Best practice per l'autenticazione e-mail - Metodi ottimali per l'installazione di SPF, DKIM e DMARC

Sommario

Introduzione

In questa guida vengono descritte tre tecnologie di autenticazione della posta elettronica attualmente in uso: SPF, DKIM e DMARC e vengono illustrati vari aspetti della relativa implementazione. Vengono discusse diverse situazioni reali dell'architettura della posta elettronica e le linee guida per la loro implementazione nel set di prodotti Cisco Email Security. Poiché si tratta di una guida pratica alle best practice, alcuni dei materiali più complessi verranno omessi. Se necessario, alcuni concetti possono essere semplificati o accorciati per facilitare la comprensione della questione presentata.

Requisiti di conoscenza dei prodotti

Questa guida è un documento di livello avanzato. Per completare la presentazione, il lettore deve essere in possesso di una conoscenza del prodotto Cisco Email Security Appliance al livello di certificazione Cisco Email Security Field Engineer. Inoltre, i lettori devono avere un forte comando di DNS e SMTP e il loro funzionamento. La conoscenza delle nozioni di base di SPF, DKIM e DMARC è un vantaggio.

Autenticazione e-mail - Breve panoramica

Sender Policy Framework (SPF)

Sender Policy Framework è stato pubblicato per la prima volta nel 2006 come RFC4408. La versione corrente è specificata in RFC7208 e aggiornata in RFC7372. In sostanza, fornisce un modo semplice per un proprietario di dominio di annunciare le proprie origini e-mail legittime ai destinatari utilizzando il DNS. Sebbene SPF autentichi principalmente l'indirizzo del percorso di ritorno (MAIL FROM), la specifica consiglia (e fornisce un meccanismo) di autenticare anche l'argomento HELO/EHLO SMTP (FQDN del gateway del mittente trasmesso durante la conversazione SMTP).

SPF utilizza record di risorse DNS di tipo TXT con sintassi piuttosto semplice:

```
spirit.com       text = "v=spf1 mx a ip4:38.103.84.0/24 a:mx3.spirit.com
a:mx4.spirit.com include:spf.protection.outlook.com ~all"
```

Il precedente record Spirit Airlines consente di inviare e-mail dagli indirizzi @spirit.com da una particolare subnet /24, due macchine identificate da un FQDN e l'ambiente Microsoft Office365. Il qualificatore "~all" alla fine indica ai ricevitori di considerare qualsiasi altra fonte come Soft Fail, una delle due modalità di errore di SPF. Si noti che i mittenti non specificano l'azione che i destinatari devono eseguire sui messaggi con errori, il grado di errore.

Delta, invece, utilizza un regime SPF diverso:

```
delta.com text = "v=spf1 a:smtp.hosts.delta.com
include:_spf.vendor.delta.com -all"
```

Per ridurre al minimo il numero di query DNS richieste, Delta ha creato un singolo record "A" in cui sono elencati tutti i gateway SMTP. Forniscono inoltre un record SPF separato per i fornitori in "_spf.vendor.delta.com". Includono anche istruzioni per **Hard Fail** qualsiasi messaggio non autenticato da SPF (qualificatore "all"). Possiamo esaminare ulteriormente il record SPF dei fornitori:

```
_spf.vendor.delta.com text = "v=spf1 include:_spf-delta.vrli.com
include:_spf-ncr.delta.com a:delta-spf.niceondemand.com
include:_spf.airfrance.fr include:_spf.qemailserver.com
include:skytel.com include:epsl1.com ?all"
```

Quindi, le email dei mittenti @delta.com possono legittimamente provenire, per esempio, dai gateway di posta elettronica di Air France.

United, invece, utilizza uno schema SPF molto più semplice:

```
testo united.com = "v=spf1 include:spf.enviaremails.com.br
include:spf.usa.net include:coair.com ip4:161.215.0.0/16
ip4:209.87.112.0/20 ip4:74.112.71.93 ip4:74.209.251.0/24 mx ~all"
```

Oltre ai propri gateway di posta aziendali, includono i provider di e-mail marketing ("usa.net" e "enviaremails.com.br"), i gateway legacy di Continental Air Lines, oltre a tutti gli elementi elencati nei record MX (meccanismo "MX"). Tenere presente che MX (un gateway di posta **in arrivo** per un dominio) potrebbe non essere uguale a **in uscita**. Mentre per le aziende più piccole di solito sono le stesse, le organizzazioni più grandi hanno un'infrastruttura separata per la gestione della posta in arrivo e per la gestione separata della consegna in uscita.

Èinoltre opportuno notare che tutti gli esempi riportati sopra fanno ampio uso di riferimenti DNS aggiuntivi (meccanismi "include"). Tuttavia, per motivi di prestazioni, la specifica SPF limita a **dieci** il numero totale di ricerche DNS necessarie per recuperare un record finale. Qualsiasi ricerca SPF con oltre 10 livelli di ricorsione DNS avrà esito negativo.

Posta identificata chiavi di dominio (DKIM)

DKIM, specificato nelle RFC 5585, 6376 e 5863, è una fusione di due proposte storiche: DomainKeys di Yahoo e posta Internet identificata di Cisco. Fornisce ai mittenti un modo semplice per firmare in modo crittografico i messaggi in uscita e includere le firme (insieme ad altri metadati di verifica) in un'intestazione di posta elettronica ("DKIM-Signature"). I mittenti pubblicano la propria chiave pubblica nel DNS, semplificando in tal modo il recupero della chiave e la verifica delle firme da parte dei destinatari. DKIM non autentica l'origine dei messaggi fisici, ma si basa sul fatto che se l'origine è in possesso della chiave privata dell'organizzazione mittente, è implicitamente autorizzata a inviare un messaggio di posta elettronica per suo conto.

Per implementare DKIM, l'organizzazione di invio genera una o più coppie di chiavi pubbliche e pubblica le chiavi pubbliche nel DNS come record TXT. A ogni coppia di chiavi viene fatto riferimento da un "selettore" in modo che i verificatori DKIM possano distinguere tra le chiavi. I messaggi in uscita verranno firmati e verrà inserita l'intestazione DKIM-Signature:

```
Firma DKIM: v=1; a=rsa-sha1; c=rilassato/rilassato; s=unito;
d=news.united.com;h=MIME-Version:Content-Type:Content-Transfer-
Encoding:Date:To:From:Reply-To:Subject:List-Unsubscribe:Message-ID;
i=MileagePlus@news.united.com; bh=IBSWR4yzI1PSRYtWLx4SRDSWII4=;

b=HrN5QINgnXwqkx+Zc/9VZys+yhikrP6wSZVu35KA0jfgYzhzSdfA2nA8D2JYIFTNLO8j4D
GmKhH1MMTyYgwYqT01rEwL0V8MEY1MzxTrzijkLPGqt/sK1WZt9pBacWRw1fMQLf3BxZ3jaY
tLoJMRwxtgoWdfHU35CsFG2CNYLo=
```

Il formato della firma è abbastanza semplice. "a" specifica gli algoritmi utilizzati per la firma, "c" specifica lo schema o gli schemi di canonizzazione utilizzati [1], "s" è il selettore o il riferimento alla chiave, "d" è il dominio di firma. Il resto dell'intestazione DKIM-Signature è specifico del messaggio: "h" elenca le intestazioni firmate, "i" elenca l'identità dell'utente firmatario e, infine, l'intestazione termina con due hash separati: "bh" è un hash di intestazioni firmate, mentre "b" è il valore hash per il corpo del messaggio.

Quando riceve un messaggio con firma DKIM, il destinatario cercherà la chiave pubblica creando la seguente query DNS:

```
<selector>._domainkey.<dominio di firma>
```

come specificato nell'intestazione DKIM-Signature. Per l'esempio precedente, la query sarà "united._domainkey.news.united.com":

```
united._domainkey.news.united.com text = "g=*\; k=rsa\; n=" "Contatto"
"postmaster@responsys.com" "con" "qualsiasi" "domande" "relative"
"questa" "firma" "\;
p=MIGfMA0GCSqGSIb3DQEBAQUA4GNADCBiQKBgQC/Vh/xq+sSRLhL5CRU1drFTGMXX/Q2KkW
gl35hO4v6dTy5Qmxcuv5AwqxLiz9d0jBaxtuvYALjlGkxmk5MemAOcCr97GlW7Cr11
Ln87qdTmyE5LevnTXxVDMjIfQJt6OFzmw6Tp1t05NPWh0PbyUohZYt4qpcbiz9Kc3UB2IBwI
DAQAB\;"
```

Il record DNS restituito contiene la chiave e altri parametri facoltativi. [2]

Il problema principale con DKIM è che le specifiche iniziali non consentivano la pubblicità che un mittente utilizza DKIM. Così, se un messaggio arriva senza una firma, non c'è un modo facile per il destinatario di sapere che avrebbe dovuto essere firmato e che in quel caso, è molto probabilmente non autentico. Dal momento che una singola organizzazione può (e molto spesso utilizzerà) diversi selettori, non è banale "indovinare" se un dominio è abilitato per DKIM. Per questo è stato sviluppato uno standard separato, Author Domain Signing Practices, ma a causa del basso utilizzo e di altri problemi è stato obsoleto nel 2013 senza successori.

DMARC (Domain-based Message Authentication, Reporting And Conformance)

DMARC è la più giovane delle tre tecnologie di autenticazione e-mail trattate ed è stata sviluppata appositamente per risolvere le carenze di SPF e DKIM. A differenza degli altri due, autentica l'intestazione Da di un messaggio e si collega ai controlli precedentemente eseguiti dagli altri due. DMARC è specificato in RFC7489.

Il valore aggiunto di DMARC su SPF e DKIM comprende:

- Verificare che tutte le identità disponibili (HELO, MAIL FROM e/o dominio di firma DKIM) siano allineate (esattamente corrispondenti o subordinate) all'intestazione From
- Fornire al proprietario del dominio del mittente un mezzo per specificare un criterio per i destinatari in merito alla modalità di gestione dei messaggi con errori
- Fornire ai proprietari del dominio mittente un servizio di feedback per essere informati di eventuali messaggi non riusciti, semplificando l'identificazione di campagne di phishing o errori nell'assegnazione dei criteri SPF/DKIM/DMARC

DMARC utilizza inoltre un semplice meccanismo di distribuzione dei criteri basato su DNS:

```
_dmarc.aa.com text = "v=DMARC1\; p=nessuno\; fo=1\; ri=3600\;
rua=mailto:american@rua.agari.com,mailto:dmarc@aa.com\;
ruf=mailto:american@ruf.agari.com,mailto:dmarc@aa.com"
```

L'unico tag obbligatorio nella specifica dei criteri DMARC è "p", che specifica i criteri da utilizzare nei messaggi con errori. Può essere uno dei tre valori seguenti: nessuno, quarantena, rifiuto.

Nella maggior parte dei casi, i parametri facoltativi utilizzati hanno a che fare con il reporting: "rua" specifica un URL (un mailto: o un URL http:// (utilizzando il metodo POST) per inviare report aggregati giornalieri su tutti i messaggi con errori che sembrano provenire da un particolare dominio. "ruf" specifica un URL per l'invio immediato di rapporti dettagliati sugli errori per ogni messaggio con errori.

In base alle specifiche, un ricevitore **deve** rispettare la policy pubblicizzata. In caso contrario, **devono** informare il proprietario del dominio mittente nel report aggregato.

Il concetto centrale di DMARC è il cosiddetto allineamento dell'identificatore. L'allineamento degli identificatori definisce il modo in cui un messaggio può superare la verifica DMARC. Gli identificatori SPF e DKIM sono allineati separatamente e un messaggio deve passare **uno qualsiasi** di essi per passare DMARC in generale. Tuttavia, esiste un'opzione dei criteri DMARC in cui il mittente può richiedere che venga generato un report di errore anche se un allineamento viene superato, ma l'altro non riesce. Nell'esempio precedente, il tag "fo" è impostato su "1".

Esistono due modi per i messaggi di aderire all'allineamento dell'identificatore DKIM o SPF, rigoroso e rilassato. La rigorosa conformità indica che il nome di dominio completo (FQDN) dell'intestazione From deve corrispondere completamente all'ID del dominio di firma (tag "d") della firma DKIM o al nome di dominio completo (FQDN) del comando MAIL FROM SMTP per SPF. Relaxed, invece, consente a Header From FQDN di essere un sottodominio dei due precedentemente menzionati. Questo ha implicazioni importanti quando deleghi il traffico e-mail a terzi, che sarà discusso più avanti nel documento.

Considerazioni sulla distribuzione di SPF

SPF per ricevitori

La verifica SPF è una funzionalità semplice da configurare sulle appliance virtuali Cisco Email Security Appliance o Cloud Email Security. Per il resto del presente documento, ogni riferimento all'ESA comprenderà anche il CES.

La verifica SPF è configurata in Criteri di flusso della posta. Il modo più semplice per eseguirla a livello globale è attivarla nella sezione Parametri dei criteri predefiniti dei listener appropriati. Se si utilizza lo stesso listener per la raccolta della posta in entrata e in uscita, verificare che il criterio di flusso della posta "INOLTRATO" abbia la verifica SPF impostata su "Disattivato".

Poiché SPF non consente di specificare l'azione politica da intraprendere, la verifica SPF (e DKIM, come vedremo più avanti) verifica solo il messaggio e inserisce una serie di intestazioni per ogni controllo SPF eseguito:

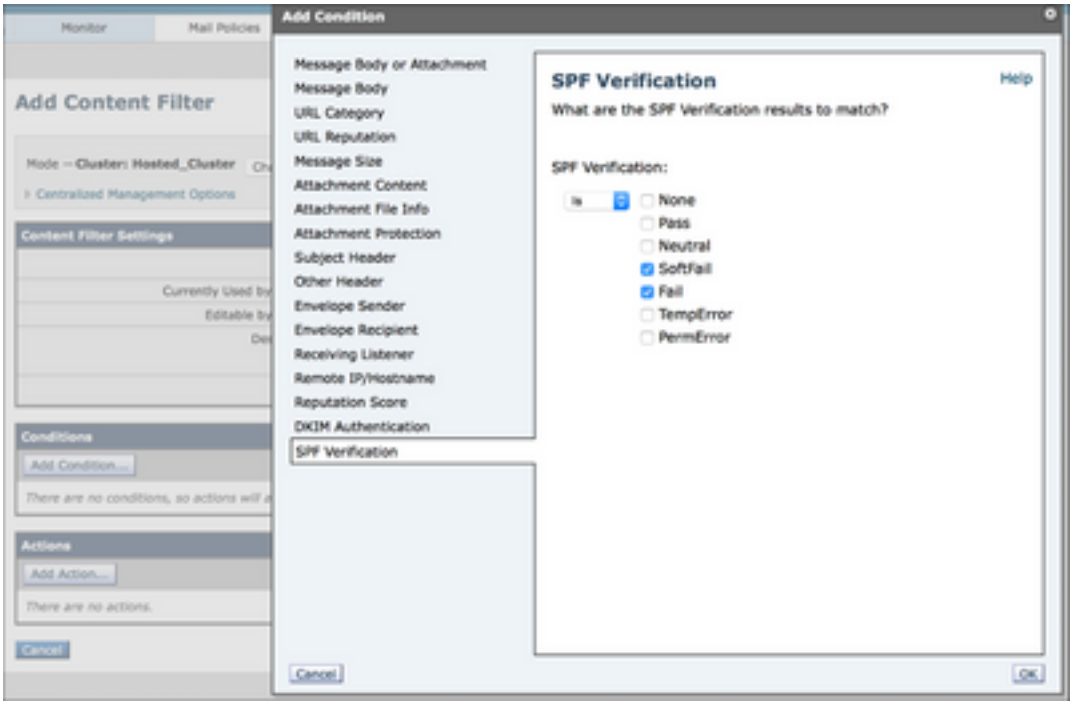
```
Received-SPF: Accetta (mx1.hc4-93.c3s2.smtpi.com: dominio di

  united.5765@envfrm.rsys2.com designa 12.130.136.195 come

  allowed sender) identity=mailfrom;

  client-ip=12.130.136.195; receiver=mx1.hc4-93.c3s2.smtpi.com;

  envelope-from="united.5765@envfrm.rsys2.com";

  x-sender="united.5765@envfrm.rsys2.com"

  conformità x=sidf_compatible; x-record-type="v=spf1"

Received-SPF: Nessuno (mx1.hc4-93.c3s2.smtpi.com: nessun mittente

  informazioni sull'autenticità disponibili dal dominio di
```

```
postmaster@omp.news.united.com) identity=helo;

client-ip=12.130.136.195; receiver=mx1.hc4-93.c3s2.smtpi.com;

envelope-from="united.5765@envfrm.rsys2.com";

x-sender="postmaster@omp.news.united.com"

conformità x=sidf_compatible
```

Si noti che per questo messaggio, due "identità" sono state verificate da SPF: "mailfrom" come richiesto dalla specifica e "helo" come raccomandato dalla stessa. Il messaggio passerà formalmente SPF, poiché solo il primo è rilevante per la conformità SPF, ma alcuni riceventi possono sanzionare i mittenti che non includono record SPF anche per le loro identità HELO. È pertanto buona norma includere i nomi host dei gateway di posta in uscita nei record SPF.

Dopo la verifica di un messaggio da parte dei criteri di flusso della posta, spetta agli amministratori locali configurare l'azione da eseguire. A tale scopo, utilizzare la regola del filtro messaggi SPF-status() [3] oppure creare un filtro contenuti in arrivo utilizzando lo stesso filtro e applicandolo ai criteri di posta in arrivo appropriati.

Immagine 1: Condizione filtro contenuto verifica SPF



Le operazioni filtro consigliate consistono nell'eliminare i messaggi che hanno esito negativo ("-all" nel record SPF) e nel mettere in quarantena i messaggi che hanno esito negativo ("~all" nel record SPF) in una quarantena dei criteri. Tuttavia, questa operazione può variare a seconda dei requisiti di sicurezza. Alcuni ricevitori si limitano a contrassegnare i messaggi con errori o non eseguono alcuna azione visibile, ma li segnalano agli amministratori.

Recentemente c'è stato un aumento significativo nella popolarità di SPF, ma molti domini pubblicano record SPF incompleti o errati. Per essere sicuri, si può decidere di mettere in quarantena tutti i messaggi SPF-fail, e monitorare la quarantena per un po', per assicurarsi che non ci siano "falsi positivi".

Se Fornisci Servizi Di Posta Elettronica Per Altri Domini O Terze Parti

Se si forniscono servizi di hosting o di recapito di e-mail a terzi, questi dovranno aggiungere i nomi host e gli indirizzi IP utilizzati per recapitare i messaggi ai propri record SPF. Il modo più semplice per fare ciò è che il fornitore crei un record SPF "ombrello" e che i clienti utilizzino il meccanismo di "inclusione" nei record SPF.

```
testo suncountry.com = "v=spf1 mx ip4:207.238.249.242 ip4:146.88.177.148
ip4:146.88.177.149 ip4:67.109.66.68 ip4:198.179.134.238
ip4:107.20.237.57 ip4:207.87.182.66 ip4:199.66.248.0/22 include:cust-
spf.exacttarget.com ~all"
```

Come si può vedere, Sun Country controlla alcune e-mail, ma le sue e-mail di marketing vengono affidate a terzi. L'espansione del record a cui si fa riferimento rivela un elenco di indirizzi IP correnti utilizzati dal provider di servizi di posta marketing:

```
cust-spf.exacttarget.com text = " v=spf1 ip4:64.132.92.0/24
ip4:64.132.88.0/23 ip4:66.231.80.0/20 ip4:68.232.192.0/20
ip4:199.122.120.0/21 ip4:207.67.38.0/24 ip4:207.67.98.192/27
ip4:207.250.68.0/24 ip4:209.43.22.0/28 ip4:198.245.80.0/20
ip4:136.147.128.0/20 ip4:13.147.176.0/20 111.0.0/18 -all"
```

Questa flessibilità consente ai provider di servizi di posta elettronica di scalare senza dover contattare ogni cliente per modificare i propri record DNS.

Se si utilizzano servizi di posta elettronica di terze parti

Analogamente al paragrafo precedente, se si utilizzano servizi di posta elettronica di terze parti e si desidera stabilire un flusso di posta completamente verificato da SPF, è necessario includere i propri record SPF.

```
jetblue.com testo descrittivo "v=spf1 include:_spf.qualtrics.com ?all"
```

JetBlue utilizza il servizio di analisi Qualtrics e l'unica cosa che devono fare è includere un record SPF corretto da Qualtrics. Analogamente, la maggior parte degli ESP fornisce record SPF da includere nei record dei propri clienti.

Se il vostro ESP o email marketer non fornisce record SPF, dovrete elencare i loro gateway di posta in uscita direttamente nel vostro. Tuttavia, è responsabilità dell'utente mantenere accurati tali record e se il provider aggiunge altri gateway o modifica gli indirizzi IP o i nomi host, il flusso di posta potrebbe essere compromesso.

Ulteriori pericoli derivanti dalla condivisione di risorse da parte di terze parti che non sono consapevoli di SPF: Se un ESP utilizza lo stesso indirizzo IP per recapitare messaggi e-mail di diversi clienti, è tecnicamente possibile per un cliente generare messaggi validi SPF fingendo di essere un altro cliente che recapita attraverso la stessa interfaccia. Per questo motivo, prima di implementare eventuali restrizioni SPF, è necessario analizzare le politiche di sicurezza dell'MSP e la consapevolezza dell'autenticazione della posta elettronica. Se non hanno risposte alle tue domande, considerando come SPF è uno dei meccanismi di base della fiducia su Internet, ti consigliamo vivamente di riconsiderare la tua scelta di MSP. Non si tratta solo di sicurezza: SPF, DKIM, DMARC e altri mittenti, le migliori pratiche [4]impiegate dagli MSP sono una garanzia di realizzabilità. Se l'MSP non li segue o li segue in modo non corretto, ciò diminuirà la loro

affidabilità con i sistemi di ricezione di grandi dimensioni e potrebbe ritardare o perfino bloccare i messaggi.

(Sub)Domini senza traffico e-mail

La maggior parte delle organizzazioni possiede oggi diversi domini a scopo di marketing, ma ne utilizza solo uno attivamente per il traffico e-mail aziendale. Anche se l'SPF è correttamente implementato nel dominio di produzione, gli attori malfunzionanti possono comunque utilizzare altri domini che non sono attivamente utilizzati per un messaggio di posta elettronica allo scopo di falsificare l'identità di un'organizzazione. SPF può impedire che ciò avvenga tramite uno speciale record SPF "deny all" - per qualsiasi dominio (e sottodominio!) che non genera traffico e-mail, pubblicare "v=spf1 -all" nel DNS. Un esempio eccellente è openspf.org - il sito web del Consiglio SPF.

Poiché la delega SPF è valida solo per un singolo dominio, è fondamentale pubblicare anche i record SPF "deny all" per qualsiasi sottodominio che si sta utilizzando che potrebbe non generare un messaggio di posta elettronica. Anche se il tuo dominio di produzione ha un record SPF "regolare", fai un ulteriore sforzo per aggiungere record "nega tutti" ai tuoi sottodomini senza traffico. E ancora - non dimenticate che ricevere non equivale a mandare: Un dominio può benissimo ricevere e-mail, ma non sarà mai un'origine. Questo è vero per i domini di marketing a breve termine (ad esempio eventi, promozioni limitate nel tempo, lanci di prodotti...), dove le e-mail in arrivo a quei domini vengono recapitate al tuo dominio di produzione, e qualsiasi risposta a quelle e-mail verrà recapitata dal dominio di produzione. Questi domini a breve termine avranno un record MX valido, ma dovrebbero avere un record SPF che li identifichi come anche nessuna **origine** di posta elettronica.

Considerazioni sulla distribuzione di DKIM

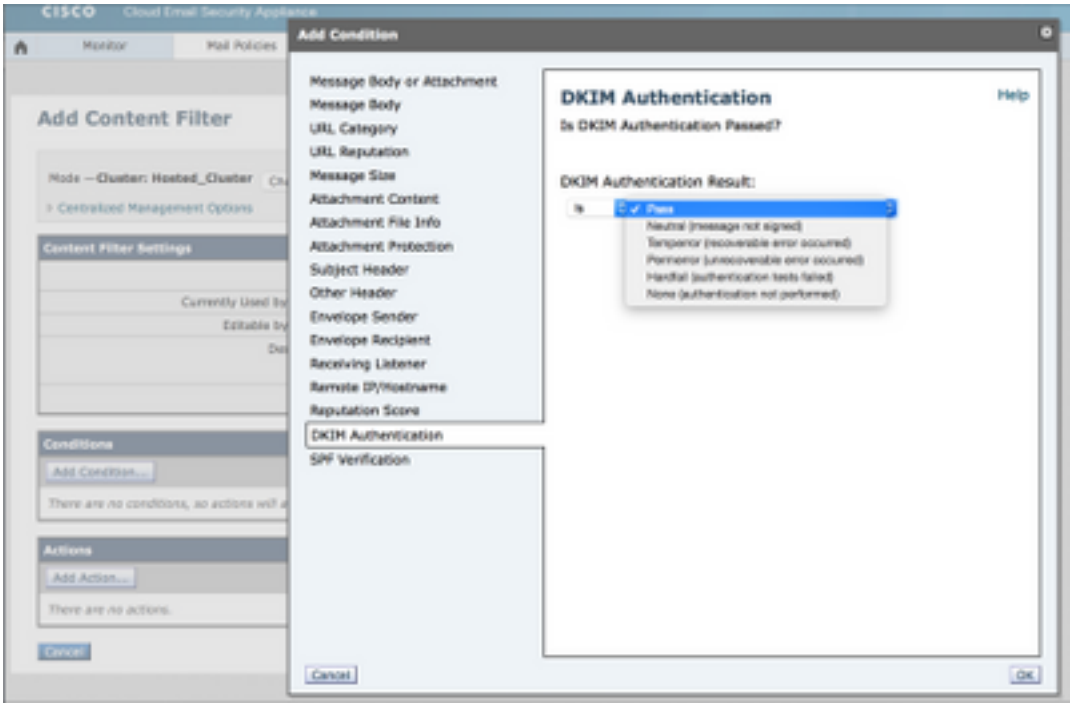
DKIM Per Ricevitori

La configurazione della verifica DKIM sull'ESA è simile alla verifica SPF. Nei Parametri predefiniti dei criteri di flusso della posta, è sufficiente attivare Verifica DKIM su "Attivata". Anche in questo caso, poiché DKIM non consente alcuna specifica di criteri, si limiterà a verificare la firma e a inserire un'intestazione "Authentication-Results":

```
Risultati autenticazione: mx1.hc4-93.c3s2.smtpi.com; dkim=pass (firma
verificata) header.i=MileagePlus@news.united.com
```

Qualsiasi azione basata sui risultati della verifica DKIM deve essere eseguita dai filtri dei contenuti:

Immagine 2: Condizione filtro contenuto verifica DKIM



A differenza di SPF, che è semplice, DKIM modifica il testo del messaggio effettivo, pertanto alcuni parametri possono essere limitati. Facoltativamente, è possibile creare profili di verifica DKIM e assegnare profili di verifica diversi a criteri di flusso di posta diversi. Consentono di limitare le dimensioni delle firme accettate, impostare le azioni di errore per il recupero della chiave e configurare la profondità della verifica DKIM.

Quando un messaggio passa attraverso più gateway, può essere firmato più volte e quindi contenere più firme. Affinché un messaggio superi la verifica DKIM, è necessario verificare **qualsiasi** firma. Per impostazione predefinita, l'ESA verifica fino a cinque firme.

A causa dell'apertura storica di SMTP e e-mail e della riluttanza di Internet globale ad adattarsi ai cambiamenti (positivi), ci sono ancora diverse situazioni in cui le firme DKIM potrebbero legittimamente fallire, come quando i gestori delle liste di distribuzione inoltrano direttamente ma modificano i messaggi o quando i messaggi vengono inoltrati direttamente piuttosto che come allegati ai nuovi messaggi. Per questo motivo, in generale, per i messaggi che non superano il test DKIM è consigliabile applicare la quarantena o l'applicazione di tag, anziché eliminarli.

Preparazione della firma con DKIM

Prima di attivare la firma DKIM nella policy di flusso della posta INOLTRATA, è necessario generare/importare le chiavi, creare i profili di firma DKIM e pubblicare le chiavi pubbliche nel DNS.

Se si firma per un singolo dominio, il processo è semplice. Generare la coppia di chiavi, creare il profilo di firma singolo nella sezione Chiavi di dominio dei criteri di posta e fare clic sull'opzione "Genera" in "Record di testo DNS" quando il profilo è pronto. Pubblicare la chiave generata nel DNS. Infine, attivare la firma DKIM nei criteri di flusso della posta.

Diventa più complicato se firmi per più domini distinti. In tal caso, sono disponibili due opzioni:

1. Utilizza un singolo profilo di firma per firmare tutti i domini. La chiave pubblica (singola) verrà archiviata nella zona DNS del dominio "primario" e le firme DKIM faranno riferimento a tale chiave. Questa tecnica è stata spesso utilizzata dagli ESP in passato, consentendo loro di

firmare su larga scala, senza dover interagire con lo spazio DNS dei singoli clienti [5].
2. Creare un profilo di firma separato per ogni dominio per cui si firma. Ciò rende la configurazione iniziale più complessa, ma offre maggiore flessibilità per il futuro. Creare una coppia di chiavi per ogni dominio, creare un profilo specificando un solo dominio (e i relativi sottodomini) nella sezione "Profile Users" e pubblicare la chiave pubblica pertinente nella zona DNS del dominio specifico.

Anche se l'opzione #1 è più facile da utilizzare, tenere presente che alla fine interromperà DMARC. Poiché DMARC richiede che l'ID del dominio di firma sia allineato all'intestazione Da, l'allineamento dell'identificatore con DKIM avrà esito negativo. Se l'SPF viene configurato correttamente, è possibile procedere senza problemi. Per superare la verifica DMARC, l'allineamento dell'identificatore SPF è fondamentale.

Tuttavia, implementando l'opzione 2 fin dall'inizio, non è necessario preoccuparsi di DMARC ed è piuttosto facile revocare o riconfigurare il servizio di firma per un solo dominio. Inoltre, se si forniscono **alcuni** servizi e-mail per un dominio di terze parti, molto probabilmente sarà necessario ottenere la chiave da utilizzare (e importarlo nella vostra ESA). La chiave sarà specifica del dominio, pertanto sarà necessario creare un profilo separato.

Se si utilizzano servizi di posta elettronica di terze parti

In generale, se si utilizza la firma DKIM e si scarica parte dell'elaborazione della posta elettronica (ad esempio le e-mail di marketing) a una terza parte, non si desidera che utilizzino gli stessi tasti utilizzati nella produzione. Questa è una delle ragioni principali per l'esistenza di Selettori in DKIM. È invece consigliabile generare una nuova coppia di chiavi, pubblicare la parte pubblica nella zona DNS e consegnare la chiave segreta all'altra parte. In questo modo è possibile revocare rapidamente la chiave in caso di problemi, mantenendo intatta l'infrastruttura di produzione DKIM.

Sebbene non sia necessario per DKIM (i messaggi relativi allo stesso dominio possono essere firmati con più chiavi diverse), è buona norma fornire un sottodominio distinto per qualsiasi e-mail gestita da terze parti. Ciò semplificherà il monitoraggio dei messaggi e consentirà un'implementazione più precisa di DMARC in un secondo momento. Ad esempio, si considerino le cinque intestazioni DKIM-Signature di più messaggi inviati da Lufthansa:

```
Firma DKIM: v=1; a=rsa-sha1; c=rilassato/rilassato; s=lufthansa;
d=newsletter.milesandmore.com;

Firma DKIM: v=1; a=rsa-sha1; c=rilassato/rilassato; s=lufthansa2;
d=newsletter.lufthansa.com;

Firma DKIM: v=1; a=rsa-sha1; c=rilassato/rilassato; s=lufthansa3;
d=lh.lufthansa.com;

Firma DKIM: v=1; a=rsa-sha1; c=rilassato/rilassato; s=lufthansa4
d=e.milesandmore.com

Firma DKIM: v=1; a=rsa-sha1; c=rilassato/rilassato; s=lufthansa5 d=fly-
lh.lufthansa.com;
```

Èpossibile osservare che Lufthansa utilizza cinque chiavi (selettori) diverse suddivise in cinque sottodomini distinti di due domini di produzione primari (lufthansa.com e milesandmore.com). Ciò significa che ognuno di questi può essere controllato in modo indipendente e può essere esternalizzato a un diverso provider di servizi di messaggistica.

Considerazioni sulla distribuzione di DMARC

DMARC per ricevitori

La verifica DMARC sull'ESA è basata sul profilo, ma a differenza di DKIM, il profilo predefinito deve essere modificato per essere conforme alla specifica. Per impostazione predefinita, l'ESA non rifiuta mai alcun messaggio a meno che non sia esplicitamente indicato dal cliente, quindi per il profilo di verifica DMARC predefinito tutte le azioni vengono impostate su "Nessuna azione". Inoltre, per abilitare la generazione corretta del report, è necessario modificare "Impostazioni globali" della sezione DMARC di "Criteri di posta".

Una volta impostato un profilo, la verifica DMARC, come gli altri due, viene impostata nella sezione Impostazioni predefinite dei criteri di flusso della posta. Assicurarsi di selezionare la casella per inviare report di feedback aggregati - questa è probabilmente la caratteristica più importante di DMARC per il mittente. Al momento della stesura di questo documento, l'ESA non supporta la generazione di rapporti di errore per messaggio (tag "ruf" della politica DMARC).

Poiché le azioni dei criteri DMARC vengono consigliate dal mittente, a differenza di SPF o DKIM, non sono disponibili azioni specifiche configurabili al di fuori della configurazione del profilo. Non è necessario creare filtri dei contenuti.

La verifica DMARC aggiungerà ulteriori campi all'intestazione Authentication-Results:

```
Risultati autenticazione: mx1.hc4-93.c3s2.smtpi.com; dkim=pass (firma
verificata) header.i=MileagePlus@news.united.com; dmarc=pass (p=none
dis=none) d=news.united.com
```

Nell'esempio precedente, risulta che DMARC è stato verificato in base all'allineamento dell'identificatore DKIM e che il mittente ha richiesto il criterio "none" (nessuno). Ciò indica che si trovano attualmente nella fase di monitoraggio della distribuzione DMARC.

Se Fornisci Servizi Di Posta Elettronica Per Altri Domini O Terze Parti

La principale preoccupazione degli ESP per la conformità al DMARC è di ottenere un corretto allineamento degli identificatori. Durante la pianificazione di DMARC, assicurarsi che l'SPF sia impostato correttamente, che tutti gli altri domini rilevanti dispongano dei gateway in uscita nei record SPF e che non inviino messaggi che non verranno allineati, principalmente utilizzando domini diversi per l'identità MAIL FROM e Header From. Questo errore viene spesso generato da applicazioni che inviano notifiche o avvisi tramite posta elettronica, in quanto gli autori delle applicazioni ignorano le conseguenze dell'incoerenza delle identità di posta elettronica.

Come descritto in precedenza, assicurarsi di utilizzare un profilo di firma DKIM distinto per ogni dominio e che il profilo di firma faccia riferimento in modo corretto al dominio per cui si sta firmando, come utilizzato in Intestazione da. Se si utilizzano i propri sottodomini, è **possibile** firmare con una sola chiave, ma assicurarsi di impostare la propria adesione a DKIM per rilassarsi nella politica DMARC ("adkim="r").

In generale, se si forniscono servizi e-mail per un maggior numero di terze parti su cui non si ha un controllo diretto, è buona norma scrivere un documento di orientamento su come inviare un'e-mail che è più probabile che consegnerà. Poiché la posta elettronica da utente a utente è generalmente ben gestita, questa funzione funge principalmente da documento di policy per gli

autori delle applicazioni negli esempi sopra citati.

Se si utilizzano servizi di posta elettronica di terze parti

Se si utilizzano server di terze parti per il recapito di parte del traffico di posta elettronica, il modo migliore è delegare un sottodominio separato (o un dominio completamente diverso) al provider di terze parti. In questo modo possono gestire i record SPF in base alle esigenze, disporre di un'infrastruttura di firma DKIM separata e non interferire con il traffico di produzione. In questo caso, i criteri DMARC per la posta elettronica in outsourcing possono essere diversi da quelli interni. Come già accennato, quando si prende in considerazione l'e-mail consegnata da terze parti, assicurarsi sempre che gli identificatori siano allineati e che la conformità a DKIM e SPF sia impostata in modo appropriato nei criteri DMARC.

(Sub)Domini senza traffico e-mail

Un altro miglioramento di DMARC rispetto alle tecnologie di autenticazione e-mail precedenti è la gestione dei sottodomini. Per impostazione predefinita, i criteri DMARC di un determinato dominio vengono applicati a tutti i relativi sottodomini. Quando si recuperano i record dei criteri DMARC, se non è possibile trovare alcun record a livello Intestazione da FQDN, i riceventi devono determinare il dominio organizzativo [6] del mittente e cercare un record dei criteri in tale posizione.

Tuttavia, i criteri DMARC per un dominio organizzativo possono anche specificare un criterio di sottodominio separato (tag "sp" di un record DMARC) che verrà applicato a tutti i sottodomini che non dispongono di un criterio DMARC esplicito pubblicato.

Nello scenario descritto in precedenza nel capitolo SPF, è possibile:

1. Pubblica un record DMARC esplicito per tutti i sottodomini che **sono** origini di posta elettronica legittime.
2. Pubblicare un criterio Sottodominio di tipo "rifiuto" nel record del criterio Dominio organizzazione per rifiutare automaticamente tutti i messaggi di posta elettronica che eseguono lo spoofing di domini non di invio

Questo tipo di strutturazione dell'autenticazione e-mail offre la migliore protezione possibile dell'infrastruttura e del marchio.

Problemi specifici di DMARC

Il DMARC presenta diversi potenziali problemi, tutti dovuti alla natura e alle carenze di altre tecnologie di autenticazione a cui fa riferimento. Il problema è che DMARC ha fatto emergere questi problemi spingendo attivamente una policy per rifiutare l'e-mail e correlando tutti i diversi identificativi del mittente in un messaggio.

La maggior parte dei problemi si verifica con le mailing list e il software di gestione delle mailing list. I messaggi di posta elettronica inviati a una lista di distribuzione vengono ridistribuiti a tutti i destinatari. Tuttavia, il messaggio e-mail risultante, con l'indirizzo del mittente del mittente originale, verrà recapitato dall'infrastruttura di hosting del gestore della lista di distribuzione, pertanto i controlli SPF per Intestazione - Da non verranno eseguiti (la maggior parte dei gestori della lista di distribuzione utilizza l'indirizzo della lista come Busta - Da (MAIL FROM) e l'indirizzo del mittente originale come Intestazione - Da).

Dal momento che DMARC non è in grado di eseguire SPF, è possibile fare affidamento su DKIM,

tuttavia, la maggior parte dei responsabili delle liste di distribuzione aggiunge anche piè di pagina ai messaggi o contrassegna gli oggetti con il nome dell'elenco, interrompendo così la verifica della firma DKIM.

Gli autori di DKIM suggeriscono diverse soluzioni al problema, tutte di cui si riducono ai responsabili della lista di distribuzione che devono utilizzare l'indirizzo della lista in tutti gli indirizzi Da e che indicano l'indirizzo originale del mittente con un altro mezzo.

Problemi simili derivano dai messaggi inoltrati semplicemente copiando il messaggio originale tramite SMTP nel nuovo destinatario. Tuttavia, la maggior parte degli agenti di posta elettronica attualmente in uso formeranno correttamente un nuovo messaggio e includeranno il messaggio inoltrato in linea o come allegato al nuovo. I messaggi inoltrati in questo modo passeranno DMARC se l'utente di inoltro passa (ovviamente, non è possibile stabilire l'autenticità del messaggio originale).

Esempio Di Piano D'Azione Per L'Implementazione Dell'Autenticazione Della Posta Elettronica

Anche se le tecnologie sono semplici, la strada per implementare un'infrastruttura di autenticazione e-mail completa può essere lunga e tortuosa. Per le organizzazioni di piccole dimensioni e per quelle con flussi di posta controllati, sarà piuttosto semplice, mentre per gli ambienti di grandi dimensioni può essere estremamente difficile. Non è raro che le grandi imprese assumano consulenze per gestire il progetto di implementazione.,

Passaggio 1: DKIM

DKIM è relativamente poco intrusivo in quanto i messaggi non firmati non subiranno alcun rifiuto. Prima di procedere all'attuazione, tenere conto di tutti i punti menzionati in precedenza. Contattare eventuali terze parti alle quali si potrebbe delegare la firma, assicurarsi che le terze parti supportino la firma DKIM e considerare la strategia di gestione selettori. Alcune organizzazioni conservano chiavi (selettori) separate per unità organizzative diverse. Per una maggiore sicurezza, è possibile prendere in considerazione la rotazione periodica delle chiavi, ma è consigliabile non eliminare le vecchie chiavi finché non vengono recapitati tutti i messaggi in transito.

Occorre prestare particolare attenzione alle dimensioni delle chiavi. Sebbene in generale "più è meglio", è necessario tenere presente che la creazione di due firme digitali per messaggio (inclusa la canonizzazione, ecc.) è un'attività molto dispendiosa in termini di CPU e può influenzare le prestazioni dei gateway di posta in uscita. A causa del sovraccarico di elaborazione, 2048 bit è la più grande dimensione di chiave pratica utilizzabile, ma per la maggior parte delle installazioni, le chiavi a 1024 bit rappresentano un buon compromesso tra prestazioni e sicurezza.

Per una corretta implementazione successiva di DMARC, è necessario:

1. identificare tutti i domini inviati come, inclusi i sottodomini
2. genera chiavi DKIM e crea profili di firma per ogni dominio
3. consegnare le chiavi private pertinenti a terze parti
4. pubblica tutte le chiavi pubbliche nelle zone DNS pertinenti
5. verificare che terze parti siano pronte per iniziare la firma
6. attiva l'accesso DKIM alla politica sul flusso di posta RELAYED su tutte le ESA

7. notifica a terzi di iniziare la firma

Passaggio 2: SPF

L'implementazione corretta di SPF sarà probabilmente la parte più impegnativa e dispendiosa in termini di tempo di qualsiasi implementazione dell'infrastruttura di autenticazione della posta elettronica. Dal momento che l'e-mail era molto semplice da utilizzare e gestire e completamente aperta dal punto di vista della sicurezza e dell'accesso, le organizzazioni storicamente non applicavano regole severe su chi e come utilizzarla. Di conseguenza, la maggior parte delle organizzazioni non dispone attualmente di una visualizzazione completa di tutte le diverse fonti di posta elettronica, sia dall'interno che dall'esterno. Il problema principale dell'implementazione di SPF è quello di scoprire chi attualmente invia e-mail in modo legittimo per conto dell'utente.

Elementi da cercare:

1. destinazioni ovvie: server Exchange o altri server groupware o gateway di posta in uscita
2. qualsiasi soluzione DLP o altro sistema di elaborazione e-mail che possa generare notifiche esterne
3. Sistemi CRM che inviano informazioni che interagiscono con i clienti
4. diverse applicazioni di terze parti che possono inviare e-mail
5. lab, test o altri server che possono inviare e-mail
6. personal computer e dispositivi configurati per l'invio diretto di un messaggio e-mail esterno

L'elenco di cui sopra non è completo, in quanto le organizzazioni hanno ambienti diversi, ma deve essere considerato come una linea guida generale su cosa cercare. Una volta identificate (la maggior parte) le fonti di posta elettronica, è possibile fare un passo indietro e, invece di autorizzare ogni singola fonte esistente, pulire l'elenco. Idealmente, tutte le e-mail in uscita dovrebbero essere recapitate attraverso i gateway della posta in uscita con alcune eccezioni giustificate. Se si dispone di una propria soluzione o si utilizza una soluzione di posta di marketing di terze parti, è consigliabile utilizzare un'infrastruttura separata rispetto ai gateway di posta elettronica di produzione. Se la rete di recapito della posta è eccezionalmente complessa, è possibile procedere con la documentazione dello stato corrente nell'SPF, ma occorre del tempo per risistemare la situazione in futuro.

Se servite più domini sulla stessa infrastruttura, potete creare un singolo record SPF universale e farvi riferimento in singoli domini utilizzando il meccanismo di inclusione. Assicurarsi che i record SPF non siano troppo larghi; Ad esempio, se solo cinque computer in una rete /24 inviano SMTP, aggiungere questi cinque indirizzi IP singoli all'SPF, anziché all'intera rete. Cerca di rendere i tuoi documenti il più possibile specifici, in modo da ridurre al minimo il rischio di messaggi di posta elettronica dannosi che potrebbero compromettere la tua identità.

Iniziare con un'opzione softfail per mittenti non corrispondenti ("~all"). Cambiarlo in hardfail (-all) solo quando si è sicuri al 100% di aver identificato **tutte le** fonti di posta elettronica, altrimenti si rischia di perdere l'e-mail di produzione. In seguito, dopo aver implementato DMARC e averlo eseguito in modalità di monitoraggio per un certo periodo di tempo, sarà possibile identificare i sistemi mancanti e aggiornare i record SPF per completarli. Solo in questo caso sarà possibile impostare l'SPF su hardfail.

Passaggio 3: DMARC

Una volta che DKIM e SPF sono configurati nel modo più completo possibile, è il momento di creare i criteri DMARC. Se si dispone di un'infrastruttura e-mail complessa, prendere in

considerazione tutte le situazioni citate nei capitoli precedenti e prepararsi a distribuire più record DMARC.

Creare alias di posta elettronica che riceveranno i report o creare un'applicazione Web in grado di acquisirli. Non ci sono indirizzi e-mail rigorosamente definiti da utilizzare per questo, ma aiuta se sono descrittivi, ad esempio rua@domain.com, dmarc.rua@domain.com, mailauth-rua@domain.com, ecc. Accertarsi di disporre di un processo che consenta a un operatore di monitorare questi indirizzi e modificare in modo appropriato la configurazione di SPF, DKIM e DMARC, oppure avvisare il team di sicurezza in caso di campagna di spoofing. Inizialmente il carico di lavoro sarà considerevole, in quanto i record verranno modificati per coprire eventuali errori verificatisi durante la configurazione di SPF e DKIM. Dopo un po' di tempo, i rapporti indicano probabilmente solo tentativi di spoofing.

Inizialmente, impostare i criteri DMARC su "none" (nessuno) e l'opzione legale per inviare rapporti per **eventuali** controlli non riusciti ("fo=1"). In questo modo verranno rilevati rapidamente eventuali errori nell'SPF e nel DKIM senza influenzare il traffico. Quando sei soddisfatto del contenuto delle segnalazioni inviate, modifica il criterio impostandolo su "quarantena" o "rifiuta", a seconda della politica e della preferenza di sicurezza. Inoltre, assicurarsi che gli operatori analizzino continuamente i report DMARC ricevuti per rilevare eventuali falsi positivi.

L'implementazione completa e corretta di DMARC non è un'attività di piccole dimensioni. Mentre alcuni risultati (e l'"implementazione" formale di DMARC) possono essere ottenuti pubblicando una serie incompleta di record e una politica di "nessuno", è nel miglior interesse sia dell'organizzazione mittente che di Internet nel suo complesso che tutti lo implementino nella piena misura delle sue capacità.

Per quanto riguarda le scadenze, di seguito viene fornita una descrizione molto approssimativa delle singole fasi di un progetto tipico. Di nuovo, poiché ogni organizzazione è diversa, queste sono tutt'altro che accurate:

1. Pianificazione e preparazione DKIM	2-4 settimane
2. Esecuzioni dei test DKIM	2 settimane
3. SPF - identificazione mittente legittimo	2-4 settimane
4. Preparazione della politica DMARC	2 settimane
5. Esecuzione dei test dei record SPF e DMARC	4-8 settimane
6. Esecuzione dei test di SPF con errori hardware	2 settimane
7. Esecuzione dei test DMARC con quarantena/rifiuto	4 settimane
8. Monitoraggio delle relazioni DMARC e adeguamento di conseguenza di SPF/DKIM	continuo

Èprobabile che le organizzazioni di piccole dimensioni abbiano una durata più breve della maggior parte dei passaggi, in particolare i passaggi 3 e 4. Indipendentemente dalla semplicità dell'infrastruttura e-mail che si ritiene di poter utilizzare, assegnare sempre un ampio periodo di tempo durante le esecuzioni dei test e monitorare attentamente i report di feedback per individuare eventuali errori.

Le organizzazioni più grandi potrebbero sperimentare una durata ancora più lunga delle stesse fasi, con requisiti di test più rigorosi. Non è raro che le aziende con infrastrutture di posta elettronica complesse si avvalgano di assistenza esterna, non solo per l'aspetto tecnico dell'implementazione dell'autenticazione della posta elettronica, ma anche per gestire l'intero progetto e coordinare team e reparti.

Ulteriori riferimenti

- Sito di riferimento per SPF: http://www.openspf.org
- Il Consiglio DKIM: http://www.dkim.org
- Sito Web principale DMARC, gestito da The Trusted Domain Project: http://www.dmarc.org
- dmarcian - un sito di risorse e guida gestito da Tim Draegen, uno degli autori di DMARC. Visitare la sezione "Strumenti": http://www.dmarcian.com
- Strumento di convalida dei record di Online Trust Alliance: https://otalliance.org/resources/spf-dmarc-record-validator
- Assistente record DMARC - un altro strumento utile per creare i record DMARC: http://www.kitterman.com/dmarc/assistant.html
- Strumenti di test record SPF: http://www.kitterman.com/spf/validate.html
- "Non essere un phishing: Deep Dive Into Email Authentication Techniques", una presentazione di Cisco Live 2014 su BRKSEC-3770: https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76627

[1] La canonizzazione esula dall'ambito del presente documento. Fare riferimento al materiale nella sezione "Ulteriori riferimenti" per ulteriori informazioni sulla canonizzazione DKIM.

[2] Anche i parametri dei record DNS DKIM esulano dall'ambito di questo documento.

[3] La creazione di filtri messaggi esula tuttavia dalle finalità del presente documento. Per assistenza, fare riferimento ai manuali dell'utente di AsyncOS for Email.

[4] M3AAWG ha definito un'eccellente serie di migliori pratiche applicate e rispettate dalla maggior parte del settore. Il documento relativo alle best practice per i mittenti è disponibile all'indirizzo https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

[5] Questo comportamento sfrutta il fatto che in origine DKIM non verifica affatto l'origine del messaggio come indicato in MAIL FROM o Header From. Viene solo verificato che il parametro ID dominio di firma (parametro "d" della firma DKIM e parametro "Nome dominio" nel profilo di firma) ospita effettivamente la chiave pubblica della coppia utilizzata per firmare il messaggio. L'autenticità del mittente è implicita nella firma dell'intestazione "Da". Assicurati di elencare tutti i domini (e sottodomini) che accedi nella sezione "Utenti del profilo".

[6] In genere, un dominio situato un livello al di sotto del TLD o del prefisso ccTLD pertinente (.ac.uk, .com.sg ecc.)