PERFORMANCE HEROES. ONLINE

Whitepaper

Den Spam-Filtern an den Kragen

So kommen Ihre Newsletter sicher an

Inhaltsverzeichnis

Einleitung 3

1 Spam-Filter und Spam-Score 4

Spam: Wie aus dem SPAM ein Spam wurde 4
Wortherkunft 4
Wortbedeutung 4

Spam-Filter: Fresszellen mit präzisem Appetit 5
Funktion 5
Mögliche Antispam-Techniken 7
Abfrage von Blacklists 7

Newsletter-Optimierung: Wozu denn das? 10
Versand ausschöpfen: Umsatz steigern ohne Mehrkosten 10
Blacklisting vermeiden 10

2 Newsletter Optimierung 11

Optimierung des Inhalts 11
Absender 11
Betreff 14
Inhalt bzw. Mail-Body 16
Links 18
Fake-Links 18
Tools zum Analysieren des gesamten Newsletters 18

Technische Optimierung 19
Mail-Server 19
Versandsysteme 21
DNS-Optimierung 22

Sonstige Optimierung 28
Blacklists überwachen und ggf. Austragung bantragen 28
Sender-Score-Reputation überprüfen 28
Vorgehen 28
Umgang mit Hard- und Softbounces 29

3 Checkliste 30

Fazit 31

Einleitung

Der Spam-Anteil im weltweiten E-Mai-Verkehr liegt bei etwa 57 Prozent. Allein in Deutschland wurden 150 Millionen Spam-Mails an einem einzigen Tag registriert (Statista). So ist es verständlich, dass Mailbox-Provider ihre Nutzer mit Hilfe scharf gestellter Spam-Filter vor den Massen an unerwünschten E-Mails schützen.

Nun gehören Sie als E-Mail-Marketer zu den seriösen Mailversendern. Trotz dessen stehen Sie vor der Herausforderung, die Mailbox-Provider davon zu überzeugen, dass Ihre Werbe-Emails erwünscht und vertrauensvoll sind. Die Newsletter sollen die Postfächer der Empfänger erreichen und von diesen gelesen werden und nicht fälschlicherweise als Spam deklariert in Spam-Filtern landen. Was also tun?

Der nachfolgende Artikel informiert über wichtige Parameter, die im Zusammenhang mit Spam-Filtern stehen und bei der Optimierung berücksichtigt werden sollten. Zum Beispiel erfahren Sie etwas über die Funktionsweise von Spam-Filtern und mögliche Ursachen für eine Spam-Mail-Einstufung. Auch finden Sie Hinweise für das Monitoring und konkrete Optimierungsansätze.

Wir geben Ihnen einen Fahrplan, mit dem Sie Ihre E-Mail-Kampagnen gezielt überprüfen und optimieren können.

1 Spam-Filter und Spam-Score

Spam: Wie aus dem SPAM ein Spam wurde.

Wortherkunft

Der Marken-Name SPAM schmückt ursprünglich in gelben Großbuchstaben Fleischkonserven der amerikanischen Hormel Food Kooperation.

Das in Dosen produzierte Mittagessenfleisch erobert seit 1937 den Markt. Zuerst als Proviant für die alliierten Truppen, dann als Fleischnahrung für die gemeine Bevölkerung. Das Dosenfleisch war in der Nachkriegszeit trotz Rationalisierung fast überall und für jeden frei erhältlich. Die Öffentlichkeit konsumierte es mit einer gewissen Vorsicht.

Schließlich spielt die britische Komiker-Gruppe Monty Python in einem ihrer Sketche mit dem Marken-Namen SPAM. Er dominiert zunehmend die Dialoge, bis eine normale Unterhaltung der Protagonisten kaum noch möglich ist. Er spammt sozusagen die Konversation. Der Begriff Spam für aufdringlich empfundene Informationsfluten ist in aller Munde. Hier der Link zum YouTube:

- Video: https://youtu.be/zLih-WQwBSc

Mit der ersten großen Werbeattacke durch die amerikanischen Anwälte Martha Siegel und Laurence Canter etabliert sich Spam als regulärer Ausdruck für unerwünschten Massen-Emails. Die beiden Anwälte ließen ein Programm schreiben, das ihre Werbebotschaft im weltweiten Informationsforum Usenet publizierte. Ihre Message: Gegen Honorar haben wir Tricks, wie die alljährlich stattfindende Green-Card-Lotterie zu gewinnen ist.

Wortbedeutung

E-Mails, die **in Massen** und **unaufgefordert** verschickt werden, erhalten die Bezeichnung **Spam**.

- Von „unaufgefordert“ spricht man, wenn die explizite und nachweisbare Erlaubnis für den Erhalt von E-Mails durch den Adressaten fehlt.
- Der Begriff „in Massen“ weist darauf hin, dass die E-Mails in großer Zahl und mit nahezu identischem Inhalt verschickt werden.

Beide Kriterien „unaufgefordert“ und „in Massen“ müssen gleichermaßen erfüllt sein, um eine E-Mail als Spam zu klassifizieren.

Spam-Filter: Fresszellen mit präzisem Appetit

Das weit verbreitete und als Open-Source-Projekt zugängliche Anti-Spam-System **„SpamAssassin“** dient hier beispielhaft als Erklärungs-Modell. Im Internet ist zu lesen, dass Internet-Service-Provider wie beispielsweise Gmail, Hotmail, Yahoo!, Mail, Gmx oder web.de diesen Spam-Filter einsetzen. Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) sind die Spam-Klassifizierungs-Verfahren der E-Mail-Anbieter sehr vielfältig und nicht im Detail bekannt. Auch eigene Systeme kommen zum Einsatz.

Funktion

Spam-Filter sind **Programme**, die E-Mail-Nachrichten mit Hilfe bestimmter Anti-Spam-Techniken überprüfen. Jedes einzelne **Prüfverfahren** verwendet eine Vielzahl an Kriterien, die **mit Punkt-Werten versehen** sind. Die eingehende Mail wird auf jede einzelne dieser Kriterien hin untersucht. Trifft eine Bedingung zu, so gibt es eine entsprechende Punktwertung. Diese kann positiv oder negativ sein. Positive Werte erhöhen die Wahrscheinlichkeit, im Spam-Filter zu landen.

Beispiel SpamAssassin: Test-Kriterien zum Thema Bild-Text-Verhältnis

Test-Name	Bedingung/Regel	Punkt-Wert
HTML_IMAGE_ONLY_04	Außer Bildern nur 0-400 Zeichen Text	3.5
HTML_IMAGE_ONLY_08	Außer Bildern nur 400-800 Zeichen Text	3.0
HTML_IMAGE_ONLY_12	Außer Bildern nur 800-1200 Zeichen Text	2.5

Erklärung: Der genannte SpamAssassin-Test meldet ein positives Ergebnis, sobald

- es sich um eine HTML-E-Mail handelt,
- mindestens ein Bild enthalten ist und
- die Größe des E-Mail-Body (inkl. nicht sichtbarer HTML-Anteile) zwischen 800 und 1200 Bytes liegt.

Hintergrund: Bei der Übertragung wird eine HTML-E-Mail in mehrere Teile zerlegt. Ein Teil davon ist immer vom Typ „text/html“.Sollten Bilder enthalten sein, werden diese in weitere Segmente entsprechend des Inhaltes (z.B. „image/png“) separiert. Bei der Bewertung des oben aufgeführten Test-Ausschnitts wird nun geprüft,ob

- ein Segment vom Typ „text/html“ vorhanden ist,
- ein Segment vom Typ „image/png“ oder „image/jpg“ vorhanden ist
- und es wird verglichen, ob die Größe des Segments „text/html“ innerhalb 800 und 1200 Bytes liegt. Hier wird die gesamte Größe des Segments festgestellt, inclusive aller HTML-Zeichen.

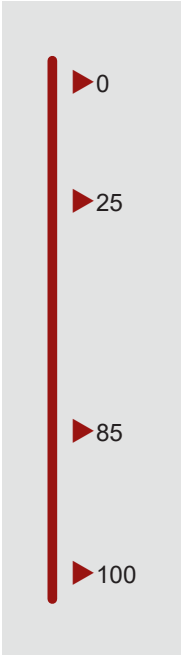
Wenn die E-Mail alle Tests durchlaufen hat, werden diese einzelnen regelspezifischen Punktwerte addiert. Die Summe bildet dann den sogenannten **Spam-Score**.

Der Spam-Score an sich hat jedoch noch keine Aussagekraft. Der Administrator, der das Anti-Spam-System auf dem Server des E-Mail-Service-Providers betreut, gibt dem Spam-Score eine Bedeutung. Er legt sogenannte **Schwellenwerte** fest.

Sobald ein Spam-Score diesen Schwellenwert überschreitet, passiert etwas mit der E-Mail: Sie wird unter Quarantäne gestellt, markiert, gelöscht oder abgewiesen. Je nachdem, welche Aktion der Administrator mit den definierten Schwellenwerten verknüpft.

Der von SpamAssassin im Standard vorgeschlagene Schwellenwert von Fünf scheint für die meisten Anwendungsfälle geeignet. So das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Ein modellhaftes Beispiel für die Festlegung von Schwellenwerten:
Nehmen wir an, der Spam-Score liegt auf einer Skala zwischen 0 und 100. Der Wert 0 steht für 100%igen Ham, der Wert 100 entspricht 100%igem Spam.



Der Administrator legt nun fest, dass alle E-Mails mit einem Spam-Score zwischen 0 und 25 Punkten dem Empfänger zugestellt werden. Erfahrungen sagen ihm, dass in einem solchen Fall kein Spam vorliegen wird.

Der Administrator definiert weitere Schwellenwerte. Er ist sich nicht sicher, ob es sich bei der E-Mail-Nachricht um eine Spam-Mail handelt oder nicht. Diese zusätzlichen Schwellenwerte koppelt der Administrator an verschiedene Maßnahmen. Er kann die Nachricht unter Quarantäne stellen oder als eventuellen Spam im Betreff markieren und zustellen.

Ab 85 Punkten lässt er die E-Mails automatisch löschen.

Schwellenwerte sind Administratorensache und entscheiden darüber, ob eine E-Mail zugestellt wird oder nicht.

Diese mit Punkt-Werten hinterlegten Regeln und Faktoren spielen in verschiedenen **Anti-Spam-Techniken** eine Rolle. SpamAssassin arbeitet modular und kombiniert mehrere Anti-Spam-Werkzeuge. Einige finden Sie nachfolgend kurz vorgestellt.

Mögliche Antispam-Techniken

Abfrage von Blacklists

Blacklists sind Negativlisten, die den Domain-Namen und die IP-Adresse spam-auffälliger Versandquellen festhalten. Blacklists können lokal durch den Admin oder zentral durch Unternehmen gepflegt sein. Das Anti-Spam-Filter-Programm greift auf diese Einträge zu und vergleicht sie mit den Adress-Angaben der zu untersuchenden E-Mail.

- **Beispiele für zentrale Blacklists**

Spamhaus ZEN:	http://www.spamhaus.org/zen/
SpamCop:	http://www.spamcop.net/
Mailspike:	http://www.mailspike.net/

- **Beispiele für Blacklist-Suchmaschinen**

AntispamSniper:	http://antispamsniper.com/dnsbl.php
DNSBL:	https://www.dnsbl.info/dnsbl-database-check.php
Kloth.net:	http://www.kloth.net/services/dnsbl.php

Abfrage von Whitelists

Whitelists bilden das Gegenstück zu den Blacklists. Auch sie lassen sich lokal oder zentral anlegen und pflegen. In zentralen Whitelists findet man Organisationen oder Absender, die sich dafür verbürgt haben, keinen Spam zu verschicken. Die Certified Senders Alliance (CSA) ist beispielsweise eine solche Organisation. Nutzt man ein von der CSA zertifiziertes Versandsystem, verringert sich die Gefahr erheblich, auf einer Blacklist und damit tief im Spam-Filter zu landen.

Performance Heroes GmbH verwendet ausschließlich Versandsysteme, die von der CSA zertifiziert sind.

- **Beispiele für zentrale Whitelists**

CSA:	https://certified-senders.org
DNSWL:	http://www.dnswl.org/
ISIPP:	http://www.isipp.com/email-accreditation/

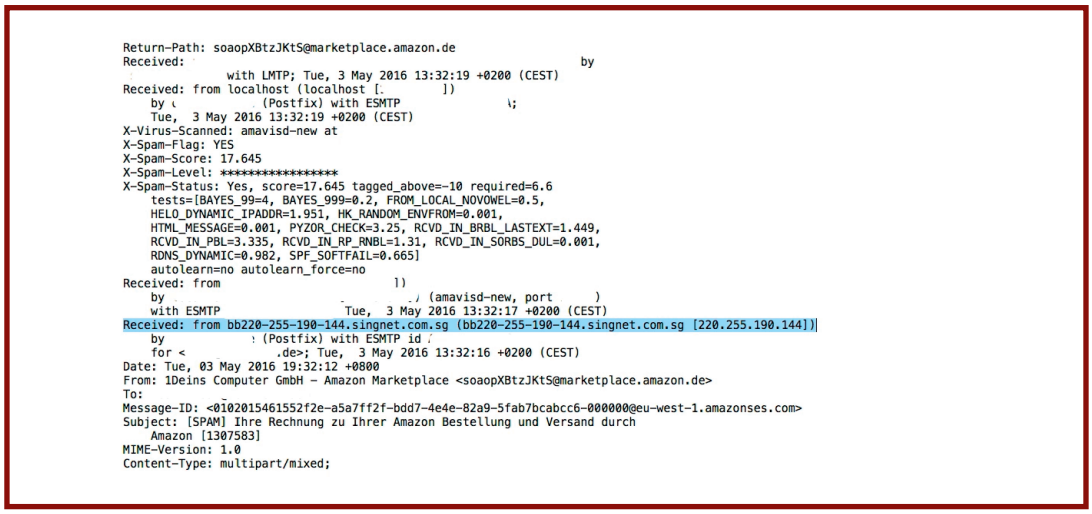
Analyse des E-Mail-Headers

Den E-Mail-Header stellt man sich als eine Art Briefkopf der Mail-Nachricht vor. Er enthält **Informationen** zum **Absender, Empfänger,** zum **Versand-Datum** oder auch zum **Übertragungsweg** der Nachricht. Im E-Mail-Header lässt sich beispielsweise überprüfen, ob der Server-Name und die IP-Adresse des Absenders identisch sind. Wenn nicht, dann ist Vorsicht geboten.

SpamAssassin führt hier verschiedene DNS-Abfragen durch, um sicher zu stellen, dass der versendende Mailserver auch wirklich zum Versand der E-Mail berechtigt ist. Das Thema DNS-Optimierung finden Sie im nächsten Kapitel ausführlich erläutert.

▶ So finden Sie den E-Mail Header in Outlook:

- ▷ Im Vorschaufenster des Mail-Clients wählen Sie mit Doppelklick eine Nachricht aus.
- ▷ Über „Datei" => „Eigenschaften“ öffnet sich das Fenster „Eigenschaften“.
- ▷ Dort finden Sie unter „Internetkopfzeilen“ den E-Mail-Header Ihrer ausgewählten Nachricht.



```
Return-Path: soaopXBtzJKtS@marketplace.amazon.de
Received:                                                          by
            with LMTP; Tue, 3 May 2016 13:32:19 +0200 (CEST)
Received: from localhost (localhost [.          ])
    by ‹            (Postfix) with ESMTP              \;
    Tue,  3 May 2016 13:32:19 +0200 (CEST)
X-Virus-Scanned: amavisd-new at
X-Spam-Flag: YES
X-Spam-Score: 17.645
X-Spam-Level: ******************
X-Spam-Status: Yes, score=17.645 tagged_above=-10 required=6.6
    tests=[BAYES_99=4, BAYES_999=0.2, FROM_LOCAL_NOVOWEL=0.5,
    HELO_DYNAMIC_IPADDR=1.951, HK_RANDOM_ENVFROM=0.001,
    HTML_MESSAGE=0.001, PYZOR_CHECK=3.25, RCVD_IN_BRBL_LASTEXT=1.449,
    RCVD_IN_PBL=3.335, RCVD_IN_RP_RNBL=1.31, RCVD_IN_SORBS_DUL=0.001,
    RDNS_DYNAMIC=0.982, SPF_SOFTFAIL=0.665]
    autolearn=no autolearn_force=no
Received: from                          ])
    by                                  (amavisd-new, port      )
    with ESMTP                  Tue,  3 May 2016 13:32:17 +0200 (CEST)
Received: from bb220-255-190-144.singnet.com.sg (bb220-255-190-144.singnet.com.sg [220.255.190.144])
    by            (Postfix) with ESMTP id
    for <           .de>; Tue,  3 May 2016 13:32:16 +0200 (CEST)
Date: Tue, 03 May 2016 19:32:12 +0800
From: 1Deins Computer GmbH - Amazon Marketplace <soaopXBtzJKtS@marketplace.amazon.de>
To:
Message-ID: <0102015461552f2e-a5a7ff2f-bdd7-4e4e-82a9-5fab7bcabcc6-000000@eu-west-1.amazonses.com>
Subject: [SPAM] Ihre Rechnung zu Ihrer Amazon Bestellung und Versand durch
    Amazon [1307583]
MIME-Version: 1.0
Content-Type: multipart/mixed;
```

Quelle: https://www.netzwelt.de/news/158678-spam-e-mails-so-ermittelt-wahren-absender-gefaelschter-mails.html

Schlüsselwort-Filter

Die Schlüsselwort-Filter durchstöbern den Inhaltsbereich einer E-Mail nach Wörtern und Sätzen, die in typischen Spam-Mails vorkommen. Das betrifft sowohl die Betreffzeile als auch den Fließtext. Spam-Signal-Wörter sind z.B.: Viagra, Sex, Million, kostenlos, gratis und viele mehr.

- Eine Übersicht möglicher Spam-Wörter finden Sie als Download auf unserer Website (siehe Link auf Seite 14).

Bayes-Filter

Der Bayes-Filter arbeitet mit **bedingten Wahrscheinlichkeiten**. Er überprüft eingehende E-Mails auf spamverdächtige Inhalte. Bestimmte Begriffe oder Phrasen werden oft nur in Spam-Mails gebraucht und kommen in Ham-Mails nicht vor. Werden diese Begriffe nun in einer neuen Mail identifiziert, handelt es sich bei dieser Nachricht mit größerer Wahrscheinlichkeit um Spam.

Der Bayes-Filter **muss trainiert werden**, bevor er zuverlässig funktioniert.
Das bedeutet, dass man ihn mit einer großen Anzahl an Spam- und Ham-E-Mails füttert und eine entsprechende Datenbank mit bereits verarbeiteten Wörtern und Tokens (Dollar-Zeichen, IP-Adressen, etc.) anlegt.

Diese Wörter und Tokens werden mit einem Wahrscheinlichkeitswert markiert. Die Wahrscheinlichkeit basiert hierbei auf Berechnungen, in die einfließt, wie oft das in der Spam-Mail verwendete Wort/der Token im Vergleich mit erwünschten Nachrichten (Ham) vorkommt.

Ursachen

Es gibt eine Vielzahl an Gründen, warum eine E-Mail an „Spam-Punkten“ gewinnt und im Spam-Filter landet. Diese können

- **technisch** bedingt sein.
  Die Nutzung eines nicht zertifizierten Versandsystems oder eine unzureichende DNS-Konfiguration ist spamverdächtig.
- **im E-Mail-Header** zu finden sein.
  Der Zeitstempel ist fehlerhaft oder die Absende-Adresse stimmt nicht mit der Sende-ID überein.
- den **Inhalt des Newsletters** betreffen.
  Der Newsletter verwendet spamverdächtige Signal-Wörter oder besitzt einen zu hohen Bildanteil.
- durch eine unseriöse **Link-Gestaltung** provoziert sein.
  Die Verwendung von Link-Verkürzern oder der Gebrauch von Fake-Links wird mit „Spam-Punkten“ abgestraft.
- auf die **Reputation** des Versenders zurückzuführen sein.

Newsletter-Optimierung: Wozu denn das?

Es ist wichtig, während der Gestaltung und dem Versand von Newslettern die Spam-Filter zu berücksichtigen und die E-Mails in Richtung „Ham“ zu optimieren, auch wenn Sie eine große Menge an E-Mails verschicken.

Versand ausschöpfen: Umsatz steigern ohne Mehrkosten

Je mehr von den verschickten E-Mails in den Postfächern der Empfänger landen, desto größer ist die Chance, dass diese auch geöffnet und gelesen werden können. Dies schafft die Möglichkeit, den Umsatz zu erhöhen ohne dass dadurch Mehrkosten entstehen.

Michael Kornfeld zeigt in seinem Fachartikel zum Thema Aufwand und Nutzen von E-Mail-Optimierungsmaßnahmen anhand eines Rechenbeispiels den deutlichen Zuwachs an Gewinn, wenn sich die Öffnungsrate nur um ein Prozent, von 25% auf 26%, erhöht. Sein Fazit: Der ROI (Return On Investment) verbessert sich um 11%!

- Hier der Link zum Fachartikel:
  https://www.email-marketing-forum.de/fachartikel/details/2025-wieviel-unterschied-ein-prozentpunkt-machen-kann/168347

Wenn Ihre spamorientierte Newsletter-Optimierung eine Steigerung der Zustellrate um ein Prozent bewirkt, dann haben Sie mehr als ein Prozent zusätzliche Empfänger, die Ihre Newsletter öffnen, anklicken und mit Conversions beantworten können. Bezogen auf obiges Rechenbeispiel führt dies zu einer deutlichen Anhebung des ROI. Ohne zusätzliche Kosten wie zum Beispiel Versandkosten oder Buchungskosten bei dem Einsatz von Fremdlisten.

Blacklisting vermeiden

Wer seinen Newsletter nicht optimiert, wird früher oder später auf einer Blacklist landen. Dies beschädigt nicht nur den Ruf sondern wirkt sich ebenfalls negativ auf die Zustellrate aus. Selbst reguläre Kontakte mit Kunden und Geschäftspartnern können als Folge blockiert sein. Wer das Blacklisten seines Unternehmens nicht rechtzeitig erkennt und hier gegensteuert, wird es zunehmend schwer haben, sich aus diesen Sperrlisten wieder austragen zu lassen.

2 Newsletter Optimierung

Optimierung des Inhalts

Absender

Laut des Lehrbuches „Online Marketing Grundlagen“ der Webmasters Akademie besagt eine Studie, dass mehr als 60% der User **zuerst auf den Absender schauen.** Für 70% der Empfänger ist das **Wiedererkennen** des Absenders ein wichtiger Grund, die E-Mail zu öffnen.

Absender-Adresse und Absender-Name

Professionelle Versandsysteme bieten die Option, mit der Absende-Adresse nicht nur die E-Mail-Adresse anzugeben, sondern auch den Namen des Absenders. Beides, E-Mail-Adresse und Absender-Name sind Informationen, die Spam-Filter untersuchen und bewerten. Darüber hinaus regen diese Angaben den Leser an, die Werbe-E-Mail mit Interesse zu öffnen. Nutzten Sie die Möglichkeit, sowohl Absender-Name als auch E-Mail-Adresse wohlüberlegt zu vergeben.

- Beispiel zweier Newsletter-Vorschauen:

Das erste Beispiel zeigt einen kurzen und eindeutigen Absender-Name, das zweite Beispiel einen zu langen und uneindeutigen Absender-Name.

Absender-Adresse

In der Absender-Adresse sollte die **Marke**, das **Unternehmen** oder der **E-Mail-Versender** für den Empfänger klar ersichtlich sein. Das schafft Vertrauen und erhöht den Wiedererkennungswert.

Sie sollte nicht aus einer schlecht greifbaren und verwirrenden Zeichenfolge bestehen. Eine Absender-Adresse wie newsletter@autohorst.de wirkt wahrscheinlich vertrauenswürdiger mit größerem Wiedererkennungseffekt als nl-z21@cro28-ka-16lf.gov.br. Einmal ausgewählt bleibt die **Absender-Adresse** im Gegensatz zum Absender-Name **unverändert** bestehen.

Verwenden Sie **keine noreply@-... Mail-Adresse** für den Versand Ihrer Newsletter. Eine solche Absender-Adresse klingt zum einen dialogfeindlich und wird zum anderen mit Spam-Punkten abgestraft. Die CSA lehnt die Nutzung von noreply@-... Mail-Adressen ebenfalls ab. Sie empfiehlt, eine **valide Absender-Adresse** einzusetzen, sodass der Empfänger mit Ihnen als Mail-Versender direkt in Kontakt treten kann.

Nutzen Sie für den normalen E-Mail-Verkehr und für den Newsletter-Versand **unterschiedliche Domains**. Denn falls Sie mit Ihrem Newsletter doch einmal auf einer Blacklist landen sollten, beeinflusst das nicht Ihren regulären Mail-Kontakt zu Kunden und Geschäftspartnern.

Absender-Name

Der Absender-Name bietet Ihnen einen größeren Gestaltungs-Spielraum
als die Absender-Adresse. Der Absender-Name ist **veränderbar**. So haben Sie die Möglichkeit, je nach Newsletter-Thema den Absender-Namen auf den Inhalt des Newsletters abzustimmen. Dies bietet sich an, wenn Sie viele verschiedene Arten von Werbe-Mails verschicken. Wichtig ist, dass der Absender-Name das **Kern-Thema** Ihres Newsletters aufgreift. Kurz und verständlich.

- Die Öffnungsrate erhöht sich deutlich, wenn Absender-Name, Betreff und Preheader aufeinander aufbauen und mit klaren, prägnanten Worten die Kernbotschaft Ihrer Werbe-E-Mail vermitteln.

Im Falle einer unternehmensinternen Newsletter-Versendung sollte der Absender-Name die Firma oder die Marke widerspiegeln, auf den sich der Newsletter bezieht. Wählen Sie hier einen Absender-Namen, den Sie langfristig und gleichbleibend einsetzen. Das steigert den Wiedererkennungswert und fördert das Vertrauen.

- Beispiele für die Darstellung von Absender, Betreff und Preheader in unterschiedlichen Mail-Clients (stationär und mobil):

- Beispiel für eine gelungene Abstimmung von Absender-Name, Betreff und Preheader:

Absenderlänge:
Ihr gewählter Absender sollte **nicht mehr als 20 Zeichen** fassen. Die meisten E-Mail-Programmen schneiden im Übersichtsbereich des Mail-Clients den Absender-Namen nach etwa 20 Zeichen ab.

Ganz generell:
Vergeben Sie einen Absender-Namen! Fehlt der Name in der Absender-Adresse, haben Sie wieder ein paar Punkte mehr auf Ihrem Spam-Konto.

Betreff

In der Bedeutsamkeit folgt die Optimierung des Betreffs direkt nach der DNS-Optimierung. Spam-Filter verwenden für die Betreffzeile viele Testregeln.

Spamverdächtige Trigger-Wörter und Phrasen

Vermeiden Sie spamverdächtige Wörter und Phrasen, wie zum Beispiel: Viagra, Sex, kostenlos, gratis, Million, kaufen, hier klicken und viele mehr.
In Spam-Filter-Systemen sind komplexe Regeln hinterlegt, welche die Betreffzeile gerade auf solche Ausdrücke hin untersucht.

- Hier finden Sie eine Auswahl an Spam-Trigger-Wörter, die es zu vermeiden gilt: https://performanceheroes.de/downloads/

Betreff-Länge

Achten Sie auf die Länge des Betreffs. Dieser sollte nicht zu kurz und auch nicht zu lang sein. Beides ist schlecht für den Spam-Score. Allgemein empfohlen sind **40-60 Zeichen**. Der Spam-Filter SpamAssassin empfiehlt 50 Zeichen. Einige Mail-Clients schneiden den Betreff jedoch schon nach 30 Zeichen ab.

Betreff-Inhalt

Der Betreff sollte **prägnant, sachlich und informativ** sein. Er greift das Thema der E-Mail auf.

Großschreibung

Schreiben Sie Ihre Betreffzeile nicht in einer Folge von GROSSBUCHSTABEN. Das wirkt aus Erfahrung spamverdächtig und wird auch so in den Spam-Tests mit Spam-Punkten bewertet. Darüber hinaus gleicht es eher einem unfreundlichen Schreien. Das motiviert den Leser nicht unbedingt, Ihren Newsletter zu öffnen. Laut SpamAssassin betrifft die Negativ-Wertung von Großschreibung auch die Verwendung von Abkürzungen wie B2B, SEO.

Wiederholung

Verwenden Sie nicht zu viele Satzzeichen in Folge. Spam-Filter mögen keine Wiederholung. Laut SpamAssassin gelten Satzzeichen, die drei oder mehr als drei Mal in Folge vorkommen bereits als Wiederholung und werden mit Spam-Punkten abgestraft. Beispiele: +++, !!!, ---; 10.000, !?!?!?

Emojis

Emojis im Betreff sprechen den Leser an. Sie schaffen einen zusätzlichen Reiz zum Öffnen der Werbe-Mail. Jedoch bereiten Emojis einigen Mail-Clients Probleme mit der Darstellung. Und Spam-Filter könnten diese zusätzliche Information an Zeichen, Zahlen und Buchstaben eventuell als Spam markieren.

Fazit: Verwenden Sie Emojis sparsam und auf das Newsletter-Thema abgestimmt. Prüfen Sie vor Versand, ob die Emojis in den Betriebssystemen Ihrer Nutzer korrekt angezeigt werden.

- **Ein Ausschnitt aus einem A-/B-Test: Betreffzeile mit vs. ohne Emojis**

  - **Ohne Emoji:** Ein Hörgerät verändert auch Ihr Leben
    Öffnungen: 1713, Öffner: 1533, Klicks: 76, Klicker: 23
  - **Mit Emoji:** Ein Hörgerät verändert auch Ihr Leben 🦻
    Öffnungen: 1843, Öffner: 1585, Klicks: 117, Klicker: 23

Das Beispiel zeigt einen Auszug einer Dokumentation von Versänden, die im Rahmen einer kleinen A/B-Testung zum Thema „Wirkungungsweise von Emojis im Betreff“ durchgeführt wurden. Der Emoji kann ein Impulsgeber sein. Die Öffnungsrate ist gewachsen.

Weitere Empfehlungen:

Vermeiden Sie im Betreff Superlative. Auch das ist aus Erfahrung spamverdächtig und wird entsprechend bewertet.

Täuschen Sie im Betreff keine Weiterleitung oder Antwort vor wie: Re:... oder Wg:…

Inhalt bzw. Mail-Body

Der E-Mail-Body birgt ebenfalls Stolpersteine für eine mögliche Spam-Einstufung Ihres Newsletters. Diese kann begründet sein in einem fehlerhaften HTML-Code oder durch die Verwendung spamverdächtigen Ausdrücke. Lesen Sie hier, an welchen Stellschrauben Sie Ihren Newsletter optimieren und damit Spam-Filter weit hinter sich lassen können.

Spamverdächtige Trigger-Wörter und Phrasen

Für den Fließtext gilt wie für den Betreff: Vermeiden Sie spamverdächtige Trigger-Wörter und Phrasen. Verzichten Sie auf Wiederholungen. Vergessen Sie die Großschreibung ganzer Wörter oder Sätze. Schreiben Sie auch gängige Kürzel wie BMW oder ADAC aus. Spamfilter mögen kein „Schreien“, keine Wiederholung und keine spamverdächtigen Ausdrücke.

Verhältnis Text zu Bild

Fassen Sie Ihren Newsletter nicht in einer einzigen JPG- oder PNG-Datei zusammen. Achten Sie auf ein ausgewogenes Verhältnis zwischen Text und Bild in Ihrem HTML-Newsletter. Empfohlen wird eine **Relation von 1/3 Bild- zu 2/3 Text**. Spammer umgehen gerne wortbezogene Spam-Tests, in dem sie Ihre Botschaften und Texte in Bilder verpacken. Deshalb reagieren Spam-Filter auf reine Bild-Newsletter sehr empfindlich.

Personalisierung

Eine persönliche Ansprache erzeugt Vertrauen und gilt Spam-Filtern als Indiz dafür, dass der Angesprochene den Newsletter auch wirklich bekommen möchte. Spam-Filter honorieren das. Nutzen Sie die personalisierte Ansprache **an prominenten Stellen** wie im Preheader, im Betreff, zu Beginn des Fließtextes oder innerhalb des Call-to-Action-Buttons. Professionelle Versandsysteme bieten Ihnen hierfür die entsprechenden Personalisierungs-Funktionen an. Erfüllt der Newsletter in einem Spam-Test die Regel „keine Ansprache“ oder „Neutrale Ansprache“ (Hallo, Hey, usw.), gibt es eine entsprechende Punktwertung, die Ihren Spam-Score weiter erhöht.

Grammatik und Rechtschreibung

Ein grammatikalisch und orthographisch korrekt verfasster Newsletter unterstreicht Ihre Seriosität. Dies ist sowohl für den Empfänger als auch für die Spam-Filter relevant. Die Erfahrung, dass Spammer gerne populäre Übersetzungs-Programme für ihre Botschaften mit entsprechend holprigen Ergebnissen nutzen, berücksichtigen Spamfilter in ihrem Regelwerk.

Multipart-Format

Eine **Text-Variante alternativ zum HTML-Format** anzubieten ist Pflicht. Spammer bevorzugen das HTML-Format. Entweder müssen Sie eigenständig eine Textversion entwickeln oder die Funktion der Versandsoftware extrahiert diese automatisch aus der HTML-Version. Die Textvariante sollte sich nah am Inhalt des HTML-Newsletters orientieren und Abmeldeinformationen anbieten.

Valides HTML

Achten Sie darauf, dass Ihr Newsletter in einem validen HTML-Code geschrieben ist, der auch von allen E-Mail-Readern gelesen und interpretiert werden kann. Das bedeutet

- „Old-School-HTML“,
- die Nutzung von Tabellen für die Gestaltung und
- Responsive Design.

Überlagern Sie das Dokument nicht mit zusätzlichen Codes und Scripts. Das kann auch dazu führen, dass Ihr Newsletter nicht in allen Clients korrekt angezeigt wird.

Größe des Newsletters

Der Newsletter sollte **zwischen 20Kb und 50KB** groß sein. Die meisten Spam-Mails sind erfahrungsgemäß kleiner als 20KB, mit Anhängen ausgestattet jedoch häufig größer als 50Kb. Die Mail-Größe ist auch ein Kriterium für mögliche Spam-Punkte.

Impressumspflicht

Das Fehlen des Impressums kann zu Abmahnungen führen und auch den Spam-Score deutlich erhöhen. Laut Telemediengesetz besteht eine Impressumspflicht als Volltext für gewerblich ausgerichtete Websites. Die CSA setzt als zwingendes Kriterium das Vorhandensein eines Impressums, das leicht erkennbar ist und alle Pflichtangaben enthält. Diese sind im Kriterium-Katalog der CSA aufgeführt.

Links

Fake-Links

Verwenden Sie keine Fake-Links in Ihrem Newsletter. Der Anker-Text eines Links als auch der Link selbst dürfen sich nicht widersprechen. Hier ein fiktives Beispiel für einen fake-verdächtigen Link. Der Anker-Text lautet: *www.amazon.de*. Der Link dahinter schreibt sich: *href="http://www.slek_77anne1276.net.* So eine Differenz erkennen Spam-Filter und füllen Ihr Spam-Konto mit Spam-Punkten.

Erreichbarkeit

Achten Sie darauf, dass Ihre Links im Newsletter erreichbar sind und nicht eine Fehlermeldung wie zum Beispiel einen HTTP-Statuscode 503 (Server steht temporär nicht zur Verfügung) provozieren.

URL-Shortener

Nutzen Sie keine URL Shortener. Kurz-URL-Dienstleister sind negativ behaftet, da diese sehr gerne von Spammern genutzt werden. URL- Short-Dienstleister erstellen eine kurze URL und verweisen mittels einer http-Weiterleitung von der gekürzten auf die ursprüngliche URL.

Die gekürzten Links sind aufgrund ihrer Kompaktheit für den Empfänger attraktiver, jedoch erkennt der Leser nicht mehr, auf welche Seite er durch die Verlinkung geleitet wird. So werden hinter den Kurz-URLs häufig Pishing und Malware Seiten versteckt, damit die Nutzer diese unbedacht besuchen.

Tools zum Analysieren des gesamten Newsletters

- **Newsletters-Test-Tools: „Wie spamverdächtig ist mein Newsletter?“**

  mail tester: https://www.mail-tester.com
  IsNotSpam: http://isnotspam.com/

Technische Optimierung

Mit der wohlüberlegten Organisation technischer Faktoren, steigern Sie die Wirtschaftlichkeit Ihrer Kampagnen. Hier erfahren Sie, welche wesentlichen Komponenten Sie optimieren können, um die Zustellrate Ihres Versandvolumens möglichst voll auszuschöpfen.

Mail-Server

Standort

Bei der Wahl des E-Mail-Service-Providers ist es empfehlenswert, darauf zu achten, dass sowohl Firmensitz als auch Serverort **innerhalb der EU** liegen.
So gehen Sie sicher, dass für Ihren genutzten Mail-Space zumindest die EU-Standards bezüglich Datensicherheit, Datenschutz und Zugriffsrecht gelten bzw. die des EU-Landes, in welchem der Service-Provider seinen Unternehmenssitz hat.

Denn Spammer verlagern gerne Geschäftsstelle und Rechner in Länder, die entweder nicht Willens oder nicht in der Lage sind, effektiv gegen Spam vorzugehen. Deshalb nehmen Spam-Filter auch den Server-Ort in ihr Regel- und Punktwerte-System auf.

- **Test-Tool Server-Standort: „Wo steht mein genutzter Server?“**
  Auf nachfolgenden Websites können Sie die IP-Adresse Ihrer Domain und das Land, in welchem diese gehostet wird, ermitteln.

  Pagedesign GmbH: www.utrace.de
  Tf-network.de: https://www.dein-ip-check.de/

Zertifikat

Sie haben auch die Möglichkeit, sich für einen Service-Provider zu entscheiden, der durch die **Certified Senders Alliance** (CSA) zertifiziert ist und der eine **ISO 27001-Zertifizierun**g besitzt.

Die **CSA-Zertifizierung** Ihres Service-Providers bewirkt, dass seine mit Gütesiegel bescheinigte Vertrauenswürdigkeit auch Ihre Reputation hebt und schützt. Ihr Service-Provider steht mit seiner IP-Adresse auf einer Whitelist. Die Zustellrate Ihrer Newsletter erhöht sich deutlich, wenn Spam-Filter Ihren Mail-Provider auf einer CSA-Whitelist finden. Die Qualitätsanforderungen, die sowohl der zertifizierte Teilnehmer als auch seine Vertragspartner erfüllen müssen, sind streng und vermeiden die Zusendung von Spam.

Der Versender verpflichtet sich z.B., die Namen und die IP-Adressen aller verwendeter Ausgangs-Mails-Server zu benennen. Er belegt, dass die genutzten Mails-Server unter seiner alleinigen Kontrolle liegen und den vorgeschriebenen Sicherheitsstandards entsprechen.

Bei Nichteinhalten der Standards drohen dem jeweilig zertifizierten Versender teure Sanktionen. Ein eng umschriebener Handlungsspielraum, der aber auch Sicherheit schafft, Schutz bietet und die Zustellbarkeit Ihrer kommerziellen E-Mail-Post erhöht. .

- Unter https://certified-senders.org/participants/ erhalten Sie eine Übersicht der von der CSA zertifizierten Mailbox-Provider.

Eine noch entscheidendere Rolle spielt die CSA im Zusammenhang mit den Newsletter- Versandsystemen, die Sie nutzen.
Ausführliche Informationen hierzu finden Sie im Abschnitt Versandsysteme.

Das **ISO 27001-Zertifikat** bescheinigt Ihrem Mailserveranbieter einen sehr hohen Standard im Informationssicherheits-Management. Auch das wirkt sich positiv auf Ihren Spam-Score aus.

Offenes Relay

Mail-Server, die den Versand von E-Mails ohne jegliche Authentifizierung und Prüfung des Absenders an beliebige Empfänger ermöglichen, werden als offenes Relay bezeichnet. Gehen Sie sicher, dass der von Ihnen benutzte Mail-Server kein offenes Relay ist.

Offene Relais werden von Spammern im Internet automatisiert gefunden und dann für den Versand ihrer Botschaften sofort und sehr gerne genutzt.Identifiziert der Spam-Filter Ihren genutzten Mail-Server als offenes Relay, schnellt Ihr Spam-Score in die Höhe. Dies ist äußerst schlecht für Ihre Reputation.

- **Test-Tool Offfenes Relay: „Wird mein Server als Offenes Relay genutzt?“**

SolarWinds:	https://tools.dnsstuff.com
MXToolbox:	https://mxtoolbox.com/diagnostic.aspx

TSL-Verschlüsselung

Vielleicht ganz selbstverständlich und trotz dessen erwähnenswert ist die Verschlüsselung Ihrer Nachrichten mit Hilfe des TSL-Zertifikats (Transport Layer Security) zur sicheren Datenübertragung Ihrer Mailings.

Versandsysteme

Anforderungen

Die nächste relevante Entscheidung, die Sie treffen müssen, ist die Wahl eines für Sie geeigneten E-Mail-Versandsystems. Vernünftig ist der Einsatz einer serverseitigen E-Mail-Marketing-Anwendung. Es gibt viele professionelle Anbieter am Markt.

Maßgebend ist, dass die Versandsoftware **zertifiziert** ist durch die **Certified Senders Alliance (CSA).**

Die Certified Senders Alliance (CSA) ist ein Service von eco, der als größter Verband der Internetwirtschaft in Europa seit 1995 das Internet gestaltet, neue Technologien fördert, die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien vertritt und Rahmenbedingungen schafft. Die CSA ist in Kooperation mit dem Deutschen Dialogmarketing Verband (DDV) im Jahr 2004 entstanden. **Die CSA bildet eine neutrale Schnittstelle zwischen Mailboxprovidern und Versendern kommerzieller E-Mails.** Verbesserung der E-Mail Die Zustellbarkeit der E-Mails wird bei den teilnehmenden Partnern verbessert und die Reputation durch Identifizierung von Schwachstellen geschützt.

Quelle: https://certified-senders.org/de/about-csa/

Die Nutzung eines CSA zertifizierten Versandsystems bringt Ihnen einen entscheidenden Vorteil in der Zustellbarkeit. Die IP-Adresse Ihres Versandsystem-Betreibers steht auf der CSA-Whitelist. Spam-Filter berücksichtigen das bei der Prüfung und stufen Ihre Newsletter als seriös ein. Die Zahl der Mailings, die es in die Empfangs-Postfächer schafft, steigt damit rapide.

Als Vertragspartner eines von der CSA zertifizierten Versandsystem-Betreibers haben Sie ebenfalls die Verpflichtung, den Kriterien-Katalog zu erfüllen. Hohe Auflagen, die jedoch auch Vorteile bringen. Der Empfänger kann sicher sein, dass die erhaltene Werbe-E-Mail von einem seriösen Versender kommt. Das versendende Unternehmen verbucht eine **deutlich höhere Zustellrate**.

- Eine Auflistung aller von der CSA zertifizierten Versandsysteme finden Sie unter: https://certified-senders.org/participants/
- Die Liste der CSA-Auflagen an eine Zertifikation kann öffentlich eingesehen werden unter: https://certified-senders.org/wp-content/uploads/2017/08/CSA-Aufnahmekriterien.pdf.

Weitere Anforderungen

Weiter sollte das Versandsystem Funktionen für rechtskonforme Anmelde- **(Double-Opt-In)** und Abmelde-Prozesse anbieten und die lokale **Pflege von White- und Blacklists** ermöglichen.

Ebenfalls wichtig ist die Bereitstellung von Methoden zum differenzierten Umgang mit **Hard- und Softbounces**.

Vorteilhaft ist auch, dass im Backstage-Bereich Ihres Versandsystem-Betreibers die **Anlaufstellen zu den verschiedenen Service-Providern** bekannt sind. Falls Ihre Domain doch einmal von einzelnen Mail-Providern blockiert sein sollte, kann Ihr Versandsystem-Betreiber schnell und gezielt mit den entsprechenden Providern Kontakt aufnehmen, um das Problem zu beheben.

DNS-Optimierung

Die Optimierung im Bereich des Domain Name Systems ist eine der wichtigsten Maßnahmen, die Sie vornehmen müssen, um an Spamfiltern vorbei zu kommen.

Auch mit einem noch so ansprechenden Newsletter werden Sie mit 100%iger Wahrscheinlichkeit früher oder später im Spam-Filter landen, wenn Sie hier nicht die entsprechenden Einträge vornehmen, die Ihre Domain eindeutig und fälschungssicher als berechtigten Absender bestätigen. Fehlende Einträge im DNS-System bestrafen die Spam-Filter mit Spam-Punkten.

Grundlegendes:

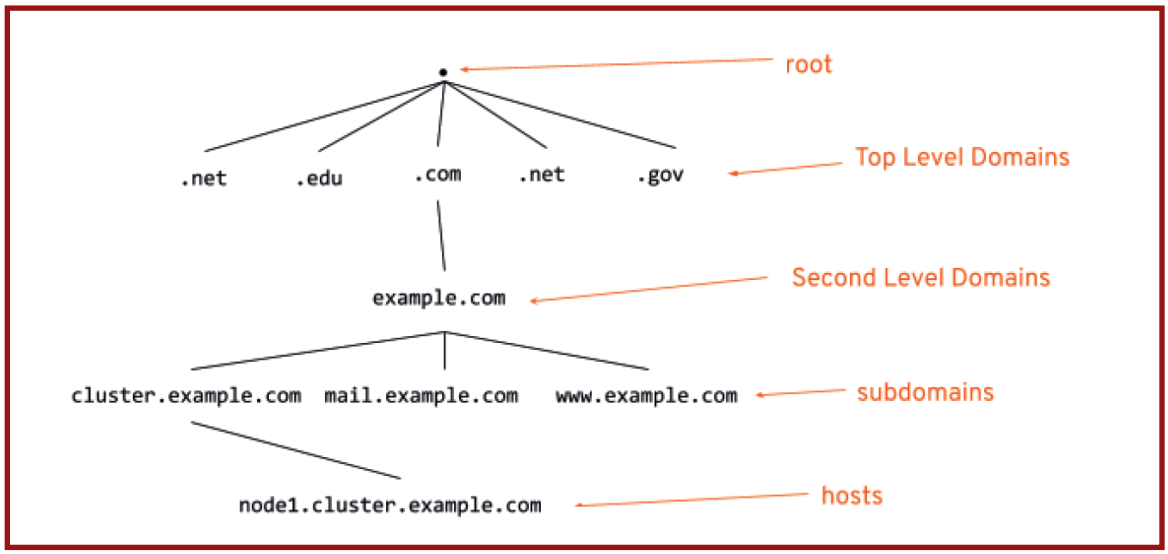
Im Internet erfolgt der Informations-Austausch zwischen den einzelnen Rechnern ausschließlich über sogenannte IP-Adressen. Jedem Rechner wird eine solche IP-Adresse zugewiesen. Sein Standort im Internet lässt sich damit eindeutig und fälschungssicher definieren.

Die IP-Adresse besteht aus vier Zahlenblöcken mit Ziffern jeweils zwischen 0 und 255. Die ersten drei Zahlenblöcke beziehen sich auf das Netzwerk, der letzte Zahlenblock steht für die Host-ID. Beispiel für eine fiktive IP-Adresse: 178.28.250.77

Diese Nummern sind für den täglichen Gebrauch jedoch recht schwer zu merken. Daher verwendet man Namen für die einzelnen Server im Internet.

Domain-Name-System

Das **Domain-Name-System (DNS)** ist eine Art Verzeichnis, das beide Informationen, den Namen als auch die IP-Adresse in Beziehung setzt. Man kann es abfragen wie ein Wörterbuch. Mit seiner Hilfe erfolgt der Transfer vom bekannten Domain-Namen zu seiner ihm zugehörigen IP-Adresse. Diesen Übersetzungsweg nennt man DNS Lookup oder Namens-zu-IP-Auflösung. Im umgekehrten Fall wird die lesbare IP-Adresse ihrem Domain-Namen zugewiesen und dies mit dem Begriff Reverse DNS Lookup markiert.



Das Bild zeigt die Struktur der verteilten, hierarchichen DNS-Datenbanken.und entstammt folgender Quelle: https://www.redhat.com/sysadmin/dns-domain-name-servers

▶ Test-Tool für das DNS-Lookup: „Wie lautet meine IP-Adresse?“

Mit der Programm-Funktion *nslookup*, die in Mac OS X- und Windows Betriebssystemen standardmäßig mit ausgeliefert wird, können Sie erfragen, welche IP-Adresse hinter einem Domain-Name steht und umgekehrt. Eine wichtige Basisinformation für weitere Recherchen.

▷ Vorgehen unter Windows:

1. Sie klicken auf Start bzw. auf das Windows-Symbol unten links.
2. Tippen Sie dort das Wort „Eingabeaufforderung“.
3. Es öffnet sich ein Fenster mit einem Editor.
4. Hier geben Sie in den lookup-Befehl ein.
   Die Syntax des Befehls lautet:
   nslookup Leerzeichen Domainname oder
   nslookup Leerzeichen IP-Adresse.
5. Die Eingabe bestätigen Sie mit Escape.

▷ **Vorgehen unter Mac OSX X-Betriebssystemen:**

1. Öffnen Sie auf Ihrem Mac das Netzwerkdienstprogramm, das sich
2. im Ordner „/System/Library/CoreServices/Applications/“ befindet.
3. Klicken Sie auf „Lookup“.
4. Geben Sie die Adresse eines Domain-Namens (z.B. www.apple.com) oder eine numerische IP-Adresse ein
5. und klicken dann auf „Lookup“.

Sender Policity Framework (SPF)

Das SPF ist eine Anti-Spam-Maßnahme, die der Absender-Authentifizierung dient. In der für die Domain zuständigen DNS-Zone hinterlegt der Domain-Inhaber eine spezielle Informationseinheit. In dieser dokumentiert er, welche Mailserver berechtigt sind, seine Domain zu verschicken. Der empfangende Mailserver greift auf diese Einträge im DNS-System zu und gleicht nun die IP-Adresse des sendenden Mailservers mit den für die Domain berechtigten Mailservern ab.

Ist die sendende IP-Adresse im SPF-Record nicht hinterlegt, kann die E-Mail über den SPF-Spam-Schutz der Service-Provider identifiziert und als Spam markiert und abgelehnt werden. Der SPF-Eintrag wird aus Sicherheitsgründen als zwingend vorausgesetzt.

▶ **Test-Tools für den SPF-Lookup:**
„Besitzt meine Domain einen SPF-Eintrag?“

InterNexum GmbH:	https://www.spf-record.de
EasyDMARC:	https://easydmarc.com/tools
MXToolBox.Inc:	https://mxtoolbox.com

▶ **SPF-Eintrag erstellen**

Sie können den SPF-Eintrag gegen Honorar erstellen lassen, ihn in Ihrem Admin-Bereich automatisch generieren oder diesen auch selbst manuell einrichten.

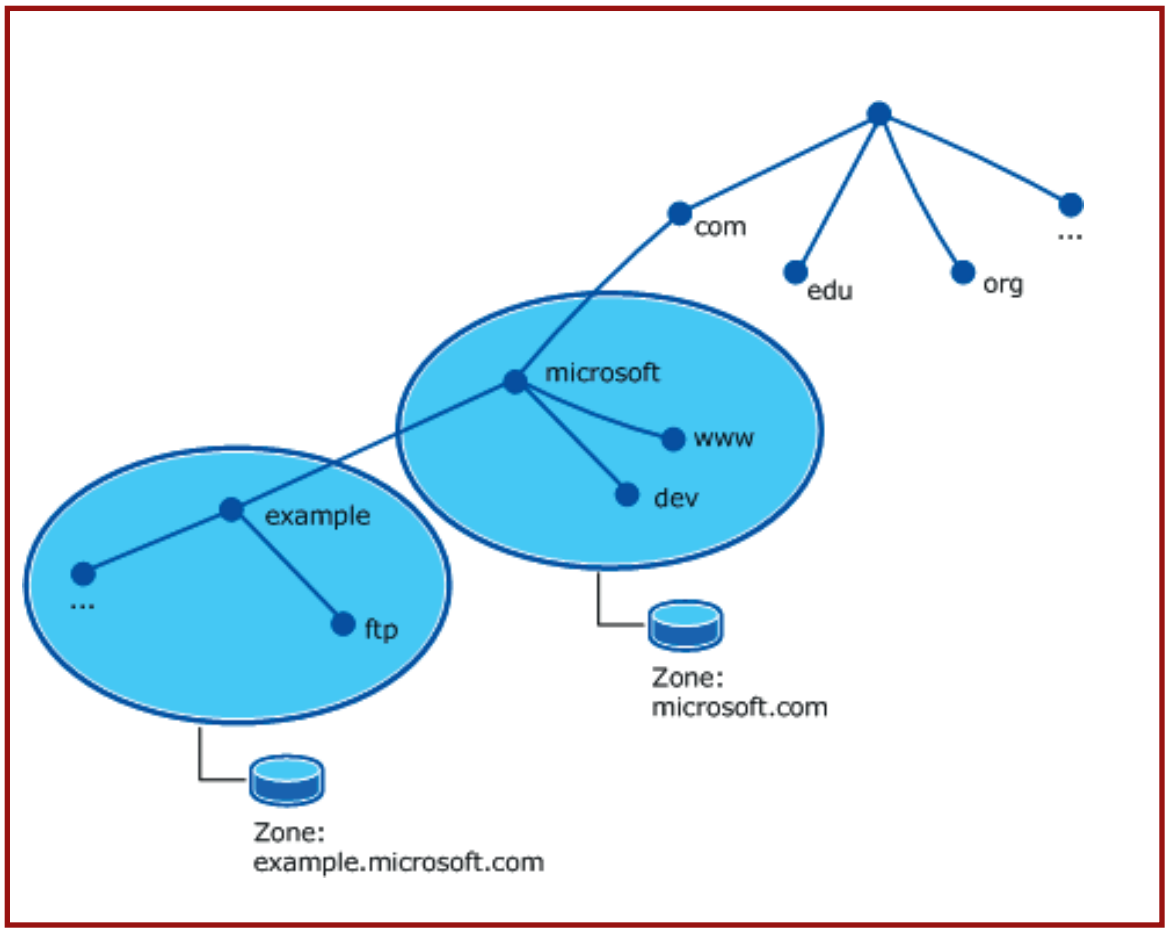
Der Link führt Sie zu einer Anleitung zum Thema SPF-Konfiguration: https://blog.k-webs.ch/2016-10-spf-im-detail-korrektes-einrichten-von-spf-records.html

Professionelle Versandsysteme übernehmen für Sie den SPF-Eintrag.

DNS-Zone

Im Domain Name System sind eine Vielzahl an Rechnern eingebunden, die einer verteilten und hierarchisch gegliederten Aufgaben-Struktur folgen. Der Root-Namens-Server speichert Informationen über alle existierenden Top-Level-Namens-Server. Jeder einzelne dieser Top-Level-Namens-Server speichert wiederum Informationen zu den Second-Level-Namens-Servern, die zu seiner Top-Level-Domain gehören. Die Second-Level-Namens-Server besitzen dann Informationen zum eigentlichen Hostnamen.

Eine DNS-Zone ist der DNS-Server, der für eine bestimmte Domain im Hierarchie-Baum zuständig ist.



Dieses Bild veranschaulicht den Begriff DNS-Zone und entstammt folgender Quelle:https://forsenergy.com/en-us/dnsmgr/html/2ad68d86-7a68-4363-b1b0-18fa66970dba.htm

Domain Keys Identified Mail (DKIM)

Der DKIM-Standard ist ein weiteres Verfahren zur Absender-Authentifizierung. Der versendende Mailserver errechnet nach einem bestimmten Algorithmus aus den Inhalten der E-Mail einen Hashwert. Im nächsten Schritt verschlüsselt er den errechneten Hashwert mit Hilfe eines „privaten Schlüssels“, der nur dem Domain-Inhaber bekannt ist. Den so verschlüsselten Hashwert setzt er im Header der Mail als Signatur. Das Gegenstück zum privaten Schlüssel, den sogenannten „öffentlichen Schlüssel“ hinterlegt er im DNS-Server des Domain-Inhabers.

Der empfangende Mail-Server ruft auf dem DNS-Server des Senders dessen öffentlichen Schlüssel ab. Mit diesem entschlüsselt er die Signatur. Passt der öffentliche Schlüssel nicht zur Signatur, kann er die Signatur nicht auflösen. Ein möglicher Hinweis darauf, dass die E-Mail nicht von dem Mail-Servergesendet wurde, der im E-Mail-Header angegeben ist. Hier könnte eine betrügerische Aktivitäten zu Grunde liegen.

Mit der erfolgreichen Entschlüsselung der Signatur erhält der empfangende Mail-Server wieder den Hashwert des Mail-Inhaltes. Diesen vergleicht er mit einem selbst errechneten Hashwert. Stimmen beide Hash-Wert nicht überein, dann weiß der Empfänger, dass die E-Mail verändert wurde. Stimmen jedoch beide Werte überein, ist die Identität gesichert und eine mögliche Manipulation des Inhaltes ausgeschlossen.

Abhängig vom Ergebnis der Prüfung, kann die E-Mail-Nachricht durch den empfangenden Mail-Server als Spam eingestuft und abgelehnt werden.

- **Test-Tools für das DKIM-Lookup:**
  „Besitzt meine Domain einen DKIM-Eintrag?“

MXToolBox.Inc:	https://mxtoolbox.com
DMARC Analyzer:	https://www.dmarcanalyzer.com
EasyDMARC:	https://easydmarc.com/tools/DKIM/

- **DKIM-Eintrag erstellen**

  Im Admin-Bereich Ihrer Domain haben Sie die Möglichkeit, einen DKIM-Eintrag generieren zu lassen oder diesen dort manuell zu konfigurieren. Professionelle Versandsysteme übernehmen diesen Eintrag für Sie.

Domain-based Message Authentification, Reporting and Conformance (DMARC)

Der DMARC-Eintrag wird ebenfalls in der DNS-Zone des Domain-Inhabers hinterlegt und bietet eine zusätzliche Methode, die der Verfälschung oder Verschleierung des Absenders entgegenwirkt.

Der DMARC-Standard integriert sowohl SPF als auch DKIM-Informationen und fügt diesen noch eine Handlungsanweisung und ein Reporting hinzu. Die Handlungsanweisung enthält Informationen, wie der Empfänger mit der E-Mail-Nachricht umgehen soll, falls diese sich nicht authentifizieren lässt.

Um den DMARC-Check zu bestehen, muss eine Nachricht sowohl den SPF- als auch den DKIM-Abgleich erfolgreich absolvieren.

- Test-Tools für das DMARC-Lookup:
  Besitzt meine Domain einen DMARC-Eintrag?

MXToolBox.Inc:	https://mxtoolbox.com
DMARC Analyzer:	https://www.dmarcanalyzer.com
Wildbit LLC:	https://dmarc.postmarkapp.com

- DMARC-Eintrag einrichten

  Im Admin-Bereich Ihres Mail-Spaces haben Sie die Möglichkeit, einen DMARC- Eintrag generieren zu lassen oder diesen manuell zu konfigurieren. Professionelle Versandsysteme übernehmen für Sie die Einrichtung.

Dies sind die wichtigsten Optimierungs-Ansätze im technischen Bereich. Tipp: Die Durchführung gehört in die Hände eines im E-Mail-Marketing erfahrenen Informations-Technikers.

Sonstige Optimierung

Blacklists überwachen und ggf. Austragung bantragen

Vorgehen:

Recherchieren Sie, auf welcher Blacklist Sie stehen könnten.
Dafür benötigen Sie zuerst Ihre IP-Adresse. Falls Sie fündig geworden sind, und die ermittelte Ursache beseitigen konnten beantragen Sie die Löschung der IP aus dieser Blacklist.

- **Testtools für die Blacklist-Recherche:**
  Steht meine Domain auf einer Blacklist?

AntispamSniper:	http://antispamsniper.com/dnsbl.php
DNSBL:	https://www.dnsbl.info/dnsbl-database-check.php
Kloth.net:	http://www.kloth.net/services/dnsbl.php
MXToolbox:	https://mxtoolbox.com
Senderscore:	https://www.senderscore.org/blocklistlookup/

Sender-Score-Reputation überprüfen

Vorgehen:

Führen Sie die Überprüfung regelmäßig durch. Die Sender-Score-Reputation ist schlecht manipulierbar und schwer zu beeinflussen. Sie entsteht hauptsächlich durch die Bewertung der Empfänger. Aber Sie haben einen Hinweis darauf, dass irgendetwas schiefläuft. Im schlimmsten Fall müssen Sie die Domain wechseln und wieder von 0 anfangen.

- **Testtool zum Abfragen des Sender Scores:**
  Wie ist mein Sender-Score?

Senderscore:	https://www.senderscore.org/blocklistlookup
Barracuda:	https://www.barracudacentral.org/lookups
Talos:	https://talosintelligence.com

Umgang mit Hard- und Softbounces

Ein Bounce entsteht, wenn eine E-Mail-Nachricht als Unzustellbar von einem Mailserver zurückgeschickt wird. Man unterscheidet zwischen zwei verschiedenen Arten von Bounces: Hard-Bounce und Soft-Bounce.

Bei einem **Hard-Bounce** war die Zustellung nicht möglich. Die E-Mail schafft es nicht bis zum Mail-Server des Empfängers. Diese Unzustellbarkeit besteht permanent infolge einer ungültigen oder nicht mehr bestehenden E-Mail-Adresse.

Kann die E-Mail aufgrund eines temporären Umstandes nicht zugestellt werden, spricht man von einem **Soft-Bounce**. Die E-Mail-Adresse ist in diesem Fall beim Mail-Server bekannt. Sie schafft es bis zum Mail-Server des Empfängers, gelangt jedoch nicht in dessen Postfach. Ursache für einen Soft-Bounce könnte ein überfülltes Postfach des Empfängers sein, eine zu große E-Mail oder auch ein zeitweilig nicht erreichbarer Mail-Server.

Wenn Sie E-Mails immer wieder ansprechen, die wiederholt einen Bounce erzeugen, kann dies als Spam gewertet werden und Ihre Reputation negativ beeinflussen.

Die CSA fordert, dass der Versender E-Mail-Adressen von der Mailingliste nehmen muss, wenn nach dem Beschicken dieser Adressen die Nichtexistenz des Postfachs erkannt wird, spätestens jedoch, wenn drei Hard Bounces erfolgten. Mehr dazu finden Sie im Kriterien-Katalog der CSA unter: https://certified-senders.org/wp-content/uploads/2017/08/CSA-Aufnahmekriterien.pdf

Deshalb ist es wichtig, ein entsprechendes Bounce-Management einzuführen und darauf zu achten, dass das von Ihnen gewählte Versandsystem hierfür Lösungen anbietet. Das bedeutet, dass das Versandsystem Bounces erkennt, zwischen Soft- und Hard-Bounces unterscheiden kann und Ihnen Filtersysteme an die Hand legt, mit denen Sie Ihren Verteiler regelmäßig aktualisieren können.

3 Checkliste

Kriterium	Domain
Domain-Name	
IP-Adresse	
Server	
Server-Name	
Server-Standort	
Provider	
Server Zertifikat	
Offenes Relay	
E-Mail	
E-Mail_Adresse	
DNS SPF-Eintrag	
DNS DKIM-Eintrag	
DNS DMARC-Eintrag	
Versandsystem	
Zertifikat	
IP-Adresse	
Server-Name	
Server-Standort	
An- und Abmelde-Funktion	
Pflege von White- und Blacklists	
Umgang mit Hard- und Softbounces	
Reputation	
Whitelist-Eintrag	
Blacklist-Eintrag	
Sender-Score	

Fazit

Zusammenfassend lässt sich sagen, dass der Bereich Optimierung im E-Mail-Marketing umfangreich und komplex ist. Er reicht von der Technik über den Mail-Inhalt bis hin zur Verteiler- und Reputations-Pflege. Auch externe Faktoren können ursächlich sein, wie z.B. die Einführung neuer Spamkriterien bei den Mail-Providern oder relevanten Organisationen. Da heißt es Augen auf und testen, prüfen, optimieren.

Anliegen dieses Beitrages ist es, auf mögliche und wesentliche Stellschrauben im Optimierungsprozess aufmerksam zu machen und konkrete Lösungsansätze und Anlaufstellen zu bieten.

Jetzt sind Sie gefragt und wir wünschen Ihnen viel Erfolg und eine hohe Zustellrate!

Quellenangabe:

Antispam – Strategien Bundesamt für Sicherheit in der Informationstechnik
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikatio nen/Studien/Antispam/Antispam-Strategien.pdf?__blob=publicationFile&v=2

Bachelorarbeit von Carsten Schulz
https://edoc.sub.uni-hamburg.de/haw/volltexte/2008/612/pdf/BA_Schulz.pdf

SpamAssassin von Alistar McDonald
https://books.google.de/

SpamAssassin
https://cwiki.apache.org/confluence/display/SPAMASSASSIN/SpamAssassin

CSA Certified Senders Alliance
https://certified-senders.org/de/

Spamhaus
https://www.spamhaus.org/consumer/definition/

EDV-Lehrgang
https://www.edv-lehrgang.de/ip-adressen-in-netzwerken/

Vielen Dank!

Annette Müller (Text und Gestaltung)

Ann-Isabell Hnida (Geschäftsführerin)

Performance Heroes Online GmbH
Conventsraße 12
22089 Hamburg

Tel. 040/18 13 503 16
Fax: 040/18 13 503 11
E-Mail: a.hnida@performanceheroes.de