VERBAND DER INTERNETWIRTSCHAFT E.V.

Best Practices für E-Mail-Marketing

... Wie Werbemails beim Empfänger in der Inbox ankommen

eco Kompetenzgruppe E-Mail

Inhaltsverzeichnis

Autoren: Marius Bauer (Experian Marketing Services), Mathias Ullrich (optivo GmbH), Florian Vierke (Mapp Digital)

Redaktion: Mathias Ullrich (optivo GmbH)

Mitarbeit: Sebastiaan de Vos (MailMike.net), Sven Krohlas (1&1 Mail & Media GmbH), Gunther Nitzsche (NetCologne Gesellschaft für Telekommunikation mbH)

Dank an: Andre Görmer (Mapp Digital), Arne Laske (optivo GmbH), Alexander Zeh (eco - Verband der Internetwirtschaft e.V.)

Einleitung

E-Mail-Marketing ist ein effizienter und kostengünstiger Teil des Online-Marketing-Mixes. In einer Befragung des Bundesverbands Digitale Wirtschaft (BVDW) e.V. gaben 84 % aller Befragten an, E-Mail für Online-Bestellungen zu nutzen (mehr Informationen zu dieser Umfrage gibt es bei der Fokusgruppe E-Mail des BVDW)[1]. Es ist für kleine und mittelständige Unternehmen ohne große Ressourcen oder Budgets ein Leichtes, ein E-Mail-Marketing-Programm aufzusetzen um so Kunden und Interessenten über aktuelle Produkte, Waren oder Dienstleistungen zu informieren.

Doch ganz so einfach ist es nicht. Damit die Werbebotschaften auch den Empfänger erreichen, genügt es nicht, „einfach so" loszulegen. Nicht jede E-Mail, die versendet wird, landet auch in der Inbox des Empfängers. Manche E-Mails werden direkt vom empfangenden Mailserver abgelehnt, andere werden in den „Junk"- bzw. „Spam"-Ordner zugestellt. Dieser Guide erläutert, wie man mit einfachen Maßnahmen sein E-Mail-Marketing so aufbaut, dass die E-Mails beim Empfänger wirklich ankommen.

Risiken

E-Mail Marketing bietet, richtig umgesetzt, ein großes Umsatzpotential. Jedoch gibt es auch Risiken für den Erfolg. Zum einen können Mailbox-Provider ganze Kampagnen ablehnen. Ein sogenanntes Blocking kann beispielsweise einsetzen, wenn zu viele nicht existierende E-Mail-Adressen angeschrieben werden oder wenn sogenannte Spam-Fallen (siehe „Datenerhebung – Was sind Spam-Fallen?") angeschrieben werden. Mit einem Blocking will der Mailbox-Providers seine eigene Infrastruktur und seine Nutzer schützen. Ein Blocking ist im Regelfall leicht festzustellen, da der Mailbox-Provider die E-Mails nicht annimmt und mit einem Fehlercode quittiert (siehe „Listenhygiene - Bounces").

Das zweite Risiko und die entsprechenden Auswirkungen lassen sich nur schwer feststellen. Sobald ein Mailbox-Provider die E-Mails nicht mehr in die Inbox einsortiert, sondern in den „Junk"-Ordner, ist dies nur über die Öffnungsrate zu erkennen. Grade bei Ziel-Domains mit kleinem Anteil am Mailing fällt dies kaum auf.

Beide Risiken haben einen großen Einfluss auf den Erfolg des E-Mail-Marketings. Nachrichten, die nicht zugestellt werden oder im „Junk"-Ordner landen, generieren keinen oder nur sehr wenig Umsatz.

[1] http://www.bvdw.org/medien/bvdw-whitepaper-zur-wechselwirkung-von-e-mail-und-social-media?media=7575

Reputation

Ein wichtiger Begriff ist im Rahmen der E-Mail-Zustellbarkeit der Begriff Reputation. Die Reputation beschreibt vereinfacht ausgedrückt das Ansehen, das der Werbetreibende beim Mailbox-Provider hat. Hier zählt nicht nur der erste Eindruck. Vielmehr ist eine Veränderung der Reputation – sowohl positiv als auch negativ - immer ein laufender Prozess. Durch einen einzelnen Fehler kann sich die Reputation durchaus nachhaltig verschlechtern. Diese dann wieder zu verbessern dauert ungleich länger.

Es gibt auch keine feste Zahl, an der sich die Reputation eines Werbetreibenden festmachen lässt. Jeder Mailbox-Provider arbeitet mit individuellen, unterschiedlich gewichteten Faktoren. Im Jahr 2014 sagte der Gmail Produktmanager Sri Harsha Somanchi in einem Interview[2], dass Gmail mehrere hundert verschiedene Faktoren verwendet, deren Gewichtung ständig geändert werde.

Einer der wichtigsten Faktoren ist das Engagement der Empfänger: Wie interagieren diese mit den E-Mail-Kampagnen? Dies kann positiv sein (Öffnungen, Klicks, Weiterleitungen usw.) oder negativ (ungelesen gelöscht, Markierung als Spam usw.).

Die Reputation hilft dem Mailbox-Provider zu entscheiden, ob und in welchen Ordner ein Newsletter zugestellt wird.

E-Mail-Provider oder rechtliche Vorgaben: Wer bestimmt die Spielregeln?

Einem juristischen Risiko setzt sich jeder Werbetreibende aus. In Europa ist E-Mail-Marketing nur mit vorheriger Einwilligung des Empfängers erlaubt. Ausnahmsweise und unter gewissen Voraussetzungen ist es zulässig, eigene Kunden mit Werbung für ähnliche Waren und Dienstleistungen zu beschicken.

Ein Mailbox-Provider entscheidet nicht nur entsprechend der Rechtslage, wenn er eingehende E-Mails bewertet, sondern auch danach, wie seine Nutzer mit den Newslettern in der Vergangenheit umgegangen sind. Der Fokus des Mailbox-Providers liegt immer auf seinen Nutzern und dem Schutz seiner Infrastruktur. Er hat keine wirkliche Verpflichtung, eine E-Mail zuzustellen. Da viele Dienste sich über Werbung finanzieren, ist es natürlich in deren Interesse, die Nutzer glücklich zu machen.

In Europa haben wir ein sehr hohes Datenschutzbewusstsein. Häufig gibt es Beschwerden der Empfänger von Werbung, viele verlangen Auskünfte vom Sender zur Nutzung und Speicherung ihrer Daten. Der Weg zum Anwalt ist daher recht kurz. Man kommt also um ein legal und sauber aufgestelltes E-Mail-Marketing nicht herum. Details dazu gibt es in der „eco Richtlinie für zulässiges E-Mail-Marketing[3]“ und natürlich beim Unternehmensjuristen.

[2] http://emailexpert.org/9-gmail-fbl-myths/

[3] https://certified-senders.eu/wp-content/uploads/2016/09/Marketing-Richtlinie.pdf

Meine nächsten Schritte als Werbetreibender?

Der erste Schritt sollte immer die Wahl eines professionellen E-Mail Service-Providers (ESP) sein. Der ESP stellt die technische Infrastruktur zur Verfügung, die zwingend erforderlich ist, um E-Mails erfolgreich zuzustellen. Der ESP unterstützt auch in Hinblick auf die Authentifizierungsmaßnahmen (siehe „Technische Grundlagen - Authentifizierung").

Ein Trugschluss ist es allerdings zu glauben, der ESP sei allein für die Zustellung verantwortlich oder könne sämtliche Probleme lösen. Sicherlich kann der Dienstleister unterstützen, aber neben den technischen Grundlagen kommt es vor allem auf die Datenerhebung, auf Listen-Hygiene und auf Inhalt an. Was es genau zu tun gibt, wird in den folgenden Kapiteln beschrieben.

Datenerhebung

Wesentlicher Bestandteil des E-Mail-Marketings ist natürlich die Akquise neuer Empfänger. Wie dieser Prozess aufzusetzen ist, um die Risiken so gering wie möglich zu halten, wird in diesem Kapitel beschrieben.

Die Einwilligung

Zentraler Ausgangspunkt muss immer eine aktive und informierte Einwilligung des Betroffenen sein. Dieser juristische Ausdruck beschreibt die Anmeldung über eine Newsletter-Anmeldeseite auf der Homepage oder im Shop.

Aktiv bedeutet in diesem Zusammenhang, dass der künftige Abonnent „etwas tun muss", um den Newsletter zu erhalten. Üblicherweise stellt das Klicken auf den Button für das Newsletter-Abo diese Aktivität dar.

Aber auch eine Checkbox, die der Kunde im Bestell- oder Registrierprozess aktiv anwählen muss, kann eine solche Aktivität sein. Wichtig ist dabei, dass eine Checkbox an der Stelle nicht bereits angewählt sein darf (das wäre dann ein sogenanntes "Opt-Out"). Dadurch kann es passieren, dass der Neukunde diese Option übersieht und damit nicht zu einem Abonnenten wird. Dennoch wäre dies im Resultat besser, als wenn der Kunde übersieht, dass er aktiv werden muss, um den Newsletter abzubestellen und dann beim Erhalt negativ überrascht wird.

Der zweite Aspekt ist die sogenannte Verifizierung, mit der sichergestellt werden soll, dass der Inhaber der E-Mail-Adresse auch der Einwilligende ist. Ist die Einwilligung nicht verifiziert, dann ist es für Dritte möglich, Anmeldungen mit beliebigen Adressen durchzuführen. Die gängigste und zuverlässigste Methode ist das Double-Opt-In-Verfahren, bei dem der Empfänger nach der Einwilligung noch eine E-Mail mit Bestätigungs-Link zur Verifizierung erhält, um seine Einwilligung aktiv zu bestätigen. Damit werden Spam-Fallen (siehe „Datenerhebung – Was sind Spam-Fallen?") und falsche Anmeldungen (egal ob zufällig oder böswillig) vermieden, die Empfängerliste ist in Summe hochwertiger. Auch rechtlich ist man mit dem Double-Opt-In-Verfahren auf der sicheren Seite, da dieses Verfahren von vielen Seiten, wie dem Düsseldorfer Kreis[4] (Konferenz der Datenschutzbeauftragten des Bundes und der Länder), empfohlen wird.

Transparenz

Ein sehr wichtiger Aspekt der Datenerhebung ist es, dem künftigen Empfänger so transparent wie möglich darzustellen, was ihn erwartet. Dies beginnt bereits bei dem Hinweis auf die Double-Opt-In-E-Mail, die versendet wird und bestätigt werden muss.

[4] https://www.lda.bayern.de/media/ah_werbung.pdf , Seite 11

Wichtig ist, dass der Empfänger weiß, was er erwarten kann und in welcher Frequenz. Je besser der Empfänger über Inhalte, Frequenz und Absender, aber auch die Möglichkeiten des Widerrufs informiert wird, desto geringer ist die Wahrscheinlichkeit von Beschwerden.

Was sind Spam-Fallen?

Spam-Fallen sind E-Mail-Adressen, die von Anbietern von Anti-Spam-Lösungen oder Mailbox-Providern genutzt werden, um Spam-Filteralgorithmen zu verbessern oder Versender abzustrafen, die sich nicht an die Grundregeln halten. Spam-Fallen gibt es in zwei Hauptarten:

- „pristine traps “: E-Mail-Adressen, die nie aktiv in Benutzung waren
- „recycled traps “: E-Mail-Adressen, die ehemals normal genutzt wurden und nach der Abschaltung in eine Spam-Falle umgewandelt wurden

Schreibt man also Spam-Fallen an, dann weist das entweder auf eine fehlende Verifizierung hin (wie ein Double-Opt-In-Verfahren) oder auf ein fehlerhaftes Bounce-Management. In beiden Fällen können Probleme für den Werbetreibenden entstehen, die dazu führen können, dass die Reputation des Versenders leidet und dadurch Werbebotschaften nicht beim Empfänger ankommen. Wenn über einen E-Mail-Service-Provider versendet wird, kann auch dieser Probleme wie Blockings bekommen.

Direktkunden

Sowohl in Deutschland, aber auch in ganz Europa ist es rechtlich möglich, eigenen Direktkunden Werbung für eigene ähnliche Produkte oder Dienstleistungen zu senden. Allerdings ist eine rechtlich saubere Ausgestaltung insbesondere in Deutschland sehr aufwändig, da für die Zustellbarkeit einiges beachtet werden muss. Die rechtlichen Auflagen lassen sich nachlesen in der „eco Richtlinie für zulässiges E-Mail-Marketing“.

Das erste Risiko bilden wieder Spam-Fallen, denn im Regelfall verifizieren Online-Shops die E-Mail-Adressen ihrer Kunden nicht. Somit können Spam-Fallen in den Verteiler geraten, wenn Kunden, absichtlich oder aus Versehen, eine nicht gültige E-Mail Adresse angeben. Die Aktivitäten im Shop geben keinen Hinweis auf solch eine falsche E-Mail-Adresse, denn die hindert nicht immer am Shoppen.

Ein weiteres Problem kann durch den Versand an Direktkunden ohne deren Einwilligung entstehen: Viele Menschen kennen diese Ausnahme im Gesetz einfach nicht. Für viele Empfänger kommt dann die Werbung überraschend. Das führt zwangsläufig zu Beschwerden. Wenn der Empfänger eine Nachricht als „Junk“ markiert, dann schadet das der Reputation des Werbetreibenden unabhängig von den rechtlichen Vorgaben.

Der sauberste Weg ist immer, eine aktive Einwilligung im Bestellprozess einzuholen. Dazu ergänzt man bei der Stammdatenabfrage einfach eine nicht vorausgewählte Checkbox, um sich direkt zum Newsletter anmelden zu können.

Der „Worst Case“ wäre es, einerseits diese Option anzubieten und anschließend, unabhängig von der Entscheidung des Kunden, ihm „ähnliche Waren und Dienstleistungen“ anzubieten. Das ist gegenüber dem Kunden sehr intransparent und provoziert Beschwerden.

Listenhygiene

Bounces

Vereinfacht ausgedrückt ist ein Bounce der Hinweis des empfangenden Mailservers, dass die Mail nicht zugestellt werden kann. Bei jedem Massenversand gibt es Bounces. Die sollten entsprechend ihrer Kategorisierung verarbeitet werden. Es ist wichtig zu beachten, dass eine gewisse Anzahl unzustellbarer Nachrichten (auch in Anlehnung an die Zeit der Postwurf „Rückläufer") durchaus akzeptabel ist.

Hardbounces

Bei Hardbounces handelt es sich um permanente Unzustellbarkeiten. Der angeschriebene Empfänger existiert nicht (user-unknown). Manchmal existiert auch die Domain nicht oder nicht mehr (domain-unknown).

Hardbounces werden gemeinhin als äußerst schädlich für die Reputation eines Versenders angesehen. Voraussetzung dafür ist natürlich, dass sie mehrfach pro Empfänger vorkommen. Es sollte also fortlaufend sichergestellt sein, dass zuverlässig kategorisierte Hardbounces mit entsprechenden E-Mail Adressen direkt aus der Empfängerliste entfernt werden.

Softbounces

Besteht eine noch so kleine Möglichkeit, den Empfänger zukünftig wieder zu erreichen, spricht man von einem Softbounce. Häufige Beispiele sind:

a) **Mailbox-full:** Der User hat keinen Speicher mehr zur Verfügung um die E-Mail anzunehmen. Wird die Mailbox in Zukunft aufgeräumt und somit durch den User wieder Speicherplatz freigegeben, ändert sich dieser Zustand und E-Mails können wieder angenommen werden. Diese Thematik verschiebt sich regional. In Deutschland nimmt die Zahl der ISPs mit kleinen Mailboxen (im Free-Modus) ab und damit auch die Zahl der vollen Mailboxen. Kommt es heutzutage zu solchen Bounces bei deutschen ISPs, tendiert man schon eher zum Ausschluss solcher Empfänger, da meist eine lange Zeit der Inaktivität vorangegangen ist.

b) **Spam-Reject:** Eine Abweisung auf Grund von Spam-Verdacht liegt entweder an der Reputation der Domain/IP oder an der Nachricht an sich. Zumeist sind solche Abweisungen auch umfassend für sämtliche User eines ISPs. Da eine negative Reputation in der Regel reversibel ist, wird sich bei angemessener Reaktion auf einen solchen Vorfall auch die Annahmebereitschaft des ISPs wieder ändern. Daher sollten solche Bounces eher als Arbeitsanweisung denn als Deaktivierungsempfehlung verstanden werden.

c) **Andere:** Es gibt natürlich noch viele weitere Ursachen dafür, weshalb Nachrichten nicht angenommen werden. Diese sind gegebenenfalls auf Einzelfallbasis zu prüfen und entsprechend einer automatisierten Verarbeitungsroutine hinzuzufügen.

Die automatische und zeitnahe Verarbeitung der Bounces ist in jedem Fall Pflicht. Einige E-Mail Service-Provider bieten auch automatische Reaktivierungen für Softbounces an. Idealerweise stellt der ESP der Wahl eine automatisierte De- und Reaktivierungs-Routine zur Verfügung. Diese sollte an das jeweilige Versandverhalten angepasst werden.

Abmeldungen

Abmeldungen sind eine aktive Form der Bewertung einer Marketing-Kommunikation. Ein vormals aktiver Empfänger von Newslettern einer bestimmten Marke ist nun nicht länger interessiert und bestellt den Empfang für die Zukunft ab.

Schwund ist zu vermeiden. Anders als bei Softbounces jedoch gibt es hier keinerlei Raum für Verhandlungen oder Interpretationen. Zumeist ist der Abmelde-Link zu klein und zu unauffällig platziert, als dass man diesen versehentlich hätte klicken können.

Es gibt verschiedene Möglichkeiten, den Empfänger zu veränderten Konditionen im Verteiler zu behalten. So haben Versender in der Vergangenheit bereits sehr gute Erfahrungen mit dem sogenannten Preference-Center gemacht. Auf dieser Seite kann der Empfänger seine Vorlieben oder die Frequenz einstellen. Es spricht nichts dagegen, dem abmeldewilligen Empfänger die Möglichkeit zu geben, die Frequenz der Newsletter anzupassen. Nicht selten wurden für den Geschmack Einzelner lediglich zu viele E-Mails in zu kurzer Zeit versendet.

Dringend vermieden werden sollte die künstliche Erschwerung einer Abmeldung. Das bewusste Verschleppen der Abmeldung durch nachgeschaltete Landing-Pages, Double-Opt-Out oder Captcha führt mittelfristig zu Reputationsverlusten durch Spam-Beschwerden der User, die nach einer zu langen Abmeldestrecke einfach aufgegeben haben.

Feedback Loops

Neben Abmeldungen sind Beschwerden eine Möglichkeit für den Empfänger, E-Mails mit unerwünschtem Inhalt oder von unliebsamen Absendern aus dem eigenen Blickfeld zu entfernen. Sobald sich ein Nutzer über Spam beschwert und eine E-Mail entsprechend markiert hat, verschiebt der Mailbox-Provider sämtliche zukünftigen Nachrichten des Absenders in den Spam-Ordner.

Eine versenderseitige Deaktivierung auf Basis der erfolgten Spam-Beschwerde ist eine weitere Möglichkeit. Um dies zu ermöglichen, bieten einige Mailbox-Provider die Möglichkeit an, einen Complaint-Feedback-Loop einzurichten.

Die technische Lösung ist einfach: Im Beschwerdefall sendet der Empfänger eine E-Mail in einem bestimmten Format an den Absender zurück als Hinweis, dass er diese Mail nicht möchte. Diese E-Mail beinhaltet die E-Mail im Klartext (was auch das Argument der deutschen Mailbox-Provider und Google ist, einen solchen Mechanismus nicht anzubieten). Mithilfe dieser Informationen ist der Versender dann im Stande, den Empfänger zu identifizieren und nicht mehr anzuschreiben. Es werden also in Zukunft keine weiteren werblichen E-Mails mehr an diesen Empfänger versendet.

Ausgenommen von dieser Regel sind natürlich Transaktions-Mails, die zu einem späteren Zeitpunkt etwa im Rahmen eines Bestellprozesses vom Beschwerdeführer ausgelöst werden.

Beispiel: Hat sich max.mueller@example.com montags über die Werbemail beschwert, bestellt dann mittwochs einen Artikel, so kann und muss die Bestell-, Versand und Bezahlbestätigung weiterhin ausgeliefert werden.

Generell gilt heute, dass nicht gewürdigte Beschwerden (bei vorhandenem Feedback Loop) äußerst negative Auswirkungen auf die Reputation als Versender haben können.

Manuelle Antworten

E-Mail ist eine Unterkategorie des Dialogmarketings. Das bedeutet, dass Antworten der Empfänger möglich sind. Nicht zuletzt deswegen gilt es heute nicht als standesgemäß, „no-reply@"-Absender-Adressen zu verwenden. Auch sollten die manuellen Antworten nicht nur empfangen, sondern auch verarbeitet werden können.

Eine Anbindung an die hausinterne Kundenbetreuung ist empfehlenswert. Das ist auch hilfreich, wenn es zu Unklarheiten mit den im Newsletter angebotenen Artikeln kommt.

Auch hier ist ein gewisser Automatisierungsgrad möglich und auch von Anfang an zu empfehlen. Natürlich können immer auch themenbezogene Fragestellungen in den Antworten enthalten sein, oft genug beschränken sich die Antworten jedoch auf wortkarge Aufforderungen zur Beendigung des Newsletter-Abonnements.

Inhalte

Engagement

Wie in den vorangegangenen Kapiteln beschrieben, gehören die Öffnungs- und Klickraten (*Engagement*) zu den wichtigsten messbaren Kriterien für eine gute Reputation. Ziel muss es also sein, diese Kennzahlen im Auge zu behalten und sinkende Werte kritisch zu hinterfragen. Sie sind das erste Indiz dafür, eine falsche Zielgruppe gewählt zu haben oder weisen auf einen Versand von Inhalten mit niedriger Relevanz hin.

Relevanz

Eine Öffnung symbolisiert dem Mailbox-Provider zunächst einmal Interesse am Inhalt der E-Mail. Durch einen Klick bescheinigt er der E-Mail nachdrücklich Relevanz, da

a) er dem Versender der E-Mail das Vertrauen entgegenbringt, einen enthaltenen Link zu öffnen,
b) er weiterführendes Interesse am Inhalt der E-Mail hat,
c) ihm der Versender offensichtlich bekannt und der Inhalt ausdrücklich erwünscht ist.

Relevanz ist heute das wichtigste Kriterium für die erfolgreiche Zustellung von E-Mails. Themen oder Wording spielen nur noch eine untergeordnete Rolle – solange die Inhalte relevant für den Endkunden sind, gibt es keine Einschränkungen mehr.

Achtung: Relevanz ist ein subjektiver Begriff – jeder empfindet andere Inhalte als relevant. Von daher lässt sich eine hohe Relevanz nur mit genauer Kenntnis der Zielgruppe erreichen.

Transparenz

Ein weiterer wichtiger Punkt ist die Transparenz bzw. der Wiedererkennungswert der Nachrichten. Je genauer der Endkunde weiß,

a) welche Inhalte er
b) wie häufig
c) zu welcher Zeit
d) von welchem Absender und sogar
e) in welcher Farbe/Schriftart

bekommt, desto positiver wirkt sich das auf das Öffnungs- und insbesondere das Beschwerdeverhalten der Empfänger aus. Es ist ebenfalls wichtig, dass der Nutzer sich jederzeit ohne große Hürden abmelden kann – auch hier können Beschwerden und damit eine negative Reputation vermieden werden. Ein ausführliches Impressum mit Link auf AGB schafft Vertrauen – eine wichtige Grundlage zum langfristigen Aufbau eines engagierten Zielgruppenverteilers.

Technische Grundlagen

Authentifizierung[5]

Die Sicherheit der elektronischen Post ist von den Anfängen der E-Mail in den 1980er Jahren an ein kontroverses Diskussionsthema – bis heute. Der Erfolg und gleichzeitig auch die Schwäche der E-Mail liegen in ihrer Einfachheit und der großen Verbreitung. In den Anfangsjahren war das Thema Spam noch viel weiter von einer Lösung entfernt als heute. Der Datenschutz war kaum geregelt. Heute gibt es weitreichende Möglichkeiten, Sicherheit und Authentifizierung herzustellen.

Diverse Technologien ermöglichen eine verbesserte Sicherheit und Authentifizierung von E-Mail Nachrichten. Diese sind im Detail:

SPF (Sender Policy Framework)

Im sogenannten Domain Name System wird hinterlegt, welche IP-Adressen im Namen der Domain E-Mails versenden dürfen. SPF ist schnell und einfach implementiert, kann jedoch nicht über Weiterleitungen oder Mailinglisten (sogenannte indirekte Mailflows) hinweg funktionieren. Es ist daher im alleinigen Einsatz ungeeignet zur Authentifizierung von Versendern.

DKIM (Domain Keys Identified Mail)

Die E-Mail wird mit einer digitalen Signatur versehen, welche vom Empfänger über den öffentlichen Schlüssel im DNS verifiziert werden kann. Somit kann erkannt werden, dass die E-Mail auf dem Versandweg verfälscht oder der Absender geändert wurde. Das Verfahren gilt als Basis der domain-basierten Reputationsbemessung.

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

DMARC vereinheitlicht die Nutzung von SPF und DKIM und ermöglicht es, eine Policy für den Mailbox Provider zu setzen. Diese gibt dann vor, wie im Falle eines fehlgeschlagenen Tests mit der Nachricht umgegangen werden sollte. Zusätzlich ermöglicht DMARC ein Reporting an den Versender, der somit erfährt, wie viele Nachrichten positiv bzw. negativ getestet wurden. Das Verfahren dient dem Schutz der eigenen Marke und dem Kampf gegen Phishing. Unsere Empfehlung ist es, DMARC auf die Haupt-Domain anzuwenden und somit die gesamte Marke zu schützen (und nicht nur eine austauschbare Sub-Domain davon). Mittels der „reject-policy" kann

[5] Erstveröffentlichung auf dem Blog der Teradata GmbH: Sicherheit & Authentifizierung – welche Technologien gibt es im E-Mail-Marketing? [F.Vierke, Juli 2016] http://blogs.teradata.com/teradata-applications/de/sicherheit-authenzifizierung-welche-technologien-gibt-es-im-e-mail-marketing/

eine Marke aktiv verhindern, dass eine Nachricht mit fehlgeschlagener oder fehlender Authentifizierung an den Empfänger zugestellt wird.

TLS (Transport Layer Security)

Verschlüsselung des Transportwegs zwischen Versender und Empfänger. E-Mails werden verschlüsselt übertragen und können auf dem Versandweg nicht mitgelesen werden (siehe auch einen Blog-Artikel[6] von Florian Vierke zum Thema Verschlüsselung).

Was kann/muss ich selbst tun, was der ESP?

Bei der Entscheidung für einen Versanddienstleister sind, neben Preis und persönlicher Sympathie, vor allem die Inklusivleistungen entscheidend. In der Regel bieten die meisten Marktteilnehmer plattformseitig alles an, was man braucht, um gutes E-Mail-Marketing zu betreiben.

Manuelle Antworten können durch Einstellungen in der Plattform begrenzt werden. (Nehme ich alle Nachrichten an meine Antwortadresse an oder doch nur Antworten auf von mir versendete Nachrichten? Der Unterschied ist immens!)

Bounce-Handling gehört auch zum Standard. Die Feineinstellungen erfolgen immer in Abhängigkeit zum aktuellen Versandverhalten. Entsprechend muss auch eine Anpassung dieser Einstellungen erfolgen, wenn die Versandfrequenz steigt oder sinkt.

DNS-basierte Authentifizierungen

SPF wird von ESPs, die auf Domain-Delegation setzen, automatisch für die IPs gesetzt, die der Versender zukünftig benutzen wird. Sollte der ESP das sogenannte Domain-Pointing ermöglichen, wird dieser eine umfassende Anleitung bereitstellen und so die eigenhändige Einrichtung des notwendigen TXT-Records im DNS-Bereich einer Versand-Domain ermöglichen.

DKIM (DomainKeys Identified Mail): Auch hier wird derjenige ESP, der auf Domain-Delegation setzt, das bessere Kundenerlebnis anbieten. Die Einrichtung erfolgt nach Beauftragung bzw. automatisch ohne weiteres Zutun durch den Kunden. Bietet der ESP Domain-Pointing an oder besteht der Versender darauf, die Domain selbst zu verwalten, wird auch hier in der Regel eine umfassende Anleitung zur Verfügung gestellt.

DNS-basierte Reportings

DMARC (Domain-based Message Authentication, Reporting and Conformance): Die Einrichtung dieses Standards erfolgt durch den ESP im Falle einer delegierten Versand-Domain auf Zuruf (durch Beauftragung). Wurde die Domain gepointet (oder DMARC auf der Haupt-Domain

[6] http://blogs.teradata.com/teradata-applications/de/sicherheit-und-verschluesselung-im-e-mail-marketing/

eingerichtet), so stellt der ESP auch hier wieder eine umfassende Anleitung bzw. Hilfestellung zur Verfügung.

Transportverschlüsselung

TLS (Transport Layer Security): Die ESPs sind in allen Fällen die Verwalter der Versandserver (Mail Transfer Agents). Der TLS-verschlüsselte Aufbau einer Verbindung zu Servern der ISPs, welche die Verschlüsselung unterstützen, erfolgt von dort aus. Daher handelt es sich, unabhängig davon wie die Domain verwaltet wird (Delegation oder Pointing) um eine Dienstleistung durch den ESP

Quellen und Verweise

Die neueste Version dieses Dokuments ist online im Blog der Kompetenzgruppe E-Mail zum Download verfügbar.

https://e-mail.eco.de/downloads.html

Über eco - Verband der Internetwirtschaft e.V.

eco (www.eco.de) ist mit über 1.000 Mitgliedsunternehmen der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet der eco Verband maßgeblich die Entwicklung des Internet in Deutschland, fördert neue Technologien, Infrastrukturen und Märkte, formt Rahmenbedingungen und vertritt die Interessen der Mitglieder gegenüber der Politik und in internationalen Gremien. In den eco Kompetenzgruppen sind alle wichtigen Experten und Entscheidungsträger der Internetwirtschaft vertreten und treiben aktuelle und zukünftige Internetthemen voran.

Spezielle eco Services helfen, den Markt für Anbieter und Anwender transparenter zu machen, unsere Gütesiegel sorgen für Qualitätsstandards. Mit Beratungsangeboten für Mitglieder und unseren Services für Internetnutzer unterstützen wir bei Fragen zur Rechtslage, erhöhen die Sicherheit und verbessern den Jugendschutz.

Als Verband ist es eine unserer wichtigsten Aufgaben, die Interessen der Mitglieder gegenüber der Politik und in nationalen sowie internationalen Gremien zu vertreten. Neben unserer Hauptgeschäftsstelle in Köln haben wir ein eigenes Hauptstadtbüro in Berlin und sind bei allen relevanten politischen Entscheidungsprozessen in Brüssel vor Ort.

Mehr Informationen über die eco Kompetenzgruppe E-Mail auf dem offiziellen Blog unter https://e-mail.eco.de/