COME IMPOSTARE DMARC PER LA TUA AZIENDA

Per poter ricevere un certificato VMC (Verified Mark Certificate), l'azienda deve essere conforme al protocollo DMARC (Domain-based Message Authentication, Reporting & Conformance). Questa guida illustra i passaggi necessari per fare in modo che la tua azienda implementi correttamente il protocollo DMARC.

digicert®

digicert®

COS'È DMARC?

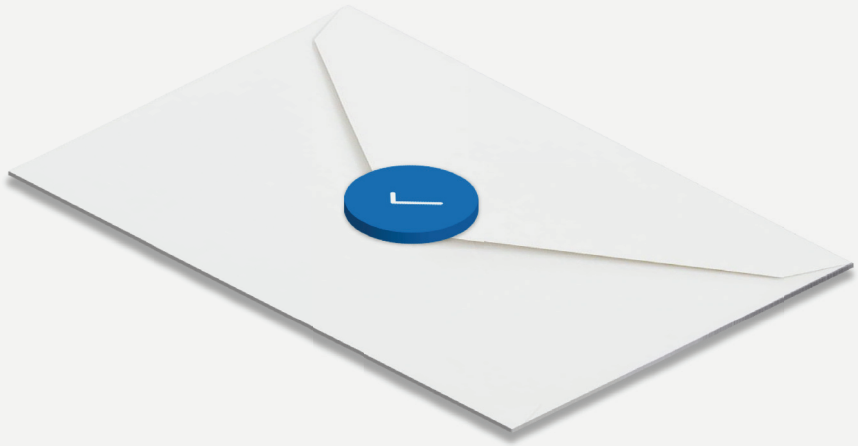
DMARC è un protocollo di autenticazione, policy e reporting per email che consente alle aziende di proteggere il proprio dominio dall'utilizzo non autorizzato, inclusi furti di identità e attacchi di phishing.

Un breve riepilogo

- DMARC è un record TXT archiviato nel DNS che consente ai destinatari delle email di verificare l'autenticità del messaggio ricevuto.
- È progettato per adattarsi al processo di autenticazione in entrata esistente di un'organizzazione e aiuta i destinatari delle email a determinare se un messaggio è "allineato" con le informazioni che il destinatario ha sul mittente.
- Le aziende hanno tre opzioni di policy per gestire i messaggi "non allineati":

- "p = none" (nessun enforcement)
- "p = quarantine"
- "p = reject"

- Affinché DMARC funzioni correttamente, è necessario impostare prima i protocolli Sender Policy Framework (SPF) e DomainKeysIdentified Mail (DKIM).
- L'azienda può verificare il proprio record DMARC tramite alcuni "strumenti" disponibili in Internet, come questo offerto da valimail.com.



UNA MIGLIORE AUTENTICAZIONE DELLE EMAIL INIZIA DA DMARC

L'obiettivo è creare un sistema di mittenti e destinatari che collaborino tra loro per migliorare le procedure di autenticazione delle email dei mittenti e permettere ai destinatari di rifiutare messaggi non autenticati.

digicert®

PERCHÉ DMARC?

DMARC offre quattro importanti vantaggi:

1. **Sicurezza**

   Proteggi le persone dallo spam, dalle frodi e dal phishing bloccando l'uso non autorizzato del tuo dominio email.

2. **Visibilità**

   Ottieni rapporti dettagliati su chi (e/o cosa) su Internet sta inviando email utilizzando il tuo dominio.

3. **Deliverability**

   Aumenti la deliverability del 5-10% ed eviti che le email vengano segnalate come SPAM.

4. **Protezione del marchio**

   Difendi il tuo marchio contro gli attacchi mirati all'identità.

dei clienti ha meno probabilità di interagire con un'azienda dopo aver subito un attacco di phishing da qualcuno che si è spacciato per tale azienda.

digicert®

COME IMPOSTARE SPF:

1. Raccogli gli indirizzi IP utilizzati per inviare email dal tuo dominio, inclusi:
    - Server web
    - Server email in ufficio
    - Server email dell'ISP
    - Eventuali server email di terze parti
2. Fai un elenco dei tuoi domini di invio e di quelli non di invio.
3. Crea un record SPF in .txt per ogni dominio utilizzando un editor di testo (ad esempio Notepad++, Vim, Nano, ecc.)

    Esempio 1: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:x.x.x.x -all
    Esempio 2: v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:thirdparty.com -all

4. Pubblica il tuo SPF su DNS.

    Se gestisci il tuo DNS, aggiungi un nuovo record TXT contenente il testo SPF. Se non gestisci il tuo DNS, contatta l'amministratore del tuo server per aggiungere il record.

5. Una volta che il record è stato aggiunto al DNS, controllalo utilizzando uno strumento di controllo SPF.

COS'È SPF?

Non farti sorprendere da mittenti non autorizzati. Neutralizzali!

SPF è lo standard che ha aperto la strada al concetto di autenticazione delle email basata sul dominio. Previene lo spoofing consentendo ai proprietari di domini di approvare automaticamente gli indirizzi IP dei server autorizzati a inviare email per conto del dominio. Se un server di posta con un indirizzo IP che non è nell'elenco cerca di inviare email utilizzando quel dominio, SPF lo blocca.

digicert®

COME IMPOSTARE DKIM:

1. **Scegli un selettore DKIM.**

   Deve essere una semplice stringa di testo definita dall'utente che verrà aggiunta al nome di dominio per facilitare l'identificazione della chiave pubblica DKIM (ad es. “standard”).

   Esempio: “standard._domain.example.com” = nome host

2. **Genera una coppia di chiavi pubblica-privata per il tuo dominio.**

3. **Crea e pubblica un nuovo record TXT**

   Crea un nuovo record tramite la tua console di gestione DNS usando la chiave pubblica della coppia qui sopra.

   Esempio: v=DKIM1; p=YourPublicKey

COS'È DKIM?

Evita che le email vengano manomesse durante il transito

DKIM è uno standard di autenticazione delle email che utilizza la crittografia a chiave pubblica/privata per firmare le email.

Viene utilizzato per verificare che l'email provenga dal dominio a cui è associata la chiave DKIM e che non sia stata modificata durante il transito.

IMPOSTAZIONE DELLA MODALITÀ DI MONITORAGGIO DI DMARC

1. Assicurati di aver impostato correttamente SPF e DKIM
2. Crea un record DNS

   Il record DMARC “txt” deve essere denominato in modo simile a “_dmarc.your_domain.com.”

   Esempio: “v=DMARC1;p=none; rua=mailto:dmarcreports@your_domain.com”

   Se gestisci il DNS per il tuo dominio, crea un record DMARC “p=none” (modalità di monitoraggio) allo stesso modo dei record SPF e DKIM.

   Se non gestisci il DNS, chiedi al tuo provider DNS di creare il record DMARC per te.

3. Testa il tuo record DMARC tramite uno strumento di controllo DMARC-

digicert®

CHE COS'È LA MODALITÀ DI MONITORAGGIO DI DMARC?

Acquisisci visibilità sul traffico in uscita dal tuo dominio

La modalità di monitoraggio consente ai proprietari di domini di esaminare i rapporti DMARC contenenti il traffico di email per il dominio stesso.

I report identificano potenziali messaggi di errore che verrebbero messi in quarantena o rifiutati una volta che DMARC è impostato per un enforcement completo. Inoltre, i report DMARC mostrano informazioni su tutti i sistemi e servizi che inviano email dal dominio monitorato.

NOTA: la modalità di monitoraggio non fornisce alcun livello di enforcement. Le email che non superano l'autenticazione vengono recapitate normalmente, evitando potenziali interruzioni durante l'implementazione di DMARC.

digicert®

TAG COMUNI USATI NEI RECORD .TXT DI DMARC

NOME TAG	OBBLIGATORIO	SCOPO
V	OBBLIGATORIO	VERSIONE PROTOCOLLO
P	OBBLIGATORIO	VERSIONE POLITICA
PCT	FACOLTATIVO	% DI MESSAGGI SOGGETTI A FILTRAGGIO
RUA	FACOLTATIVO	REPORTING UTI DEL REPORT AGGREGATO
SP	FACOLTATIVO	POLICY PER SOTTODOMINI DEL DOMINIO

digicert®

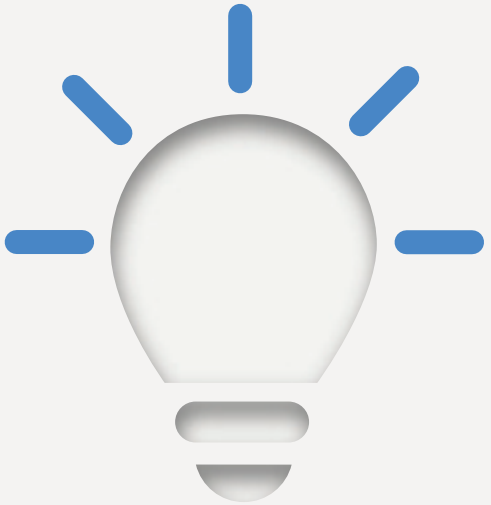
QUALI INFORMAZIONI FORNISCE IL REPORT DMARC?

Il report mostra ai proprietari del dominio quanti messaggi fraudolenti stanno usando il loro dominio, da dove provengono e se sia possibile fermarli con una policy di “quarantine” o di “reject” di DMARC.

Per ogni destinatario viene creato un file XML che include i seguenti campi:

- Un conteggio dei messaggi da ognuno di questi indirizzi IP
- L'azione adottata su questi messaggi in base alla policy DMARC mostrata
- I risultati SPF per questi messaggi
- I risultati DKIM per questi messaggi

Anche se leggibile, il rapporto XML non è pratico. I proprietari di un dominio potrebbero preferire un lettore di report DMARC, come Valimail o un altro fornitore di servizi DMARC.



4 MODI PER UTILIZZARE IL REPORT DMARC

Prima di avviare l'enforcement è importante dotarsi di un buon livello di base

1. Identifica il traffico contrassegnato come non legittimo.

2. Cerca le email legittime contrassegnate come non legittime da DMARC. Una volta avviato l'enforcement, a seconda della policy le email possono essere rifiutate o messe in quarantena (“rejected” o “quarantined”).

3. Contatta potenziali proprietari di sistemi/applicazioni per chiarire la legittimità delle email contrassegnate come non legittime.

4. Se necessario, aggiorna il tuo record SPF inserendo gli indirizzi nella lista degli indirizzi IP legittimi ma non inclusi in precedenza.

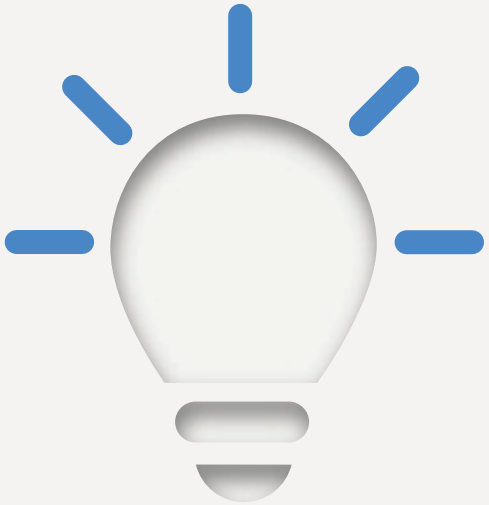
digicert®

USA I REPORT DMARC PER FARE ORDINE NEL SISTEMA PRIMA DI AVVIARE L'ENFORCEMENT

L'analisi dei report DMARC può richiedere molto tempo. Tuttavia, se i proprietari di domini non verificano o identificano erroneamente i mittenti, possono finire per bloccare le email "buone" quando la policy DMARC è impostata sull'enforcement ("quarantine" o "reject"), il che può allungare ulteriormente i tempi compromettendo l'efficienza dell'operazione.

Ecco quindi alcune attività interne suggerite prima di iniziare l'enforcement DMARC:

- Fai l'inventario di tutti i mittenti di email identificati dal report DMARC e di altri menzionati dagli stakeholder
- Per ogni servizio/mittente email, identifica un proprietario
- Classifica i servizi di invio come autorizzati, non autorizzati o nocivi
- Identifica, con il supporto degli stakeholder, qualsiasi altro mittente che potrebbe non comparire nel report DMARC
- Chiedi conferma agli stakeholder di ogni nuovo mittente identificato
- Aggiorna il tuo record SPF con l'indirizzo IP del mittente email legittimo appena rilevato



RACCOMANDAZIONI PER LE COMUNICAZIONI PRE-ENFORCEMENT

5 consigli per migliorare l'adozione

- Documenta una policy di implementazione e condividila con gli stakeholder.
- Contatta un fornitore di supporto DMARC come Valimail se le attività DMARC sono troppo impegnative o ti serve assistenza.
- Comunica i nuovi risultati dei report DMARC non appena sono disponibili.
- Avvia la distribuzione DMARC come progetto interno.
- Chiedi al tuo team dirigenziale di farsi promotore del progetto.

PER QUANTO TEMPO DMARC DEVE RESTARE IN MODALITÀ DI MONITORAGGIO?

Il tempo varia da un'azienda all'altra, e le grandi aziende spesso impiegano più tempo rispetto a quelle piccole. Pianifica le attività per settimane o mesi.

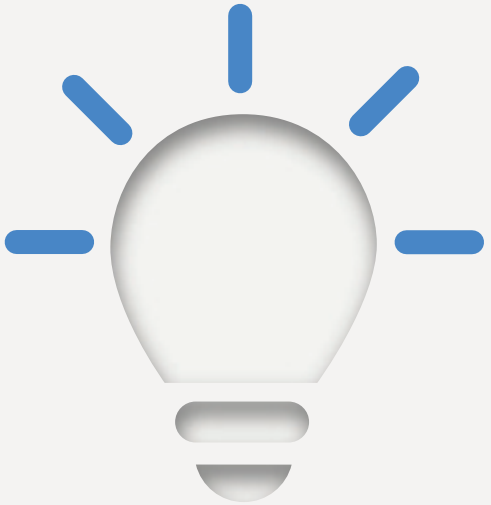
Quando sei sicuro che il tuo inventario sia completo, che tutti i mittenti autorizzati siano stati mappati e la tua organizzazione sia sufficientemente informata, passa alla fase di quarantena.

Quando è attiva la modalità di quarantena, i messaggi che non superano l'autenticazione vengono messi in quarantena. Di solito questo significa che i messaggi vengono recapitati nella cartella spam di un utente.

COME IMPOSTARE L'ENFORCEMENT DELLA QUARANTENA DI DMARC

1. Accedi al tuo server DNS e cerca il record DMARC
2. Apri il record DMARC per il dominio specificato e aggiorna la policy da “p=none” a “p=quarantine”
   Esempio: “v=DMARC;p=quarantine;pct=10;rua=mailto:dmarcreports@you_domain.com”
3. Aggiungi il flag “pct” (% di messaggi soggetti a filtro). Ti consigliamo di iniziare con il 10%.
4. Aumenta gradualmente la percentuale di messaggi filtrati fino a “pct=100” (100%) quando hai preso familiarità con il sistema.

   NOTA: Devi essere a “pct=100” per soddisfare gli standard BIMI e VMC, ma la tua policy può essere “quarantine” o “reject”.



COME FUNZIONA IL FLAGGING:

- Se una policy viene specificata come diversa da “p=none”, verrà applicata secondo la percentuale nel flag “pct”
- Al resto verrà applicata la successiva policy meno restrittiva (ad es. per un record DMARC con “p=quarantine” e “pct=10”, verrebbe messo in quarantena il 10% del traffico in errore e l'altro 90% verrebbe consegnato normalmente)

UNA VOLTA RAGGIUNTO IL FILTRAGGIO DEL 100%, PUOI PASSARE A "P=REJECT", IL MASSIMO LIVELLO DI ENFORCEMENT.

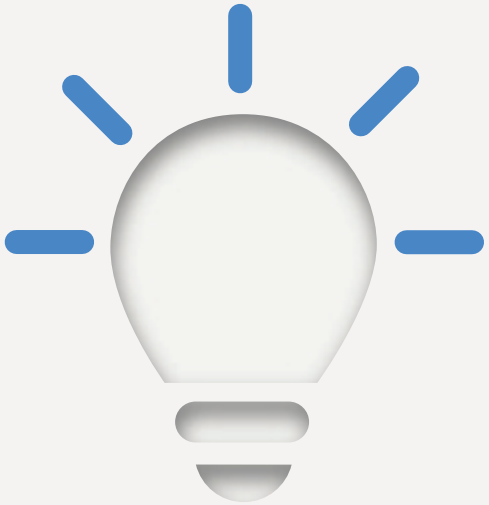
digicert®

COME IMPOSTARE LA POLICY REJECT DI DMARC

1. Apri il tuo record DMARC tramite la tua console DNS
2. Modifica “p=quarantine” in “p=reject”
   Esempio: “v=DMARC;p=reject;pct=100;rua=mailto:dmarcreports @ you_domain.com
3. Salva il record

CONSIGLIO: è particolarmente importante continuare il monitoraggio in questa fase, per evitare che email legittime vengano rifiutate ed eliminate.

Hai altre domande? Scrivici oggi a contactus@digicert.com o visitaci su https://www.digicert.com/it/tls-ssl/verified-mark-certificates/



CHE COSA FA LA POLICY REJECT ALLE EMAIL?

Tutti i messaggi che non superano il controllo DMARC (email non autorizzate) vengono bloccati/eliminati, il destinatario non li riceverà mai né sarà a conoscenza della loro cancellazione.