von Nachteil, wenn die E-Mail-Adresse nicht aktuell ist und die Spam-E-Mail nicht geöffnet oder gar gelesen wird.

Offline Medien: Die fehlende Aktualität der E-Mail-Adressen ist aus Sicht der E-Mail-Spam-Versender besonders bei Offline-Datensammlungen ein Problem. So werden Datenträger, wie beispielsweise USB-Sticks oder CD-ROMs, die mit einer großen Anzahl an E-Mail-Adressen gefüllt sind, für wenige hundert Dollar verkauft. Die darauf enthaltenen E-Mail-Adressen sind oftmals so veraltet, dass sie nicht mehr genutzt werden. Aus diesem Grund sind diese Offline-Datensammlungen für professionelle E-Mail-Spam-Versender uninteressant und werden eher von sogenannten „Newcomern“ in der E-Mail-Spam-Szene genutzt. Diese haben wenig Erfahrung auf diesem Gebiet und wollen für einen sehr geringen Aufwand E-Mail-Spam zum Beispiel in Form von Werbung für ihr Produkt versenden.

Website-Impressen und „Whois-Datenbanken“: Um die Aktualität ihrer Datensammlungen zu gewährleisten, setzen professionelle E-Mail-Spam-Versender bzw. die „Lieferanten“ der E-Mail-Adressen Techniken ein, mit deren Hilfe sie neue E-Mail-Adressen verifizieren können. Eine Möglichkeit zur Beschaffung weiterer E-Mail-Adressen ist die Nutzung von Tools, die bspw. die Impressen von Onlineshops oder anderer Websites nach E-Mail-Adressen durchsuchen. Stoßen sie dabei auf bis dato nicht erfasste Adressen, werden diese in die Datenbank aufgenommen. Diese Vorgehensweise ist aufgrund unzähliger Websites mit öffentlich zugänglichen Impressen eine durchaus lukrative Methode, um kostengünstig an E-Mail-Adressen zu gelangen. Ähnlich wird beim Auslesen sogenannter „Whois-Datenbanken“ vorgegangen. In diesen Whois-Datenbanken werden öffentlich Inhaber und Administratoren von Web-Domains zusammen mit ihren E-Mail-Adressen eingepflegt. Zwar ist das massenhafte Auslesen dieser Datenbanken nicht erlaubt, was aber die „E-Mail-Spam-Versender“ nicht davon abhält, auf diese Weise neue E-Mail-Adressen zu beschaffen.

Missbrauch „gehackter" Adressbücher: Neben der Nutzung öffentlicher Quellen, wie Impressen von Websites und „Whois-Datenbanken", können auch Adressbücher der Empfänger von E-Mail-Spam missbraucht werden. Wird beispielsweise durch den Versand von Malware, Viren oder Spyware unbemerkt die Kontrolle über den Rechner des „Opfers" übernommen, öffnen sich dem E-Mail-Spam-Versender oder dem Hersteller der Schadsoftware sowohl das Adressbuch des „Opfers" als auch dessen private Daten auf Festplatten oder dem lokal auf dem Rechner gespeicherten Browser Cache. Dort werden unter Umständen auch Passwörter und sonstige Benutzerdaten für diverse Online-Shops und Online-Banking-Seiten vorgehalten.

Es werden also verifizierte, wenn auch mitunter nicht aktuelle E-Mail-Adressen, von den E-Mail-Spam-Versendern selbst vorgehalten, aus externen Datenbanken entwendet, von externen Anbietern angekauft oder durch Durchsuchung von Impressen akquiriert. Eine weitere Möglichkeit der Beschaffung neuer E-Mail-Adressen ist die Akquirierung durch systematisches oder unsystematisches Erraten.

Systematisches Erraten neuer E-Mail-Adressen: Es gibt allerdings auch E-Mail-Adressen, die aus keiner der o. g. Quellen entnommen werden können, nämlich jene, die frisch erstellt wurden, nur sehr privat genutzt werden oder die aus sonstigen Gründen den „E-Mail-Spam-Versendern" und sonstigen öffentlichen Diensten, abgesehen vom jeweiligen E-Mail-Provider, unbekannt sind. Um diese Adressen herausfinden zu können, erraten die E-Mail-Spam-Versender zunächst E-Mail-Adressen. Dabei Nutzen sie bspw. eine Liste an Vornamen und Nachnamen und kombinieren diese. Eine derartige Syntax kann dann wie folgt aussehen: „max.mustermann@provider.de" Dieses Vorgehen nennt man auch „Wörterbuchangriff".[33]

Unsystematisches Erraten neuer E-Mail-Adressen: Eine andere Methode, die sog. „brute force attack", verwendet jede mögliche Kombination an Zeichen und generiert daraus E-Mail-Adressen.[34]

Im Anschluss an das systematische oder unsystematische Erraten neuer E-Mail-Adressen ist eine **Verifizierung der E-Mail-Adressen** erforderlich: Die durch ein Erraten generierten E-Mail-Adressen werden anhand des Versands einer Test-E-Mail an den E-Mail-Server des Providers auf Existenz geprüft. Der E-Mail-Server generiert dann bei Nicht-Existenz der E-Mail-Adresse eine Fehlermeldung und schickt diese zurück an den Absender. So kann der E-Mail-Spam-Versender auf die tatsächlich existierenden E-Mail-Adressen schließen. Nachdem die Existenz verifiziert wurde, können die E-Mail-Adressen ggf. noch auf Aktualität geprüft werden, indem eine Antwort durch die Empfänger provoziert wird. Im besten Fall hat der Empfänger eine sog. „auto reply" Einstellung vorgenommen, die automatisch auf jede eingehende E-

33 Vgl. Rouse, Margarete: Wörterbuchangriff (Dictionary Attack), Online im Internet: https://www.searchsecurity.de/definition/Woerterbuchangriff-Dictionary-Attack, 14.11.2018.

34 Vgl. Schmitz, Peter: Definition Brute Force – Was ist ein Brute-Force-Angriff?, Online im Internet: https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/, 17.01.2018 & Topf, Jochen; et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, 2005, S. 27.

Mail antwortet. Diese Rückmeldung kann den E-Mail-Spam-Versender bspw. darauf hinweisen, dass der Empfänger bis zu einem bestimmten Datum oder einer bestimmten Uhrzeit nicht zu erreichen ist.[35]

Die Existenz einer E-Mail-Adresse stellt also für den „E-Mail-Spam-Versender“ das notwendige und die Aktualität derselben das hinreichende Kriterium für die Attraktivität des Empfängers dar. E-Mail-Adressen, deren aktuelle Nutzung nachgewiesen wurde, werden somit bevorzugt mit E-Mail-Spam versorgt. Die in diesem Kapitel gewonnenen Erkenntnisse sind besonders in Kapitel 4.2.1 relevant.

3.3 Spam-Server und Open Relays

Nachdem im vorherigen Kapitel die Techniken und Vorgehensweisen zur Beschaffung von E-Mail-Adressen, die die Empfänger des E-Mail-Spams darstellen, aufgezeigt und erläutert wurden, widmet sich dieses Kapitel den technischen Maßnahmen, die der „Spam-Versender“ ergreifen muss, um die Spam-E-Mails den Empfängern zustellen zu können. Dazu wird zunächst die dazu notwendige Infrastruktur betrachtet. Nachfolgend werden unterschiedliche Versandmethoden dargestellt und jeweilige Vor- und Nachteile, sowie rechtliche Rahmenbedingungen diskutiert.

Die Art des Versands an Spam-E-Mails hat sich seit den 90er Jahren stark verändert, somit haben sich auch die erforderlichen Gegenmaßnahmen, die zur Abwehr getroffen werden müssen, geändert. Damals wurde E-Mail-Spam hauptsächlich über eigens dafür aufgesetzte und betriebene E-Mail-Server und das Ausnutzen sogenannter „Open Relays“ anderer E-Mail-Server verbreitet. Während die Beschaffung und Pflege von sog. „self hosted“ Servern mit relativ hohen Kosten und technischem Aufwand verbunden ist, ist das Ausnutzen fremder E-Mail-Server deutlich kostengünstiger.[36]

Um die technischen Hintergründe zum Ausnutzen dieser „Open Relays“ verstehen zu können, müssen zuvor zwei Begriffe definiert werden. Zum einen der Begriff „Domain“ und zum anderen der Begriff „E-Mail-Domain“. Der Begriff „Domain“ beschreibt im Kontext der Informationstechnik eine Gliederungseinheit im Internet bezüglich der hierarchisch aufgebauten Rechnernamen. Dabei teilt sich die Domain in zwei Teile auf: Der erste Teil ist die sog. „Top-Level-Domain“ und stellt zum Beispiel das Länderkürzel „.de“ in „google.de“ dar. Der zweite Teil ist die sog. „Secondary-Domain“ und stellt im o. g. Beispiel „google“ in „google.de“ dar. Wie schon zu erkennen, ist die Domain Teil bspw. einer Website-Adresse.[37]

35 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 26 ff.

36 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 24 f.

37 Vgl. Siepermann, Markus: Domain – Ausführliche Definition, Online im Internet: https://wirtschaftslexikon.gabler.de/definition/domain-34780, 24.11.2018.

Der Begriff „E-Mail-Domain“ stellt eine Erweiterung zur allgemeinen Domain dar. Sie ist genauso wie die Domain in eine Top- und Secondary-Domain aufgeteilt. Die E-Mail-Domain ist stets in der E-Mail-Adresse erkennbar und stellt die Zeichenfolge nach dem „@“ dar. So ist die Domain der E-Mail-Adresse aus dem zuvor genannten Beispiel „max.mustermann@provider.de“ gleich „provider.de“.[38]

Bis in die 1990er Jahre war es zur Gewährleistung eines möglichst friktionslosen E-Mail-Verkehrs üblich, dass E-Mail-Server auch als „Open Relay“ fungierten. Durch ein „Open Relay“ wird ermöglicht, dass E-Mail-Server E-Mails nicht nur von der eigenen Domain an die eigene Domain senden können, sondern dass auch E-Mails aus anderen Domains über den E-Mail-Server gesendet werden können. Es wird einem Nutzer aus einer fremden Domain also ermöglicht, dass er ohne Hindernisse E-Mails versenden kann, sodass er keinen eigenen E-Mail-Server betreiben oder den E-Mail-Server seiner eigenen Domain nutzen muss. Diese Funktion der E-Mail-Server war in den 1990er Jahren beabsichtigt und hatte den Hintergrund, dass im Falle eines E-Mail-Server-Ausfalls die Nutzer auf einen beliebigen anderen E-Mail-Server ausweichen konnten, um den E-Mail-Verkehr aufrecht zu erhalten. Da dies aber E-Mail-Spam-Versender dazu einlud, ihren Spam über fremde E-Mail-Server zu versenden, wurde die Funktion entfernt und damit die „Open Relays“ geschlossen.

In der heutigen Zeit sind „Open Relays“ eher selten und hauptsächlich das Produkt fehlerhaft konfigurierter E-Mail-Server.[39] Da E-Mail-Spam u. U. rechtliche Konsequenzen für den Versender haben kann, sollte der Betreiber eines E-Mail-Servers darauf achten, dass der E-Mail-Server gegenüber derartiger Ausnutzung abgesichert ist, da er durch die im E-Mail-Header enthaltenen Informationen über den Absender als ein solcher identifiziert werden und damit zur Verantwortung gezogen werden könnte.[40]

Die Nutzung von selbst betriebenen E-Mail-Servern und das Ausnutzen anderer E-Mail-Server ist zwar heute noch relativ populär, aber aufgrund einfacher Abwehrmaßnahmen unattraktiv für E-Mail-Spam-Versender geworden. Da E-Mail-Server, ob selbst betrieben oder fremder Natur, immer zu einer Domain gehören und somit nur über einen festen IP-Adressbereich kommunizieren können, können sie relativ leicht als Quelle von E-Mail-Spam identifiziert werden. Das führt dazu, dass E-Mail-Spam aus festen Adressbereichen mit sehr einfachen Mitteln vermieden werden kann.[41] Vor diesem Hintergrund werden heutzutage neue Techniken zur Versendung von E-Mail-Spam genutzt, um dem Empfänger die Abwehr zu erschweren und die Zustellung

38 Vgl. Notenboom, Leo: Whats the Difference Between an Email Domain, an Email Account, and an Email Adress?, Online im Internet: https://askleo.com/whats-difference-email-domain-email-account-email-address/, 20.11.2018 & Herrmann, Dominik: Beobachtungsmöglichkeiten im Domain Name System – Angriffe auf die Privatsphäre und Techniken zum Selbstdatenschutz, 2014, S. 20 ff.

39 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 24 f.

40 Vgl. Speichert, Horst: Praxis des IT-Rechts - Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, a. a. O., S. 204-209.

41 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 67 f.

besser gewährleisten zu können. Dabei bedient der E-Mail-Spam-Versender sich einerseits sog. „Open Proxies“ und andererseits ferngesteuerter PC-Systeme. Diese Vorgehensweisen werden nachfolgend detaillierter erläutert.

Open Proxies: Bei der oben beschriebenen Nutzung eines E-Mail-Servers entsteht für den Sender von E-Mail-Spam ein Problem: Egal welchen Weg er wählt, er wird ohne weitere Verschleierung als Sender von E-Mail-Spam identifiziert werden können und kann somit relativ leicht und direkt abgewehrt werden. Es gilt für ihn also sicherzustellen, dass der Weg, den die Spam-E-Mail zurücklegt, nur bis zum versendenden E-Mail-Server nachvollziehbar ist und seine Identität somit verborgen bleibt. Dazu macht er sich sog. „Open Proxies“ zu Nutze. „Proxies“ haben die Aufgabe, den Datenfluss im Internet zu erleichtern. So kann auf einem Proxy Server ein Cache vorgehalten werden, um Web-Inhalte lokal zu speichern und diese auf Anfrage dem jeweiligen Client (der die Anfrage gestellt hat) zur Verfügung zu stellen. Dies hilft dabei, häufig wiederkehrende Anfragen mit möglichst geringem Aufwand zu bearbeiten. Der Proxy Server nimmt dabei eine Stellvertreter-Rolle ein, d. h., werden angefragte Daten nicht im Cache vorgehalten, fragt er eigenständig bei dem anzufragenden Webserver die gewünschten Daten an und stellt sie dem Client zur Verfügung. Während des ganzen Prozesses hat der Client selbst nie direkten Kontakt zu dem Webserver, welcher ihm die Daten zur Verfügung stellen soll. Er ist also bei der Abfrage der Daten anonym, da der Proxy Server stellvertretend für ihn handelt.[42]

Der Proxy Server prüft dabei im besten Fall, ob die Anfrage des Clients legitim ist, bevor er sie bearbeitet. Ist dies nicht der Fall und der Proxy bearbeitet alle an ihn gestellten Anfragen unabhängig der Identität des Clients, spricht man von einem „Open Proxy“. Dies macht sich der E-Mail-Spam-Versender zu Nutze und versendet über den Proxy Server Spam-E-Mails, sodass die Identität des Versenders verschleiert bleibt und komplexere Abwehrmaßnahmen gegen den E-Mail-Spam getroffen werden müssen.[43]

Fernsteuerbare PC-Systeme: Es sind allerdings nicht nur die fehlerhaft konfigurierten „Proxies“, die es dem E-Mail-Spam-Versender ermöglichen, anonym E-Mail-Spam zu versenden. Auch PC-Systeme, die zuvor bspw. durch Spam-E-Mails mit Viren und Malware „infiziert“ wurden, können Aufgaben ähnlich eines Proxy-Servers übernehmen. Dabei werden die „infizierten“ PC-Systeme von den E-Mail-Spam-Versendern ferngesteuert und werden somit zum Instrument für die Versendung von E-Mail-Spam. Sie fungieren dabei genauso wie ein Proxy Server.[44]

42 Vgl. Donner, Andreas: Definition – Was ist ein Proxy Server?, Online im Internet: https://www.ip-insider.de/was-ist-ein-proxy-server-a-665349/, 01.08.2017.

43 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 24 f.

44 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 24 f.

Weiterhin können „infizierte“ PC-Systeme auch dahingehend ausgenutzt werden, dass Kennwörter und Benutzerdaten für bspw. den jeweiligen E-Mail-Account missbraucht werden. Somit können im Namen der „Opfer“ Spam-E-Mails über die Mail-Server der jeweiligen Provider versendet werden. Dies hat Vor- und Nachteile sowohl für die Versender als auch für die Empfänger des E-Mail-Spams.[45] Diese werden in Kapitel 4.2 näher erläutert.

Die Fernsteuerung fremder PC-Systeme hat für die E-Mail-Spam-Versender jedoch nicht nur den Nutzen des Versendens von Spam-E-Mails, sondern sie können die PC-Systeme auch zu sog. „Bot-Netzen“ zusammenfassen, mit denen sie dann DoS[46]-Angriffe gegen sämtliche Internet-Anwendungen durchführen können. Die Mitnutzung der PC-Systeme fällt deren Besitzern aufgrund der heutzutage großen Leistungsreserven der PC-Systeme eher selten auf.[47]

3.4 Arten des E-Mail-Spams

Nachdem in Kapitel 2.4 die verschiedenen Arten des E-Mail-Spams genannt wurden, sollen in diesem Kapitel Erkenntnisse über Gefahrenpotentiale sowie Intentionen der Versender gewonnen werden. Dazu werden die Arten des E-Mail-Spams noch einmal erarbeitet und im Anschluss auf ihre jeweiligen Gefahren untersucht.

Während es sich bei dem in Kapitel 2.3 definierten Begriff E-Mail-Spam um das massenhafte Versenden kommerzieller Werbung handelt, kann E-Mail-Spam auch wesentlich gefährlichere Inhalte transportieren. Dabei wird auf die Gutgläubigkeit und Unwissenheit einiger Teilnehmer des E-Mail-Verkehrs gesetzt. Andererseits können aber auch unzureichend gesicherte PC-Systeme das Ziel von E-Mail-Spam sein. Ersteres ist beim sog. „Phishing“ und „Spoofing“ der Fall. Diese Phänomene können getrennt voneinander, aber auch in Kombination auftreten. Beim „Phishing“ wird versucht, an Nutzerdaten und Passwörter für Online-Services, zu gelangen welche das „Opfer“ nutzt. Um dies möglichst glaubwürdig gestalten zu können, verweisen „Phishing-E-Mails“ zumeist auf sog. „Spoofing-Websites“. Diese Websites sind zum Teil täuschend echt wirkende Nachbildungen von originalen Websites. Die „Opfer“ werden in der „Phishing-E-Mail“ dazu aufgefordert, auf der Website ihre Nutzerdaten und Passwörter einzugeben. Somit kann sich der Sender des E-Mail-Spams oder dessen Auftraggeber Nutzerdaten der „Op-

45 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 24 ff.

46 DoS ist die Abkürzung für den Begriff „Denial of Service“ und bedeutet übersetzt so etwas wie: „Verweigerung des Dienstes“. In der Informationstechnik wird mit diesem Begriff die nicht Erreichbarkeit eines Internetdienstes beschrieben. Ein DoS-Angriff kann dazu führen, dass ein Internetdienst aufgrund von Überlastung, durch bspw. eine zu große Anzahl gleichzeitiger Zugriffsversuche von Internetnutzern, vorübergehend zusammenbricht und somit nicht mehr erreichbar ist.

47 Vgl. Bierschenk, Hans-J., et al: Sicherheit für Systeme und Netze in Unternehmen – Einführung in die IT-Sicherheit und Leitfaden für erste Maßnahmen, 2003, S. 23 ff.

fer“ aneignen und in deren Namen beispielsweise Banktransfers vornehmen. Besonders interessant sind die Login-Informationen für Online-Zahlungsdienste und Webshops in denen Zahlungsinformationen hinterlegt sind, um direkt oder indirekt das Geld der „Opfer“ zu stehlen.[48]

Beim „E-Mail-Spoofing“ ist auf das Kapitel 2.4 zu verweisen. Dort ist das Phänomen bereits anhand eines Beispiels erklärt. Das Ziel von E-Mail-Spoofing ist im Grunde das Gleiche wie beim „Phishing“: Es soll Geld entwendet werden. In beiden Fällen kommt es seitens der „Opfer“ darauf an, die Echtheit und Glaubwürdigkeit der E-Mails zu hinterfragen und nicht unbedacht Login-Daten preiszugeben bzw. Geld an ominöse Personen zu senden. Die Gefahr, die diese beiden Arten des E-Mail-Spams bergen, ist der Verlust finanzieller Mittel und ggf. je nachdem welches Benutzerkonto (bspw. Social Media) ausgespäht wurde, der Verlust von Reputation.[49]

E-Mail-Spam-Versender setzen jedoch nicht nur auf die Fehleranfälligkeit des Faktors Mensch, sondern auch auf unzureichend abgesicherte PC-Systeme, wie bspw. PCs, die seit längerer Zeit kein Betriebssystemupdate mehr erhalten haben oder PCs, auf denen keine Anti-Viren-Software installiert ist. In solche Systeme können mit Hilfe des E-Mail-Spams Viren und Trojaner eingeschleust werden, die dem Versender den Zugriff auf den PC ermöglichen können oder lediglich Informationen beschaffen, die auf dem Rechner gespeichert wurden. Dabei kann es sich wiederum um Login-Daten handeln. Auf diese Weise lassen sich mit Hilfe der infizierten PC-Systeme mehrere Ziele gleichzeitig erreichen. Ein Ziel ist die bereits erwähnte Beschaffung von Informationen: Dazu zählt unter anderem die Beschaffung neuer E-Mail-Adressen aus den Adressbüchern der „Opfer“. Weiterhin können die Rechner durch Fernsteuerung auch anderweitig missbraucht werden.[50] Gefahren, die durch Fernsteuerung privater PC-Systeme entstehen können und die Ziele, die E-Mail-Spam-Versender dabei verfolgen, wurden bereits in Kapitel 3.3 erläutert.

Zusammenfassend kann E-Mail-Spam in seinen verschiedenen Ausprägungen von einer eher geringen bis hin zu einer großen Gefahr werden, sowohl für private Haushalte als auch für Unternehmen. Kommerzielle und nicht-kommerzielle Werbung haben abgesehen von ihren zeitlichen und nervenaufreibenden Auswirkungen auf den Empfänger ein eher geringes Gefahrenpotential. Dahingegen haben Phishing und Spoofing ein signifikant höheres Gefahrenpotential, da es hierbei unachtsamem Umgang mit dem E-Mail-Spam zu finanziellen Verlusten kommen kann. E-Mail-Spam, in dem jegliche Art von Schadsoftware enthalten ist, birgt das höchste Gefahrenpotential, da es schon bei kleinstem Fehlverhalten der Empfänger zu großen Schäden

48 Vgl. Stiller, Helmut: Gabler Wirtschaftslexikon: Phishing Definition, Online im Internet: https://wirtschaftslexikon.gabler.de/definition/phishing-53396, 12.12.2018.

49 Vgl. o. V.: Spam, Phishing & Co – Phishing, Online im Internet: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html, 16.11.2018.

50 Vgl. o. V.: Elektronik Kompendium - Sicherheitsrisiken und Sicherheitslücken in der Netzwerktechnik, Online im Internet: https://www.elektronik-kompendium.de/sites/net/1811091.htm, 12.12.2018.

kommen kann. Allerdings kann gegen E-Mail-Spam unabhängig seiner Ausprägung rechtlich vorgegangen werden. Die dadurch entstehenden Konsequenzen für den Versender von E-Mail-Spam können je nach Art des E-Mail-Spams unterschiedlich schwer ausfallen.[51]

4 Maßnahmen zur Abwehr von E-Mail-Spam

4.1 Systematisierung der Maßnahmen

Ziel dieses Kapitel ist es, die in Kapitel 3 erlangten Erkenntnisse zu nutzen, um Maßnahmen zur Abwehr der jeweiligen „Spam-Angriffe“ zu erarbeiten. Kapitel 4 stellt weiterhin die Empfängerseite des E-Mail-Spams dar und ist zur Gliederung der Maßnahmen in zwei größere Teilkapitel aufgeteilt. Zum einen wird die Client-Seite im Hinblick auf die Maßnahmen zur Abwehr von E-Mail-Spam betrachtet und zum anderen die Server-Seite.

In Teilkapitel 4.2 werden Abwehrmaßnahmen gegen E-Mail-Spam erläutert. Dabei wird der Blick auf die Client-Seite gerichtet. Dementsprechend werden in Kapitel 4.2.1 präventive Maßnahmen vorgestellt. Dieses Kapitel hat einen starken Bezug auf das Kapitel 3.2. Weiterhin werden in Kapitel 4.2.2 grundlegende reaktive Konzepte zur Abwehr von E-Mail-Spam erarbeitet. Ferner werden Einstellungen von E-Mail-Filtern vorgestellt. In Kapitel 4.2.3 werden dann die im vorherigen Kapitel erläuterten reaktiven Konzepte in Tools und Systeme übertragen, die dem Anwender die Auseinandersetzung mit dem E-Mail-Spam erleichtern sollen.

Im Teilkapitel 4.3 werden anschließend Maßnahmen diskutiert, die auf der Server-Seite ergriffen werden können, um gegen E-Mail-Spam vorzugehen. Kapitel 4.3.1 zeigt obligatorische und optionale Server-Konfigurationen, die der Betreiber vornehmen kann, um sich selbst und seine Clients vor den Folgen von E-Mail-Spam zu schützen. Ferner werden Problematiken erläutert, denen sich speziell der Betreiber eines E-Mail-Servers gegenüber sieht. Dazu nimmt das Kapitel Bezug auf das Kapitel 3.3.

Kapitel 4.3.2 bewertet die Server-seitigen Maßnahmen und betrachtet die jeweiligen Vor- und Nachteile sowie deren Effektivität und Effizienz.

4.2 Client-seitige Maßnahmen

4.2.1 Präventive Maßnahmen gegen E-Mail-Spam

Nachdem in Kapitel 3 die Grundlagen zur Versendung von E-Mail-Spam erläutert wurden, sollen nun eine Reihe von Abwehrmaßnahmen diskutiert werden. Dazu werden in diesem Kapitel

51 Vgl. Speichert, Horst: Praxis des IT-Rechts - Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, a. a. O., S. 208 ff.

zunächst präventive Maßnahmen erläutert, die der Anwender treffen kann. Es handelt sich hierbei um Maßnahmen, die dem Anwender dabei helfen, die eigene E-Mail-Adresse vor den E-Mail-Spam-Versendern zu verbergen. Wie bereits in Kapitel 3.2 erläutert, ist eine Grundlage zur Versendung von E-Mail-Spam die Kenntnis der E-Mail-Adressen der Empfänger.[52] Es gilt also zu versuchen, die eigene E-Mail-Adresse so unbekannt wie möglich zu halten, um von den E-Mail-Spam-Versendern „unentdeckt" zu bleiben. Hierzu sollen einige Vorgehensweisen erläutert werden:

- Umgang mit der eigenen E-Mail-Adresse
- Nutzung von „Wegwerfadressen"
- Verhaltensregeln beim Umgang mit E-Mail-Spam

Umgang mit der eigenen E-Mail-Adresse: Voraussetzung für die nachfolgend erläuterten Maßnahmen ist, dass die E-Mail-Adresse noch weitgehend „unentdeckt" von E-Mail-Spam-Versendern ist. Dies ist besonders relevant für jene E-Mail-Adressen, die erst „frisch" erstellt wurden und kaum am E-Mail-Verkehr teilgenommen haben. Dabei gilt zu beachten, dass ein Anwender mehr als nur eine E-Mail-Adresse haben kann[53] und sich somit auch „frische" E-Mail-Adressen erstellen kann, die vorerst „frei" von E-Mail-Spam sein sollten. Um eine E-Mail-Adresse gegenüber E-Mail-Spam-Versendern so unentdeckt wie möglich zu halten, sollte sie nur mit ausgewählten Kontakten geteilt werden. Die Nutzung einer E-Mail-Adresse ist insbesondere in zwei Fällen interessant: Zum einen bei der Kontaktaufnahme mit Onlineshops oder zur Nutzung sonstiger Online-Dienste und zum anderen zum direkten Austausch von Informationen zwischen zwei oder mehreren Personen. Wird die E-Mail-Adresse zur Teilnahme an Online-Diensten genutzt, sollte geprüft werden, ob dieser Dienst seriös ist oder ob er u. U. die Kontaktinformationen, darunter die E-Mail-Adresse, weiterverbreitet oder sogar verkauft. Bei privater oder gewerblicher Nutzung einer E-Mail-Adresse ist darauf zu achten, dass Personen, mit denen E-Mail-Kontakt gepflegt werden soll, als vertrauenswürdig eingestuft werden. Dies kann sowohl durch persönlichen Kontakt, als auch über Empfehlungen anderer vertrauenswürdiger Personen geschehen. Ziel ist es also, die Kontakte mit Bedacht auszuwählen, um sicherstellen zu können, dass die eigene E-Mail-Adresse nicht ins Visier der E-Mail-Spam-Versender gelangt.[54]

Nutzung von „Wegwerfadressen": Sollen auch Online-Dienste oder Personen kontaktiert werden, die eher weniger vertrauenswürdig erscheinen oder soll die eigene E-Mail-Adresse in einen großen E-Mail-Verteiler aufgenommen werden, dessen Mitglieder nicht vollständig bekannt sind, entsteht ein Zielkonflikt mit dem zuvor genannten Vorgehen. In diesem Fall würde

52 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 26 f.

53 Vgl. o. V.: Wie viele private E-Mail-Adressen haben Sie?, Online im Internet: https://de.statista.com/statistik/daten/studie/29349/umfrage/anzahl-der-privaten-e-mail-adressen-pro-internetnutzer/, 13.12.2018.

54 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 26 f.

die E-Mail-Adresse u. U. auch Personen bekannt werden, die Informationen über die eigene E-Mail-Adresse weiterverbreiten, bspw. durch die Aufnahme der eigenen E-Mail-Adresse in weitere E-Mail-Verteiler. Somit würde sie eventuell auch E-Mail-Spam-Versendern bekannt werden. Um einer derartigen Unsicherheit zu begegnen, kann der Anwender sogenannte „Wegwerfadressen“ verwenden. Es wird also eine E-Mail-Adresse erstellt oder verwendet, mit der zu den o. g. Parteien Kontakt aufgenommen werden kann. Der daraus entstehende E-Mail-Spam wird dann von der „Wegwerfadresse“ aufgefangen und landet nicht im Postfach der eigentlich genutzten und unbekannten E-Mail-Adresse. Allerdings gehen so auch die wünschenswerten E-Mails verloren, die bei der „Wegwerfadresse“ eingehen.[55] Um dies zu umgehen, werden E-Mails von bestimmten Kontakten einfach an die nach außen hin unbekannte E-Mail-Adresse weitergeleitet. Dazu kann im E-Mail-Client eine Einstellung vorgenommen werden. Der Sender der E-Mail sieht dabei nicht, ob und an wen die E-Mail weitergeleitet wird. Somit bleibt die Ziel-E-Mail-Adresse „geheim“. Wenn auf eine E-Mail geantwortet werden soll, dann wird sie von der „Wegwerfadresse“ aus beantwortet und nicht von der „geheimen“ Adresse. Wird die Antwort auf der „geheimen“ Adresse erstellt und über die „Wegwerfadresse“ weitergeleitet, so wird dem Empfänger die „geheime“ Adresse offenbart. Damit die „Wegwerfadresse“ also ihre Aufgabe erfüllen kann, darf nur in die Richtung der „geheimen“ Adresse weitergeleitet werden.

Verhaltensregeln beim Umgang mit E-Mail-Spam: Sollte trotz des vorsichtigen Umgangs mit der eigenen E-Mail-Adresse dennoch E-Mail-Spam den Weg ins Postfach des Anwenders finden, gilt es, sich richtig zu verhalten. E-Mail-Spam kann auch unabhängig von der Bekanntheit der E-Mail-Adresse ins Postfach gelangen. Dies kann z. B. dann der Fall sein, wenn E-Mail-Spam-Versender die in Kapitel 3.2 erläuterten Verfahren anwenden. Dazu zählen „Wörterbuchattacken“ und „Brute Force Attacken“. Wie bereits erläutert, versuchen E-Mail-Spam-Versender herauszufinden, ob eine E-Mail-Adresse existiert und ob diese aktiv genutzt wird. In diesem Fall sollte der Empfänger auf keinen Fall auf den E-Mail-Spam antworten, egal wie verlockend die Inhalte der E-Mail auch sein mögen, denn sonst ist die E-Mail-Adresse eine priorisierte Adresse für E-Mail-Spam, da ihre Aktualität bestätigt wurde. Um ungewollte „auto replies“ zu verhindern, sollte eine Einstellung vorgenommen werden, sodass automatische Antworten nur an bestimmte Kontakte versendet oder ganz unterbunden werden.[56] Wurde der E-Mail-Spam identifiziert, sollte er umgehend und bestenfalls ungeöffnet gelöscht werden. Das nicht Öffnen von E-Mail-Spam verhindert auch, dass Schadsoftware, die sich im Anhang des E-Mail-Spams verbergen kann, Zugriff auf den PC erhalten kann.[57]

55 Vgl. Kratzenberg, Marco: Wegwerf-E-Mails – Anbieter und Funktionen, Online im Internet: https://www.giga.de/extra/email/specials/wegwerf-email-erstellen-anbieter-funktionen, 19.02.2018.

56 Vgl. Noteboom, Leo: How Can I Automatically Reply to Spammer To Tell Them to Stop?, Online im Internet: https://askleo.com/how-can-i-automatically-reply-to-spammers-tell-them-to-stop/, 21.11.2018.

57 Vgl. o. V.: IT-Grundschutz – M5.54 Umgang mit unerwünschten E-Mails, Online im Internet: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05054.html, 23.11.2018.

Präventive Maßnahmen gegen E-Mail-Spam können also dabei helfen, eingehenden E-Mail-Spam über einen gewissen Zeitraum zu unterbinden oder auf ein Minimum zu reduzieren. Dennoch kann E-Mail-Spam, wie bereits erläutert, in das Postfach des Anwenders gelangen. Unter Umständen kann dies dann auch zu einem größeren Problem werden, z. B. wenn auf E-Mail-Spam geantwortet wird oder wenn die E-Mail-Spam-Versender E-Mail-Spam unabhängig der Aktualität von E-Mail-Adressen versenden. Denn egal wie gut die E-Mail-Adresse „versteckt" wird, die E-Mail-Spam-Versender können mit Hilfe von „Wörterbuchattacken" und „Brute Force Attacken" ohne großen Aufwand herausfinden, ob E-Mail-Adressen existieren.[58]

Daher sind präventive Maßnahmen gegen E-Mail-Spam zwar hilfreich, aber keineswegs umfassend schützend gegen E-Mail-Spam. Weitere Maßnahmen, die Client-seitig zur Abwehr von E-Mail-Spam ergriffen werden können, werden im nächsten Kapitel erläutert.

4.2.2 Konfiguration der Client-seitigen E-Mail-Filter

Wie bereits im vorherigen Kapitel erläutert, bieten präventive Maßnahmen nur eingeschränkt Schutz vor E-Mail-Spam. Es wird dem Versender von E-Mail-Spam durch die genannten präventiven Maßnahmen erschwert, Kenntnis über die eigene E-Mail-Adresse zu erhalten. Trotz des Befolgens der Verhaltensregeln kann es dazu kommen, dass E-Mail-Spam ins Postfach des Empfängers gelangt. Deshalb werden nun Maßnahmen erläutert, die als Reaktion auf den empfangenen E-Mail-Spam ergriffen werden können, um in Zukunft die Anzahl der empfangenen Spam-E-Mails verringern zu können. Diese Maßnahmen beinhalten Einstellungen der im jeweiligen Client enthaltenen E-Mail-Filter-Optionen.

Zu diesen Filter-Optionen zählen grundlegend:

- Blacklisting
- Whitelisting
- Heuristische Inhaltsanalyse
- Statistische Inhaltsanalyse

Mit der Einführung von technischen Filtermaßnahmen müssen zunächst noch zwei Begriffe eingeführt werden: „false negatives" und „false positives". Diese Begriffe beschreiben im Kontext des E-Mail-Spams Fehler, die bei der Filterung von E-Mails entstehen können. Bislang wurde davon ausgegangen, dass keine technischen Filtermaßnahmen ergriffen werden und somit alle eingehenden E-Mails im Posteingang landen. Mit der Einführung eines Filters existiert nun neben dem regulären Posteingang auch ein sog. „Spam-Ordner", in den automatisch die als E-Mail-Spam gekennzeichneten E-Mails verschoben werden können.

58 Vgl. Schmitz, Peter: Definition Brute Force – Was ist ein Brute-Force-Angriff?, a. a. O. & Rouse, Margarete: Wörterbuchangriff (Dictionary Attack), a. a. O.

Wird eine eingegangene Spam-E-Mail vom Filter nicht als solche erkannt, wird sie fälschlicherweise im regulären Posteingang abgelegt. Bei diesem Fehler handelt es sich um ein sog. „false negative". Ebenso kann es vorkommen, dass eine gewünschte E-Mail fälschlicherweise als E-Mail-Spam gekennzeichnet wird und somit nicht im Posteingang, sondern im „Spam-Ordner" abgelegt wird. Diese fehlerhafte Zuordnung wird als „false positive" bezeichnet.[59]

Blacklisting: Blacklisting beschreibt ein Verfahren, bei dem bestimmte Sender von E-Mails blockiert werden können. Es wird also eine Einstellung am E-Mail-Filter vorgenommen, die E-Mails von unerwünschten Personen automatisch im „Spam-Ordner" ablegt. Dies kann als eine Reaktion auf E-Mail-Spam oder vorsorglich durchgeführt werden. Die als E-Mail-Spam-Versender identifizierten Personen können auf verschiedenen Ebenen blockiert werden. Auf der ersten Ebene kann explizit die E-Mail-Adresse des Senders blockiert werden, sodass die von dort aus gesendeten E-Mails im „Spam-Ordner" abgelegt werden. Versender von E-Mail-Spam können, wie bereits erläutert, ihre E-Mail-Adresse leicht fälschen oder eine andere E-Mail-Adresse verwenden. Daher ist es für den Empfänger ratsam einzelne IP-Adressen oder ganze IP-Adressbereiche zu blockieren, sofern diese als Quelle des E-Mail-Spams identifiziert wurden (zweite Ebene). Dies hat zur Folge, dass der zum Versenden des E-Mail-Spam verwendete Rechner oder das ganze Netzwerk blockiert wird. Auf der dritten Ebene können E-Mails, die aus einer bestimmten Domain versendet wurden, blockiert werden. Beispiele für solche Domains sind „.ru" für alle E-Mail-Adressen aus Russland, „provider.com" für alle E-Mail-Adressen, die zu einem bestimmten E-Mail-Provider gehören oder „domain.com" für alle E-Mail-Adressen, die zu einer anderen bestimmten Domain gehören. Für jede zusätzlich blockierte Ebene nimmt die Gefahr von „false negatives" ab. Gleichzeitig nimmt jedoch Gefahr von „false positives" zu.[60]

Whitelisting: Das Whitelisting stellt eine Ergänzung zum Blacklisting dar. Es kann ebenso wie das Blacklisting auf den gleichen Ebenen eingesetzt werden. Whitelisting wird verwendet, um das zunehmende Aufkommen von „false positives" durch den Einsatz umfangreichen Blacklistings zu verringern. Wurden bspw. sämtliche E-Mail-Adressen aus Russland gesperrt aber der Empfänger pflegt E-Mail-Kontakt zu einer in Russland ansässigen Person, so muss er diese auf die sog. „Whitelist" (weiße Liste) setzen. Die Whitelist enthält alle E-Mail-, IP-Adressen oder Domains von oder aus denen E-Mails empfangen werden sollen.[61] Ein extremes Beispiel von Whitelisting ist das Blockieren aller E-Mail-Adressen und das Zulassen weniger ausgewählter

59 Vgl. o.V.: Übermitteln von Spam-, Nicht-Spamnachrichten und Nachrichten, die als betrügerische Phishing-Angriffe angesehen werden, an Microsoft zur Analyse, Online im Internet: https://docs.microsoft.com/de-de/office365/securitycompliance/submit-spam-non-spam-and-phishing-scam-messages-to-microsoft-for-analysis, 11.06.2018.

60 Vgl. Beins, Friederike: Die ultimative Einführung in E-Mail Spam-Filter und Blacklists, Online im Internet: https://www.newsletter2go.de/blog/spam-filter-blacklists-email-marketing/, 06.12.2016.

61 Vgl. o. V.: Online Marketing Lexikon – Whitelist, Online im Internet: https://www.unternehmer.de/lexikon/online-marketing-lexikon/whitelist, 24.11.2018.

E-Mail-Adressen. Dies ist besonders für jene Personen interessant, die nur sehr wenig E-Mail-Verkehr haben oder eher als Initiator eines Kontaktes auftreten.

Der Einsatz von Whitelisting ist somit zwar am effektivsten gegen E-Mail-Spam, aber hat auch eine sehr hohe Anfälligkeit für „false positives". Am effizientesten ist Whitelisting jedoch als Ergänzung zu einem moderaten Einsatz von Blacklisting, sodass die Anzahl von „false negatives" und „false positives" möglichst gering gehalten wird.[62] Das Verhältnis der beiden Methoden gilt es für jeden Anwender individuell herauszufinden und ist abhängig vom jeweiligen Einsatz des E-Mail-Dienstes. Es gilt sowohl die Blacklist als auch die Whitelist kontinuierlich zu pflegen, um dem E-Mail-Spam möglichst effektiv und effizient gegenüber zu treten.

Heuristische Inhaltsanalyse: Beim Verfahren der heuristischen Inhaltsanalyse werden Regeln festgelegt, nach denen das Filtersystem den Inhalt einer eingehenden E-Mail bewerten kann. So kann ein solches Filtersystem bspw. erkennen, welche Informationen in der Betreffzeile und im Textteil der E-Mail enthalten sind. Die im Vorfeld zu definierenden Regeln können bspw. dafür sorgen, dass E-Mails, die bestimmte häufig in E-Mail-Spam auftretende Wörter enthalten, aussortiert werden. Zu diesen Wörtern zählen z. B. „Viagra" oder „Make Money Fast". Eine weitere Regel könnte E-Mails aussortieren, die Links zu Web Sites enthalten. Merkmal der heuristischen Inhaltsanalyse ist, dass sämtliche Regeln vor dem Einsatz der Software definiert werden müssen. Das heißt, dass diese Methode nur reagierend auf zuvor erhaltenen E-Mail-Spam wirken kann. Da E-Mail-Spam aber meist sehr ähnlich aufgebaut und formuliert ist, ist diese Methode recht effektiv. Der E-Mail-Spam-Versender kann versuchen, ein solches System zu umgehen, indem er z. B. statt „Viagra" „Vi@gra" schreibt. Allerdings können diese Veränderung der Wörter in das Regelwerk des Systems aufgenommen werden und sorgen zusätzlich noch dafür, dass E-Mail-Spam eindeutig identifiziert werden kann.[63]

Statistische Inhaltsanalyse: Ähnlich wie die heuristische Inhaltsanalyse untersucht auch die statistische Inhaltsanalyse den Inhalt einer E-Mail. Allerdings arbeitet die statistische Inhaltsanalyse nicht mit zuvor festgelegten Regeln, sondern nach einem statistischen Verfahren. Es werden dabei Daten aus zuvor als E-Mail-Spam identifizierten E-Mails gesammelt. Diese Daten werden auf signifikantes Aufkommen von bestimmten Zeichen- oder Wortketten untersucht, um in Zukunft E-Mail-Spam von Nicht-E-Mail-Spam zu unterscheiden und den E-Mail-Spam ausfiltern zu können.

Anders als bei der heuristischen Inhaltsanalyse muss die statistische Inhaltsanalyse zunächst mit dem „Spam" und „Nicht-Spam" vertraut gemacht werden, um bei einem späteren Einsatz zwischen beiden differenzieren zu können und die Fehlerwahrscheinlichkeit zu reduzieren.

62 Vgl. o. V.: Online Marketing Lexikon – Whitelist, Online im Internet: https://www.unternehmer.de/lexikon/online-marketing-lexikon/whitelist, 24.11.2018.

63 Vgl. Groh, Dennis: BAN SPAM – Der Schutz vor unerwünschten E-Mails im Rechtsvergleich zwischen Deutschland und Australien, 2014, S. 37 ff.

Vorteil der statistischen Inhaltsanalyse gegenüber der heuristischen Inhaltsanalyse ist, dass nach der Startphase kaum noch inhaltliche Pflege für das System nötig ist, da es sich selbst beibringt, „Spam“ und „Nicht-Spam“ zu unterscheiden. Kommt es zu Fehlern, können diese allerdings nur durch erneutes „Anlernen“ behoben werden.[64]

Vor dem Hintergrund, dass möglichst wenige „false positives“ auftreten dürfen, schützen alle diese Filtereinstellungen dennoch nicht vollständig vor E-Mail-Spam. Denn wenn es lediglich das Ziel wäre, keinen E-Mail-Spam im Posteingang vorzufinden, würde es genügen, mit strikten „Whitelist“-Einstellungen zu arbeiten. Allerdings ist dies häufig nicht der Fall. Daher müssen zu einem ausreichend guten Schutz vor E-Mail-Spam verschiedene Methoden kombiniert werden, um eine möglichst niedrige Quote von „false negatives“ bei einer gegebenen Quote von „false positives“ zu erreichen. Dem „normalen“ Teilnehmer am E-Mail-Verkehr bleibt keine andere Wahl, als die ein oder andere Spam-E-Mail, welche den Filter umgangen hat, von Hand auszufiltern und zu löschen. Gleichzeitig ist es nötig, sofern „false positives“ zugelassen werden, den „Spam-Ordner“ nach gewünschten E-Mails zu durchsuchen. Ein Hilfsmittel, bspw. in Unternehmen, können zusätzlich zu den Filtersystemen auch Hilfskräfte sein, die genau diese Aufgabe erledigen.[65]

4.2.3 Systeme und Tools gegen E-Mail-Spam

Die im vorigen Kapitel aufgezeigten Verfahren beschreiben Vorgehensweisen, um E-Mail-Spam systematisch auszufiltern. In diesem Kapitel sollen ausgewählte Tools und Systeme gezeigt werden, die diese Aufgaben erledigen können. Dazu werden zum einen die Filtersysteme gezeigt, die in die E-Mail-Clients integriert sind und zum anderen Tools und Anwendungssysteme, die den E-Mail-Client beim Erkennen von E-Mail-Spam unterstützen.

Für den Umgang mit E-Mails und insbesondere E-Mail-Spam empfiehlt sich die Nutzung eines lokalen E-Mail-Clients, der auf dem PC des Anwenders installiert ist. Der Umgang mit Spam-E-Mails auf E-Mail-Web-Clients gestaltet sich zumeist sehr umständlich und unübersichtlich im Vergleich zu lokalen E-Mail-Clients. Zu den bekanntesten und meist genutzten lokalen E-Mail-Clients gehören „Microsoft Outlook“, „Mozilla Thunderbird“, „Gmail“ und „Apple Mail“.[66]

Anhand von Microsoft Outlook 2016 soll nachfolgend dargestellt werden, welche Möglichkeiten der Anwender beim Umgang mit unerwünschten E-Mails hat. Zunächst kann der Anwender, sollte er E-Mail-Spam im Posteingang identifiziert haben, durch Rechtsklick auf die E-Mail,

64 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a.a.O., S. 104 ff.

65 Vgl. Topf, J. et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 86 f.

66 Vgl. Beins, Friederike: Anteile der E-Mail-Clients im E-Mail Marketing 2015, Online im Internet: https://www.newsletter2go.de/blog/e-mail-clients-2015/, 05.11.2015.

den Kontakt, der den E-Mail-Spam versendet hat, manuell sperren. Er kann aber auch ebenso E-Mails von Kontakten, die fälschlicherweise im „Spam-Ordner“ gelandet sind, durch gleiches Vorgehen manuell freigeben (siehe Abb. 2). Wurde ein Kontakt gesperrt oder freigegeben, werden nachfolgende E-Mails entweder als E-Mail-Spam oder zulässige E-Mails behandelt.

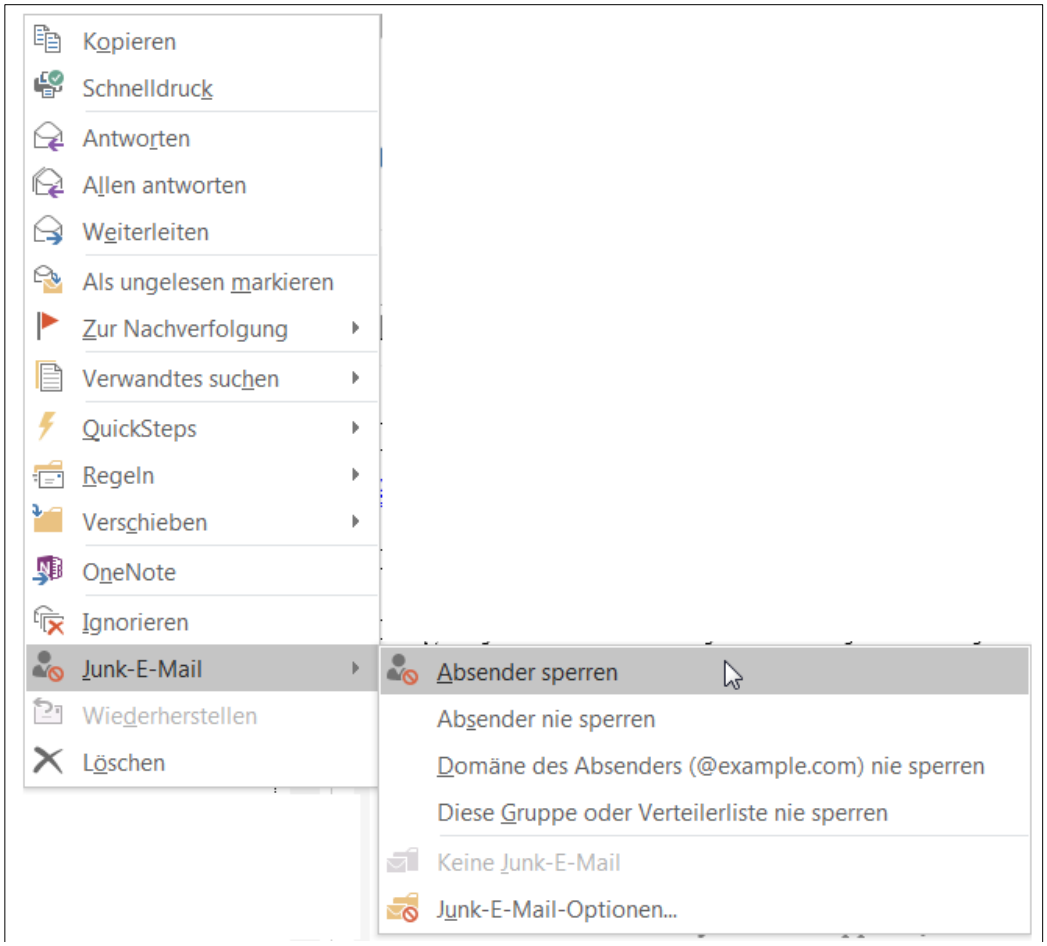

Abb. 2: Sperren von Absendern in MS Outlook 2016

Die manuell eingerichteten Filterregeln können in der Liste der blockierte Absender (Blacklist) und der sicheren Absender (Whitelist) eingesehen und bearbeitet werden. Diese Listen können durch Anklicken des Menüpunktes „Junk-E-Mail-Optionen“ geöffnet werden. Weiterhin können unter dem Menüpunkt „International“ Domains und Zeichensätze blockiert werden. So werden bspw., sofern derartige Einstellungen getroffen wurden, E-Mails aus dem Ausland oder mit ausländischen Zeichensätzen (bspw. arabisch) als Spam gekennzeichnet und automatisch im „Spam-Ordner“ abgelegt. Unter dem Menüpunkt „Optionen“ kann der Grad des E-Mail-Spam-Schutzes angepasst werden. Je höher der Grad des Schutzes, desto geringer die Wahrscheinlichkeit für „false negatives“ und desto höher die Wahrscheinlichkeit der „false postitives“ (siehe Abbildung 3).

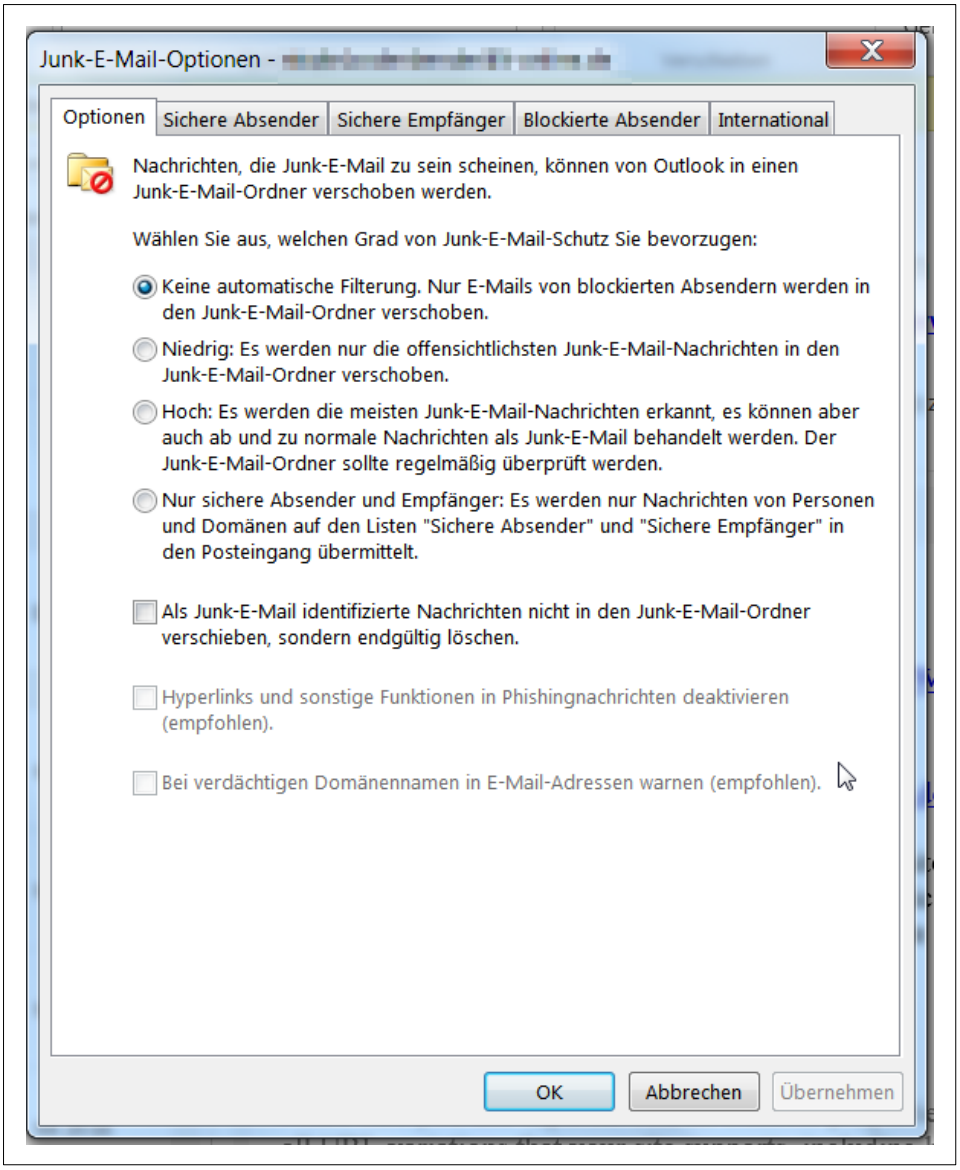

Abb. 3: Junk-E-Mail-Optionen in MS Outlook 2016

Es werden dem Anwender also „Black-“ und „Whitelisting“-Optionen angeboten, sowie eine automatische Filterung nach E-Mail-Spam, dessen Vorgehensweise hier nicht weiter erläutert werden soll. Je nach Präferenzen des Anwenders muss dieser sehr viele manuelle Einstellungen vornehmen, um die Fehlerwahrscheinlichkeiten auf ein annehmbares Niveau zu regulieren und so den Aufwand zu minimieren. Die hier am Beispiel von Microsoft Outlook 2016 dargestellten Filteroptionen können mehr oder weniger übersichtlich auch in anderen E-Mail-Clients eingestellt werden.

Unterstützend zu den im Client eingerichteten Filteroptionen wirken externe Tools, die es dem Anwender erleichtern sollen, E-Mail-Spam zu vermeiden. In dieser Arbeit werden zwei ausgewählte Tools vorgestellt. Zum einen das Tool „Spamihilator“[67] und zum anderen im Anhang

67 Vgl. die Web Site des Herstellers der Software „Spamihilator“, Online im Internet: https://www.spamihilator.com/de/, 17.12.2018.

das Tool „SpamSieve“[68]. Während das Tool „Spamihilator“ alle großen E-Mail-Clients außer Apple-Mail abdeckt, bedient „SpamSieve“ hauptsächliche Apple-Mail Anwender.

Der „Spamihilator“ ist ein kostenloses Software-Produkt, welches unabhängig vom E-Mail-Client auf dem PC des Anwenders installiert werden kann. Es greift dabei auf den E-Mail-Client zu und erlaubt es dem Anwender, Einstellungen zum Filtern von E-Mails zu erstellen und in den E-Mail-Client zu implementieren. Wie der soeben vorgestellte E-Mail-Client, ermöglicht auch der „Spamihilator“ dem Anwender das Einrichten und Verwalten von „Black-“ und „Whitelists“, ist aber aufgrund der schlicht gehaltenen Menüleiste deutlich übersichtlicher gestaltet (siehe Abbildung 4).

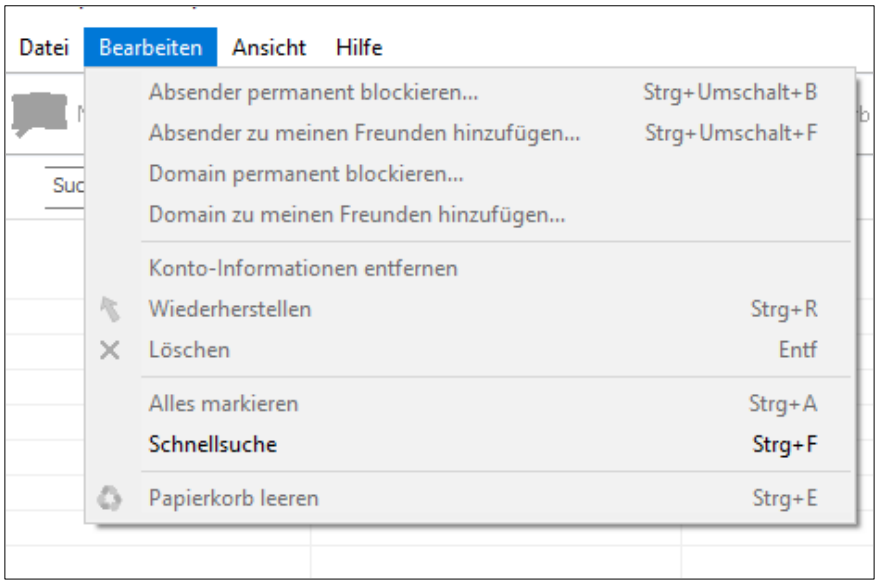

Abb. 4: Sperren von Absendern im „Spamihilator“

Dieser Vorteil resultiert vor allem daraus, dass das externe Filterprogramm nur den Zweck des intuitiven Verwaltens von E-Mail-Spam erfüllt. Neben einem übersichtlicheren manuellen Verwalten von Spam-E-Mails kann die Software weiterhin erlernen, ob es sich bei einer empfangenen E-Mail um E-Mail-Spam handelt oder nicht. Dazu muss die Software allerdings angelernt werden. Dies gelingt mit Hilfe des sog. „Trainingsbereiches“ (siehe Abbildung 5). Dort muss der Software durch manuelles Filtern beigebracht werden, ob es sich bei einer E-Mail um E-Mail-Spam handelt oder nicht. Nachdem die E-Mails als „Spam“ oder „Non-Spam“ gekennzeichnet wurden, muss die Eingabe mit dem Button „Lernen!“ bestätigt werden. Nachfolgend kann das System eigenständig zwischen E-Mail-Spam und Nicht-E-Mail-Spam differenzieren und erleichtert dem Anwender den Umgang mit E-Mail-Spam. Das soeben dargestellte Verfahren basiert auf der statistischen Inhaltsanalyse.[69]

68 Vgl. die Web Site des Herstellers der Software „SpamSieve“, Online im Internet: https://c-command.com/spamsieve/, 17.12.2018.

69 Vgl. Krämer, Michel: Der lernende Filter, Online im Internet: https://www.spamihilator.com/de/docs/learningfilter/, 15.12.2018.

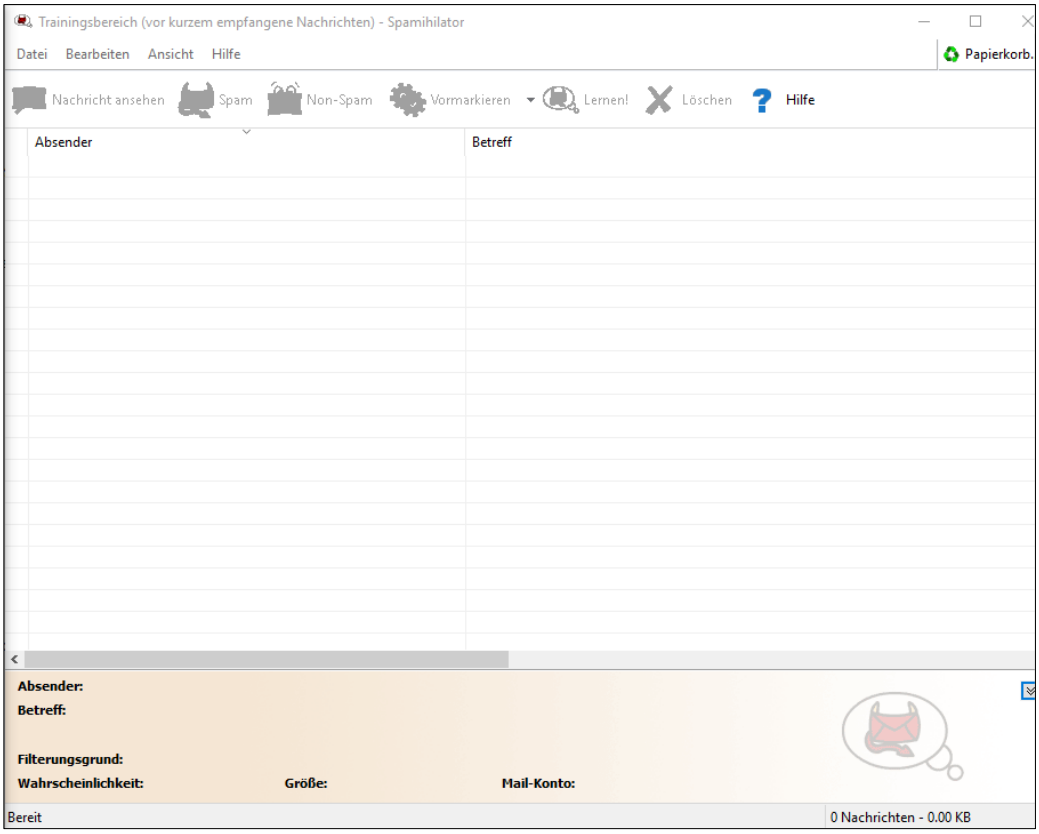

Abb. 5: „Trainingsbereich“ des „Spamihilators“

Weiterhin kann eine heuristische Inhaltsanalyse mit Hilfe eines Wortfilters durchgeführt werden. Es werden also, wie bereits im vorherigen Kapitel erläutert, Wörter und Wortketten definiert, die auf E-Mail-Spam hindeuten können. Anhand dieses Filters wird anschließend geprüft, ob es sich um E-Mail-Spam handeln könnte.[70] Ebenso können in E-Mail-Spam enthaltene Links zu externen Web Sites erkannt und unwirksam gemacht werden. So werden E-Mails, die einen Link enthalten entweder direkt als Spam identifiziert oder der darin enthaltene Link kann nicht durch Anklicken aufgerufen werden. Dies schützt den Anwender bspw. vor Phishing-Attacken.[71]

Das extern arbeitende E-Mail-Spam-Filterprogramm kann dem Anwender also durch umfassende Filtermaßnahmen dabei helfen, sich vor E-Mail-Spam zu schützen. Dabei ist das Programm aber auch für Laien sehr intuitiv zu bedienen und durch eine umfangreiche Dokumentation leicht zu verstehen.[72] Es kombiniert also die Vorteile des verbesserten Schutzes und einer einfacheren Bedienung gegenüber dem „normalen“ E-Mail-Client.

70 Vgl. Krämer, Michel: Der Wortfilter, Online im Internet: https://www.spamihilator.com/de/docs/wordfilter/, 15.12.2018.

71 Vgl. Krämer, Michel: Der Link-Filter, Online im Internet: https://www.spamihilator.com/de/docs/linkfilter/, 15.12.2018.

72 Vgl. Krämer, Michel: spamihilator.com: Dokumentation, Online im Internet: https://www.spamihilator.com/de/ docs/, 15.12.2018.

4.3 Server-seitige Maßnahmen

4.3.1 Konfiguration des E-Mail-Servers

Nachdem im vorherigen Kapitel Filtermaßnahmen und Tools zur Abwehr von E-Mail-Spam auf der Client-Seite erläutert wurden, werden in diesem Kapitel Server-seitige Maßnahmen gegen E-Mail-Spam vorgestellt. Auf dem Weg einer E-Mail vom Sender zum Empfänger passiert die E-Mail, wie in Kapitel 2.2 dargestellt, mindestens einen E-Mail-Server und mindestens zwei E-Mail-Clients. Daher können neben den Client-seitigen Maßnahmen gegen E-Mail-Spam auch Maßnahmen auf den zur Versendung notwendigen E-Mail-Servern ergriffen werden.

Die nachfolgend beschriebenen Konfigurationen eines E-Mail-Servers sollen beispielhaft darstellen, welche Maßnahmen getroffen werden können (optionale Einstellungen), um gegen E-Mail-Spam vorzugehen. Die Betreiber von E-Mail-Servern können den Nutzern der jeweiligen E-Mail-Server das Vorgehen gegen E-Mail-Spam durch eine Vorfilterung des eingehenden E-Mail-Verkehrs erleichtern. Dabei ist ein Betreiber eines E-Mail-Servers, z. B. der E-Mail-Provider, jedoch nicht verpflichtet, eine Filterung durchzuführen. Es ist sogar aus Sicht des Providers davon abzuraten, den E-Mail-Verkehr seiner Kunden unbefugt zu filtern, da dabei erwünschte E-Mails aussortiert werden können („false positives“) und somit eine Zustellung an den Empfänger unterbunden würde. In diesem Fall würde sich der Provider aufgrund einer sog. „Mail-Unterdrückung“ strafbar machen. Der Betreiber eines E-Mail-Servers kann lediglich von den Nutzern gebeten werden, eine Vorfilterung des eingehenden E-Mail-Verkehrs vorzunehmen. Durch eine derartige Anweisung eines Nutzers macht sich der Betreiber eines E-Mail-Servers bei der Filterung nicht strafbar, hat dabei jedoch die Pflicht, den Nutzer über die Gefahr von „false positives“ aufzuklären.[73] Bei der Filterung des E-Mail-Spams kann der Betreiber eines E-Mail-Servers an verschiedenen Stellen ansetzen: [74]

- Vor Versand der E-Mail
- Vor Annahme eingehender E-Mails
- Vor Zustellung an den Empfänger

An dieser Stelle ist zu beachten, dass die nachfolgend beschriebenen Maßnahmen nur mit Einwilligung bzw. im Auftrag der Nutzer getroffen werden dürfen. Einige Maßnahmen sind nach deutschem Recht kritisch zu betrachten. Da E-Mail-Spam häufig aus dem Ausland versendet wird, werden sie dennoch vorgestellt.

73 Vgl. Speichert, Horst: Praxis des IT-Rechts - Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, a. a. O., S. 214 ff.

74 Vgl. zu den nachfolgenden Ausführungen zur Filterung des E-Mail-Spams durch die Betreiber von E-Mail-Servern Topf, Jochen; et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 73 ff.

Vor Versand der E-Mail: Bevor die E-Mail an den E-Mail-Server des Empfängers übermittelt wird, muss die E-Mail zuerst dem E-Mail-Server des Versenders übergeben werden. Genau an dieser Stelle kann eine erste Filterung vorgenommen werden. Dabei können die gleichen Verfahren wie auf der Client-Seite eingesetzt werden. Es können also identifizierte E-Mail-Spam-Versender blockiert werden (Blacklisting). Ebenso können heuristische und statistische Inhaltsanalysen durchgeführt und somit offensichtlicher E-Mail-Spam aussortiert werden. Weiterhin kann der E-Mail-Server feststellen, an wie viele E-Mail-Adressen eine E-Mail adressiert ist. Dies kann ein weiterer Hinweis auf der Suche nach E-Mail-Spam sein.

Vor Annahme eingehender E-Mails: Hat der E-Mail-Spam den E-Mail-Server auf der Versenderseite verlassen, kann nun der empfängerseitige E-Mail-Server die Annahme des E-Mail-Spams verweigern. Auch an dieser Stelle können die zuvor genannten Filtermaßnahmen eingesetzt werden.

Vor Zustellung an den Empfänger: Nachdem die E-Mail vom E-Mail-Server des Empfängers angenommen wurde, soll sie dem Empfänger zugestellt werden. Einige E-Mail-Server übergeben die eingegangenen E-Mails erst an dieser Stelle einem Filterprogramm. Ein solches Filterprogramm geht bei der Filterung ebenfalls nach den zuvor genannten Methoden vor. Das Ergebnis der Filterung ist entweder die finale Zustellung einer E-Mail an den Empfänger oder die Rücksendung einer Fehlermeldung an den Empfänger („bounce“).

Im besten Fall arbeiten die Filter auf dem Weg vom Sender zum Empfänger mit einer zunehmend feineren Filterungsquote. Das heißt, dass die erste „Filterstation“ nur den offensichtlichsten E-Mail-Spam aussortiert und so weiter. Denn die durch den E-Mail-Server aussortierten E-Mails, egal ob E-Mail-Spam oder nicht, werden dem Empfänger nicht präsentiert. Aus diesem Grund muss die Quote der „false positives“ auf ein Minimum reduziert werden.

Allgemein sollte bei der Konfiguration des E-Mail-Servers darauf geachtet werden, „Open Relays“ zu schließen. Somit wird es den E-Mail-Spam-Versendern erschwert, den E-Mail-Spam zu versenden. Wird so die Mitnutzung des E-Mail-Servers durch E-Mail-Spam-Versender unterbunden, sorgt dies auch für eine Einsparung der zum Übermitteln von E-Mails benötigten Ressourcen.

4.3.2 Bewertung der Server-seitigen Maßnahmen

Nachdem im vorherigen Kapitel die Ansatzpunkte der Filtermaßnahmen auf den E-Mail-Servern vorgestellt wurden, werden in diesem Kapitel Vor- und Nachteile der jeweiligen „Filterstationen“ diskutiert. Eine Filterung an jeder der zuvor genannten Station führt zu einer Reduktion der benötigten Ressourcen an den jeweils nachfolgenden Stationen. Die dabei eingesparten Ressourcen sind hauptsächlich Aufwand für die Filterung und Bandbreite auf dem jeweiligen Server.

Wird E-Mail-Spam bereits vor Versand identifiziert und aussortiert, spart dies den Empfängern Zeit und Ressourcen. Gleichzeitig spart auch der Betreiber des E-Mail-Servers auf der Versenderseite Ressourcen ein. Allerdings ist eine derartige Filterung für E-Mail-Server, die in Deutschland betrieben werden, aus juristischer Sicht unzulässig, da sie möglicherweise die Zustellung gewünschter E-Mails unterdrücken. Außerdem hat der Empfänger keinerlei Einfluss auf den Betreiber des E-Mail-Servers des Versenders und kann diesem somit keine Erlaubnis für eine derartige Vorfilterung erteilen.[75]

Wird E-Mail-Spam vor der Annahme durch den empfängerseitigen E-Mail-Server ausgefiltert, spart der Betreiber dieses E-Mail-Servers Bandbreite ein, da er den E-Mail-Spam nicht weiterverarbeiten und selbst keine Fehlermeldung („bounce“) an den Versender senden muss.[76]

Wird der E-Mail-Spam auf dem empfängerseitigen E-Mail-Server angenommen und erst dort als E-Mail-Spam identifiziert und aussortiert, spart dies zwar dem Empfänger den Aufwand der eigenständigen Filterung, hat aber für den Betreiber des Servers zu Folge, dass dieser eine Fehlermeldung an den Versender senden muss. Dies kann aufgrund der daraus entstehenden „bounces“ zu kollateralem E-Mail-Spam führen.[77]

Der größte Nachteil, der bei der Filterung der E-Mails durch einen E-Mail-Server entsteht, bekommt der Empfänger der E-Mails zu spüren. Da die als E-Mail-Spam identifizierten E-Mails aussortiert und gelöscht werden, werden sie dem Empfänger nicht zugestellt. Dadurch besteht die Gefahr, dass eventuell erwünschte E-Mails niemals den Empfänger erreichen. Im Zweifel gelten solche E-Mails dann als zugestellt, haben den Empfänger jedoch nie erreicht. Die Folgen können für den Empfänger unangenehm sein, da bspw. Mahnungen oder Rechnungen nicht wahrgenommen werden können. Der Empfänger ist jedoch verpflichtet, auch die als E-Mail-Spam identifizierten E-Mails zu sichten. Durch diesen Umstand können rechtliche Konsequenzen folgen.[78]

Aus diesem Grund sollte der Empfänger gut abwägen, ob und in welchem Ausmaß eine Vorfilterung durch den E-Mail-Server durchgeführt werden soll. Eine Möglichkeit ist es, den Betreiber des E-Mail-Servers anzuweisen, die E-Mails zwar zu filtern aber dennoch zuzustellen. Auf diese Weise können E-Mails als E-Mail-Spam gekennzeichnet werden, kommen dennoch beim Empfänger an. So wäre er gegenüber der oben geschilderten Gefahr abgesichert.

75 Vgl. Speichert, Horst: Praxis des IT-Rechts - Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, a. a. O., S. 217 f.

76 Vgl. Topf, Jochen; et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 74.

77 Vgl. Topf, Jochen; et al: Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, a. a. O., S. 75.

78 Vgl. Speichert, Horst: Praxis des IT-Rechts - Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, a. a. O., S. 213 ff.

Im nachfolgenden Kapitel soll abschließend ein Ausblick auf die zukünftig zu erwartenden Entwicklungen des E-Mail-Spam gegeben werden. Weiterhin sollen mögliche Alternativen zum E-Mail-Verkehr genannt werden, um Spam vermeiden zu können. Außerdem sollen mögliche Risiken diskutiert werden, die durch E-Mail-Spam vor dem Hintergrund der steigenden Vernetzung entstehen können.

5 Ausblick

Der E-Mail-Dienst ist nach wie vor einer der wichtigsten Kommunikationskanäle, sowohl (und insbesondere) für Unternehmen, als auch für Privatpersonen. Die Anzahl versendeter und empfangener E-Mails und somit auch der E-Mail-Spam nimmt weiterhin stetig zu. Daher wird die Problematik, die der E-Mail-Spam erzeugt auch weiterhin von großer Bedeutung sein.[79] Wie aus dieser Arbeit zu entnehmen ist, entsteht durch E-Mail-Spam ein ständiges „Wettrüsten“ zwischen Sender und Empfänger. Während die Empfänger ihre Abwehrmaßnahmen ständig verbessern müssen, um nicht im E-Mail-Spam zu versinken, müssen E-Mail-Spam-Versender ständig neue Wege finden, um ihren E-Mail-Spam erfolgreich zustellen zu können.

Durch die zunehmende Vernetzung technischer Geräte kann E-Mail-Spam und die teilweise darin enthaltene Schadsoftware großen Schaden in Wirtschaft und Gesellschaft anrichten. Beispielsweise könnten voll vernetzte Krankenhäuser oder produzierende Unternehmen mit einem Schlag komplett lahmgelegt werden. Der dadurch entstehende Schaden wäre immens.

Ein aktuelles Beispiel dafür ist eine „Trojaner-Welle“, die über Phishing-E-Mails verbreitet wird. Verantwortlich für diese sog. „Emotet-Mails“ ist eine kriminelle Organisation. Deren Ziel dabei ist es, über sog. „Spear Phishing“ Schadsoftware in Unternehmen einzuschleusen. Dabei wird den Empfängern durch die leicht manipulierbaren Absenderadressen eine ihnen bekannte Identität vorgespielt. Dies kann bspw. ein Kollege aus dem eigenen Unternehmen sein. Da die Empfänger die scheinbaren Sender der E-Mail kennen, schöpfen sie keinen Verdacht über den Inhalt der E-Mail. Die Empfänger werden dazu verleitet, den Anhang der E-Mail zu öffnen. Sobald der Anhang der E-Mail geöffnet wurde, dringt die Schadsoftware selbst in gesicherte Netze ein. Zu den Opfern zählen derzeit sogar Regierungen und Rüstungskonzerne.[80]

Damit verbunden ist die ständige Sorge der Nutzer des E-Mail-Dienstes, dass ihre Abwehrmaßnahmen nicht ausreichen könnten, um effektiv E-Mail-Spam und die damit einhergehenden Gefahren abwehren zu können. Daher werden aus den erarbeiteten Inhalten dieser Arbeit zwei Konzepte abgeleitet, die Spam aus einem Kommunikationskanal aussperren können.

79 Vgl. Kramp, Linda: E-Mail-Aufkommen nimmt weltweit weiter zu, a. a. O., 19.05.2015.

80 Vgl. Schmidt, Jürgen: Achtung Dynamit-Phishing: Gefährliche Trojaner-Welle Emotet legt ganze Firmen lahm, Online im Internet: https://www.heise.de/security/meldung/Achtung-Dynamit-Phishing-Gefaehrliche-Trojaner-Welle-legt-ganze-Firmen-lahm-4241424.html, 05.12.2018.

Eine Möglichkeit für Unternehmen dem E-Mail-Spam aus dem Weg zu gehen, wäre die Kommunikation innerhalb eines gesicherten Netzwerks. Es könnten sich Unternehmen mit ihren Zulieferern und Geschäftskunden in ein geschlossenes Netzwerk zusammenschließen und sich somit von den E-Mail-Spam-Versendern abschirmen. Dadurch könnte der bei Unternehmen entstehende Wohlfahrtsverlust nahezu gleich null gesetzt werden. Allerdings würden private Nutzer des E-Mail-Dienstes davon eher wenig profitieren.

Die größte Hoffnung für die Nutzer des E-Mail-Dienstes ist wohl die künstliche Intelligenz: Ein Programm, welches E-Mail-Spam nahezu ohne Fehlerquote von gewünschten E-Mails unterscheiden kann. Bislang kann nur ein dafür geschulter Mensch eine derart geringe Fehlerquote erzielen. Eine Person zur Filterung von E-Mails einzusetzen ist aber, wie in Kapitel 2.3 erläutert, selbst bei einer Beschäftigung zum Mindestlohn unwirtschaftlich. Diesen Nachteil hätte eine künstliche Intelligenz jedoch nicht. Derzeit ist nur eine Annäherung an derartige Ergebnisse bei der Filterung von E-Mails durch den Einsatz statistischer Inhaltsanalysen möglich.

Anhang

Zu Kapitel 4.2.3:

Nachfolgend wird wie in Kapitel 4.2.3 erwähnt ergänzend zum „Spamihilator“ das Tool „SpamSieve“ vorgestellt. Da der „Spamihilator“ unterstützend zu vielen der großen E-Mail-Clients, nur nicht mit Apple Mail, eingesetzt werden kann, wird nun „SpamSieve“ als Tool zur Unterstützung von Apple Mail betrachtet. „SpamSieve“ geht bei der Abwehr von E-Mail-Spam ähnlich vor wie „Spamihilator“.

„SpamSieve“ fungiert dabei als Add On für Apple Mail und ist in den E-Mail-Client integriert. Der E-Mail-Spam ist daher unter Zuhilfenahme von „SpamSieve“ für den Benutzer intuitiv und unkompliziert zu verwalten.

Die Funktionen, die „SpamSieve“ dem Benutzer zur Verfügung stellt, sind nahezu identisch zu den Funktionen, die der „Spamihilator“ bereitstellt. Es wird dem Benutzer ermöglicht, Black- (bzw. Block-) und Whitelists zu erstellen und zu pflegen, sowie E-Mail-Spam über heuristische und statistische Inhaltsanalysen herauszufiltern. Die Bedienoberfläche ist jedoch an Apple Mail angepasst, da das „SpamSieve“ in Apple Mail integriert wird. Dies ist ein erheblicher Vorteil gegenüber dem „Spamihilator“, welcher als externes Programm neben dem E-Mail-Client ausgeführt werden muss.

Das „SpamSieve“ bietet dem Benutzer also eine einfach zu verwaltende und umfassend wirksame Abwehr gegen E-Mail-Spam. Es stellt dabei eine Ergänzung zum E-Mail-Client dar.[81]

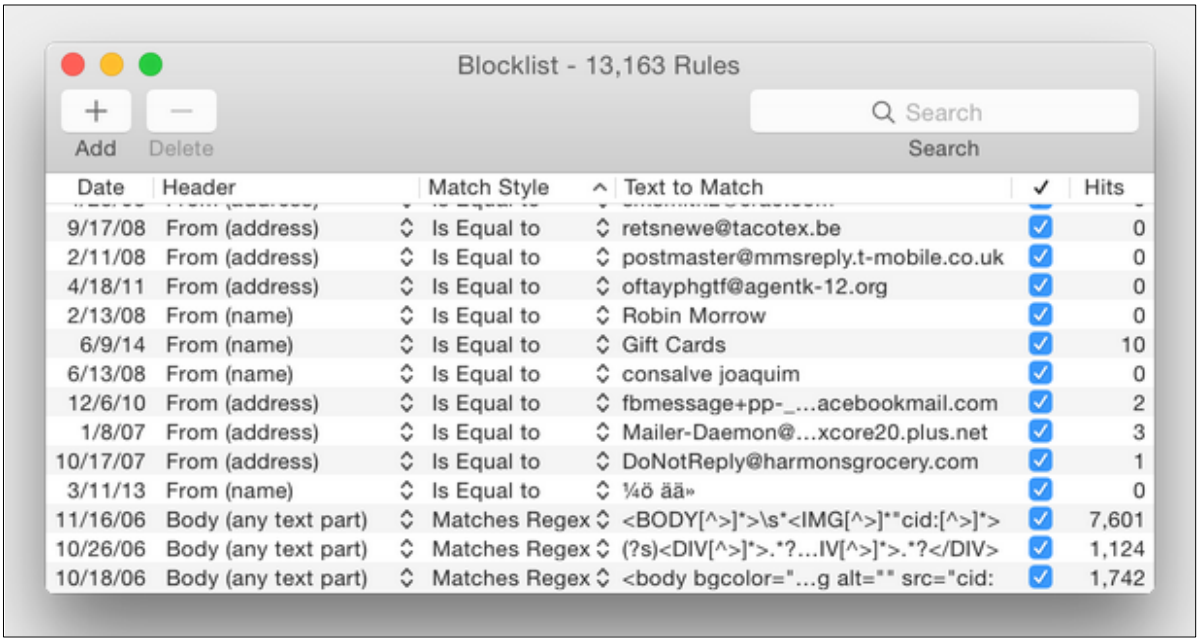

Abb. 6: „SpamSieve“ Blocklist

81 Vgl. die Web Site des Herstellers der Software „SpamSieve“, Online im Internet: https://c-command.com/spamsieve/features, 17.12.2018.

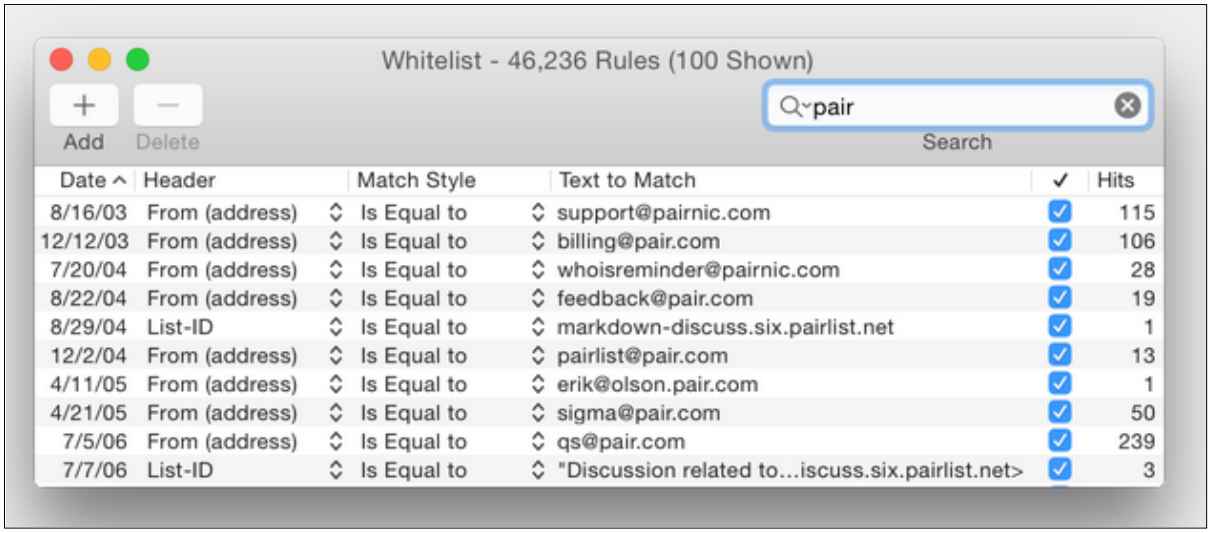

Abb. 7: „SpamSieve“ Whitelist

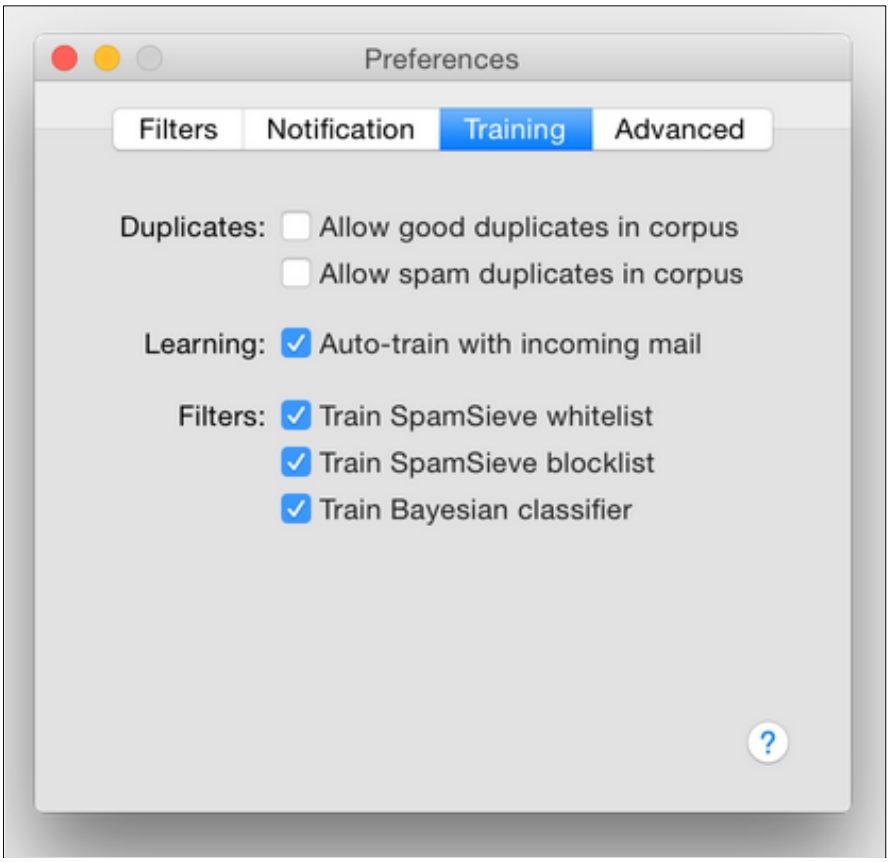

Abb. 8: Training der statistischen Inhaltsanalyse in „SpamSieve“

Literaturverzeichnis

1. **Beins, Friederike:** Anteile der E-Mail-Clients im E-Mail Marketing 2015, Online im Internet: https://www.newsletter2go.de/blog/e-mail-clients-2015/, 05.11.2015.
2. **Beins, Friederike:** Die ultimative Einführung in E-Mail Spam-Filter und Blacklists, Online im Internet: https://www.newsletter2go.de/blog/spam-filter-blacklists-email-marketing/, abgerufen am 06.12.2016.
3. **Bierschenk, Hans-J., et al:** Sicherheit für Systeme und Netze in Unternehmen – Einführung in die IT-Sicherheit und Leitfaden für erste Maßnahmen, 2003.
4. **Eckert, Claudia:** IT-Sicherheit - Konzepte - Verfahren – Protokolle, München, Wien: Oldenbourg Verlag 2005.
5. **Dent, Kyle:** Postfix - Ein sicherer und leicht zu verwaltender MTA für Unix, 2. Auflage, Köln: O'Reilly 2005.
6. **Donner, Andreas:** Definition – Was ist ein Proxy Server?, Online im Internet: https://www.ip-insider.de/was-ist-ein-proxy-server-a-665349/, 01.08.2017.
7. **Groh, Dennis:** BAN SPAM – Der Schutz vor unerwünschten E-Mails im Rechtsvergleich zwischen Deutschland und Australien, 2014.
8. **Herrmann, Dominik:** Beobachtungsmöglichkeiten im Domain Name System – Angriffe auf die Privatsphäre und Techniken zum Selbstdatenschutz, 2014.
9. **Krämer, Michel:** spamihilator.com: Dokumentation, Online im Internet: https://www.spamihilator.com/de/docs/, abgerufen am 15.12.2018.
10. **Kramp, Linda:** E-Mail-Aufkommen nimmt weltweit weiter zu, Online im Internet: https://newsroom.web.de/2015/05/19/e-mail-aufkommen-nimmt-weltweit-weiter-zu/, 19.05.2015.
11. **Kratzenberg, Marco:** Wegwerf-E-Mails – Anbieter und Funktionen, Online im Internet: https://www.giga.de/extra/email/specials/wegwerf-email-erstellen-anbieter-funktionen, 19.02.2018.
12. **Kreitling, Holger:** Wie Monty Python das Wort „Spam" erfanden, Online im Internet: https://www.welt.de/kultur/article3078427/Wie-Monty-Python-das-Wort-Spam-erfanden.html, 25.01.2009.
13. **Notenboom, Leo:** Whats the Difference Between an Email Domain, an Email Account, and an Email Adress?, Online im Internet: https://askleo.com/whats-difference-email-domain-email-account-email-address/, abgerufen am 20.11.2018.

14. **Pempel, Kacper:** Spam verursacht jährlich einen Schaden von 38 Mrd. Euro, Online im Internet: https://diepresse.com/home/techscience/internet/sicherheit/1430918/Spam-verursacht-jaehrlich-Schaden-von-38-Mrd-Euro-, 16.07.2013

15. **Rao, Justin; Reiley, David:** The Economics of Spam, Online im Internet: https://www.aeaweb.org/articles?id=10.1257/jep.26.3.87, abgerufen am 03.11.2018.

16. **Rouse, Margarete:** Wörterbuchangriff (Dictionary Attack), Online im Internet: https://www.searchsecurity.de/definition/Woerterbuchangriff-Dictionary-Attack, abgerufen am 14.11.2018.

17. **Schmidt, Jürgen:** Achtung Dynamit-Phishing: Gefährliche Trojaner-Welle Emotet legt ganze Firmen lahm, Online im Internet: https://www.heise.de/security/meldung/Achtung-Dynamit-Phishing-Gefaehrliche-Trojaner-Welle-legt-ganze-Firmen-lahm-4241424.html, 05.12.2018.

18. **Schmitz, Peter:** Definition Brute Force – Was ist ein Brute-Force-Angriff?, Online im Internet: https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/, 17.01.2018.

19. **Schneider, Markus; Winter, Christian; Yannikos, York:** Untersuchung von Spam-Eigenschaften kostenfreier Email-Dienste, 2010.

20. **Siepermann, Markus:** Gabler Wirtschaftslexikon: Domain Definition, Online im Internet: https://wirtschaftslexikon.gabler.de/definition/domain-34780, abgerufen am 24.11.2018.

21. **Sjurts, Insa:** Gabler Wirtschaftslexikon: E-Mail Definition, Online im Internet: https://wirtschaftslexikon.gabler.de/definition/e-mail-33576, abgerufen am 6.11.2018.

22. **Speichert, Horst:** Praxis des IT-Rechts - Praktische Rechtsfragen der IT-Sicherheit und Internetnutzung, 2. Auflage, Wiesbaden: Vieweg 2007.

23. **Stiller, Helmut**: Gabler Wirtschaftslexikon: Phishing Definition, Online im Internet: https://wirtschaftslexikon.gabler.de/definition/phishing-53396, abgerufen am 12.12.2018.

24. **Topf, Jochen; Etrich, Matthias; Heidrich, Jörg; Romeo, Leslie; Thorbrügge, Marco; Ungerer, Bert:** Antispam - Strategien - Unerwünschte E-Mails erkennen und abwehren, 2005.

25. **Wagner, Patrick:** Spamfilter haben immer weniger zu tun, Online im Internet: https://de.statista.com/infografik/14912/anteil-von-spam-am-weltweiten-mailverkehr/, 30.07.2018.

26. **o. V.:** C-Command Software – SpamSieve, Online im Internet: https://c-command.com/spamsieve/, abgerufen am 17.12.2018.

27. **o. V.:** Deutsches Institut für Vertrauen und Sicherheit im Internet: 30 Jahre E-Mail: wichtigstes Kommunikationsmedium der älteren Generation?, Online im Internet: https://www.divsi.de/30-jahre-e-mail-wichtigstes-kommunikationsmedium-der-aelteren-generation/, 12.08.2014.

28. **o. V.:** Elektronik Kompendium - Sicherheitsrisiken und Sicherheitslücken in der Netzwerktechnik, Online im Internet: https://www.elektronik-kompendium.de/sites/net/1811091.htm, abgerufen am 12.12.2018.

29. **o. V.:** IT-Grundschutz – M5.54 Umgang mit unerwünschten E-Mails, Online im Internet: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05054.html, abgerufen am 23.11.2018.

30. **o. V.:** Online Marketing Lexikon – Whitelist, Online im Internet: https://www.unternehmer.de/lexikon/online-marketing-lexikon/whitelist, abgerufen am 24.11.2018.

31. **o. V.:** Prognose zur Anzahl der täglich versendeten und empfangenen E-Mails weltweit von 2018 bis 2022 (in Milliarden), Online im Internet: https://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/, abgerufen am 03.11.2018.

32. **o. V.:** Spam, Phishing & Co – Phishing, Online im Internet: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html, abgerufen am 16.11.2018.

33. **o.V.:** Übermitteln von Spam-, Nicht-Spamnachrichten und Nachrichten, die als betrügerische Phishing-Angriffe angesehen werden, an Microsoft zur Analyse, Online im Internet: https://docs.microsoft.com/de-de/office365/securitycompliance/submit-spam-non-spam-and-phishing-scam-messages-to-microsoft-for-analysis, abgerufen am 11.06.2018.

34. **o. V.:** verbraucherzentrale.de: Spam: E-Mail-Müll im Internet, Online im Internet: https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/spam-email-muell-im-internet-10757, 03.05.2018.

35. **o. V.:** verbraucherzentrale.de: So lesen Sie den Mail-Header, Online im Internet: https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/so-lesen-sie-den-mailheader-6077, abgerufen am 6.11.2018.

36. **o. V.:** Wie viele private E-Mail-Adressen haben Sie?, Online im Internet: https://de.statista.com/statistik/daten/studie/29349/umfrage/anzahl-der-privaten-e-mail-adressen-pro-internetnutzer/, abgerufen am 13.12.2018.

37. **o. V.:** wisu das wirtschaftsstudium: IT-Security – wohl nur ein Traum, 04.2017.

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: http://wiwi.uni-giessen.de/home/Schwickert/arbeitspapiere/

Herausgeber: Prof. Dr. Axel C. Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse http://wiwi.uni-giessen.de/home/ Schwickert/arbeitspapiere/.