

## DMARC und Domain Alignment im E-Mail-Marketing

### Vertrauen ist die beste Basis

Es läuft nicht immer alles rund im Internet. Spam, Phishing, Man in the Middle Attacken, Spoofing, die Liste der Bösewichte im Netz und ihrer ausgefeilten Methoden ist lang. Und in fast allen Fällen ist ein Medium beteiligt, das wir alle täglich nutzen, die E-Mail. Dabei nutzen Cyberkriminelle aus nachvollziehbaren Gründen nicht ihre eigene Identität als Absender. Vielmehr bedienen sie sich gerne bei renommierten Unternehmen und Marken, oft bei Banken, Payment-Diensten, Online-Shops oder Zustellfirmen. Grundsätzlich kann es aber jede Marke treffen.

Die Vielzahl an Fallen und Fallstricken macht misstrauisch. So misstrauisch, dass viele Internet Service Provider (ISPs) eine Mail genau prüfen, bevor sie diese an ihre Kunden, die Mailempfänger, weiterleiten. Insbesondere kleinere ISPs gehen sogar so weit, zunächst einmal alle eingehenden Mails abzuweisen und einen Bounce Code zurückzugeben, darauf hoffend, dass seriöse Versender einen zweiten Zustellversuch starten (Greylisting). Andere ISPs verlangen Authentifizierungsmaßnahmen der Mailversender oder die Zertifizierung der Mailversender auf einer Whitelist (zum Beispiel bei der Certified Senders Alliance CSA), um E-Mails zuzustellen.

Für Brands ist das ein Problem. Denn sie haben ja ein großes Interesse daran, dass ihre Mails auch den Adressaten erreichen. Der große Türöffner bei den ISPs ist Vertrauen. Stufen ISPs einen Mailversender als vertrauenswürdig ein, ist die Wahrscheinlichkeit sehr groß, dass die Mail auch im Posteingang zugestellt wird. Dieses Vertrauen, das Tobias Herkula, Manager Anti Spam Research Team bei Cyren, als „Computational Trust“ bezeichnet, muss man sich aber erst einmal verdienen. Und hier kommt das sogenannte Domain Alignment ins Spiel. Domain Alignment bedeutet, dass die in SPF (Sender Policy Framework) und DKIM (DomainKeys Identified Mail) verwendeten Domains zumindest teilweise mit der From Adresse der Mail übereinstimmen müssen. Für weitere Informationen bezüglich Protect Brand Identity in Email siehe [hier](#). SPF und DKIM sind gängige Spezifikationen zur Mail Authentifizierung und die From-Adresse ist die Mailadresse, die dem Empfänger der Mail als Absenderadresse angezeigt wird. Einfach gesagt, bei einem klassischen Papierbrief würden die Absenderadresse auf dem Umschlag, der Absender auf dem Brief, als auch die Unterschrift unter dem Brief

übereinstimmen. Eigentlich ist das selbstverständlich, oder würden Sie einem Brief vertrauen, bei dem auf Umschlag und Brief unterschiedliche Adressen angegeben sind?

Ganz so einfach ist es bei E-Mails allerdings nicht, denn viele Marketeers greifen bei ihren Mailings auf externe Dienstleister, die E-Mail-Service-Provider (ESP) zurück. Und spätestens dann stimmen die From-Adresse im Header der Mail und die physikalische Adresse nicht mehr überein und das Domain Alignment ist nicht mehr gegeben.

Domain Alignment ist aber auch zwingende Voraussetzung für die Implementierung von DMARC (Domain-based Message Authentication, Reporting and Conformance), einem weiteren Authentifizierungsverfahren, das von vielen großen ISPs wie beispielsweise AOL, Microsoft oder Google unterstützt wird. DMARC basiert auf den gängigen Spezifikationen SPF und DKIM und macht Mails damit für ISPs klar identifizierbar. Zusätzlich kann der Versender (die Marke) festlegen, wie der ISP Mails handhaben soll, die nur scheinbar von ihm stammen.

Fazit: Für Marketeers im E-Mail-Marketing ist eine gute Reputation und damit Vertrauenswürdigkeit enorm wichtig, denn sie hat direkten Einfluss auf die Zustellbarkeit von E-Mails. Durch die Implementierung von DMARC und das damit verbundene Domain Alignment können Brands sicherstellen, dass ihre Identität nicht missbraucht wird und damit großer Schaden an der Markenreputation entsteht. Marketeers im Bereich E-Mail-Marketing sollten daher das Thema DMARC mit ihrem E-Mail Service Provider besprechen. Nähere Informationen zu DMARC und Domain Alignment gibt es auch bei der Certified Senders Alliance unter <https://certified-senders.org/library/>.

*Autor: Sebastian Kluth, Technical Lead CSA*