DMARC: un record dns per proteggere noi stessi e i nostri clienti dall’email SCAM

Author : Marco Giuricin

Date : 7 Marzo 2019

Cos’è lo SCAM?

SCAM è un tentativo pianificato di truffa con metodi di ingegneria sociale, come ad esempio fingere di essere qualcun altro, o qualcos’altro, a scopo fraudolento.

Questo può essere fatto di persona, per telefono, tramite profili social, siti web e anche tramite email, sfruttando ulteriori tecniche malevole come **spam** e **phishing**.

Un tipico esempio di Scam è la "truffa alla nigeriana", in cui viene inviata un'email nella quale si parla di grosse somme di denaro che dovrebbero essere trasferite (o recuperate) da una banca estera che chiede alcune garanzie come la cittadinanza, un conto corrente, un deposito cauzionale. Lo scammer perciò chiede aiuto sia per trasferire il denaro tramite il conto di chi legge, sia per anticipare il deposito cauzionale; come ricompensa si promette una percentuale del denaro recuperato, che non arriverà mai.

Altri **classici esempi** di Scam sono email che condizionano una vincita a una qualsiasi lotteria al versamento di una certa tassa: ovviamente, non esiste nessuna vincita e la tassa pagata viene rubata.

Un moderno esempio di Scam via chat telegram è il giveaway di cryptovalute in cui, se si versano un tot di token in un wallet a scopo di “verifica del mittente”, ne ritorneranno 10 volte tanti al wallet mittente dal wallet destinatario… ma ovviamente non succederà mai.

Nell’era del marketing, l’email è ancora uno strumento utilizzatissimo ma - essendo datato e non nato sicuro “by design” - è ancora molto appetibile per i malintenzionati.

Figura 1 (blog.prisync.com)

Quando qualche nostro cliente è vittima di scam tramite email e qualcuno si sta fingendo un dipendente o una mailing list della nostra azienda, si entra in **una situazione antipatica, con implicazioni giuridiche** (vedi GDPR) in cui è certamente meglio dimostrare di aver fatto di tutto per proteggere noi stessi e gli altri da questo fenomeno.

Quello che certamente dobbiamo evitare che accada è che qualcuno sia in grado di inviare una email dal dominio di posta della nostra compagnia: un discorso è se lo scammer “finge” di essere un mittente accreditato, un altro discorso è se riesce ad “esserlo” veramente.

Infatti, volendo fare un esempio recente, è relativamente semplice per chi ha dimestichezza con le email capire se il mittente ci scrive da PosteItaliane.it o se si è vittime della truffa postepay e bancoposta semplicemente andando ad espandere i dettagli del mittente della email per vedere se arriva dal dominio @posteitaliane.it: **l’indirizzo sarà pincopallino@posteitaliane.it e non weioru9932923@2387ss.ru**, a prescindere dal nome visualizzato nella email; a meno che qualcuno sia riuscito a rubare le credenziali di accesso di un account valido, implementando il DMARC in modo sufficientemente restrittivo non sarebbe possibile ricevere una email da @posteitaliane.it se non fosse stata inviata - ed autenticata - da quel dominio.

Questo sarebbe valido se le cassette di posta riceventi facessero parte di server mailbox abbastanza evoluti da implementare i metodi di autenticazione per filtrare i messaggi di posta “sospetti” compatibili con il DMARC, che al giorno d’oggi sono tutti i principali (google, facebook, microsoft, yahoo, etc…).

Cos’è il DMARC?

Acronimo di “Message-based Domain Authentication, Reporting & Conformance”, è una specifica tecnica creata da un gruppo di organizzazioni per ridurre il rischio di abusi via email

grazie all’utilizzo di una coppia di protocolli di autenticazione.

È un metodo di protezione nativo del server di posta che implementa il mittente e, quindi, del tutto diverso da filtri antispam e tecniche simili, che solitamente sono configurate dai riceventi utilizzando server ed applicazioni aggiuntive.

L’implementazione del DMARC si basa su due procedure di autenticazione ben precise: **SPF** e **DKIM**.

2. **SPF** (Sender Policy Framework) prevede l’inserimento di un record nel DNS del dominio di posta mittente che consente a determinati IP di mandare e-mail tramite quel dominio. Durante la verifica degli indirizzi IP verranno dunque identificati eventuali indirizzi email non autorizzati. La lista degli indirizzi IP certificati a cui si fa riferimento è quella presente nel “Return Path” della email. Detto in altri termini, la procedura SPF consente di riconoscere se **chi invia l’email da un determinato indirizzo email è realmente autorizzato a farlo**.
   Come vantaggio l’SPF è facile da configurare e non implica particolare overhead computazionale sui sistemi che inviano e ricevono posta elettronica.
3. **DKIM** (DomainKeys Identified Mail) fa sì che l’email in uscita venga contrassegnata con una firma digitale che il server di posta ricevente confronterà con la chiave pubblica inserita nel DNS del dominio mittente. Se la firma corrisponde alla chiave pubblica significa che il mittente è verificato e che l’email ricevuta è stata inviata, senza essere stata sottoposta a successive modifiche, dal mittente indicato nella mail che stiamo leggendo.
   Come vantaggio, Dkim non controlla gli ip dei mittenti ma richiede un minimo di overhead in invio e ricezione per elaborare la firma digitale allegata al messaggio.

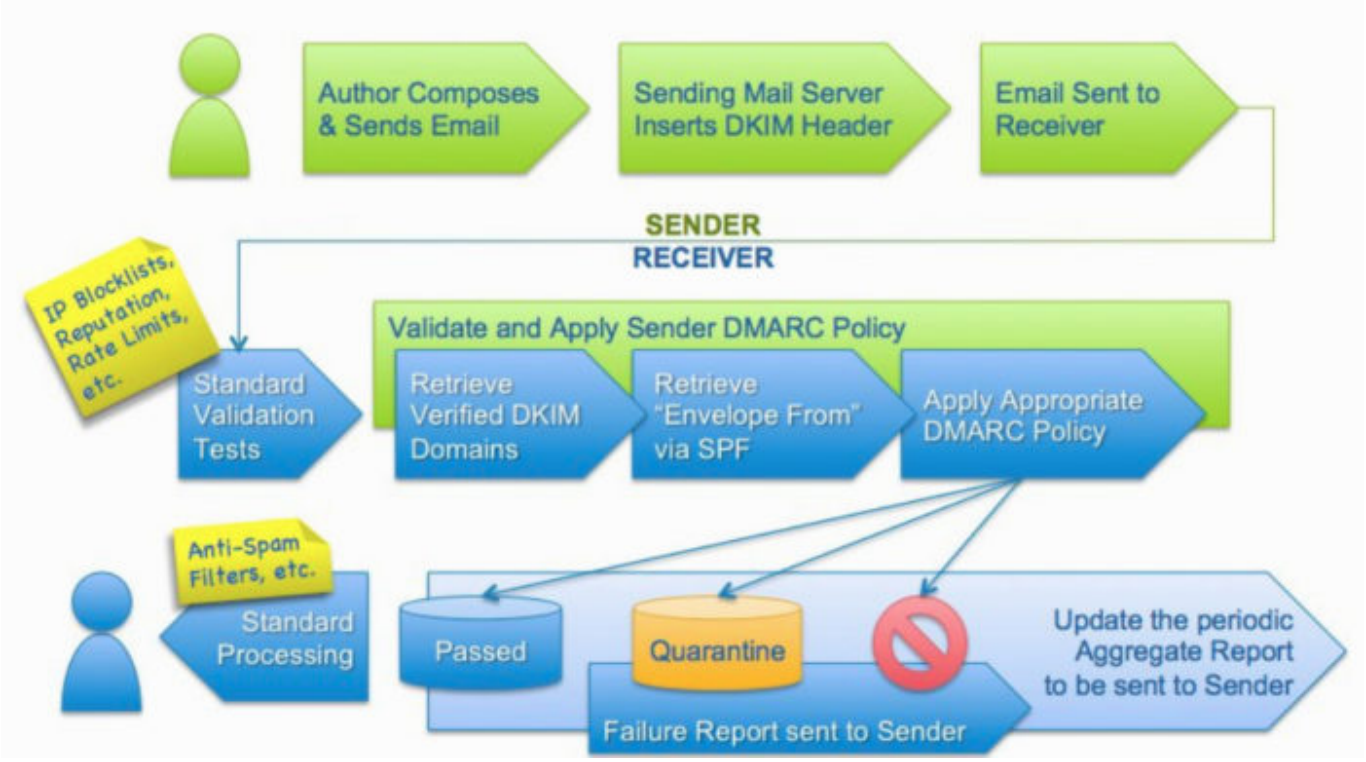

Figura 2 Flusso di posta (dmarc.org)

In sostanza, i due metodi si completano a vicenda ed è fortemente consigliato utilizzarli entrambi, soprattutto se la nostra posta passa per email forwarders che richiedono molta attenzione nel configurare il record SPF (i server di inoltro della posta potrebbero non essere presenti nella *whitelist* degli ip mittenti).

Figura 3 Email Forwarding SPF fail (dmarc.org)

Come funziona il DMARC

In effetti implementare il record DMARC è molto semplice, poiché si tratta solo di aggiungere un record DNS nello stesso dominio dns del proprio server di posta elettronica (dove esiste il record MX).

Il DMARC è una **protezione in uscita:** sono gli amministratori del dominio di posta mittente che decidono di comunicare ai riceventi come filtrare le email.

Le email considerate illecite dal server di posta ricevente (su indicazione dei record dns del mittente) potrebbero essere ricevute se la policy del mittente è *approve*, non andranno nella cassetta spam degli utenti ma verranno ignorate se la policy è *reject* oppure andranno in “junk” se la policy è quarantine.

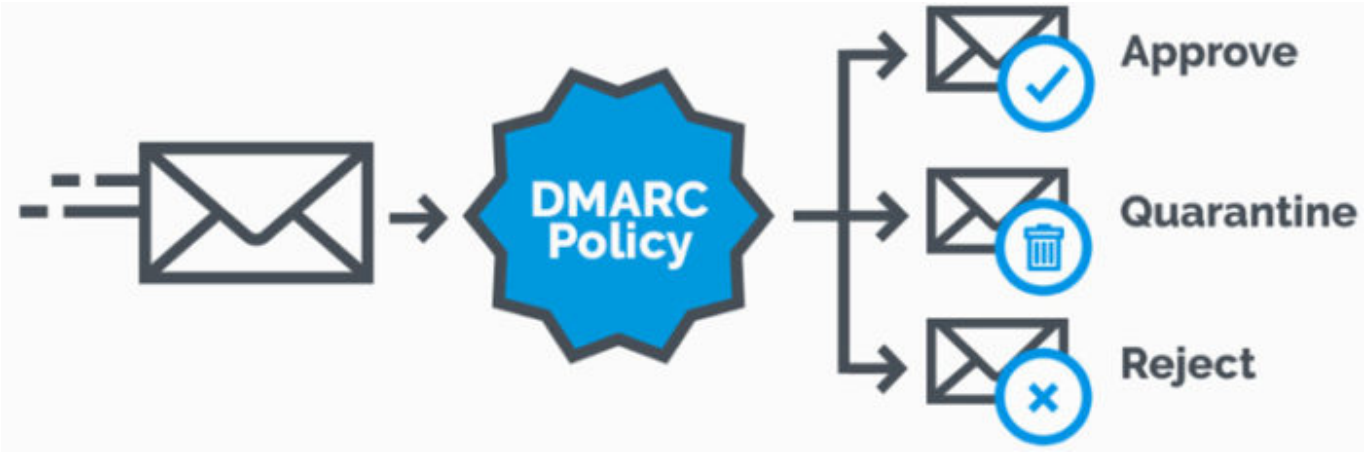

Figura 4 Policy Dmarc (www.dmarcanalyzer.com)

È possibile indicare nel record DMARC indirizzi di posta a cui inoltrare report xml e forensi delle email scartate (illegittime) per un'analisi del flusso di posta che sia anche compliant con il GDPR.

Quando per la prima volta si introduce il record DMARC **è consigliabile avere un approccio “soft”**, istruendo i destinatari ad accettare tutte le email (approve) ma notificarci quali sarebbero state scartate se avessimo impostato una policy più restrittiva: in questa fase potremmo anche non avere alcun metodo di autenticazione SPF e/o DKIM impostato.

Tramite strumenti di analisi adeguati esistenti sul mercato, possiamo andare ad affinare e correggere i nostri record DNS affinche tutte quelle newsletter inviate, ad esempio, da terzi per nostro conto siano incluse nei mittenti attendibili; fino ad arrivare al punto di applicare policy sempre più restrittive senza creare disservizi per il business della nostra azienda e, allo stesso tempo, proteggere lei ed i clienti dallo SCAM.

Figura 5 Analisi forense (vitolavecchia.altervista.org)

Questi strumenti, relativamente economici ma di grande aiuto, permettono anche di inviarci report periodici da esaminare, effettuare controlli e mandarci avvisi sulla compliance, sulla correttezza dei nostri record e - soprattutto - ci offrono la possibilità di esaminare gli headers dei feedback ricevuti dai server destinatari e gli headers delle email illegittime, utili nelle attività di

indagine forense.

Articolo a cura di **Marco Giuricin**