Domain-Alignment bei E-Mail Authentifizierung

Für den professionellen E-Mail Versand ist Authentifizierung unbedingt nötig. Wer über SPF und DKIM hinaus DMARC einsetzen möchte, muss zwingend Alignment erfüllen. Doch selbst ohne DMARC ist Alignment ein richtiger und wichtiger Schritt zu einer authentifizierten E-Mail.

Was ist Domain Alignment?

Um Alignment zu erklären muss man ein klein wenig ausholen. E-Mails haben immer zwei Absenderadressen. Zum einen die Absenderadresse, die dem Nutzer in seinem E-Mail Programm angezeigt wird. Hier spricht man von der RFC5322.From Adresse, oder einfacher auch „header from" oder „friendly from". Zum anderen gibt es den RFC5321.MailFrom, welcher in der SMTP-Kommunikation verwendet wird. Diese Adresse wird oft auch Envelope-From oder MFROM genannt und ist im Header der E-Mail als „Return-Path" gespeichert.

Der Einfachheit halber sprechen wir im Folgenden von „From" wenn wir RFC5322.From meinen, bzw. vom „Return-Path" wenn der RFC5321.MailFrom gemeint ist.

Man kann sich das ähnlich vorstellen wie bei einem klassischen Papierbrief. Der „From" ist der Autor, der auf dem eigentlichen Brief angegeben ist. Der „Return-Path" ist der Absender auf dem Umschlag, in dem der Brief versendet wird.

Damit ist auch klar, wer den Brief zurückerhält, falls er nicht zugestellt werden kann. Bei der E-Mail ist es nicht anders. Eine Benachrichtigung, dass eine E-Mail nicht zugestellt werden konnte (auch bekannt als Bounce) geht an den „Return-Path" zurück.

Alignment bezeichnet die Ausrichtung der in den beiden Techniken Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) verwendeten Domains an der From-Adresse, so dass diese zumindest teilweise übereinstimmen. Bei einer sogenannten „strict" policy muss die Domain vollständig übereinstimmen, bei einer „relaxed" policy reicht eine Übereinstimmung auf Level der organisatorischen Domain.

Beim SPF-Alignment muss die Übereinstimmung zwischen dem Return-Path und dem From gegeben sein. Beim DKIM-Alignment ist die Übereinstimmung zwischen dem d-Parameter der DKIM-Signatur (einfacher ausgedrückt: der DKIM-Domain) und dem From erforderlich.

Beispiel:

DKIM d-Parameter: example.com
From: info@news.example.com
Return-Path:
20180816094418 43e6b1a4b6e54342ab2e11b9e290p0eu@bounces.news.example.com

Bei einer relaxed policy, die dem Standard entspricht, liegt in diesem Beispiel sowohl SPF- als auch DKIM-Alignment vor. Alle drei Werte lauten auf die organisatorische Domain „example.com". Bei einer strict policy wäre kein Alignment gegeben, da keine exakte Übereinstimmung vorliegt, sondern Subdomains verwendet werden.

Warum ist Alignment wichtig?

Besonders dann, wenn man seine E-Mails nicht selbst versendet, sondern einen Dienstleister, z.B. einen E-Mail Service Provider (ESP) hinzuzieht, kann es auf den ersten Blick durchaus legitim sein, dass kein Alignment vorliegt. Der Return-Path verweist auf die Infrastruktur des ESPs, wobei der From auf den Brand verweist, der für den Inhalt der E-Mails verantwortlich ist.

Wenn man allerdings betrachtet, wofür die E-Mail Authentifizierungstechniken SPF, DKIM und Domain-based Message Authentication, Reporting and Conformance (DMARC) eingeführt worden sind ist klar, dass der Absender nur dann als authentisch betrachtet werden kann, wenn From und Return-Path, sowie die DKIM-Domain übereinstimmen.
Wenn wir uns wieder dem Beispiel mit einem Papierbrief bedienen, wird das noch deutlicher: Man würde einen Brief vermutlich nicht als vertrauenswürdig erachten, wenn sich der Absender auf dem Briefumschlag (der Return-Path), der Absender/Autor im Brief (der From) und eine abschließende Unterschrift unter dem Brief (die DKIM-Domain) alle voneinander unterscheiden.

DMARC setzt bekanntermaßen auf SPF und DKIM. Es reicht allerdings nicht aus, beim Empfänger nur die SPF und/oder DKIM Prüfung zu bestehen. Es muss darüber hinaus ein

Alignment bestehen, damit DMARC als bestanden gilt. Auch wenn es reicht, SPF oder DKIM korrekt implementiert zu haben und im Endeffekt nur bei SPF oder DKIM Alignment gegeben sein müsste, erhöht man die Fehlertoleranz bei DMARC natürlich deutlich, wenn man sowohl SPF als auch DKIM implementiert und bei beiden Alignment gegeben ist.

Fazit

Spätestens wenn man DMARC einsetzen möchte, ist Alignment zwingend nötig. Wenn man den technischen Versand nicht selbst machen möchte und sich lieber auf einen professionellen ESP als Dienstleister verlässt, ist das zweifelsohne am einfachsten zu erreichen, wenn man als Domaininhaber eine Subdomain-Delegation an den ESP durchführt. Dieser kann dann alle Authentifizierungstechniken vollständig kontrollieren und auch das Alignment sicherstellen.

Autor: Alexander Zeh, Engineering Manager, Certified Senders Alliance