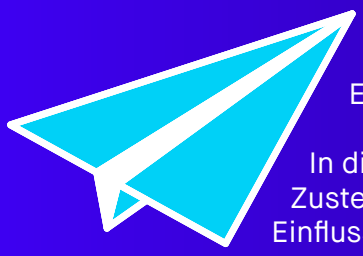
mailXpert



Die Erfolgsfaktoren der Zustellbarkeit im E-Mail-Marketing

White Paper, 2026

Die lange Reise einer E-Mail.



Bevor eine E-Mail ihre Wirkung beim Empfänger entfalten kann, muss sie es zunächst in dessen Posteingang schaffen. Auf ihrer Reise hat die E-Mail eine ganze Reihe von Hürden zu überwinden.

In diesem White Paper erfahren Sie, von welchen Faktoren die erfolgreiche Zustellung einer E-Mail abhängt und auf welche Sie direkt und indirekt Einfluss nehmen können.

SENDEN! - Aufbruch ins Ungewisse.

Wer eine E-Mail abschickt, beauftragt zunächst den Versandserver, den zuständigen Empfangsserver zu ermitteln. Dies geschieht mittels «DNS-Lookup», wo über den sogenannten MX-Eintrag erkennbar wird, welcher Mailserver beispielsweise für *empfaenger-domain.ch* zuständig ist. Der Versandserver nimmt darauf mit dem Empfangsserver Kontakt auf und klopft so an die erste Tür. Sollte der Empfangsserver kurzfristig nicht erreichbar sein, werden in der Regel automatisch weitere Versuche unternommen, bevor die Adresse als «nicht erreichbar» eingestuft wird.

Ankunft beim Empfangsserver

Der Empfangsserver wird als erstes darüber informiert, wer eine Nachricht an wen zustellen möchte. Der gesamte folgende Prozess ist vom Absender nun technisch nicht mehr nachträglich beeinflussbar und von der Infrastruktur auf der Empfängerseite abhängig. Auch wenn die Reihenfolge unterschiedlich ist, ähnelt der Prozess der Einlasskontrolle einer Diskothek und verläuft etwa nach folgendem Schema:

Greylisting: Wer neu ist, wird zunächst abgewiesen

Ein erster Schutzmechanismus von E-Mail-Providern ist das sogenannte Greylisting (oftmals bei Outlook der Fall). Dabei wird der erste Zustellversuch eines Absenders absichtlich abgewiesen und erst die folgenden Versuche angenommen. Der Grund darin liegt in der Praxis von Spam-Bots, die aufgrund des hohen Versandvolumens und des begrenzten Einsatzzeitraums ihres Servers nur Ressourcen für einen Zustellversuch aufbringen. Bei seriösen Versanddienstleistern sind indes mehrere Zustellversuche die Regel. Das Greylisting ist deshalb in der Regel unproblematisch, es führt allerdings zu einer kurzen Verzögerung der Zustellung.

Throttling: Schutz vor den Massen

Vor allem bei grösseren E-Mail Providern findet das «Throttling» Anwendung. Dabei wird die Anzahl von E-Mails eines bestimmten Absenders oder Versandservers beschränkt, welche in einem definierten Zeitraum angenommen werden. Befinden sich in der Empfängerliste eines Versandes also beispielsweise viele Adressen mit derselben Domain, wie z.B. *bluewin.ch*, kann das Throttling greifen. Dies allein ist oftmals aber noch kein Grund, E-Mails komplett abzuweisen, die Zustellung wird nach einem bestimmten Zeitraum fortgesetzt. Bei zeitkritischen E-Mails kann das zu weilen problematisch sein. Werden unter diesen E-Mails allerdings zu viele «Hardbounces» (unzustellbare E-Mails) generiert, kann die Annahme weiterer E-Mails komplett ausgesetzt werden.

Verifizierung: Die Ausweiskontrolle

Nach den ersten vorgeschalteten Schutzmechanismen analysiert der Empfangsserver jetzt den Absender. Dabei geht es nicht nur um die sichtbare (FROM) Absender-Adresse (die ja bekanntlich frei definiert werden kann), sondern um den effektiven Versender, was mittels verschiedener Verfahren überprüft wird. Dazu zählen beispielsweise SPF, DKIM und DMARC (siehe Box). Eine negative Beurteilung in einem dieser Verfahren führt normalerweise dazu, dass die E-Mail abgewiesen oder zumindest als «verdächtig» markiert wird.

SPF

(Sender Policy Framework)

- Verfahren gegen gefälschte Absender-Adressen
- Domain-Inhaber legt per DNS-Eintrag fest, welche Server Mails versenden dürfen.

DKIM

(DomainKeys Identified Mail)

- Ergänzt E-Mails mit einer
- digitaler Signatur.
- Empfangsserver prüft Signatur über DNS, bestätigt Absender-Authentizität.

DMARC

(Domain-based Message Authentication)

- Baut auf SPF und DKIM auf.
- Prüft Übereinstimmung mit sichtbarer FROM-Adresse und legt Vorgehen bei Fehlern fest (z.B. Quarantäne/Ablehnung).

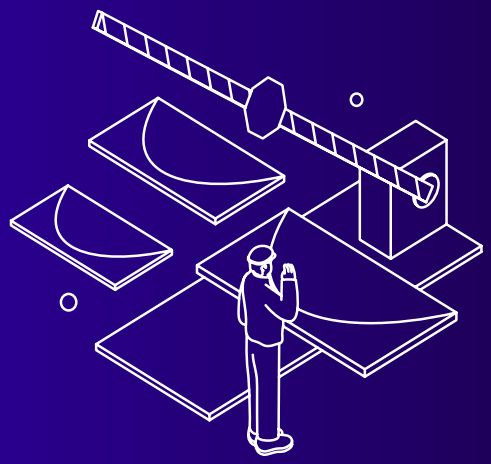
Hürden auf dem Weg in die Inbox.



Vereinfachte Darstellung einer möglichen E-Mail Reise

Neue Anforderungen an den E-Mail-Versand ab 2024 bei Google und Yahoo

Seit Februar 2024 haben Google und Yahoo neue verbindliche Anforderungen für den Massenversand von E-Mails eingeführt (=mehr als ca. 5'000 E-Mails täglich).
Ziel ist es, die Authentizität und Sicherheit des E-Mail-Verkehrs zu verbessern sowie den Missbrauch durch Spam und Phishing zu reduzieren. Seit April 2025 hat Microsoft ähnliche Anforderungen eingeführt.



Verpflichtende DMARC-Implementierung

Ab dem genannten Zeitpunkt ist die korrekte Implementierung von DMARC (Domain-based Message Authentication, Reporting & Conformance) für Absender mit hohem E-Mail-Volumen obligatorisch. DMARC sorgt dafür, dass empfangende Mailserver überprüfen können, ob eingehende Nachrichten tatsächlich vom angegebenen Absender stammen und der Inhalt nicht verändert wurde. Dabei wird auch geprüft, dass die SPF und DKIM Checks mit der sichtbaren (FROM) Absender-Adresse übereinstimmt. Dies ist ein wichtiger Schutzmechanismus gegen Spoofing.

Pflicht zum List-Unsubscribe-Header

Zusätzlich müssen alle E-Mails, die an grosse Empfängerlisten gesendet werden, einen gültigen List-Unsubscribe-Header enthalten. Dieser erlaubt es Empfängern, sich einfach und zuverlässig aus dem Verteiler auszutragen.

Grenzwerte für Bounce- und Spam-Raten

Um die Reputation der eigenen E-Mail-Domain zu wahren und die Zustellbarkeit sicherzustellen, müssen bestimmte Schwellenwerte eingehalten werden:

- Bounce-Rate: dauerhaft deutlich unter 3 %
- Spam-Beschwerden: unter 0,3 %

Überschreitungen dieser Werte können zur Einstufung als Spam-Absender führen und dazu, dass E-Mails nicht mehr zuverlässig zugestellt werden.

TLS-Verschlüsselung als Standard

Schliesslich ist auch die Transportverschlüsselung per TLS (Transport Layer Security) nun verpflichtend. Nur verschlüsselte Übertragungen gewährleisten den Schutz sensibler Inhalte während des Versands und verhindern Manipulationen oder unbefugten Zugriff auf dem Transportweg.

Whitelist: Separater Eingang für VIPs

Eine E-Mail eines verifizierten Absenders wird bei manchen E-Mail-Anbietern mit einer sogenannten Whitelist abgeglichen. Bekannte Whitelists sind beispielsweise die «Certified Senders Alliance» (CSA) und «Return Path», wobei der Fokus derartiger Whitelists oft auf bestimmten geografischen Gebieten liegt. Um als Versender in eine solche Whitelist aufgenommen zu werden, sind sowohl technische als auch rechtliche Voraussetzungen zu erfüllen und strenge Anti-Spam Richtlinien einzuhalten. Seriöse Versanddienstleister bekennen sich zu diesen Anti-SPAM Richtlinien und binden ihre Kunden in die Verantwortung ein.

Ist der Absender auf einer solchen Whitelist verzeichnet, muss die E-Mail serverseitig keinen weiteren Spam-Checks mehr standhalten. Allerdings setzen nicht alle E-Mail Provider solche Whitelists ein, Gmail von Google ist hierbeispielsweise allen voran zu erwähnen.

Blacklist: Schwarze Schafe bleiben Draussen

Um Empfänger von unseriösen Versendern zu schützen, nutzen praktisch sämtliche E-Mail Provider öffentliche und selbst aufgebaute «Blacklists». Wer als Versender auf eine solche Blacklist gerät, hat jenach Verbreitungsgrad dieser Blacklist ein kleines oder aber sehr grosses Problem. In der Folge werden bei allen Servern, welche diese Blacklist «anzapfen», alle E-Mails des entsprechenden Versenders aussortiert. Von einer Blacklist wieder entfernt zu werden, kann sich unter Umständen als schwierig erweisen. Eine Begründung ist i.d.R. Pflicht, manchmal werden gar Gebühren verlangt. In jedem Fall dauert es aber mehrere Stunden oder gar Tage, bis ein Versender wieder von der Liste gestrichen wird. Die Folgen können gravierend sein, wenn der Versender z.B. die selbe Infrastruktur auch zum Versand von Offerten, Bestellbestätigungen und anderen wichtigen Inhalten nutzt.

SPAM-CHECK - Die Spreu vom Weizen trennen.

Wenn die E-Mail weder von der White- noch Blacklist aufgegriffen wird, folgt eine Überprüfung und Bewertung durch verschiedene Algorithmen. Der Berechnung der Reputation fällt dabei meist die grösste Bedeutung zu. Haben sich beispielsweise bereits viele Benutzer über die E-Mails eines Absenders beschwert, schadet dies der Reputation. Gleiches gilt, wenn bei einem E-Mail Provider viele sogenannte Bounces anfallen, also E-Mails an Adressen, die nicht (mehr) existieren.

Spam-Traps: Agenten in Zivil

Einen äusserst hohen Reputationsverlust erleidet ein Versender, der eine E-Mail-Adresse anschreibt, hinter der sich eine «Spam-Trap» verbirgt. Spam-Traps sind E-Mail-Adressen, die von E-Mail-Providern oder Blacklist-Betreibern absichtlich erstellt, aber nicht zur Kommunikation benutzt werden. Der Gedanke dahinter: Niemand kann Kenntnis von einer solchen Adresse haben, es sei denn, er hat diese mit Hilfe von «Bots» auf einer Website entdeckt und kopiert oder von einer dubiosen Quelle in einer Liste eingekauft. Wer also eine E-Mail an eine solche Adresse schickt, hat mit Sicherheit unseriös gehandelt. Deshalb gilt: Niemals E-Mail-Adressen einkaufen oder kopieren!

Inhaltsüberprüfung: Ist die Garderobe angemessen?

Während bislang hauptsächlich der Absender und die Header-Informationen des E-Mails verifiziert wurden, muss das E-Mail als nächstes serverseitige Spamfilter passieren, die den Inhalt des E-Mails analysieren. Die hierbei eingesetzte Software und individuelle Regeln sind so vielfältig, dass es kaum möglich ist, allgemein gültige Regeln zu formulieren. Man kann lediglich davon ausgehen, dass eine E-Mail umso eher als «Spam» definiert wird, je mehr sie einer E-Mail reputationskritischer Branchen oder Praktiken gleicht. Bestimmte Schlüsselwörter, Häufung von Sonderzeichen und Grossbuchstaben usw. sind mögliche Faktoren, die den Spamverdacht aus Softwaresicht erhöhen.

Virenscan: Taschenkontrolle

Bevor eine E-Mail auf dem Server gespeichert wird, wird es auf jeden Fall auf seine Schädlichkeit überprüft. Die Anhänge werden durchleuchtet und mit bekannten Schädlingen abgeglichen. Kritische Dateiformate werden teilweise direkt ausgesondert.

URSACHENANALYSE

Weshalb ist die E-Mail hängen geblieben?

Ab dem Zeitpunkt, an dem der Empfangsserver die E-Mail annimmt, ist aus Versendersicht der Ereignishorizont erreicht. Der weitere Prozess der Überprüfung ist für den Absender technisch nicht erkennbar, was eine Analyse sehr schwierig macht.

Zustellbarkeit analysieren

Dennoch gibt es Wege, um die Zustellbarkeit zu prüfen. Tools wie «Litmus» oder «E-Mail on Acid» führen Spamtests durch, indem sie eine E-Mail an verschiedene Anbieter senden und die Zustellung auswerten. Manche Filter zeigen nur das Ergebnis, andere erklären auch die Gewichtung einzelner Faktoren. Solche Tests liefern nützliche Hinweise, ersetzen aber keine Beurteilung im Echtbetrieb. Sie eignen sich jedoch gut, um technische Schwachstellen frühzeitig zu erkennen.

Vorsicht

Trotz allem ist diesen Tools mit Vorbehalt zu vertrauen, da sie nur ein einzelnes E-Mail prüfen und nicht die Effekte eines Massenversands. Zudem berücksichtigen sie oft Provider, die für die Schweiz kaum relevant sind. Ihre Resultate sind hilfreich zur Orientierung, ersetzen jedoch keine eigene Zustellanalyse unter realen Bedingungen. Ein kontinuierliches Monitoring über verschiedene Kampagnen hinweg liefert deutlich aussagekräftigere Ergebnisse.

ANKUNFT - Fast am Ziel, aber nur fast!

Hat die E-Mail allen serverseitigen Überprüfungen standgehalten, wird es an den Empfänger ausgeliefert. Damit sind aber noch nicht alle Hürden überwunden. Viele Empfänger haben clientseitig weitere Spamfilter und Posteingangsregeln definiert, die teilweise einer eigenen Logik folgen. Bleibt eine E-Mail in einem solchen lokalen Spamfilter hängen, ist sie normalerweise zumindest im SPAM-Ordner noch abrufbar. Wenn der Benutzer diese findet und in den Posteingang bewegt, wird die nächste E-Mail gleicher Art möglicherweise direkt in den Posteingang zugestellt.

Es kommt durchaus vor, dass ein Empfänger Sie als Absender darüber informiert, dass Ihre E-Mail bei ihm im Spam-Ordner gelandet ist. Nutzen Sie diese wertvolle Information, lassen Sie sich die E-Mail weiterleiten und analysieren Sie intern oder gemeinsam mit Ihrem Versanddienstleister, was dazu geführt haben könnte. Lässt sich der Empfänger überzeugen, die Absender-Adresse zum Adressbuch hinzuzufügen, als VIP zu markieren o.ä., braucht man in Zukunft zumindest diese Hürde nicht mehr zu fürchten. Dann steht die Inbox auf Empfang.

SO FUNKTIONIEREN BLACKLISTS

Die Betreiber von Blacklists verfolgen verschiedene Ansätze zur Beurteilung von unerwünschten E-Mails und stellen diese sowohl E-Mail- Providern, als auch Unternehmen kostenlos oder gegen Gebühr zur Verfügung. Dafür werden die Blacklists in Echtzeit aktualisiert, basierend auf der Auswertung einer unvorstellbaren Datenmenge.

Es existieren mehrere Hundert Blacklist-Betreiber, bekannt sind beispielsweise Spamhaus, SpamCop und URIBL. Grundsätzlich unterscheidet man zwischen zwei Arten von Blacklists:

IP-basierte Blacklists

IP-basierte Blacklists erfassen Versandserver, von denen mutmasslich unerwünschte E-Mails versendet werden. Dazu zählen Server, die viele Beschwerden verursachen, ungesichert sind (offenes Relay) oder an Spamtraps gesendet haben.

Die Sperrung ist oft nur temporär. Ein «Delisting», also das Entfernen des eigenen Servers von der Blacklist, ist in der Regel nach dem Nachweis entsprechender Korrekturmassnahmen möglich. In gravierenden Fällen bleibt nur der Wechsel der IP-Adresse. Ein regelmässiges Monitoring hilft, Probleme frühzeitig zu erkennen und die Zustellbarkeit langfristig zu sichern.

Zudem ist eine klare Trennung von Versandumgebungen für Marketing- und Transaktionsmails empfehlenswert, um Risiken zu minimieren. Eine sorgfältige technische Konfiguration bildet dabei die Grundlage für nachhaltigen Versand-Erfolg.

Domain-basierte Blacklists

Domain-basierte Blacklists analysieren den Inhalt von E-Mails und die darin enthaltenen Links. Ziel ist es, die Nutzniesser unerwünschter Nachrichten zu treffen, da diese meist eine URL im Text platzieren. Auch Weiterleitungen werden erkannt und blockiert.

Eine «false positive», also eine irrtümlich schädliche Einstufung der eigenen Domain, kann gravierende Folgen haben: Selbst legitime E-Mails werden nicht mehr zugestellt, etwa wenn die Domain im Footer steht. Das Delisting ist schwierig, besonders wenn der Provider die Blacklists nicht offenlegt. Echtzeit-Monitoring ist unerlässlich, um schnell reagieren zu können.

Eine regelmässige Überprüfung der verwendeten Domains und Links reduziert das Risiko solcher Falschmeldungen deutlich. Ergänzend trägt eine saubere Linkstruktur in allen E-Mail-Vorlagen zur langfristigen Reputation der Absenderdomain bei.

Die 8 Erfolgsfaktoren der Zustellbarkeit im E-Mail-Marketing

Nur «saubere» Datenquellen

Versenden Sie E-Mails nur mit Double-Opt-in oder bei aktiver Geschäftsbeziehung.



#1



Listenhygiene

Versenden Sie keine E-Mails an mehrfach zurückgewiesene oder veraltete Adressen.

#2

Bereit zur Verifizierung

Setzen Sie SPF, DKIM und DMARC für sichere und verifizierte Zustellung ein.



#3



Dedizierte Versand-IP-Adresse

Nutzen Sie eine eigene Versand-IP, um Ihre Zustellrate unabhängig von anderen zu sichern.

#4



Gut sichtbare Abmeldemöglichkeiten

Leicht auffindbare Ein-Klick-Abmeldung, verhindert Spam-Markierungen und Zustellprobleme.



#5



Transparenz

Ein vollständiges Impressum im Footer schafft Vertrauen und erfüllt CSA-Richtlinien.

#6

Eigene Blacklist

Tragen Sie Abmeldewünsche in eine Blacklist ein, um versehentliche Kontakte zu vermeiden.



#7



Problematische Inhalte vermeiden

Klare Sprache, ausgewogenes Design und transparente Absenderinformationen verbessern Ihre Zustellrate.

#8

©2022-2026 by mailXpert GmbH.
mailXpert ist ein führender Schweizer Versanddienstleister mit Fokus auf E-Mail Marketing.
Der Autor Patrick Gsell ist Product Owner und Geschäftsführer.