

Leitfaden zu Reputationskennzahlen im E-Mail Marketing

Leitfaden: Reputationskennzahlen im E-Mail Marketing

von Dale Langley



Dale Langley berät Kunden in ganz Europa bereits seit über sieben Jahren stets mit dem Ziel, deren E-Mail Zustellbarkeit zu steigern und den ROI der E-Mail Kampagnen positiv zu beeinflussen.

Als Softwareentwickler verfügt Dale über einen umfassenden Erfahrungsschatz was die Entwicklung von Systemen und die Speicherung von Daten anbelangt. Diese Erfahrung bringt er in seine Beratertätigkeit ein, und gibt Kunden hilfreiche Tipps rund um die Implementierung einer robusten Versand-Architektur, für Datenanalyse, Segmentierung, Design und Versandpraktiken, um so bestmögliche Ergebnisse zu erzielen.

Auf Basis seiner Kenntnisse und Erfahrungen ist Dale Langley in der Lage, Probleme schnell zu analysieren und E-Marketern einen wertvollen Leitfaden an die Hand zu geben, wenn es um die Maximierung Ihrer Reputation im E-Mail Marketing geht.

Dieses E-Book bietet Tipps zu folgenden Problemen:

Ein Anstieg an Spam-Beschwerden	Seite 5
Ein Versand an eine oder mehrere Spamfallen	Seite 6
Rückläufer bei bestimmten Mailbox Providern mehren sich	Seite 7
Ein hoher Prozentsatz unbekannter Nutzer	Seite 8
Reverse DNS wird plötzlich nicht mehr bestanden	Seite 9
Ihre IP Adresse erscheint auf einer oder mehrerer Blacklists	Seite 10
Ein plötzlicher Anstieg abgewiesener E-Mails	Seite 11
Die DKIM Authentifizierung wird nicht bestanden	Seite 12
Mehr Nachrichten werden in den Spamorder platziert	Seite 13

Was tun?



Bei einem Anstieg an Spam-Beschwerden

Mögliche Ursachen:

- Unzureichende Anmeldeprozesse im Rahmen eines Permission-Marketings
- Änderung der E-Mail-Frequenz
- Missbrauch Ihres Mail-Servers
- Versand an gekaufte/gemietete Adressen

Lösungsmöglichkeiten:

1. Melden Sie sich für die wichtigsten Feedback Loops an: Yahoo!, Microsoft/Outlook.com (genannt JMR), AOL, Comcast, Cox, BlueTie, United Online/Netzero/Juno (UOL), Rackspace (Mailtrust), Road Runner, OpenSRS (Tucows) sowie USA.net.
2. Spam-Beschwerden können als Indikator für negative Verfahrensweisen rund um den E-Mail Versand angesehen werden. So sollten Sie auf steigende Beschwerdezahlen in Abhängigkeit zum Versandvolumen achten und Ihre Versandpraktiken überdenken, bevor sich negative Auswirkungen auf die E-Mail Zustellbarkeit bemerkbar machen.
3. Nutzen Sie einen List-Unsubscribe Header, um Ihren Abonnenten eine einfache Möglichkeit des Abmeldens zu geben und so Spam-Beschwerden zu minimieren. Gmail beispielsweise bietet zwar keinen Feedback Loop an, fragt seine Abonnenten jedoch, ob sie sich von Ihren E-Mails abmelden möchten, wenn sie diese als Spam melden – jedoch nur, wenn Ihre E-Mails einen List-Unsubscribe Header aufweisen.
Mehr Informationen zum Thema.
4. Prüfen Sie welche Bestandteile Ihrer Verteilerliste die höchsten Spam-Beschwerden hervorrufen und aus welchen Quellen diese Adressen stammen. Arbeiten Sie dann daran, die Beschwerde-Raten für diese Adressquellen zu senken, indem Sie z.B. den Anmeldeprozess überdenken oder besondere beschwerdereiche Quellen, beispielsweise gekaufte oder gemietete Adressen, nicht mehr nutzen.
5. Prüfen Sie Ihre SMTP Server auf Open Relays. Niemand sollte von außen in der Lage sein, E-Mails über Ihre Infrastruktur zu versenden.

Was tun?



Bei einem Versand an eine oder mehrere Spamfallen

Mögliche Ursachen:

- Hoher Anteil inaktiver Abonnenten
- Fehlende oder ineffektive Strategie bezüglich des Umgangs mit inaktiven Abonnenten
- Zu geringe Versandfrequenz
- Geringe Listenhygiene insbesondere beim Listenaufbau

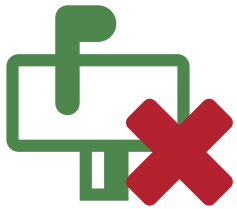
Lösungsmöglichkeiten:

Prüfen Sie Ihre Anmeldeprozesse insbesondere dahingehend, dass Sie die E-Mail Adresse des neuen Abonnenten bereits bei der Anmeldung verifizieren. Sie könnten sich beispielsweise überlegen, die E-Mail Adresse zweimal abzufragen, damit eventuelle Tippfehler ausgeschlossen werden können. Eine andere Möglichkeit ist es, die E-Mail Domain bereits bei der Anmeldung zu prüfen. Hierfür gibt es spezielle Skripte bzw. Dienste, die in die Webformulare eingebunden werden können.

Senden Sie allen neuen Abonnenten eine Bestätigung- oder Willkommens-E-Mail und entfernen Sie eventuelle Rückläufer (Hard Bounces) sofort von Ihren Verteilerlisten. Stellen Sie auch sicher, dass es neuen Abonnenten bereits im Rahmen der Willkommens-E-Mail einfach möglich ist, sich wieder von Ihren E-Mails abzumelden.

Prüfen Sie außerdem, dass Sie in punkto Listenhygiene allen bewährten Vorgehensweisen folgen und Bounces sowie inaktive Kontakte regelmäßig aus Ihren Listen löschen.

Was tun?



Wenn Bounce-Raten bei bestimmten Mailbox Providern in die Höhe schnellen

Mögliche Ursachen:

- Ihre IP-Adresse verfügt über keine oder eine zu geringe Sende-Historie
- Ihre Versandinfrastruktur weist inkorrekte Einstellungen auf
- Der ISP nutzt Greylisting-Techniken
- Sie haben die akzeptierten Schwellenwerte für unbekannte Nutzer oder Spam-Beschwerden überschritten

Lösungsmöglichkeiten:

Prüfen Sie die Bounce Logs hinsichtlich der angegebenen Gründe. Diese Information hilft Ihnen, das oder die spezifischen Probleme zu verstehen, denn der einzuschlagende Lösungsweg wird maßgeblich vom verursachenden Problem abhängig sein. Wenn Sie beispielsweise von einer neuen IP-Adresse versenden wird es notwendig sein, diese erst „aufzuwärmen“, indem sie langsam beginnen und zuerst niedrige Volumina versenden; erst allmählich sollten Sie das Versandvolumen steigern, wobei Sie stets darauf achten sollten, Beschwerden und unbekannte Nutzer so gering wie möglich zu halten.

Wenn Ihre E-Mails aufgrund von zu hohen Spam-Beschwerderaten abgewiesen werden, lesen Sie bitte unsere Empfehlungen bei Spam-Beschwerden. Wenn aber hohe unbekannte Nutzerraten für das Bouncen Ihrer Mails ursächlich verantwortlich sind, finden Sie auf der Seite zu unbekannten Nutzern hilfreiche Tipps.

Was tun?



Bei einem hohen Prozentsatz unbekannter Nutzer
(wenn die Hard Bounce Rate bei über 10 Prozent liegt)

Mögliche Ursachen:

- Versand an eine veraltete oder schlecht gepflegte Liste
- Versand an eine Liste von Kontakten, die sich ehemals von Ihrer Kommunikation abgemeldet hatten
- Der Mailbox Provider deaktiviert alte bzw. inaktive E-Mail Adressen

Lösungsmöglichkeiten:

Der Fehlercode „unbekannter Nutzer“ (unknown user) wird ausgelöst, wenn eine E-Mail an eine E-Mail-Adresse verschickt wird, die beim Mailbox Provider nicht vorhanden ist. Es kann sein, dass es sie nie gab und der Neu-Abonnent sie versehentlich oder absichtlich falsch eingegeben hat – oder aber, dass der Nutzer sein E-Mail Account aufgegeben hat.

Mailbox Provider führen eine hohe unbekannte Nutzerrate häufig auf einen so genannten Dictionary Attack zurück – also einen Spam-Angriff, bei dem Spammer durch die wahllose Kombination verschiedener Namen aus dem Wörterbuch versuchen, valide E-Mail-Adressen zu generieren, die dann (teuer) verkauft werden können. Eine andere Möglichkeit, wie auch bei legitimen Versendern hohe unbekannte Nutzerraten auftreten können, ist, wenn mangelnde oder fehlende Listenhygiene vorliegt. Folgen Sie in diesem Fall folgenden drei Schritten:

1. Stellen Sie sicher, dass Bounces mit Fehlercode „unbekannter Nutzer“ immer sofort aus Ihren Listen entfernt werden.
2. Senden Sie Ihren Abonnenten zumindest einmal im Quartal eine E-Mail.
3. Wenn Sie an eine alte Liste versenden, versenden Sie zuerst an einen kleinen Teil der Liste, um das Risiko besser einschätzen zu können.

Was tun?



Wenn Reverse DNS plötzlich nicht mehr bestanden wird

Mögliche Ursachen:

- Ausfall des DNS Servers
- Probleme bei der Netzwerkverbindung
- Es wurde eine fehlerhafte Veränderung Ihres DNS Eintrags durchgeführt

Lösungsmöglichkeiten:

1. Verifizieren Sie mithilfe der Return Path Tools, MX Toolbox oder DNS Stuff, dass Ihr DNS Eintrag verfügbar ist.
2. Setzen Sie sich mit Ihrer IT-Abteilung in Verbindung, um auszuschließen, dass Ihr DNS Eintrag verändert wurde und um sicherzugehen, dass es bei Ihrem DNS Anbieter keine Verbindungsprobleme gibt.

Was tun?



Wenn Ihre IP-Adresse auf einer Blacklist erscheint

Mögliche Ursachen:

- Ihre Verteilerliste weist Spamfallen auf
- Sie haben keine ausreichenden Prozesse zur Verarbeitung von Beschwerden und/oder Bounces implementiert

Lösungsmöglichkeiten:

Eine Blacklist wird von ISPs, Anbietern von Spam-Filter-Software oder Anti-Spam Organisationen erstellt, um Mailbox Provider und Unternehmen bei der Filterung von Spam zu unterstützen. Der Inhaber einer öffentlichen Blacklist wird diese frei zugänglich machen und es anderen Unternehmen damit ermöglichen, auf Basis der Blacklist Filterentscheidungen über eingehende E-Mails zu treffen. Um eine hohe Zustellbarkeit der eigenen Kampagnen sicherzustellen sollten legitime Versenden auf keinen Fall auf einer der folgenden wichtigsten Blacklists erscheinen: Spamhaus, SpamCop, CBL sowie der Return Path Blacklist.

Eine IP-Adresse wird u.a. dann auf eine Blacklist aufgenommen, wenn eine versendete E-Mail auf eine Spamfalle trifft (lesen Sie auch meine Kommentare zu Spamfallentreffern auf Seite 6). Wenn der Betreiber einer Blacklist auf wiederholte Spamfallentreffer aufmerksam wird bzw. ungewöhnlich hohe Spam-Beschwerden beobachtet, wird er die IP-Adresse ebenfalls auf die Blacklist setzen.

Bei manchen Blacklists reicht auch bereits ein Fehler in der Einstellung der Versandinfrastruktur – z.B. das Vorhandenseins eines Open Relays – für die Aufnahme in die Blacklist auf. Prüfen Sie deshalb Ihre Infrastruktur regelmäßig auf die Einhaltung branchenweit anerkannter Standards und Vorgehensweisen.

Was tun?



Bei einem plötzlichen Anstieg abgewiesener E-Mails

Mögliche Ursachen:

- Ein Mailbox Provider hat Ihre Versand-IP-Adresse auf die eigene Blacklist gesetzt
- Ihre IP-Adresse wurde auf eine öffentliche Blacklist gesetzt
- Sie leiden unter Reputationsproblemen, ausgelöst durch Spam-Beschwerden, Spamfallen-Treffer und/oder hohen unbekannten Nutzerraten

Lösungsmöglichkeiten:

Wenn Ihre E-Mail Zustellung plötzlich einbricht deutet das in der Regel auf eine Änderung in Ihren Versandpraktiken hin. Überlegen Sie deshalb zuerst, was kürzlich geändert wurde.

Haben Sie beispielsweise den Anbieter für Ihre Webseite oder Domain gewechselt? Und wenn ja, wurden die DNS Einträge für die korrekte Authentifizierung Ihrer E-Mails überprüft und sind diese aktuell und korrekt?

Nutzen Sie eine neue E-Mail Designvorlage oder überarbeitete Inhalte? Wenn Sie beispielsweise Ihr Branding aktualisieren, sollten Sie die neuen E-Mail-Vorlagen testen, um sicherzustellen, dass Sie das Template wählen, das optimale Response-Raten verspricht. Wenn Ihre Abonnenten Ihr neues Branding oder die neuen Inhalte nicht mehr länger mit dem ursprünglichen E-Mail-Abonnement verbinden ist es umso wahrscheinlicher, dass sie sich beschweren, sich von Ihrer Kommunikation abmelden oder E-Mails von Ihnen einfach ignorieren werden.

Haben Sie eine neue Liste in Ihren E-Mail Verteiler aufgenommen, z.B. gekaufte oder gemietete Adressen oder alte inaktive E-Mails in dem Versuch, diese wieder zu aktivieren? Die Qualität dieser Daten hat nicht nur Auswirkungen auf die Zustellbarkeit dieses Segments – sondern wirkt sich im Rahmen der Versenderreputation auf Ihr E-Mail Marketing insgesamt aus. Listenhygiene und das Engagement Ihrer Abonnenten sollten Ihr Handeln bestimmen.

Sobald Sie die Änderung identifiziert haben, die sich negativ auf Ihre E-Mail Zustellbarkeit ausgewirkt hat, können Sie die nötigen korrektiven Maßnahmen einleiten.

Was tun?



Bei Nichtbestehen der DKIM Authentifizierung

Mögliche Ursachen:

- Prüfen Sie die Länge der DKIM-Verschlüsselung
- Ist der Public Key vorhanden/gültig?

Lösungsmöglichkeiten:

Obwohl die 512 Bit Verschlüsselung geraume Zeit ausreichend war und damit weit verbreitet ist, besteht mittlerweile die Gefahr, dass dieser Schlüssel gehackt werden kann. So hat Gmail Ende 2012 begonnen E-Mails mit einer DKIM Verschlüsselung von weniger als 1024 Bit als „nicht bestanden“ zu bewerten. Lesen Sie in diesem Zusammenhang auch den Artikel von Ken Takahashi, General Manager Anti-Phishing Solutions bei Return Path, zum Thema „**Google lehnt Ihren DKIM Schlüssel ab, obwohl er völlig in Ordnung ist (und warum das eine Chance darstellt)**“, der am 7. November 2012 auf unserem Inbox Insider Blog veröffentlicht wurde.

Eine andere Ursache für ein Nichtbestehen der DKIM Authentifizierung könnte sein, dass der Public Key ungültig oder nicht vorhanden ist. Beim Public Key handelt es sich um einen DNS Eintrag der in Kombination mit einem Hashwert in die ausgehende E-Mail eingefügt wird, um diese zu validieren. Der Public Key besteht aus willkürlichen Buchstaben, so dass sich insbesondere beim Kopieren schnell Fehler einschleichen können. In Abhängigkeit von Ihrem Provider sind u.U. auch Aufhebungszeichen erforderlich. Halten Sie in diesen Fällen Rücksprache mit Ihrem Anbieter, um sicherzustellen, dass der Public Key korrekt konfiguriert wurde.

Nutzen Sie die Möglichkeit Ihre Authentifizierung kostenlos über Return Path prüfen zu lassen. Senden Sie dafür eine E-Mail von Ihrem Versandsender an checkmyauth@auth.returnpath.net und wir antworten direkt mit einem detaillierten Report an die versendende Adresse.

Was tun?



Wenn mehr E-Mail Nachrichten in den Spamordner platziert werden

Mögliche Ursachen:

- Ein Anstieg der Spam-Beschwerden, Spamfallen-Treffer oder hohe unbekannte Nutzer-Raten
- Fehlende Re-Engagement Kampagnen
- Nichtnutzung von Feedback Loops
- Auslösen von Spamfiltern

Lösungsmöglichkeiten:

Nachlassendes Engagement Ihrer Abonnenten, also negative Trends bei der Art und Weise wie Abonnenten mit Ihren E-Mails interagieren, kann sich äußerst negativ niederschlagen, nicht zuletzt in den Posteingangsraten. Deshalb ist es ratsam, frühzeitig an Re-engagement Kampagnen zu denken und diese in den E-Mail-Lebenszyklus Ihrer Abonnenten fest einzuplanen. Finden Sie heraus, wie „inaktiv“ speziell für Ihr Unternehmen definiert sein sollte, denn dies ist für jedes Business etwas unterschiedlich und eng mit dem Customer Lifecycle verknüpft.

Bieten Sie dann im Rahmen der Re-engagement Kampagne relevante Inhalte oder Informationen an, die exklusiv über Ihr Unternehmen zur Verfügung stehen. Oder aber Sie unterbreiten ein besonderes Angebot. Sie sollten sich außerdem überlegen, wann es Zeit ist, den offensichtlich nicht mehr länger interessierten Abonnenten gehen zu lassen. Vermeiden Sie in jedem Fall „belästigend“ zu wirken; eine Spam-Beschwerde wäre deutlich schwerwiegender als einen inaktiven Abonnenten gehen zu lassen.

Wenn ein Abonnent Ihre E-Mail als Spam oder Junk markiert sollten Sie ihn schnellstmöglich vom Verteiler nehmen, denn Spam-Beschwerden wirken sich im Rahmen Ihrer Versenderreputation negativ auf Ihre Zustellbarkeit insgesamt aus. Stellen Sie deshalb sicher, dass Sie sich für alle relevanten Feedback Loops angemeldet haben. Ist das der Fall erhalten Sie direkt vom betreffenden ISP eine Nachricht, wenn aufgrund einer Ihrer E-Mails eine Spam Beschwerde eingeht. Beachten Sie, dass es für die Aufnahme in Feedback Loops einige Best Practices einzuhalten gilt wie beispielsweise die Authentifizierung mit SPF und DKIM; doch für die meisten legitimen E-Marketer sollten diese Anforderungen kein

Problem darstellen.

Über Return Path

Return Path ist das weltweit führende Unternehmen im Bereich Email Intelligence. Wir analysieren mehr E-Mail Daten als irgendein anderes Unternehmen und verwenden diese Daten im Rahmen unserer Lösungen, mit dem vorrangigen Ziel, dass nur erwünschte E-Mails den Posteingang erreichen. Unter Nutzung unserer langjährigen Geschäftsbeziehungen mit Internetdienstleistern können E-Marketer mithilfe unserer Email Intelligence-Lösungen die Performance ihres E-Mail Marketings maximieren und ihre Abonnenten zugleich vor Spam und anderen Schadmails schützen. Unsere Lösungen tragen dazu bei, den ROI des E-Mail-Marketing-Kanals zu steigern und die Kundenbeziehungen zu verbessern. Internetdienstleister profitieren aufgrund verbesserter Netz Performance sowie gesteigerter Kundentreue von der Zusammenarbeit mit Return Path. Weitere Informationen finden Sie unter:

www.returnpath.de

Kanada

rpinfo-canada@returnpath.com

Großbritannien

rpinfo-uk@returnpath.com

Deutschland

rpinfo-germany@returnpath.com

Frankreich

rpinfo-france@returnpath.com

USA

rpinfo@returnpath.com

Brasilien

rpinfo-brazil@returnpath.com

Australien

rpinfo-australia@returnpath.com

