EMAIL DELIVERABILITY GUIDE 2021

So landen Ihre E-Mails zuverlässig im Posteingang

Inhalt

Definitionen

Spam

Unerwünschte
Werbung

Spam (engl.; umgangssprachlich für UBE = Unsolicited Bulk Email) sind Massen-E-Mails bzw. Werbesendungen, die im Internet verbreitet werden. Diese landen unaufgefordert in Millionen von elektronischen Postfächern. Die meisten Spam-E-Mails haben einen kommerziellen Hintergrund. Sie werden in folgende Typen unterteilt:

- kommerzieller E-Mail-Spam
- Kettenbriefe, Viruswarnungen, Hoaxes
- durch Viren versandte E-Mails
- Phishing-E-Mails

Zustellung (Zustellrate)

Bounce Handling
Implementieren

Die Zustellrate beschreibt den prozentualen Anteil der erfolgreich zugestellten E-Mails (Empfang der Mail im Posteingang des Empfängers) an den insgesamt versendeten E-Mails. Bounces, das heißt unzustellbare Nachrichten, werden hier nicht mit einbezogen.
Die Zustellrate gibt somit unter anderem Aufschluss über die Qualität der Verteilerliste. Um sie konstant hoch zu halten, bedarf es eines Bounce-Handlings, wie es in der Global-Suppression-Lösung von Retarus implementiert ist. Nicht erreichbare E-Mail-Adressen werden damit automatisch aus einem Verteiler entfernt.

Reputation / Sender Score

Je höher,
desto besser

Scores werden als gleitender Durchschnitt über einen Zeitraum von 30 Tagen berechnet und repräsentieren die Rangordnung einer IP-Adresse gegenüber anderen IP-Adressen, ähnlich wie ein Prozentrang. Je näher der Score bei 0 liegt, desto schlechter ist er; wenn er hingegen nahe an 100 liegt, hat der Versender vieles richtig gemacht.

Beschwerden: Es wird der Quotient aus der Anzahl der Beschwerden und der Anzahl der empfangenen E-Mails berechnet. Berücksichtigt wird auch, wie viele Beschwerden die betreffende IP-Adresse im Vergleich zu anderen IPs erhält.

Volumen: Das schiere Versandvolumen ist kein Anhaltspunkt für einen guten oder schlechten Ruf des Absenders. Es ist aber ein wichtiger Teil des allgemeinen Algorithmus. Zum Beispiel wird eine IP-Adresse, die 100 Nachrichten versendet

und 99 Beschwerden erhält, als problematisch eingestuft. Dagegen wird eine IP-Adresse, die 100.000 Nachrichten versendet und 99 Beschwerden erhält, als gut bewertet. Das Volumen steht also immer in Abhängigkeit zu anderen Indexwerten.

Externe Reputation: Diese Zahl gibt an, wie die IP-Adresse eines Absenders im Vergleich zu anderen auf einer Vielzahl von externen „Blacklists" und „Whitelists" gelistet ist.

Unbekannte Kontakte: Das Verhältnis der Anzahl von unbekannten Kontakten einer IP-Adresse zu anderen Adressen wird direkt aus eingehenden SMTP-Anmeldungen der beteiligten Internet Service Provider (ISPs) ermittelt. Gemessen wird, wie oft eine IP-Adresse versucht, eine Nachricht an einen nicht existierenden Empfänger zu senden.

Zurückgewiesene Nachrichten: Dieser Wert gibt an, wie oft Nachrichten verglichen mit anderen IP-Adressen einen Soft- oder Hard Bounce verursachen.

Angenommene Nachrichten: Diese Zahl repräsentiert, wie viele Nachrichten von den ISPs angenommen und an die Empfänger weitergeleitet werden. Der Wert enthält alle verschickten Nachrichten abzüglich der zurückgewiesenen.

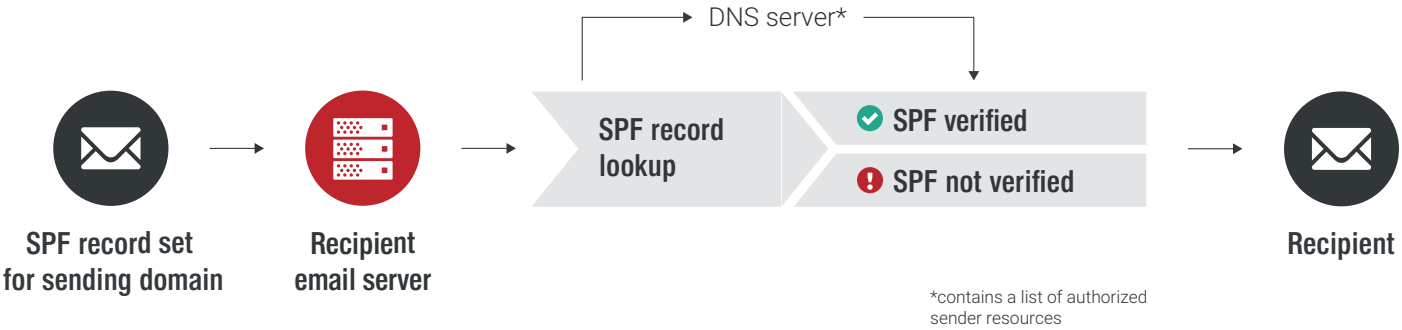
Verhältnis der angenommenen Nachrichten: Vergleicht die Anzahl der angenommenen Nachrichten mit der der insgesamt versendeten. Dazu wird der Quotient aus Anzahl der verschickten Nachrichten und angenommenen Nachrichten gebildet.

Verhältnis der unbekannten Kontakte: Die Anzahl der unbekannten Kontakte oder ungültigen E-Mail-Adressen in Relation zur Anzahl der verschickten Nachrichten.

SPF Record

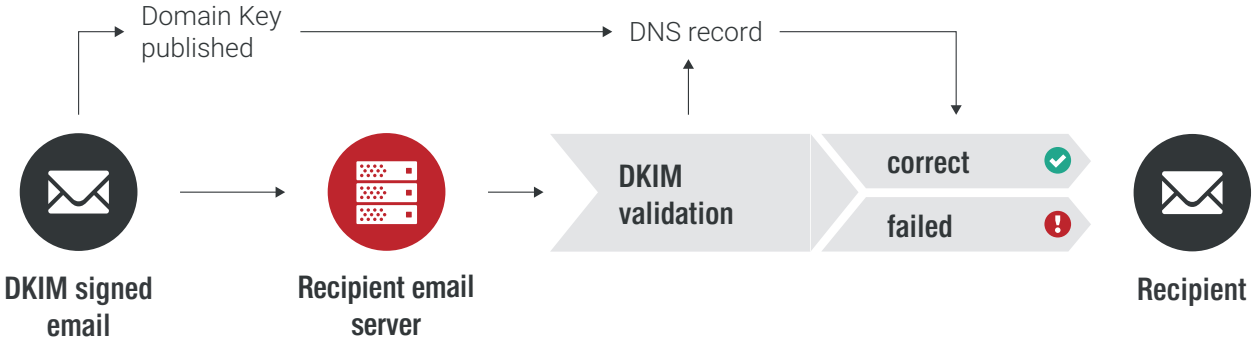
Absender im DNS

Das Sender Policy Framework (SPF; früher Sender Permitted From) soll das Fälschen von Absenderadressen einer E-Mail verhindern. Es entstand ursprünglich als Verfahren zur Abwehr von Spam. Bei SPF trägt der Inhaber einer Domain in das Domain Name System ein, welche Computer zum Versand von E-Mails für diese Domain berechtigt sind.
Der Administrator einer Domain hinterlegt dazu in der DNS-Zone einen Resource Record vom Typ TXT (der SPF Resource Record wurde durch RFC 7208 obsolet). Darin stehen die IP-Adressen aller Mail Transfer Agents (MTAs), die für die Domain E-Mails versenden dürfen. Der Empfänger prüft anhand der in den Feldern „MAIL FROM" und „HELO" angegebenen Domain, ob der Absender zum Versand berechtigt ist. Für die angegebene Domain ruft der Empfänger die SPF-Information über das Domain Name System ab und vergleicht die IP-Adresse des sendenden MTAs mit den erlaubten Adressen. Stimmt die IP-Adresse überein, so ist der angegebene Absender echt, andernfalls kann die E-Mail verworfen werden.



DKIM

DomainKeys Identified Mail (DKIM) ist ein Protokoll, um die Authentizität von E-Mail- Absendern sicherzustellen. Es wurde konzipiert, um unerwünschte E-Mails wie Spam oder Phishing einzudämmen. DomainKeys basiert auf asymmetrischer Verschlüsselung. Die E-Mail wird mit einer digitalen Signatur versehen, die der empfangende Server anhand des öffentlichen Schlüssels im Domain Name System (DNS) der Domäne überprüfen kann. Schlägt die Verifizierung fehl, hat der empfangende Mail Transfer Agent (MTA) oder das empfangende Anwendungsprogramm die Möglichkeit, die E-Mail abzuweisen oder auszusortieren.



DMARC

SPF + DKIM =
Richtlinien

DMARC, kurz für Domain-based Message Authentication, Reporting, and Conformance, ist eine ergänzende technische Spezifikation, die Absender und Empfänger von E-Mail-Nachrichten vor Spam, Spoofing und Phishing schützen soll.
Bei DMARC kann der Versender Richtlinien vorgeben, wie empfangende Mailserver die Authentifizierung von E-Mails handhaben sollen. DMARC selbst ist kein eigenständiges Protokoll, sondern baut auf den oben erwähnten Standards SPF und DKIM auf.
Die DMARC-Richtlinien zur Annahme von E-Mails veröffentlicht der Domain-Administrator als Teil der DNS-Einträge der jeweiligen Domain.
Sobald ein Posteingangsserver DMARC unterstützt und eine E-Mail empfängt, greift er auf den DNS-Eintrag zurück, um die dort hinterlegte Richtlinie für die im „From"-Header (RFC 5322) enthaltene Domäne „nachzuschlagen".
Neben dem Abgleich der DKIM-Signatur wird überprüft, ob die Nachricht von einer IP-Adresse stammt, die in den SPF-Einträgen der sendenden Domain zugelassen ist.
Nachdem die DMARC-Richtlinie angewendet wurde, meldet der empfangende Mailserver das Ergebnis an den Eigentümer der sendenden Domain. Somit wird Letzterer auch über eine etwaige missbräuchliche Nutzung seiner Domain in Kenntnis gesetzt.

BIMI

Flagge zeigen
mit Ihrem Logo

BIMI steht für Brand Indicators for Message Identification. Es handelt sich um einen noch recht neuen offenen Standard für Mailbox-Provider (MBP), der gemeinsam von mehreren großen Unternehmen wie Google, Microsoft, Yahoo und PayPal entwickelt wurde. E-Mail-Versender können mit BIMI den E-Mail-Empfängern das bekannte Logo ihrer Marke oder ihres Unternehmens als Grafik neben dem Absendernamen anzeigen, um auf einen professionellen und seriösen Absender hinzuweisen.
BIMI ist ein offener Standard, den grundsätzlich jeder Versender nutzen kann. Er setzt auf die bereits etablierten Standards SPF, DKIM und DMARC auf. Sind diese bereits umgesetzt, dann lässt sich BIMI mit entsprechend geringem Aufwand implementieren:

- Die DMARC-Richtlinie muss auf „Reject" oder „Quarantine" gesetzt sein
- Das gewünschte Logo sollte als quadratische Grafik ohne Text im Format SVG Tiny PS unter einer frei zugänglichen Web-Adresse liegen
- Innerhalb des DNS-Eintrags muss man nun noch einen TXT-Record für die betreffende „From:"-Addresse anlegen: `default._bimi.[domain] IN TXT "v=BIMI1; l=[SVG URL]; a=[PEM URL]`

Weiterführende Informationen finden Interessierte unter bimigroup.org.

Zusätzliche Definitionen in der Transactional-E-Mail-Welt

Inbox Placement Rate: Zustellrate abzüglich der Anzahl der E-Mails, die im Spam- oder Junk-Ordner gelandet sind

Soft Bounces: E-Mails, die an existierende Adressen versendet werden, aber temporär nicht zugestellt werden können (z. B. wegen Urlaubsnachricht)

Hard Bounces: E-Mails, die dauerhaft nicht zugestellt werden können (Empfänger hat das Unternehmen verlassen o. ä.)

Öffnungsrate: Anzahl Öffnungen dividiert durch die Anzahl zugestellter E-Mails

Unique Click Rate: Anzahl Klicks in einer E-Mail (ohne Mehrfachklicks eines Users) geteilt durch die Anzahl zugestellter E-Mails

Total Click Rate: Alle Klicks in einer E-Mail geteilt durch die Anzahl zugestellter E-Mails

Click to Open Rate: Unique Click Tate dividiert durch Öffnungsrate

Conversion Rate: Anzahl gezielter Aktionen geteilt durch die effektive Klickrate

Bounce Rate: Anzahl Bounces dividiert durch die Anzahl zugestellter E-Mails

Risiken und Gefahren

Doppelt schmerzhaft

In einer aktuellen Studie stellt das E-Mail-Intelligence-Unternehmen Return Path fest, dass 20 Prozent der versendeten und erwünschten E-Mails nicht bei den Empfängern ankommen. Nicht zugestellte E-Mails schaden Unternehmen in doppelter Hinsicht:

- Eine verringerte Reichweite von Marketing-Kampagnen führt zu direkten Umsatzeinbußen. Das Umsatzpotenzial, das in Deutschland jährlich in Spam-Ordnern landet, wird auf etwa 3 Milliarden Euro geschätzt.
- Durch die versehentliche Spam-Klassifizierung entstehen nicht nur finanzielle Verluste. Auch die Reputation des Unternehmens bzw. der Marke wird in Mitleidenschaft gezogen, wenn die Versandadresse auf Sperrlisten erscheint und das Unternehmen als Absender von E-Mails negativ bewertet wird.

Ursachen für Spam-Klassifizierungen

Die Ursachen für eine Einstufung als Spammer können vielfältig sein, etwa Spam Traps, „kalte" IPs, die Gestaltung der E-Mails oder Reputations-Scores. Es ist verständlich, dass Anwender ihren E-Mail-Posteingang und ihren Rechner mit Sicherheitssoftware vor Angriffen aus dem Internet schützen wollen. Dieses Sicherheitsbedürfnis der Kunden sollte man bei der Planung von E-Mail-Marketing-Maßnahmen berücksichtigen.

	SPERRLISTE	GREYLIST
Definition	• Verzeichnis von IP-Adressen und Domains, die durch den Versand unerwünschter E-Mails negativ aufgefallen sind • E-Mails, die über diese IP versendet werden, werden abgefangen/blockiert • Große E-Mail-Provider nutzen meist mehrere Sperrlisten(-Anbieter)	• Abweisen einer bislang unbekannten E-Mail- und/oder IP-Adresse beim ersten Zustellversuch • Zweiter, späterer Zustellversuch zumeist erfolgreich
Vorteile	• Schutz der Anwender vor unerwünschter-Kommunikation	• Effektive Spam-Bekämpfung: Viele Spammer geben bereits beim ersten Zustellversuch auf, echte Mail-Server führen in der Regel einen zweiten Zustellversuch aus • Nach der erfolgreichen E-Mail-Zustellung wird die Kombination von Absender, Empfänger und E-Mail-Server in die Erlaubt-liste eingetragen und Folge-Mails werden zugestellt
Nachteile	• Erwünschte E-Mails auf der Sperrliste, z. B. wenn eine ganze Domain gesperrt wird, obwohl nur eine Subdomain Spam versendet • Umsatzeinbußen und Imageschaden für den Absender – Kampagnen, die über eine gelistete IP versendet werden, werden nicht zugestellt • Aufwändiges Delisting. Man kann sich von einer Sperrliste nehmen lassen, wenn man versehentlich darauf gelandet ist. Bei mehrfachen Verstößen landen Versender u. U. allerdings permanent auf der Sperrliste • Unlauteres Geschäftsmodell	• Eine erwünschte E-Mail kann durch Grey-listing einige Minuten oder auch Stunden später eintreffe. • Einige Mail-Server-Programme generieren bereits nach dem ersten Versuch einen vorläufigen Zustellbericht an den Absender, der gegebenenfalls als fehlgeschlagene Zustellung interpretiert wird

Internationale Besonderheiten

Der Satz „Andere Länder, andere Sitten" trifft auch auf das E-Mail Marketing zu, bei dem es eine Vielzahl nationaler Regularien und Besonderheiten zu verstehen und zu beachten gilt.
Wenn Sie diese nicht einhalten, kann dies hohe Bußgelder oder sogar strafrechtliche Sanktionen nach sich ziehen.

USA – CAN SPAM Act (2003)

Das 2003 verabschiedete Bundesgesetz Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) verbietet den Versand von kommerziellen elektronischen Nachrichten (Commercial Electronic Messages, CEMs) – es sei denn, sie erfüllen die folgenden Anforderungen:

Inhaltlich

- Der kommerziellen Charakter der E-Mail muss deutlich sein (außer es wurde bereits im Vorfeld eine Zustimmung eingeholt).
- Die E-Mail muss einen korrekten Header haben.
- Die Betreffzeile muss für das Angebot im Text der Nachricht relevant sein.
- Nicht jugendfreie Inhalte sind gesondert zu kennzeichnen (Label).
- Die E-Mail muss eine gültige physische Adresse des Absenders enthalten.
- Die E-Mail muss eine Kündigungsoption enthalten, die binnen 10 Tagen bearbeitet wird („Opt-out").

Kommerzieller Charakter
muss klar sein

Sie dürfen ohne vorherige Zustimmung mit Einzelpersonen oder Unternehmen Kontakt aufnehmen, solange Sie sich an die oben genannten Anforderungen halten und keine rechtswidrigen Mittel zur Erfassung von E-Mail-Adressen einsetzen. Ein Beispiel für rechtswidrige Mittel ist die Verwendung eines automatisierten E-Mail-Generators.
Im Falle eines Verstoßes gegen das Gesetz können die Bußgelder bis zu 16.000 USD pro Verstoß und pro E-Mail betragen.

Europäische Union – DSGVO

Marktort-
prinzip

Die Datenschutz-Grundverordnung (DSGVO) ist aufgrund ihrer Natur in allen Ländern rechtsverbindlich und seit dem 25. Mai 2018 unmittelbar rechtswirksam. Die Verordnung gilt für alle Einzelpersonen und Unternehmen in der EU. Unabhängig davon, wo der Absender seinen Sitz hat, fällt jeder unter das Gesetz, der E-Mail-Adressen erwirbt und E-Mails an Empfänger in der EU sendet.

Gestaltung der E-Mail

- Jede versendete E-Mail muss ein den geltenden rechtlichen Anforderungen entsprechendes, leicht erkennbares Impressum enthalten.

Für den Versand von E-Mails mit Werbeinhalten gilt zudem:

- Der Auftraggeber einer Werbesendung muss klar erkennbar sein.
- In jeder E-Mail ist der Empfänger gesondert auf die Möglichkeit hinzuweisen, die erteilte Einwilligung in die Zusendung von E-Mails jederzeit zu widerrufen. Der Widerruf / das Abbestellen von E-Mails (Opt-out / Unsubscribe) muss dem Empfänger grundsätzlich ohne Weiteres, d. h. ohne Eingabe von Zugangsdaten wie Login und Passwort möglich sein.
- In der Kopf- und Betreffzeile der E-Mail darf weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.

Technische Konfiguration

- Absenderadressen sind registrierungspflichtig und Bestandteil der Service-Administration. Die Absenderadresse muss in der Lage sein, E-Mails zu empfangen (valider MX Record). Die Absender-Domain muss zudem über einen validen DNS-A-Record verfügen. Rollenbasierende Absender-adressen (z. B. abuse@), postmaster@) sind nicht erlaubt.
- Der Kunde muss E-Mail-Adressen unverzüglich aus den entsprechenden Verteilern entfernen, wenn sie nach dem Versand als nicht existent erkannt werden, spätestens jedoch nach drei Hard Bounces. Insgesamt darf die Hard Bounce Rate pro ISP 1,0 Prozent nicht übersteigen. Rollenbasierende Empfängeradressen (z. B. postmaster@, abuse@) werden verworfen.
- Der Kunde muss E-Mail-Adressen aus den entsprechenden Verteilern entfernen, wenn der Empfänger die E-Mail als Spam einstuft und dies meldet (complaint) oder die Einwilligung in den Versand von E Mails widerruft.

Die Verordnung gilt auch rückwirkend. Wenn Sie die Zustimmung Ihrer derzeitigen Empfänger nicht nachweisen können, dürfen Sie ihnen keine E-Mails mehr zusenden.
Die DSGVO vereinheitlicht nicht nur die Anforderungen, sondern auch die Sanktionen. Verstöße können Unternehmen maximal 4 Prozent ihres jährlichen weltweiten Umsatzes oder 20 Mio. EUR kosten, je nachdem, welcher Betrag höher ist.

China

Vorsicht mit kritischen Inhalten

Die chinesische Anti-Spam-Gesetzgebung wird durch die Maßnahmen zur Verwaltung von Internet-E-Mail-Diensten (2006) und das Verbraucherrechtsschutzgesetz (2013) definiert. Sie gilt für alle E-Mails an Bürger Chinas und Menschen, die E-Mails empfangen, während sie sich in China aufhalten. Die Voraussetzungen für einen rechtmäßigen E-Mail-Verkehr sind folgende:

- Eine ausdrückliche Zustimmung ist erforderlich (Opt-in-Ansatz).
- Die Berechtigung muss überprüfbar sein und für das Audit aufgezeichnet werden.
- Die kommerzielle Natur der E-Mail muss klar sein.
- Die Betreffzeile muss das Wort „ad" oder „advertisment" in englischer oder chinesischer Sprache enthalten.
- Die Identität oder Herkunft des Absenders darf weder absichtlich verschwiegen noch gefälscht werden.
- Die E-Mail muss gültige Kontaktmethoden enthalten, einschließlich der E-Mail-Adresse des Absenders. Die Empfänger können dann ihre Ablehnung des Empfangs weiterer E-Mails senden, die 30 Tage lang gültig sein müssen.

Inhalt

- Jede Nachricht mit werblichem Charakter fällt unter die Regulierung.
- Für jeden externen Link in einer E-Mail gibt muss schriftlich garantiert werden, dass die Nachricht keine Spyware enthält (die Situation für Bilder / Miniaturansichten ist unklar).

Besondere Einschränkungen gelten in China für Inhalte. Diese werden in Artikel 57 der Telekommunikationsverordnung vage definiert. Offensichtliche Beispiele sind politisch sensible Themen, aber auch alles, was als obszön gilt.
Die Geldbußen reichen von CNY 10.000 bis CNY 30.000 pro E-Mail. Trotz strenger Vorschriften und hoher Bußgelder gab es bisher keine spektakuläre Entscheidung. Daher bleibt Spam in China ein großes Problem.
Bevor Sie sich für E-Mail-Marketing-Aktivitäten in China interessieren, sollten Sie in jedem Fall die sehr dynamische Liste der Keywords auf der Blacklist der lokalen Behörden überprüfen.

Leitfaden für eine gute Zustellbarkeit

Die Zustellbarkeit („Deliverability") ist eine der wichtigsten Säulen im professionellen E-Mail-Marketing. Die Qualität der Systeme von Unternehmen, die E-Mail-Kampagnen versenden, ist wichtig, um Zustellbarkeitsraten hoch halten und ausbauen zu können.

Warm-up unbekannter IPs

Vorglühen
zündet besser

Die Reputation von IP-Adressen basiert größtenteils auf historischen Versandmustern und -volumen. Eine IP-Adresse, die über einen langen Zeitraum hinweg konsistente Mengen an E-Mails versendet, weist in der Regel eine hohe Zuverlässigkeit auf. Unternehmen, die dedizierte IP-Adressen verwenden, erhalten ihre Reputation als Absender aufrecht, indem sie konsistente und vorhersehbare Mengen an E-Mails versenden.
Retarus empfiehlt Folgendes zum Warm-up einer dedizierten und bisher unbekannten IP:

- Dauer des Warm-up-Prozesses: ca. 6-8 Wochen
- Anfangs ein geringes E-Mail-Volumen versenden:
  - » Max. 1.000 E-Mails an Tag 1
  - » Verdoppelung des Volumens auf Basis des Vortags
  - » Starten mit gedrosselter Versandgeschwindigkeit
  - » Langsames Steigern von Volumen, Anzahl der Empfänger, Versandgeschwindigkeit
- Parallel beginnen, die Anwenderliste zu bereinigen
- Alle verfügbaren IPs und Domains regelmäßig nutzen
- Nicht plötzlich und / oder extrem intensivieren
- Gefahr von Blacklisting gering halten (Vorsicht vor Spam Traps und Affiliate-Kampagnen)
- Während des Warm-Ups keine strategisch wichtigen, jedoch attraktive Kampagnen versenden
- Anfänglich Versand auf besonders aktive und interessierte Kunden konzentrieren

Bedeutung „Shared IP“ vs. „Dedicated IP“

Viel und oft?
Eigene IP!

Je mehr Sie sich mit dem Thema hochvolumiger E-Mail-Versand auseinandersetzen, desto häufiger werden Sie feststellen, welche zentrale Bedeutung zwei verschiedene Arten von IP-Adressen zukommt:

Shared IP: Mehrere Versender teilen sich die gleiche IP-Adresse

Dedicated IP: Ein Versender nutzt und verantwortet eine IP-Adresse exklusiv

Ihre Ziele als E-Mail-Versender sind mit entscheidend dafür, ob Sie eine dedizierte oder geteilte IP-Adresse benötigen. Dabei sollten Sie Indikatoren wie Sendevolumen, Häufigkeit sowie die Qualität Ihrer Verteiler bei der Entscheidungsfindung berücksichtigen.

Wenn Sie konstant hochvolumige Kampagnen oder transaktionale Nachrichten versenden, ist eine dedizierten IP-Adresse zu empfehlen. Sie sind allein für Ihre Reputation verantwortlich und vor unsachgemäßen Gebrauch durch Dritte geschützt.

Versenden Sie Ihre Kampagnen oder transaktionalen E-Mails in kleinerem Maße oder unregelmäßiger, empfiehlt sich eine geteilte IP-Adresse. Hier profitieren Sie von der Aktivität der weiteren Absender, um den Ruf der IP aufzubauen und zu erhalten.

Zustellrate

Einwilligung
am besten nachweisen

Eine Anmeldung per Double-Opt-in (DOI) erhöht die Qualität des Empfängerkreises. Denn es werden nur Empfänger angeschrieben, die sich selbst angemeldet haben und deren E-Mail-Adresse auch tatsächlich existiert.

DOI ist ein zweistufiges Verfahren, bei dem nach der Einwilligung im ersten Schritt im zweiten eine Bestätigung – in der Regel durch Aktivieren eines Bestätigungs-Links – erfolgt. So wird verhindert, dass bei einer Anmeldung missbräuchlich falsche oder fremde Kontaktdaten eingegeben werden.

Für einen adäquaten Nachweis muss das DOI-Verfahren ordnungsgemäß protokolliert werden und die „Bestätigungsmail“ einen Rückschluss auf die Einwilligung zulassen.

Hierzu muss die DOI-Mail:

- Datum und Uhrzeit sowie die Quelle der Adresserhebung erwähnen,
- den Text der abgegebenen Einwilligungserklärung inklusive Hinweis auf die jederzeitige Widerrufsmöglichkeit enthalten,
- beim Text der abgegebenen Einwilligungserklärung den Anforderungen an eine konkrete, separate Erklärung genügen,
- im Hinweis auf die Widerrufsmöglichkeit gemäß § 13 Abs. 3 TMG auch eine Kontaktmöglichkeit zur zukünftigen Abmeldung angeben,
- frei von anderen Erklärungen sein, d. h. sie darf nur eine separate, einzig auf die E-Mail-Werbung bezogene Einwilligung enthalten,

- zur Bestätigung der Einwilligung durch Anklicken des Bestätigungslinks zum Zurücksenden der DOI-Mail an den Versender aufordern, und
- werbefrei sein.

CSA bürgt für
Qualität

Die DOI-Mail muss darüber hinaus auch ein korrektes Impressum enthalten (vgl. § 5 TMG). Dieses kann vollständig in der Mail enthalten oder alternativ verlinkt (maximal zwei Klicks) sein.
Um die Zustellrate weiter zu erhöhen, kann bei der Newsletter-Anmeldung darum ersucht werden, den Absender zum persönlichen Adressbuch bzw. zur persönlichen Whitelist hinzuzufügen. Denn oft werden auch erwünschte E-Mails und Newsletter im Postfach des Empfängers als Spam gekennzeichnet („false positives"). Eine Mitgliedschaft des Versenders in der Certified Senders Alliance (CSA), einer zentralen Whitelist-Datenbank mit zusätzlichen Sicherheitsmechanismen, kann sich überdies positiv auf die Zustellrate auswirken.

Reputation

Stellschrauben
für den Sender Score

Da es einige Zeit dauert, einen schlechten Sender Score zu verbessern, sollten Absender ihre Reputation vom ersten Versand an kennen. Es gibt mehrere Stellschrauben im E-Mail-Marketing, die Unternehmen überprüfen und bei Bedarf anpassen können, um ihren Sender Score zu erhöhen. Die folgenden Faktoren haben den größten Einfluss auf die Zustellbarkeit von E-Mails:

Schwankendes Sendevolumen
Ein Versand gleichmäßiger E-Mail-Volumina ist für die Reputation maßgeblich – Peaks oder ähnliches können die Reputation negativ beeinflussen.

Häufigkeit der versendeten Nachrichten
Aussendungen gleichmäßig verteilt zu versenden, wirkt sich auf die Reputation positiv aus. Dabei spielt es keine Rolle, ob Unternehmen E-Mailings täglich, jeden zweiten Tag oder jede Woche versenden – dies richtet sich nach den Erfordernissen des Marketings. Es sollte lediglich sichergestellt sein, dass nach einem festen Zeitplan versandt wird. Wenn E-Mail-Marketing gut aufgebaut und stabilisiert ist, lässt sich mithilfe von Tests die optimale Frequenz für die jeweilige Zielgruppe ermitteln.

Auf einer Sperrliste stehen

Es gibt etwa 50 bekannte Blacklists, die festhalten, welche IPs Spammer sind. Retarus hat die größten und bekanntesten Blacklist-Betreiber in das aktive Monitoring aufgenommen und überwacht sie. Sollten Anwender von Retarus Transactional Email trotz Warm-up und weiteren reputationssteigernden Maßnahmen auf einer dieser Sperrlisten landen, unterstützt der Retarus Customer Service beim Delisting und recherchiert die Hintergründe. Mit den Ergebnissen können die Anwender von E-Mail for Applications ihre E-Mail-Marketing-Methoden verbessern.

Spam Traps

Dabei handelt es sich um eine E-Mail-Adresse, die früher einmal gültig war, mittlerweile Absendern jedoch als Hard Bounce angezeigt wird. Wenn ein Mail-Server registriert, dass ein Absender regelmäßig an eine ungültige Adresse Nachrichten versendet, kann diese E-Mail-Adresse zur Spam-Falle werden. Absender erhalten dann nicht länger eine Hard-Bounce-Benachrichtigung, sondern die entsprechende Nachricht wird angenommen und ihr Absender als Spammer markiert. Man sollte daher Hard Bounces im Blick behalten und seine Verteiler regelmäßig pflegen.

Spam-Berichte

Wer einen Absender für einen Spammer halten, kann ihn in Spam-Berichten melden. Das schadet dem Ruf der Absender. Deshalb sollten diese regelmäßig überprüfen, wie hoch ihre Spam-Quote ist. Anhaltspunkt: Wenn eine von 1000 Nachrichten als Spam markiert wird, besteht kein Grund zur Besorgnis.

Verteilerqualität

Auf den Verteiler
kommt es an

Die An- und Abmeldefunktion ist bei einem kundenfreundlichen, seriösen E-Mail-Versand inzwischen selbstverständlich. Ein Grund dafür sind rechtliche Rahmenbedingungen für den Versand elektronischer Post. Der Newsletter-Versand ist nur dann legal, wenn der Empfänger seine Einwilligung erteilt hat. Mitglieder einer Whitelist müssen diese Zustimmung mit Quelle und Zeitstempel nachweisen. Ebenso wichtig ist die Unsubscribe-Funktion, die jeder Newsletter enthalten muss. Ein Kunde, der das Abonnement schnell und unkompliziert kündigen kann, wird eine Nachricht nicht als Spam melden. Wichtig: Wenn sich ein Kunde aus dem Verteiler abmeldet, sollte seine Adresse möglichst sofort aus dem Verteiler entfernt und keinesfalls erneut angeschrieben werden.

Nutzung von Anhängen

ISPs prüfen sehr häufig auf Dateitypen, die potenziell gefährlich sind. Hierzu zählen insbesondere ausführbare Dateien (.exe) oder Skripte.

.ade	.js	msh	.ps1xml
.adp	.jse	.msh1	.ps2
.app	.ksh	.msh2	.ps2xml
.asp	.lib	.mshxml	.psc1
.bas	.lnk	.msh1xml	.psc2
.bat	.mad	.msh2xml	.tmp
.cer	.maf	.msi	.url
.chm	.mag	.msp	.vb
.cmd	.mam	.mst	.vbe
.com	.maq	.ops	.vbs
.cpl	.mar	.pcd	.vps
.crt	.mas	.pif	.vsmacros
csh	.mat	.plg	.vss
.der	.mau	.prf	.vst
.exe	.mav	.prg	.vsw
.fxp	.maw	.reg	.vxd
.gadget	.mda	.scf	.ws
.hlp	.mdb	.scr	.wsc
.hta	.mde	.sct	.wsf
.inf	.mdt	.shb	.wsh
.ins	.mdw	.shs	.xnk
.isp	.mdz	.sys	
.its	.msc	.ps1	

Rollenbasierte Absenderadressen

Rollenbasierte Adressen („Funktionspostfächer“) sind in der Regel Firmenadressen, die nicht von einer Person, sondern von einem Job definiert und oft von mehreren Personen verwaltet oder gar nicht überwacht werden. Einige dieser Adressarten sind mit hohen Bounce-Raten und Spam-Beschwerden verbunden. Deshalb blockiert Retarus sie auf Wunsch. Rollenbasierte E-Mail-Adressen lassen sich auch nicht zur Anmeldung für ein Konto verwenden.

abuse@	list@	spam@
admin@	noc@	support@
billing@	no-reply@	sysadmin@
compliance@	noreply@	tech@
devnull@	null@	undisclosed-recipients@
dns@	phish@	unsubscribe@
ftp@	phishing@	usenet@
hostmaster@	postmaster@	uucp@
inoc@	privacy@	webmaster@
ispfeedback@	registrar@	www@
ispsupport@	root@	
list-request@	security@	

Strategie und Priorisierung von Kampagnen

Zu einer stabilen Reputation tragen auch die richtige Strategie und Priorisierung der Kampagnen ihren Teil bei. Folgendes sollten Sie dabei beachten:

Frequenzen definieren

Zeitpunkt und Frequenz des Versands einer Kampagne haben einen entscheidenden Einfluss darauf, wie die Empfänger die Nachricht einstufen. Eine Flut von Benachrichtigungen innerhalb weniger Stunden führt mit großer Wahrscheinlichkeit zur Ablehnung beim Empfänger. Schlägt dieses Feedback auf den ISP durch, beeinflusst dies die Reputation negativ.

Priorisierung / Gruppen gezielt ansprechen

Es empfiehlt sich, wichtige Aussendungen nicht zeitgleich mit weniger wichtigen Kampagnen zu versenden. Durch das erhöhte Versandvolumen steigt das Risiko, die Reputation negativ zu beeinflussen. Dadurch sinkt die Zustellungsrate der wichtigen Kampagnen und das gesetzte Ziel wird nicht erreicht.

Differenzierte Ausgangskanäle nutzen und klar trennen

Über separate Versandstränge lassen sich hohe Zustellraten für Kampagnen erhalten. Kampagnen sollten nicht über die Haupt-Domain ausgesandt werden, sondern über entsprechende Sub-Domains. Noch besser ist es, dedizierte IP-Adressen zu nutzen.

Gestaltung von E-Mails

In der Kopf- und Betreffzeile von E-Mails darf weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält. Jede versendete E-Mail muss ein den geltenden rechtlichen Anforderungen entsprechendes, leicht erkennbares Impressum enthalten.

Betreffzeile

- Sollte stets vorhanden sein
- Kurz, aber aussagekräftig
- Keine Kapitalisierung oder Sonderzeichen
- Keine Spam-verdächtigen Begriffe (Sex, gratis, …)
- Passend zum Inhalt der E-Mail
- Keine Wortwiederholungen

Tipps für optimale E-Mail-Gestaltung

Relevanz für die Empfänger deutlich machen

Konzentrieren Sie sich auf ein spezielles Thema und legen Sie dieses deutlich dar.

Above-the-Fold-Space nutzen

Positionieren Sie die wichtigsten Bausteine in der E-Mail ganz oben, sodass sie direkt ins Auge springen.

Passende Handlungsaufforderungen einfügen

Machen Sie dem Leser deutlich, was er tun soll und was er dafür bekommt.

Bilder mit Dateinamen versehen

Kennzeichnen Sie Bilder mit einem sprechenden Dateinamen, damit der Leser den Inhalt versteht, auch wenn das Bild nicht geladen wird.

Spam-Begriffe vermeiden

Vermeiden Sie Begriffe, die mit Geld oder Gewinn zu tun haben, damit Ihr Newsletter im Posteingang landet und nicht als Spam gewertet wird.

Social Media Shares ermöglichen

Fügen Sie eine Funktion zum Teilen ein, damit der Leser den Newsletter weiterverteilen kann.

Personalisiert schreiben

Der Empfänger fühlt sich direkt angesprochen, wenn er seinen Namen liest. Fügen Sie daher in der Anrede den Namen des Empfängers ein.

Für den Versand von E-Mails mit Werbeinhalten gilt zudem:
Der Auftraggeber einer Werbesendung muss klar erkennbar sein. In jeder E-Mail ist der Empfänger gesondert auf die Möglichkeit hinzuweisen, die erteilte Einwilligung in die Zusendung von E-Mails jederzeit zu widerrufen. Der Widerruf / das Abbestellen von E-Mails (Opt-Out / Unsubscribe) muss dem Empfänger grundsätzlich ohne Weiteres, das heißt ohne die Eingabe von Zugangsdaten (zum Beispiel Login und Passwort) möglich sein.

Wie Sie Retarus Transactional Email bei der Deliverability unterstützt, erklären wir Ihnen gerne in einem persönlichen Gespräch:

www.retarus.de/contact

Hinweis: Alle Informationen in diesem Guide wurden nach bestem Wissen und Gewissen recherchiert und geben den Stand zum Zeitpunkt der Erstellung wieder. Es wird daraufhin hingewiesen, dass dennoch keine Haftung für Richtigkeit, Aktualität und Vollständigkeit übernommen werden kann. Insbesondere ersetzt dieses Schriftstück keine juristische Beratung im Einzelfall.

Verfasser retarus GmbH Stand: Januar 2021