Architettura DMARC - Allineamento degli identificatori

Sommario

Introduzione

In questo documento vengono descritti i concetti generali dell'architettura DMARC (Domain-based Message Authentication, Reporting and Conformance) e i requisiti di allineamento di Sender Policy Framework (SPF) e DomainKeys Identified Mail (DKIM) in relazione a DMARC.

Terminologia

In questa sezione vengono descritti e definiti alcuni dei termini chiave utilizzati nel documento.

- **EHLO/HELO** - Comandi che forniscono l'identità di un client SMTP durante l'inizializzazione di una sessione SMTP come definito nella RFC 5321.
- **Intestazione Da** - Da: specifica gli autori di un messaggio. In genere include il nome visualizzato, ovvero quello mostrato a un utente finale dal client di posta, e un indirizzo di posta elettronica contenente una parte locale e un nome di dominio, ad esempio "Mario Rossi" <johndoe@example.com>, come definito nella RFC 5322.
- **MAIL FROM**: deriva dal comando MAIL all'inizio di una sessione SMTP e fornisce l'identificazione del mittente come definito in RFC5321. È anche ampiamente noto come mittente della busta, percorso di ritorno o indirizzo di rimbalzo.

DMARC - Allineamento identificatori

DMARC associa l'autenticazione DKIM e SPF a quanto elencato nell'intestazione From. Questo avviene per *allineamento*. L'allineamento richiede che l'identità del dominio autenticata da SPF e DKIM corrisponda al dominio nell'indirizzo di posta elettronica visibile all'utente finale.

Cominciamo con cosa è un identificatore e perché sono importanti in riferimento al DMARC.

Identificatori

Gli identificatori identificano un nome di dominio da autenticare.

Identificatori in riferimento al DMARC:

- SPF

  SPF autentica il dominio visualizzato nella sezione MAIL FROM o EHLO/HELO della conversazione SMTP o in entrambi. Questi domini possono essere diversi e in genere non sono visibili all'utente finale.

- DKIM

  DKIM autentica il dominio di firma applicato a una firma all'interno del tag *d=*.

Questi identificatori (SPF e DKIM) vengono autenticati in base all'identificatore di dominio derivato nell'intestazione From. Il dominio dell'intestazione From viene utilizzato perché è il campo MUA (Mail User Agent) più comune per l'iniziatore del messaggio ed è quello utilizzato dagli utenti finali per identificare l'origine del messaggio (un mittente), il che rende l'intestazione From un target principale per eventuali abusi.

> **Attenzione:** DMARC è in grado di proteggere l'utilizzo non consentito solo per un'intestazione From valida.

Impossibile utilizzare DMARC su:

- Intestazioni RFC 5322 errate, assenti o ripetute
- Intestazioni non conformi perché non verranno convalidate
- Quando nell'intestazione sono presenti più identità di dominio (*)

Èpertanto necessario che esista un processo aggiuntivo a DMARC per identificare i messaggi con intestazioni non conformi in formato non valido e implementare un modo per contrassegnarli e renderli visibili come intestazioni non DMARC idonee.

(*) DMARC deve estrarre una singola identità di dominio dall'intestazione. Se nell'intestazione sono presenti più indirizzi e-mail, l'intestazione verrà ignorata nella maggior parte delle implementazioni DMARC. Le intestazioni di elaborazione con più identità di dominio sono

dichiarate fuori ambito nella specifica DMARC.

Quando Cisco ESA è in grado di rilevare più di un'identità di dominio, lascia un messaggio appropriato nei log di posta:

```
(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)
```

Allineamento identificatore

L'allineamento degli identificatori definisce una relazione tra il dominio autenticato da SPF e/o DKIM e l'intestazione From. L'allineamento è un processo di corrispondenza che deve essere ulteriormente soddisfatto dopo la verifica di SPF e/o DKIM. Il processo di autenticazione DMARC richiede che almeno uno degli identificatori (identità di dominio) utilizzati da SPF o DKIM sia allineato alla parte di dominio dell'indirizzo di intestazione From.

DMARC introduce due modalità di allineamento:

- la modalità **strict** richiede una corrispondenza esatta (allineamento) tra i nomi di dominio
- **la** modalità **rilassata** consente il sottodominio dello stesso dominio

L'allineamento degli identificatori è necessario perché un messaggio può contenere una firma valida da qualsiasi dominio, inclusi i domini utilizzati da una lista di distribuzione o anche da un attore non valido. Pertanto, il semplice fatto di recare una firma valida non è sufficiente per dedurre l'autenticità del Dominio Autore.

Allineamento DKIM

L'identificatore di dominio DKIM viene ottenuto esaminando il tag *d=* in una firma DKIM e viene confrontato con il dominio di intestazione From per verificare correttamente una firma DKIM.

Ad esempio, il messaggio può essere firmato per conto del dominio d=blog.cisco.com, che identifica il dominio *blog.cisco.com* come firmatario. DMARC utilizza questo dominio e lo confronta con la parte dominio dell'intestazione From (ad esempio, noreply@cisco.com). L'allineamento tra questi identificatori avrà *esito negativo* in modalità rigorosa ma verrà superato in modalità rilassata.

Nota: Un singolo messaggio di posta elettronica può contenere più firme DKIM e viene

considerato un "passaggio" DMARC se una firma DKIM viene allineata e verificata.

Allineamento SPF

Il meccanismo SPF (spfv1) autentica gli identificatori di dominio forniti da:

- Identità MAIL FROM (comando MAIL FROM)
- Identità HELO/EHLO (comando HELO/EHLO)

L'identità del dominio MAIL FROM tenta di essere autenticata per impostazione predefinita. L'identità del dominio HELO viene autenticata da DMARC solo per i messaggi con un'identità MAIL FROM vuota, come i messaggi di rimbalzo.

Ad esempio, un messaggio viene inviato con un indirizzo MAIL FROM diverso (noreply@blog.cisco.com) rispetto a quello contenuto nell'intestazione From (noreply@cisco.com). La parte relativa all'identità del dominio MAIL FROM di noreply**@blog.cisco.com** verrà allineata al dominio dell'intestazione From di noreply**@cisco.com** in modalità rilassata ma *non* in modalità rigorosa.

Tag modalità allineamento

Le modalità di allineamento DMARC possono essere definite in un record dei criteri DMARC utilizzando i tag **adkim** e **aspf** in modalità di allineamento. Questi tag indicano la modalità necessaria per l'allineamento degli identificatori DKIM o SPF.

Le modalità possono essere impostate su rilassato o rigoroso, con rilassato come impostazione predefinita se non è presente alcun tag. Questa impostazione può essere impostata sotto il valore del tag come:

- **r: modalità rilassata**
- **s: modalità strict**

Riferimento

- RFC5321 - Protocollo di trasferimento di posta semplice
- RFC532 - Formato messaggio Internet
- RFC6376 - Firme DKIM (DomainKeys Identified Mail)
- RFC 7208 - Sender Policy Framework (SPF) per l'autorizzazione dell'uso dei domini nella posta elettronica
- RFC 7489 - Autenticazione, reporting e conformità dei messaggi basati su dominio (DMARC)