mailXpert

WHITE PAPER

Die Erfolgsfaktoren der Zustellbarkeit im E-Mail-Marketing.

Die lange Reise einer E-Mail.

Bevor eine E-Mail beim Empfänger die gewünschte Wirkung erzielen kann, gilt es, erst mal bis in dessen Inbox zu gelangen. Der Weg dorthin ist weiter als gemeinhin angemommen: Auf ihrer Reise hat die E-Mail eine ganze Reihe von Hürden zu überwinden, die sowohl für den Absender als auch den Empfänger normalerweise unsichtbar sind.

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 dem folgenden Schema:

Greylisting: Wer neu ist, wird zunächst abgewiesen

Ein erster Schutzmechanismus von E-Mail-Providern ist das sogenannte Greylisting. 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 zuweilen 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...
steht für *Sender Policy Framework* und ist ein Verfahren, dass die Fälschung der Absender-Adresse einer E-Mail verhindern hilft. Dabei bestimmt der Inhaber einer Domain mittels DNS-Eintrag, welche Server für den Versand von E-Mails mit dieser Absenderdomain zulässig sind.

DKIM...
steht für *DomainKeys Identified Mail* und ergänzt E-Mails mit einer digitalen Signatur, die vom Empfangsserver über den DNS-Eintrag verifiziert werden kann. Damit wird die Authentizität des Absenders sichergestellt.

DMARC...
steht für *Domain-based Message Authentication, Reporting & Conformance* und baut auf SPF und DKIM auf resp. ergänzt diese um Anweisungen, wie die Authentifizierung genau erfolgen soll.

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 hier beispielsweise 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 je nach 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.

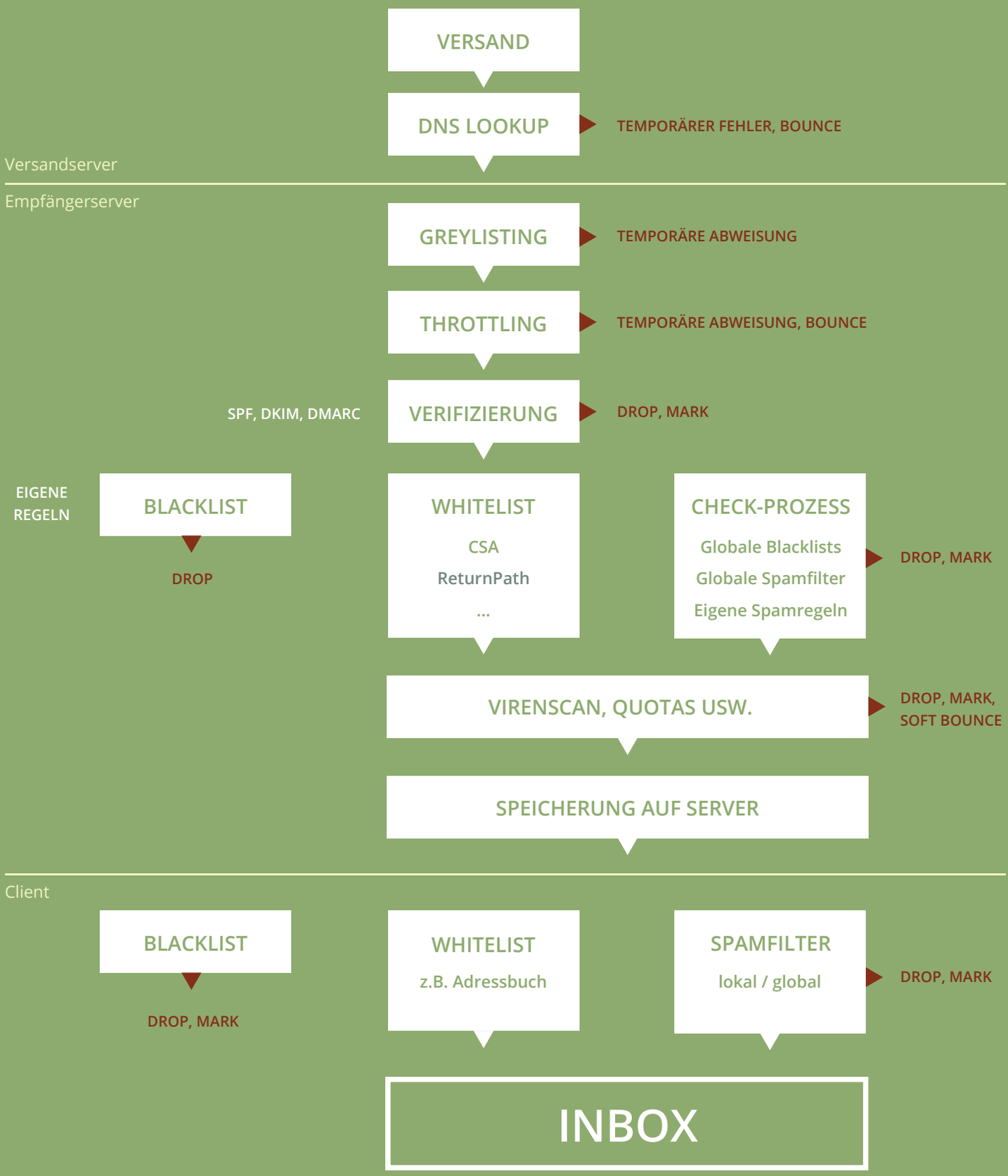
Ursachenanalyse: Weshalb ist die E-Mail hängen geblieben?

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.

Dennoch gibt es Wege oder zumindest Anhaltspunkte, um die Zustellbarkeit zu ermitteln. Tools wie «Litmus» oder «E-Mail on Acid» führen solche Spamtests durch. Dabei wird eine E-Mail an dutzende von E-Mail-Adressen bei verschiedenen E-Mail Anbietern versendet und analysiert, ob und wie diese zugestellt werden. Manche Spamfilter verraten nur die endgültige Bewertung (Spam/kein Spam), andere sind auskunftsfreudiger und legen dar, welche Faktoren wie stark gewichtet wurden.

Trotz allem ist diesen Tools mit Vorsicht zu vertrauen, weil sie ein einzelnes E-Mail und nicht die Folgen eines Massenversandes analysieren und zudem meist E-Mail-Provider analysieren, die für die schweizerischen Gegebenheiten beschränkt relevant sind.

Hürden auf dem Weg in die Inbox.



Vereinfachte Darstellung einer möglichen E-Mail Reise.

sind mögliche Faktoren, die den Spamverdacht aus Softwaresicht erhöhen.

Virenscan: Tascheninspektion
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.

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
Die IP-basierten Blacklists melden alle Versandserver, von denen mutmasslich unerwünschte E-Mails verschickt werden. Dazu werden Server gezählt, die viele Beschwerden durch Benutzer hervorrufen, Server die ungesichert scheinen (offenes Relay) oder solche, die an eine Spamtrap verschickt haben.

Die Sperrung ist teilweise nur temporärer Natur. Ein «Delisting», also das Entfernen des eigenen Servers von der Blacklist ist meist möglich bei Nachweis von entsprechenden Massnahmen. Im schlimmsten Fall muss die IP-Adresse des Versandservers gewechselt werden.

Domain-basierte Blacklists
Domain-basierte Blacklists gründen auf der Analyse des Inhalts von E-Mails und darin vorkommender Links. Die Absicht zielt darauf, die Nutzniesser von unerwünschten E-Mails zu treffen, da diese im E-Mail meistens irgendwo eine URL hinterlegt haben, worauf der Empfänger geführt werden soll. Auch Weiterleitungen werden erkannt und E-Mails mit entsprechenden Links gesperrt.

Ein «false positive», also eine irrtümlich schädliche Interpretation der eigenen Domain ist besonders ärgerlich: Kunden könnten auch normale Geschäfts-E-Mails nicht mehr erhalten, wenn die Domain beispielsweise im persönlichen Footer Ihrer E-Mails enthalten ist. Das Delisting kann sich vor allem dann als schwierig erweisen, wenn ein E-Mail Provider nicht bekannt gibt, welche Blacklists er einsetzt.

Ein Blacklist-Monitoring in Echtzeit durch den Versanddienstleister ist unverzichtbar, um schnell auf derartige Vorkommnisse reagieren zu können.

Ihr Anteil am Erfolg als Versender.

Regel Nr. 1: Nur «saubere» Datenquellen
Verwenden Sie nur E-Mail-Adressen von Empfängern, die Ihnen diese selbständig, willentlich und transparent zu diesem Zweck zur Verfügung gestellt haben oder mit denen Sie in einer aktiven Geschäftsbeziehung stehen. Wenn Sie eine Anmeldung via Website/Microsite bereitstellen, muss diese in jedem Fall im «double-opt-in» Verfahren erfolgen. Versenden Sie niemals E-Mails an eingekaufte oder von einer sonstigen Quelle kopierte E-Mail-Adressen. Die Folgen können rechtlich und finanziell verheerend sein!

Regel Nr. 2: Listenhygiene
Versenden Sie keine E-Mails an ungültige Adressen (Bounces) von denen Sie mehr als einmal die Rückmeldung erhalten haben, dass die Adresse nicht existiert. Die meisten Versandtools übernehmen das für Sie bei entsprechender Konfiguration automatisch. Widerstehen Sie deshalb auch der Versuchung, «eine alte Liste» als Datenquelle zu verwenden.

Regel Nr. 3: Seien Sie bereit für die Verifizierung
Nutzen Sie die Verfahren SPF, DKIM und DMARC zu Ihrem Vorteil. Setzen Sie die technischen Anforderungen zusammen mit Ihrem IT- sowie Ihrem Versanddienstleister um. Einmaliger Aufwand - fortwährende Sicherheit!

Regel Nr. 4: Dedizierte Versand-IP-Adresse
Bei den meisten Versandtools teilen Sie die Versand-IP mit anderen Parteien. Das kann dazu führen, dass sich Reputationsprobleme anderenorts auf Ihren Versand auswirken können. Wenn sie die Möglichkeit haben, über eine exklusiv für Sie bereitgestellte IP-Adresse zu versenden, sollten Sie diese wahrnehmen.

Regel Nr. 5: Gut sichtbare Abmeldemöglichkeit
Bieten Sie dem Empfänger jederzeit eine einfache und klar ersichtliche Abmeldemöglichkeit. Diese zu verstecken ist kontraproduktiv: Je nach E-Mail-Provider wird er möglicherweise auf einen Button im Sinne von «als SPAM markieren» klicken, was sich dann auf die Zustellbarkeit der anderen E-Mails auswirkt. Die Abmeldung sollte ausserdem in einem Schritt erfolgen («single-opt-out»).

Regel Nr. 6: Transparenz
Geben Sie sich klar zu erkennen: Wer verschickt diese E-Mail? Ein vollständiges Impressum im Footer (besser als nur ein Link) schafft Vertrauen und entspricht dem Manifest für seriöses E-Mail-Marketing der Certified Senders Alliance (CSA).

Regel Nr. 7: Eigene Blacklist
Trotz aller Sorgfalt kommt es manchmal vor, dass sich ein Empfänger per E-Mail oder telefonisch erbost bei Ihnen meldet und keinesfalls mehr kontaktiert werden möchte. Respektieren Sie dies unbedingt und tragen Sie die entsprechende E-Mail-Adresse in eine eigene Blacklist ein, wie sie die meisten Versandtools bereitstellen. Damit stellen Sie sicher, dass der Kontakt bei erneutem Kontaktimport o.ä. nicht versehentlich wieder angeschrieben wird.

Regel Nr. 8: Marktschrei vermeiden
Auch wenn Ihre Produkte, Dienstleistungen und Neuigkeiten toll sind: Verzichten Sie auf zu viel Werbesprache im E-Mail (dazu gehört auch der Betreff) und tragen Sie nicht zu dick auf (viele Ausrufezeichen, Grossbuchstaben). Widerstehen Sie auch der Versuchung, im Betreff besonders ausgefallen Neugier zu erwecken, denn Spammer versuchen genau dasselbe.

mailXpert ist ein führender Schweizer Versanddienstleister mit Fokus auf E-Mail Marketing & Automation.
Der Autor Patrick Gsell ist Product Owner und Geschäftsführer.