DMARC-Architektur - Identifikatorausrichtung

Inhalt

[Einführung](#)
[Terminologie](#)
[DMARC = Identifier Alignment](#)
[Bezeichner](#)
[Identifikatorausrichtung](#)
[DKIM-Ausrichtung](#)
[SPF-Ausrichtung](#)
[Tags des Ausrichtungsmodus](#)
[Referenz](#)

Einführung

In diesem Dokument werden allgemeine Architekturkonzepte für die domänenbasierte Message Authentication, Reporting and Conformance (DMARC) sowie Anforderungen an die Abstimmung von Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) in Bezug auf DMARC beschrieben.

Terminologie

In diesem Abschnitt werden einige der in diesem Dokument verwendeten Schlüsselbegriffe beschrieben und definiert.

- **EHLO/HELO** - Die Befehle, die die Identität eines SMTP-Clients während der Initialisierung einer SMTP-Sitzung gemäß RFC 5321 bereitstellen.
- **Von-Header** - The From: gibt den oder die Autoren einer Nachricht an. In der Regel enthält er den Anzeigenamen (was einem Endbenutzer vom Mail-Client angezeigt wird) sowie eine E-Mail-Adresse, die einen lokalen Teil und einen Domänennamen (z. B. "John Doe" <johndoe@example.com>) gemäß RFC 5322 enthält.
- **MAIL FROM** - Dies wird vom MAIL-Befehl zu Beginn einer SMTP-Sitzung abgeleitet und stellt die Absenderkennung gemäß RFC5321 bereit. Er wird auch als Umschlagabsender, Rückgabepfad oder Bounce-Adresse bezeichnet.

DMARC = Identifier Alignment

DMARC verknüpft die DKIM- und SPF-Authentifizierung mit der im Von-Header aufgeführten Authentifizierung. Dies erfolgt durch *Ausrichtung*. Die Ausrichtung erfordert, dass die von SPF und DKIM authentifizierte Domänenidentität der Domäne in der für den Endbenutzer sichtbaren E-Mail-Adresse entspricht.

Beginnen wir mit dem Bezeichner und dessen Bedeutung für DMARC.

Bezeichner

Identifikatoren identifizieren einen Domänennamen, der authentifiziert werden soll.

Identifikatoren in Bezug auf DMARC:

- SPF:

  SPF authentifiziert die Domäne, die entweder im Abschnitt MAIL FROM oder EHLO/HELO der SMTP-Konversation oder in beiden angezeigt wird. Dabei kann es sich um unterschiedliche Domänen handeln, die für den Endbenutzer in der Regel nicht sichtbar sind.

- DKIM:

  DKIM authentifiziert die Signaturdomäne, die an einer Signatur innerhalb des *d*=Tags befestigt ist.

Diese (SPF und DKIM)-IDs werden anhand der im Von-Header abgeleiteten Domänen-ID authentifiziert. Die From-Header-Domäne wird verwendet, da es das häufigste Mail User Agent (MUA)-Feld für den Ausgangspunkt der Nachricht ist und von Endbenutzern verwendet wird, um die Quelle der Nachricht zu identifizieren (ein Absender), wodurch auch der From-Header zu einem primären Ziel für Missbrauch wird.

Vorsicht: DMARC kann Missbrauch nur gegen einen gültigen Von-Header schützen.

DMARC kann nicht in folgenden Bereichen eingesetzt werden:

- Fehlerhafte, fehlende oder wiederholte RFC 5322-Header
- Nicht konforme Header, da diese nicht validiert werden
- Wenn mehr als eine Domänen-Identität im Header (*) vorhanden ist

Aus diesem Grund sollte zusätzlich zu DMARC ein Prozess existieren, um Nachrichten mit nicht konformen fehlerhaften Headern zu identifizieren und eine Möglichkeit zu implementieren, um diese als nicht DMARC-fähige Header zu markieren und sichtbar zu machen.

(*) DMARC muss eine einzige Domänen-Identität aus dem Header extrahieren. Wenn der Header mehr als eine E-Mail-Adresse enthält, wird dieser Header in den meisten DMARC-Implementierungen übersprungen. Verarbeitungs-Header mit mehr als einer Domänenidentität

werden in der DMARC-Spezifikation als Out-of-Scope angegeben.

Wenn die Cisco ESA mehr als eine Domänen-Identität erkennen kann, hinterlässt sie eine korrekte Nachricht in den E-Mail-Protokollen:

```
(Machine esa.lab.local) (SERVICE)> grep -i "verification skipped" mail_logs

Tue Oct 16 14:13:52 2018 Info: MID 2003 DMARC: Verification skipped (Sending domain could not be
determined)
```

Identifikatorausrichtung

Die Identifier-Ausrichtung definiert eine Beziehung zwischen der von SPF und/oder DKIM authentifizierten Domäne und dem Von-Header. Alignment ist ein Abgleichprozess, der nach erfolgreicher Verifizierung von SPF und/oder DKIM zusätzlich erfüllt werden muss. Beim DMARC-Authentifizierungsprozess muss mindestens einer der von SPF oder DKIM verwendeten Identifikatoren (Domänenidentität) an den Domänenteil der From-Header-Adresse angepasst werden.

DMARC führt zwei Ausrichtungsmodi ein:

- **Der strikte** Modus erfordert eine genaue Übereinstimmung (Ausrichtung) zwischen Domänennamen.
- **entspannter** Modus ermöglicht die Subdomäne derselben Domäne

Die Identifier-Alignment ist erforderlich, da eine Nachricht eine gültige Signatur von jeder Domäne enthalten kann, einschließlich der Domänen, die von einer Mailingliste oder sogar einem schlechten Akteur verwendet werden. Daher reicht das bloße Tragen einer gültigen Signatur nicht aus, um auf die Authentizität der Author Domain schließen zu können.

DKIM-Ausrichtung

Die DKIM-Domänen-ID wird durch Überprüfen des *d=*Tags in einer DKIM-Signatur ermittelt und mit der From-Header-Domäne verglichen, um eine DKIM-Signatur erfolgreich zu überprüfen.

Beispielsweise kann die Nachricht im Namen der Domäne d=blog.cisco.com signiert werden, die Domain *blog.cisco.com* als Signierer identifiziert. DMARC verwendet diese Domäne und vergleicht sie mit dem Domänenteil des Von-Headers (z. B. noreply@cisco.com). Die Ausrichtung zwischen diesen Bezeichnern *schlägt* im strikten Modus fehl, aber im entspannten Modus verläuft sie erfolgreich.

Hinweis: Eine einzelne E-Mail kann mehrere DKIM-Signaturen enthalten. Wenn eine DKIM-Signatur ausgerichtet und verifiziert ist, wird sie als "Passwort" des DMARC angesehen.

SPF-Ausrichtung

Der SPF-Mechanismus (spfv1) authentifiziert Domänenbezeichner, die von folgenden Quellen bereitgestellt werden:

- MAIL FROM Identity (MAIL FROM-Befehl)
- HELO/EHLO-Identität (HELO/EHLO-Befehl)

Die MAIL FROM-Domänenidentität versucht standardmäßig zu authentifizieren. Die HELO-Domänen-Identität wird von DMARC nur für Nachrichten mit einer leeren MAIL FROM-Identität authentifiziert, z. B. Bounce-Nachrichten.

Ein gängiges Beispiel hierfür ist, dass eine Nachricht mit einer anderen MAIL FROM-Adresse (noreply@blog.cisco.com) als im From-Header (noreply@cisco.com) gesendet wird. Der Teil "MAIL FROM domain identity" von noreply**@blog.cisco.com** entspricht der From-Header-Domäne von noreply**@cisco.com** im entspannten Modus, *jedoch nicht* im strikten Modus.

Tags des Ausrichtungsmodus

DMARC-Alignment-Modi können mithilfe von **Adkim-** und **ASPF-**Alignment-Mode-Tags in einem DMARC-Richtliniendatensatz definiert werden. Diese Tags geben an, welcher Modus für die Ausrichtung der DKIM- oder SPF-IDs erforderlich ist.

Die Modi können auf entspannt oder strikt eingestellt werden, wobei "relaxed" die Standardeinstellung ist, wenn kein Tag vorhanden ist. Diese kann unter dem Tagwert wie folgt festgelegt werden:

- **r: entspannter Modus**
- **s: strikter Modus**

Referenz

- RFC5321 - Simple Mail Transfer Protocol
- RFC5322 - Internet Message Format
- RFC6376 - DomainKeys Identified Mail (DKIM)-Signaturen
- RFC7208 - Sender Policy Framework (SPF) für die Autorisierung der Verwendung von Domänen in E-Mails

- RFC7489 - Domain-basierter DMARC (Message Authentication, Reporting and Conformance)