BEST PRACTICES
FÜR E-MAIL-MARKETING

Autoren: Marius Bauer, Mathias Ullrich, Florian Vierke

eco
VERBAND DER INTERNETWIRTSCHAFT

Inhalt

Einleitung 3
- Reputationsbegriff 3
- Risiken 3
- Spamfilter oder Rechtsvorschriften: Wer entscheidet? 3
- Wer tut was – Dienstleister oder Versender? 3

Vor dem Versand: Inhalte 4
- Datenqualität & -erhebung 4
- Datenerhebung 4
- Datenbank-Hygiene 4
- E-Mail Validierungsservices 4
- Spam-Fallen („Recycled“ und „Pristine“) 5
- Engagement als Schlüssel zur Inbox 5
- Inbox Platzierungen 6

Während des Versandes: Technische Versandgrundlagen 7
- Authentifizierungen 7
- SPF (Sender Policy Framework) 7
- DKIM (DomainKey Identified Mail) 7
- TLS (Transport Layer Security) 7
- DMARC (Domain-based Message Authentication, Reporting & Conformance) 8
- BIMI (Brand Indicators for Message Identification) 8

Versandnachbereitung: Datennachbereitungen, Responsehandling 9
- Datenqualität & -pflege 9
- Bounces 9
- Hard Bounces 9
- Soft Bounces 9
- Temporäre Bounces 10
- Abmeldungen 10
- Complaint Feedback Loops 10
- Manuelle Antworten 11

Über die Autoren 11

Ihr Ansprechpartner bei eco zum Thema E-Mail: 11

Einleitung

Reputationsbegriff

Kein Leitfaden zur Zustellbarkeit kommt ohne den Begriff "Reputation" aus. Vereinfacht gesagt ist Reputation eine Metrik, die angibt, wie gut ein Absender angesehen ist. Doch was auf den ersten Blick nach einer einfachen Messgröße aussieht, entpuppt sich schnell als sehr komplex. Denn "die" Reputation gibt es leider nicht. Jeder Mailbox-Provider arbeitet mit anderen Daten und setzt andere Schwerpunkte. So entstehen unterschiedliche Reputationen pro Mailbox Provider, teilweise sogar noch unterteilt in IP- und Domain-Reputation.

Risiken

Bei den Risiken im E-Mail-Marketing geht es vor allem um rechtliche Herausforderungen, insbesondere seit der Einführung der Datenschutzgrundverordnung. Und natürlich ist das rechtliche Risiko gerade in Deutschland vorhanden und darf auch nicht außer Acht gelassen werden. Wie die Datenerhebung auszusehen hat, dazu später mehr. Aber nicht nur hier lauern Risiken. Die Ziele im E-Mail-Marke- ting sind meist klar definiert und dank moderner Versand- und Trackingsysteme auch sehr gut nachvollziehbar, wie z.B. Umsatz oder Impressions auf der Homepage. Um diese Ziele zu erreichen, ist es jedoch notwendig, dass die E-Mails auch im Posteingang der Empfänger ankommen. Eine E-Mail im Spam-Ordner generiert selten Umsatz, dieses Dokument soll helfen, insbesondere dieses Risiko zu minimieren.

Spamfilter oder Rechtsvorschriften: Wer entscheidet?

Bei unserer Arbeit stoßen wir nicht selten auf Variationen von "aber das ist doch legal". Was zu der Frage führt, ob die Spam-Filter der Mail-Provider oder die jeweiligen rechtlichen Rahmenbedingungen bestimmen sollten, was gutes E-Mail-Marketing ist.

Da es weltweit einen riesigen Flickenteppich an Gesetzen und Vorschriften für "elektronische Werbung" gibt, kann man fast froh sein, dass die Regeln der Spamfilter bzw. der Mailbox Provider über die Zustellbarkeit einer E-Mail bestimmen, denn während es leichte Variationen gibt, ist die Richtung bei fast allen legitimen Providern die gleiche.

Wie schon bei den Risiken erwähnt, bringt eine E-Mail, die vom Provider in den Spam-Ordner verschoben wird, keinen Umsatz. Und da kein Rechtsanspruch auf Zustellung in die Inbox besteht, ist letztendlich der Spamfilter die Entscheidungsinstanz.

Wer tut was – Dienstleister oder Versender?

E-Mail-Marketing wird häufig in der Konstellation "Dienstleister" und "Versender" betrieben, wobei sich natürlich die Frage stellt, welche Aufgaben welchen Beteiligten obliegen. Das hängt immer davon ab, wie umfangreich das Angebot des Dienstleisters ist, aber grundsätzlich gilt, dass die Inhalte und Daten in der Verantwortung des Versenders liegen und die Technik beim Dienstleister.

Und hier liegt auch ein wichtiges Element der Zustellbarkeit, man kann Probleme nicht oder kaum auf der Seite des Dienstleisters lösen. Wenn Nachrichten im SPAM-Ordner landen, ist es zwar möglich, mit dem Dienstleister zusammenzuarbeiten und Lösungen zu finden. Es liegt aber in der Verantwortung des Absenders, diese auch umzusetzen.

Vor dem Versand: Inhalte

Datenqualität & -erhebung

E-Mail-Marketing steht und fällt mit den Daten. Das beginnt bei der sauberen Datenerhebung, geht über die regelmäßige Pflege der Adressdaten bis hin zur Abmeldung von Adressen.

Datenerhebung

Auch wenn die rechtlichen Rahmenbedingungen nicht die Regeln für das E-Mail-Marketing machen, ist eine rechtlich saubere Datenerhebung Pflicht. Nicht zuletzt, da gerade die deutschen Regelungen sehr nah an dem sind, was Mailbox Provider von Versendern erwarten.

Im Zentrum des Themas Datenerhebung steht die aktive und transparente Einwilligung. Nicht erst seit der Datenschutz Grundverordnung (EU-DSGVO) ist die Einwilligung der Goldene Weg Empfänger zu generieren. Einwilligung ist allerdings nicht gleich Einwilligung, deswegen sind die Adjektive "aktiv" und "transparent" so relevant.

Um die rechtlichen Voraussetzungen zu erfüllen, versuchen manche Marketer eine Einwilligung in den Datenschutzbestimmungen zu verstecken oder mit vorausgewählten Checkboxen zu arbeiten. Doch das führt nicht zu nachhaltigem Erfolg.

Aktiv bedeutet im Zusammenhang der Einwilligung, dass der Empfänger eine aktive Handlung durchführt für die Einwilligung. Sei dies das Klicken auf einen Button oder das "checken" einer Checkbox.

Transparent bedeutet zusätzlich noch, dass der potentielle Empfänger, bevor er aktiv wird, sehr genau weiß, was ihn erwartet. Im Idealfall sind alle Informationen wie Versandfrequenz, welche Inhalte angeboten werden, wie man sich abmelden kann, etc. vorhanden.

Gerade im DACH Raum hat sich das Double Opt-In Verfahren als zusätzlicher Aspekt der Datenerhebung etabliert. Das DOI wird auch als "Verifizierung" bezeichnet. Es stellt sicher, dass der Inhaber der E-Mail-Adresse auch dieselbe Person ist, die auch die Einwilligung gegeben hat. Das DOI wird auch von den deutschen Datenschutz-Aufsichtsbehörden empfohlen.

Eine weitere gängige Praxis ist es, bestehende Kunden in den Werbeverteiler mit aufzunehmen. Dies ist in Europa erlaubt, wenn auch mit hohen rechtlichen Hürden. Hier gilt es, bei der Datenerhebung möglichst transparent auf die Widerspruchsmöglichkeit hinzuweisen, nur ähnliche Produkte zu bewerben und selbstverständlich bestehende Abmeldungen zu berücksichtigen. Empfehlenswert ist es natürlich auch, bei Online-Bestellungen eine Einwilligung einzuholen.

Nähere Informationen zur Ausgestaltung der Einwilligung erhalten Sie bei Ihrem Unternehmensjuristen oder bei der CSA, die vor kurzem ihren rechtlichen Guide – die „Richtlinie für zulässiges E-Mail-Marketing" – in 7. Auflage aktualisiert hat.

Datenbank-Hygiene

Mit der Datenerhebung ist es natürlich nicht getan. Ein E-Mail-Verteiler muss ständig gepflegt werden, um den größtmöglichen Erfolg zu gewährleisten. Dazu gehört zum einen das Entfernen von Abonnenten, die sich abgemeldet haben und von Empfängern, die nicht mehr aktiv sind (mehr dazu im Kapitel Versandnachbearbeitung), aber auch die Implementierung einer Strategie zum Entfernen inaktiver Empfänger.

Das Anschreiben von Empfängern, die nicht interagieren, wirkt sich negativ auf den Zustellerfolg aus. Diese sollten daher regel- mäßig, idealerweise automatisiert, entfernt werden. Üblicherweise geschieht dies auf Basis von Öffnungen, Klicks oder anderen Metriken. Der geeignete Zeitraum variiert von Marke zu Marke, aber in den meisten Fällen sind 12 Monate ein guter Zeitraum.

E-Mail Validierungsservices

Auf dem Markt gibt es verschiedene Anbieter von sog. Validierungsservices, die mit verschiedenen Mitteln versuchen, die Echtheit einer E-Mail-Adresse sicherzustellen. Diese Services bieten meist zwei unterschiedliche Modelle an:

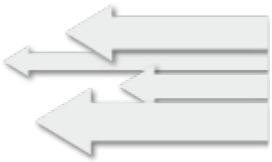
On-Demand-Validierung

Hier wird direkt bei Datenerhebung (sowohl online als auch offline) eine Validierung durchgeführt und bei möglichen Fehlern Alternativen vorgeschlagen. So lassen sich beispielsweise "Vertipper" korrigieren, bevor sich die E-Mail-Adresse als fehlerhaft herausstellt.

Die Kosten, die sich nicht in jedem Anwendungsfall rechnen, sind meist ein Nachteil dieser Variante.

Listen Validierung

In diesem Modell werden bestehende Listen geprüft und Empfehlungen gegeben, wie mit welchen Adressen umzugehen wäre.



Meist ist dieses Verfahren nicht zu teuer, allerdings sind die Erwartungen an die Ergebnisse teilweise überzogen. So darf nicht vergessen werden, dass ein solches Verfahren die Einwilligung nicht verifizieren kann und auch das nachträgliche Ändern von Datensätzen ist rechtlich fragwürdig. Auch das Identifizieren und Entfernen von Spamfallen (siehe nächstes Kapitel) ist komplexer, als es Anbieter teils erscheinen lassen.

Eine On-Demand-Validierung kann empfohlen werden, wenn der Wert einer einzelnen E-Mail-Adresse hoch genug ist, um die Kosten zu rechtfertigen.

Spam-Fallen („Recycled" und „Pristine")

Spamfalle ist ein Begriff, der oft zu hören ist, wenn es um die Qualität von Adresslisten geht. Spamfallen sind E-Mail-Adressen, die keiner natürlichen Person "gehören", sondern von verschiedenen Firmen betrieben werden, um Versender zu identifizieren, die unerwünschte Werbung versenden oder keine Datenpflege betreiben. Man kann Spamfallen grundsätzlich in zwei Kategorien unterteilen:

Recycled Traps

Diese E-Mail-Adressen gehörten früher einmal Anwendern, wurden aber irgendwann aufgegeben, so dass der Mailbox-Provider sie übernimmt und nach einer Übergangszeit als Spamfalle verwendet. Dies ermöglicht die Identifikation von Versendern, die kein Bounce-Management haben oder alte Daten anschreiben.

Pristine Traps

Diese Spamfallen waren nie etwas anderes als Spamfallen. Während es bei recycled möglich ist, dass mal eine Einwilligung vorgelegen hat, ist dies bei Pristine Traps ausgeschlossen. Werden solche E-Mail-Adressen beschickt, deutet dies auf ein Problem mit der Datenerhebung hin.

Spam-Fallen in Verteilern sind nicht ungewöhnlich, und die meisten Spam-Fallen haben keinen direkten Einfluss auf die Zustellbarkeit. Spamfallen sind aber immer ein starker Indikator dafür, dass Best Practices nicht eingehalten werden, was natürlich zu Prob- lemen führen kann. Daher ist es wichtig, Spamfallen frühzeitig zu eliminieren.

Spamfallen können leider nicht direkt identifiziert werden, da sie Betriebsgeheimnisse der Provider und Mailbox-Provider sind. Es wird aber darauf geachtet, dass diese Spamfallen kein Engagement zeigen. Daher entfernt man Spamfallen direkt mit, wenn man inaktive Empfänger bereinigt.

Engagement als Schlüssel zur Inbox

"Engagement" ist ähnlich wie "Reputation" ein Begriff, der nicht genau definiert werden kann, da jeder E-Mail-Anbieter anders damit umgeht.

Im Allgemeinen wird unter Engagement jede Interaktion seitens des Empfängers verstanden. Dabei wird grob zwischen positivem und negativem Engagement unterschieden. Zu den positiven Interaktionen zählen Öffnen, Anklicken, Beantworten und auch "aus dem Spam-Ordner fischen", zu den negativen "ungelesen löschen" oder als „Spam markieren".

Und das sind nur die offensichtlichsten Optionen. Es ist davon auszugehen, dass die Mailbox-Provider das Verhalten ihrer Nutzer noch viel genauer analysieren.

Dieses Wissen nutzen die Provider nun, um zu entscheiden, welche E-Mails in die Inbox gelangen und welche nicht. Je höher der Provider die Relevanz einer E-Mail für den Nutzer einschätzt, desto wahrscheinlicher ist die Zustellung in die Inbox.

Marketingziele und Zustellungserfolg gehen also Hand in Hand, denn positives Engagement ist immer das Ziel.

Und das betrifft dann vor allem die Inhalte der E-Mails. Hier können wir keine konkreten Empfehlungen geben, denn jeder Versender ist etwas anders, das fängt bei großen Unterschieden wie B2B oder B2C an, geht weiter über unterschiedliche Marketingziele, Zielgruppen, Produktsortiment etc.

Der Fokus muss jedoch auf der Förderung eines möglichst positiven Engagements des Empfängers liegen, auf Betreffzeilen, die zum Öffnen der E-Mail animieren, auf Inhalten, die für den Empfänger interessant sind und im Idealfall zu einem Klick führen.

So weiß der Mailbox-Provider bei der nächsten E-Mail, dass der Nutzer oder die Nutzerin an diesen Inhalten interessiert ist und die Mail landet in der Inbox.

Was ist eine Öffnung?

Diese Frage mag banal klingen, aber im Zeitalter von Google Cache, Yahoo Image Proxy oder Apple's Mail Privacy Protection (MPP) macht es Sinn, hier genauer hinzusehen.

Zunächst muss unterschieden werden, was der Marketer und was der Mailbox-Provider unter einer Öffnung versteht. Für den Provider ist eine Öffnung genau das: die aktive Handlung des Nutzers, eine E-Mail zu öffnen. Da diese Information nicht öffentlich ist, ist eine Öffnung für Marketer nicht eindeutig.

Um herauszufinden, ob ein Empfänger eine E-Mail öffnet, nutzen Marketer mit Hilfe ihrer technischen Dienstleister den Trick des "Öffnungspixels". Dabei handelt es sich um ein transparentes GIF in der Größe 1x1 Pixel. Wird dieses GIF geladen, z.B. weil eine E-Mail geöffnet wird, wird dies als Öffnung vermerkt. Dies ist jedoch keine exakte Metrik, da es einerseits möglich ist, eine E-Mail zu öffnen, ohne ein Bild zu laden, und es andererseits möglich ist, dass der Mailbox-Provider das Bild lädt, ohne dass der Nutzer aktiv wird.

Genau dies geschieht mit Apples MPP. Dies wurde mit iOS 15 eingeführt und wenn es aktiviert ist, lädt der E-Mail Client die Bilder im Hintergrund, wenn die E-Mail ankommt. Dabei wird auch das Öffnungspixel geladen, so dass die Öffnungsrate höher erscheint, als sie tatsächlich ist.

Damit ist die Öffnungsrate als alleinige Metrik vielleicht nicht mehr das Maß der Dinge, aber zusammen mit anderen KPIs nach wie vor ein brauchbares Reporting.

Inbox Platzierungen

Als Gmail 2013 die verschiedenen "Tabs" einführte, waren die Befürchtungen groß, dass E-Mails im Tab "Werbung" keine Beachtung mehr finden würden. Schnell tauchten Taktiken auf, damit Werbung von Google nicht als solche erkannt wird. Solche Taktiken gibt es hier nicht, denn sind die Tabs überhaupt ein Problem?

Der wohl wichtigste Aspekt ist, dass alle Tabs die Inbox sind. Nachrichten im Werbetab sind eben nicht "verschwunden", son- dern dort, wo der Nutzer Werbe-E-Mails erwartet. Außerdem gehen Schätzungen derzeit davon aus, dass nur etwa 20 Prozent aller Gmail-Nutzer die Tabs aktiviert haben. Hinzu kommt, dass die Gmail Apps die Tabs nicht unterstützen.

All diese Aspekte zusammen ergeben einfach das Bild, dass Werbenachrichten auch in den Werbe-Tabs zugestellt werden sollten, da dies auch die Erwartung der Nutzer ist, die die Tabs verwenden. Darüber hinaus bietet der Werbe-Tab die Möglichkeit, zusätzliche Features wie "Annotations" zu nutzen.

Während des Versandes: Technische Versandgrundlagen

Authentifizierungen

Eine der wichtigsten Voraussetzungen für den erfolgreichen Massenversand von E-Mails ist heutzutage die korrekte Authentifizierung der Absender-Domain. Mit anderen Worten: Der Absender muss nachweisen, dass er berechtigt ist, im Namen der Display-From-Adresse (auch RFC 5322.FROM) zu versenden. Diese Anforderung war im ursprünglichen E-Mail-Standard nicht enthalten und es gibt nach wie vor viele Mailserver, die E-Mails auch ohne Authentifizierung annehmen.

Im Rahmen der Phishing- und Abuse-Bekämpfung haben es die meisten großen Internet Service Provider (ISP) jedoch zur Voraussetzung gemacht, dass die Sendungen auch korrekt authentifiziert sind.

Für die Authentifizierung stehen technisch zwei Verfahren zur Verfügung: SPF (Sender Policy Framework) und DKIM (Domainkey Identified Mail).

Es wird dringend empfohlen, beide Methoden zu implementieren, da viele empfangende Mailserver nur eine der beiden Methoden überprüfen. Darüber hinaus ist man auch dann noch sicher authentifiziert, wenn eine der beiden Methoden aus technischen Gründen fehlschlägt.

SPF (Sender Policy Framework)

Mit SPF kann im DNS (Domain Name System) der Envelope From Domain (5321.FROM) per TXT-Eintrag hinterlegt werden, welche IPs für den Versand gültig sein sollen und welche nicht. So kann der empfangende Mailserver sehr schnell feststellen, ob eine Nachricht tatsächlich vom angegebenen Server stammt.

SPF ist sehr einfach zu implementieren und verbraucht keine zusätzlichen Ressourcen beim Versand. Leider hat es einige Schwächen, weshalb die meisten ISP die Authentifizierung über DKIM bevorzugen – oder SPF sogar ganz ignorieren. Dennoch sollte auf eine SPF-Implementierung nicht verzichtet werden.

Die entscheidendsten Nachteile von SPF sind:

- Bei der Weiterleitung von E-Mails scheitert SPF:
  Der empfangende Mailserver prüft die IP-Adresse des weiterleitenden Mailservers, nicht die IP-Adresse des ursprünglichen Absenders. Somit schlägt SPF beispielsweise bei der Verwendung von Mailinglisten fehl.
- Über SPF lässt sich keine einzelne Versanddomain identifizieren. Viele Infrastrukturen verwenden sogenannte "shared IPs", es werden also die gleichen IPs für mehrere Versanddomains verwendet. Auch bei einem Providerwechsel lässt sich die IP nicht "mitnehmen". Die Relevanz von IP-Reputation gegenüber Domain Reputation nimmt also zunehmend ab.

DKIM (DomainKey Identified Mail)

Mit DKIM kann die Authentifizierung auf Domänenebene implementiert werden. Dies macht das Verfahren sehr attraktiv und in der Praxis unumgänglich.

Technisch wird für DKIM ein Schlüsselpaar erzeugt, üblicherweise mit dem RSA-Verfahren und einer Schlüssellänge von 1024 oder 2048 Bit. Der private Teil des Schlüssels generiert eine Signatur, die im E-Mail-Header platziert wird. Der öffentliche Teil des Schlüssels wird im DNS abgelegt, so dass der empfangende Mailserver die Signatur eingehender Nachrichten auf Gültigkeit überprüfen kann. Der Trick dabei ist, dass die Signatur Informationen über die relevanten Headerfelder enthält und somit sicherstellen kann, dass der Header seit dem Versand nicht verändert oder gefälscht wurde. Gültige Signaturen können also nur von Personen erzeugt werden, die den zum öffentlichen Schlüssel im DNS passenden privaten Schlüssel besitzen.

TLS (Transport Layer Security)

TLS (Transport Layer Security) ist ein Protokoll, das für die sichere Übertragung von Daten über das Internet entwickelt wurde. Die Verschlüsselung erfolgt durch die Verwendung von asymmetrischen Schlüsseln, die aus einem öffentlichen Schlüssel und einem privaten Schlüssel bestehen.

TLS verschlüsselt alle Daten, die zwischen dem versendenden und dem empfangenden Server übertragen werden, so dass sie nicht von Dritten abgefangen oder manipuliert werden können.

Bereits heute nehmen einige Mailserver keine Mails mehr entgegen, die nicht über TLS gesendet werden (insbesondere nicht im Bereich der Bulk-Versendungen). In der Praxis wird fast ausschließlich TLS in den Versionen 1.2 und 1.3 verwendet, seit 2021 wird von der Verwendung von TLS 1.1 (oder niedriger) abgeraten.

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

DMARC ist ein Standard, der es Versendern ermöglicht, dem empfangenden Mailserver eine Policy für den Umgang mit nicht authentifizierten Mails der eigenen Domain mitzuteilen. Zur Auswahl stehen die Methoden "none" (keine Filterung), "quarantine" (Filterung nicht authentifizierter Mails in den Spam-Ordner) sowie "reject" (Ablehnung nicht authentifizierter Mails).

Die Authentifizierung kann mittels SPF oder DKIM erfolgen. Voraussetzung dafür ist, dass die jeweiligen Domains in einem "Alignment" stehen, also zur selben Domain gehören.

Möchte ich beispielsweise eine E-Mail von "foo.com" im Display-From (5322.From) per DKIM authentifizieren, muss meine E-Mail eine gültige DKIM-Signatur der Domain foo.com enthalten. Subdomains sind sowohl in der Signatur als auch im From erlaubt, sofern die Policy nicht explizit auf "strict" Alignment konfiguriert ist. Für den Standardfall ist ein "relaxed" Alignment ausreichend.

Möchte ich hingegen eine Mail von foo.com im Display-From (5322.From) über SPF authentifizieren, muss ich sowohl eine gültige SPF-Prüfung bestehen als auch die Domain foo.com im Envelope From verwenden. Auch hier sind Subdomains standardmäßig erlaubt.

DMARC erlaubt auch die Angabe einer E-Mail-Adresse, um Reports über die Filterung der beim Empfänger eingegangenen E-Mails zu erhalten. Nach der Aktivierung erhält man in der Regel täglich Reports von jeder Empfängerdomain, die DMARC-Reports versendet. Diese Reports liegen im maschinenlesbaren XML-Format vor und sollten mit einem Tool oder Dienst grafisch aufbereitet werden. Als kostenlose Open Source Software bietet sich "parseDMARC" (https://domainaware.github.io/parsedmarc/) an, es gibt aber auch kommerzielle Anbieter, die kein eigenes Server-Hosting voraussetzen.

BIMI (Brand Indicators for Message Identification)

Mit dem Begriff BIMI verbinden die meisten E-Mail-Marketer die Möglichkeit, das eigene Firmenlogo als Absenderbild in E-Mail-Clients zu platzieren. Die eigentliche Idee hinter BIMI geht jedoch weit über das Logo hinaus. Es geht darum, Markenkommunikation nur dann als solche darzustellen, wenn die Mails tatsächlich von der Marke versendet wurden.

Voraussetzung dafür ist, dass Marken ihr Logo bei einer offiziellen Stelle (z.B. dem Deutschen Patent- und Markenamt) als Bildmarke haben eintragen lassen. Darüber hinaus ist es notwendig, die verwendeten Domains und das Unternehmen als solches zu verifizieren. Dazu dient ein sogenanntes „Verified Mark Certificate" (VMC).

Auch der Versand muss korrekt authentifiziert werden. Hierfür steht mit DMARC bereits eine geeignete Technologie zur Verfügung. Voraussetzung für die Darstellung des BIMI-Logos in E-Mail-Clients oder E-Mail-Apps ist die Einrichtung von DMARC mit einer Policy von "quarantine" oder "reject" auf der Domain des Kunden.

Derzeit (Stand Februar 2025) wird BIMI in Verbindung mit einem VMC-Zertifikat von folgenden großen Providern unterstützt: Gmail, Yahoo, AOL, Apple (Mail App auf iOS). Auch au.com, Cloudmark, Fastmail, Laposte, 1&1, Onet, Zoho und Zoner unterstützen BIMI. (Siehe https://bimigroup.org/bimi-infographic)

Versandnachbereitung: Datennachbereitungen, Responsehandling

Datenqualität & -pflege

Genauso wichtig wie die korrekte Datenerhebung inklusive Einwilligung ist der verantwortungsvolle und bewusste Umgang "am anderen Ende" des Customer-Lifecycles. Viele E-Mail-Empfänger sind zwar eine beeindruckende, aber wenig aussagekräftige Kennzahl. Wichtiger ist der Engagement Level der jeweiligen Zielgruppen. Denn wie bereits eingangs erwähnt, ist die Interaktion der Empfänger mit den ausgespielten Inhalten entscheidend für die Reputation des Versenders. Kurz zusammengefasst: Seien Sie relevant. Immer. E-Mails werden nur an diejenigen versendet, die sie explizit angefordert haben. Niemand bleibt länger als nötig in der Datenbank.

Bounces

Der aus dem Postwesen entlehnte Begriff "Rückläufer" ist auch heute noch im Umlauf. Bounces beschreiben die Gesamtheit aller E-Mails, die beim Versand nicht zugestellt werden konnten. Die Gründe hierfür sind vielfältig. Es empfiehlt sich, für die einzelnen Bounce-Arten (s.u.) spezielle Maßnahmen zu implementieren bzw. den technischen Versender (ESP) nach den Bordmitteln und deren Einstellungsmöglichkeiten seiner jeweiligen Plattform zu fragen.

Hard Bounces

Existiert eine Adresse nicht, meldet die Versandplattform auf Basis der Rückmeldung des Internet Service Providers einen Hard Bounce.

Eine Adresse ist nicht erreichbar:

- Die Domain existiert, der User aber nicht.

Grundsätzlich sollten Hard Bounces zeitnah, idealerweise nach dem ersten Vorfall, aus der aktiven Empfängerliste verschwinden.

Soft Bounces

Besteht die Möglichkeit, den Empfänger in Zukunft wieder zu erreichen, spricht man von einem Soft Bounce. Häufige Beispiele sind:

- Mailbox-full:
  Dem Benutzer oder der Benutzerin steht kein Speicherplatz mehr zur Verfügung, um die E-Mail anzunehmen. Wird die Mailbox in Zukunft geleert und damit wieder Speicherplatz durch den Benutzer oder die Benutzerin freigegeben, ändert sich dieser Zustand und E-Mails können wieder angenommen werden. Das Problem verschiebt sich. Speicherplatz im Gigabyte-Bereich wird heute häufig bereits für kostenlose Benutzerkonten zur Verfügung gestellt. In der Regel kann daher davon ausgegangen werden, dass dieser Art von Bounce eine sehr lange Zeit der Inaktivität vorausgeht.
- Spam-Reject:
  Eine Abweisung wegen Spam-Verdachts liegt entweder an der Reputation der Domain/IP oder an der Nachricht selbst. In vielen Fällen sind solche Abweisungen auch umfassend für sämtliche Kunden eines Mailbox Providers. Negative Reputation ist reversibel. Also wird sich bei angemessener Reaktion auf einen solchen Vorfall auch die Deliverability wiederherstellen lassen.
  Es ist wichtig, zwischen persönlichen und ISP-weiten Rejects zu unterscheiden. Einige Anbieter reichen die Information, ob die Abweisung auf Basis einer generellen (Filter-, Gateway- oder Reputation-Reject) oder einer persönlichen (User-Reject) Entscheidung basiert.
- Automatische Antwort / Autoresponder:
  Dieser Übermittlungsfehler wird durch automatische Antwortnachrichten verursacht, z. B. eine Abwesenheitsnachricht, die von einem Autoresponder gesendet wird. Sie können Kontakte nach einer bestimmten Anzahl von automatischen Antworten deaktivieren, um zu vermeiden, dass zu viele Nachrichten an Kontakte gesendet werden, die über einen längeren Zeitraum abwesend sind. Viele Versanddienstleister bieten die Möglichkeit, solche Nicht-Bounces über ihre Plattform "abzufangen". Die Erfolgsquote liegt hier bei annähernd 100%.
- Kommunikation fehlgeschlagen:
  Dieser Zustellfehler wird verursacht, wenn keine Verbindung zum empfangenden Mailserver (MTA) hergestellt werden konnte.
- Ungültig:
  Dieser Rückläufer wird erzeugt, wenn die Domain der E-Mail-Adresse nicht existiert (z. B. hotnail.com statt hotmail.com) oder die Domain wegen DNS-Problemen beim ISP nicht aufgelöst werden konnte.

Die folgende Rückläuferkategorie wird verwendet, wenn der genaue Grund für die fehlgeschlagene Zustellung nicht festgestellt werden kann. Je nach Dienstleister und Plattform kommen auch Bezeichnungen wie "Unknown", "Other" und weitere in Frage.

- Andere: Es gibt viele weitere Ursachen dafür, weshalb Nachrichten nicht angenommen werden. Diese sind auf Einzelfallbasis zu prüfen und gegebenenfalls einer automatisierten Verarbeitungsroutine hinzuzufügen. Es lohnt sich immer, mit dem Dienstleister zu sprechen, um die Zuordnung fortlaufend zu verbessern.

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.

Temporäre Bounces

Während des Versandprozesses kann ein Mailbox-Provider auch die Annahme von E-Mails verzögern. Dies wird in der Regel als Vorstufe zur eigentlichen Blockung angesehen. Die größeren Anbieter am Markt begründen solche "Deferrals" auch in der Serverkommunikation entsprechend als "reputationsbedingt". Seinen Ursprung hat dieses Verfahren im so genannten Greylisting. In diesem Zusammenhang ist es wichtig zu wissen, dass (echte) Spammer extrem ressourcenschonend arbeiten. Das bedeutet, dass sie pro Adressat nur einen einzigen Zustellversuch unternehmen und danach sofort "aufgeben".

Ein technischer Versanddienstleister konfiguriert die Mailserver in der Regel so, dass mehrere Zustellversuche unternommen werden, bevor die Versuche nach einer definierten Zeit abgebrochen werden. Wenn also die Reputation mit der Zeit abnimmt, kann es zu Verzögerungen bei der Zustellung kommen, lange bevor die Öffnungs- und Klickraten sinken oder die Bounce-Raten steigen.

Abmeldungen

Eine Abmeldung ist die freundliche Form der negativen Bewertung einer Marketing-Kommunikation. Ein aktiver Newsletter-Empfänger hat kein Interesse mehr an den Inhalten und meldet sich für die Zukunft ab. Das ist ärgerlich, gehört aber zum Alltag eines jeden E-Mail-Marketers. Anders als bei Softbounces gibt es bei Abmeldungen jedoch keinen Spielraum für Verhandlungen oder Interpretationen. Oft ist der Abmeldelink klein und unauffällig platziert. Ein versehentliches Anklicken kann daher mit einiger Sicherheit ausgeschlossen werden. Es gibt verschiedene Möglichkeiten, dem Empfänger den Verbleib im Verteiler zu ermöglichen. So wird gerne mit Preference Centern gearbeitet. Dort können Abmeldungen pro Newsletter-Kategorie oder auch Frequenzanpassungen angeboten werden.

Unbedingt zu vermeiden ist es, die Abmeldung zu erschweren. So kann die Abfrage der E-Mail-Adresse in einem leeren Formular, der Versand einer E-Mail zur Bestätigung der Abmeldung durch einen Klick (Double-Opt-Out) oder auch die Notwendigkeit, sich in das Nutzerprofil einzuloggen, die Wahrscheinlichkeit einer Beschwerde deutlich erhöhen.

Complaint Feedback Loops

Eine E-Mail als Spam zu markieren ist die einfachste Möglichkeit für den Empfänger, E-Mails mit ungewünschtem Inhalt oder von ungewünschten Absendern aus seinem Posteingang zu entfernen. Sobald sich ein Benutzer oder eine Benutzerin über Spam beschwert, verschiebt der Mailbox-Provider alle zukünftigen Nachrichten des Absenders in den Spam-Ordner.

Um das Volumen an unerwünschten E-Mails, die eingehen und bearbeitet werden müssen, so gering wie möglich zu halten, haben sich viele Mailbox-Provider dazu entschlossen, den technischen Absender über die Beschwerde eines einzelnen Empfängers zu informieren. Stets mit der Erwartungshaltung, dass der Versand von Werbe-E-Mails an den betreffenden Nutzer dann unterbleibt.

Die technische Lösung erklärt sich wie folgt. Im Beschwerdefall sendet der empfangende Mailbox-Provider eine E-Mail in einem bestimmten Format an den technischen Absender (ESP) zurück. Diese E-Mail enthält alle notwendigen Informationen, die es dem Absender ermöglichen, den Empfänger zu identifizieren und nicht mehr zu kontaktieren. Es werden also in Zukunft keine weiteren Werbe-E-Mails an diesen Empfänger versendet.

Ausgenommen von dieser Regelung sind Transaktionsmails, die zu einem späteren Zeitpunkt, z.B. im Rahmen eines Bestellvorgangs, vom Beschwerdeführer ausgelöst werden.

Beispiel: Wenn sich max.mueller@example.com am Montag über die Werbemail beschwert und dann am Mittwoch einen Artikel bestellt, kann und muss die Bestell-, Versand- und Zahlungsbestätigung noch zugestellt werden.

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

Manuelle Antworten

E-Mail ist ein Instrument des Dialogs, daher werden E-Mail-Newsletter dem Dialogmarketing zugeordnet. Folgerichtig sollten Antworten der Empfänger nicht nur technisch möglich sein, sondern quasi erwartet werden.

Vermeiden Sie daher „no-reply@"-Absenderadressen, da diese suggerieren, dass eine Antwort nicht erwünscht ist.

Nutzen Sie die Erfahrungen und Kapazitäten des Versanddienstleisters, um automatische Antworten herauszufiltern und Abmeldungen von E-Mail-Antworten zu bearbeiten, damit möglichst nur noch tatsächliche Antworten der Empfänger an den Kundenservice weitergeleitet werden.

Über die Autoren

Florian Vierke
Sr. Manager, Deliverability Services | mapp

Marius Bauer
Senior Deliverability Consultant | Salesforce

Mathias Ullrich
Deliverability Services Consultant | Adobe

Florian, Marius und Mathias arbeiten seit jeweils über 12 Jahren als E-Mail Deliverability Experten auf Seiten der technischen Versanddienstleister. Sie sehen Verbandsarbeit als integral für ihre Aufgabe, Versender dabei zu unterstützen, ihre E-Mail-Kommunikationsstrategien weiterzuentwickeln. Dem gemeinsamen Wunsch, dass (wirklich) jeder bessere E-Mails versenden kann, dient dieser Leitfaden.

Ihr Ansprechpartner bei eco zum Thema E-Mail:

Michael Weirich

Projekt Manager IT-Sicherheit
eco - Verband der Internetwirtschaft e.V. Büro Köln
Lichtstraße 43h
50825 Köln
Telefon:+49 (221) 7000 48 – 193
Mobil: +49(0)171 – 554 0303
E-Mail: michael.weirich@eco.de

BEST PRACTICES
FÜR E-MAIL-MARKETING

Autoren: Marius Bauer, Mathias Ullrich, Florian Vierke

eco –Verband der Internetwirtschaft e V
Lichtstraße 43h, 50825 Köln
fon +49(0)221/700048-0
fax +49(0)221/700048-111
info@eco de
www eco de

VERBAND DER INTERNETWIRTSCHAFT