DMARC-architectuur - Herkenningsuitlijning

Inhoud

Inleiding

In dit document worden algemene DMARC-architectuurconcepten voor berichtenverificatie, rapportage en conformiteit met Domain-Based Berichtingsverificatie, alsmede Sender Policy Framework (SPF) en DomainKeys Identified Mail (DKIM)-aanpassingsvereisten met betrekking tot DMARC beschreven.

Terminologie

In dit gedeelte worden enkele van de belangrijkste termen die in dit document worden gebruikt, beschreven en gedefinieerd.

- **EHLO/HELO** - De opdrachten die de identiteit van een MTP-client leveren tijdens de initialisatie van een MTP-sessie zoals gedefinieerd in RFC 5321.
- **Van header** - The From: veld specificeert de auteur(s) van een bericht. Meestal bevat de display de naam (wat door de mailclient aan een eindgebruiker wordt getoond), evenals een e-mailadres dat een domeinnaam en een domeinnaam bevat (bijvoorbeeld "John Doe" <johndoe@example.com>) zoals gedefinieerd in RFC 5322.
- **MAIL VANAF** - Dit is afgeleid van de MAIL-opdracht aan het begin van een MTP-sessie en biedt de afzender-identificatie zoals gedefinieerd in RFC5321. Het is ook algemeen bekend als de envelopafzender, retourpad of bounce-adres.

DMARC - Identificatielijn

DMARC bindt wat DKIM en SPF authentiek verklaren aan wat in de Van header is vermeld. Dit gebeurt door *uitlijning*. Uitlijning vereist dat de domeinidentiteit die door SPF en DKIM voor eensluidend is bevonden, overeenkomt met het domein in het e-mailadres dat zichtbaar is voor de eindgebruiker.

Laten we beginnen met wat een identificator is en waarom ze belangrijk zijn in relatie tot DMARC.

Identificatiecode

Identificatienummers identificeren een domeinnaam die geauthentificeerd moet worden.

Identificatienummers onder verwijzing naar DMARC:

- SFP:

  SPF authenticeert het domein dat in MAIL VANUIT of EHLO/HELO gedeelte van het gesprek mtp, of beiden voorkomt. Dit kunnen verschillende domeinen zijn, en deze zijn typisch niet zichtbaar voor de eindgebruiker.

- DKIM:

  DKIM echt het signaaldomein dat op een handtekening is aangebracht binnen de *d=* tag.

Deze (SPF- en DKIM) identificatiegegevens zijn authentiek tegen de domeinidentificatie afgeleid in de From header. Het Van header-domein wordt gebruikt omdat het het meest voorkomende veld Mail User Agent (MUA) is voor de maker van het bericht en het veld dat door eindgebruikers wordt gebruikt om de bron van het bericht te identificeren (een zender), waardoor de Van header ook een primaire doelstelling voor misbruik is.

Voorzichtig: DMARC kan misbruik alleen beschermen tegen een geldige Van header.

DMARC kan niet werken op:

- Kop-na-vormig, afwezig of herhaald RFC 5322
- Niet-conforme headers, omdat ze niet gevalideerd zullen worden
- Wanneer er meer dan één domeinidentiteit in de header is (*)

Daarom moet er een proces naast DMARC bestaan om berichten met niet-conforme misvormde kopregels te identificeren en om een manier te implementeren om ze als niet-DMARC in aanmerking komende headers te markeren en zichtbaar te maken.

(*) DMARC moet één domein-identiteit uit de header halen. Als er meer dan één e-mailadres in de header is dan wordt deze header overgeslagen in de meeste DMARC-implementaties. Kop verwerken met meer dan één domein-identiteit wordt in de DMARC-specificatie als buiten bereik aangegeven.

Wanneer de Cisco ESA in staat is om meer dan één domein-identiteit te detecteren, geeft het een goed bericht in de maillogs:

```
(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)
```

Identificatielijn

Identifier-uitlijning definieert een relatie tussen het domein dat voor authenticatie is ingesteld door SPF en/of DKIM en de From header. Lijnuitlijning is een matchingsproces waaraan na een geslaagde verificatie van de SPF en/of de DKIM moet worden voldaan. Voor de DMARC-authenticatie moet ten minste één van de identificatoren (domeinidentiteit) die door SPF of DKIM worden gebruikt, worden uitgelijnd met het domeingedeelte van het Van header-adres.

DMARC voert twee uitlijning-modi in:

- voor **strikte** modus is een exacte overeenkomst (uitlijnen) tussen domeinnamen vereist
- **relaxed** mode staat het subdomein van hetzelfde domein toe

De herkenningsuitlijning is vereist omdat een bericht een geldige handtekening van om het even welk domein kan dragen, inclusief domeinen die door een mailinglijst of zelfs een slechte acteur worden gebruikt. Daarom is het alleen dragen van een geldige handtekening niet voldoende om de authenticiteit van het Auteur-domein te beïnvloeden.

DKIM-uitlijning

DKIM domein identifier wordt verkregen door de *d=* tag in een DKIM-handtekening te herkennen en deze wordt vergeleken met het Van header-domein om een DKIM-handtekening met succes te controleren.

Als voorbeeld kan het bericht worden getekend namens het domein d=blog.cisco.com, dat domein*blog.cisco.com* identificeert als ondertekenaar. DMARC gebruikt dit domein en vergelijkt het met het domeindeel van de Van header (bijvoorbeeld noreply@cisco.com). De uitlijning tussen deze identificatoren *faalt* in de strikte modus maar gaat over in de relaxed-modus.

> Opmerking: Eén e-mail kan meerdere DKIM-handtekeningen bevatten en deze wordt beschouwd als een DMARC- "pass" (in dat geval) als een DKIM-handtekening is uitgelijnd en verifieert.

SPF-uitlijning

Het SPF (SPF1) mechanisme authenticeert domeinidentificatoren die worden geleverd door:

- MAIL VANUIT identiteit (MAIL UIT commando)
- HELO/EHLO-identiteit (HELO/EHLO-opdracht)

De MAIL VANUIT domein identiteit probeert standaard geauthentificeerd te worden. De HELO domein identiteit wordt authentiek verklaard door DMARC slechts voor berichten met een lege MAIL VANUIT identiteit, zoals berichtjes.

Een veelvoorkomend voorbeeld hiervan is wanneer een bericht wordt verstuurd met een ander MAIL VANAF adres (noreply@blog.cisco.com) vergeleken met wat in de Van header (noreply@cisco.com) staat. De MAIL UIT het domein dat deel uitmaakt van noreply**@cisco.com** zal zich aanpassen aan het From header domein van noreply**@cisco.com** in relaxed mode maar *niet* in strikte modus.

Tags voor uitlijning

De DMARC-uitlijning kan worden gedefinieerd in een DMARC-beleidsrecord met behulp van tags **adkim** en **aspf-**uitlijning. Deze tags geven aan welke modus vereist is voor DKIM of SPF-herkenning.

U kunt de modi relatief soepel of strikt instellen, waarbij de standaardinstelling wordt ontspannen als er geen tag is. Dit kan worden ingesteld onder de waarde van de tag als:

- **r: relaxed modus**
- **s: strikte modus**

Referentie

- RFC5321 - Simple Mail-overdrachtprotocol
- RFC5322 - Opmaak van internetberichten
- RFC6376 - DomainKeys Identified Mail (DKIM)-handtekeningen
- RFC7208 - Sender Policy Framework (SPF) voor het autoriseren van gebruik van domeinen in e-mail
- RFC7489 - Domain-Based Berichtverificatie, -rapportage en -conformiteit (DMARC)