Configurazione record DMARC

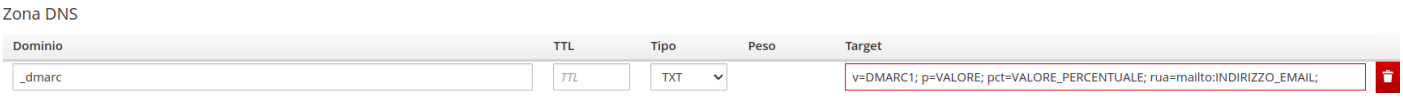
In questa guida spiegheremo come configurare il record DMARC (Domain-based Message Authentication, Reporting and Conformance), illustrando i tag che possono essere utilizzati per determinare il suo funzionamento secondo le vostre esigenze specifiche.

Questo record DNS indica al ricevente di una email come comportarsi nel caso i controlli eseguiti sui record SPF (Sender Policy Framework) e DKIM (DomainKeys Identified Mail), che certificano la validità dell'indirizzo IP e del dominio utilizzati per l'invio, dovessero fallire. Per questo motivo, per poter utilizzare il record DMARC è necessario configurare anche i record SPF e DKIM.

> I record SPF e DKIM vengono applicati solo per un dominio, nel caso siano utilizzati dei sottodomini per l'invio di email è necessario configurarli separatamente per ciascuno di essi.

> I record SPF e DKIM vengono configurati automaticamente sulle zone DNS Artera all'attivazione del nostro servizio di posta. Eventuali sottodomini non sono considerati nella configurazione predefinita delle zone DNS Artera.

Il record DMARC è di tipo TXT ed è costituito da tag che ne definiscono il funzionamento, separati da ";" ad esempio:



Dove "VALORE", "VALORE_PERCENTUALE" e "INDIRIZZO_EMAIL" sono variabili che andranno impostate secondo le vostre preferenze. Di seguito vediamo di cosa si tratta, illustrando anche altri parametri utilizzabili.

> Nelle zone DNS di Artera è possibile inserire solo il dominio di terzo livello come dominio, il sistema lo interpreterà per intero: nel caso dello screenshot di esempio _dmarc sarà interpretato come _dmarc.dominio.tld.
> Per maggiori informazioni su come modificare le zone DNS di Artera consigliamo di consultare la nostra guida Come modificare i DNS.

Cominciamo con i tag essenziali necessari per avere un controllo minimo:

- Il tag "**v=DMARC1**" definisce il protocollo DMARC.

- Il tag "**p=**VALORE" specifica l'azione da eseguire nel caso una email non superasse i controlli SPF o DKIM. La componente denominata "VALORE" nell'esempio può essere definito con:

  none: il destinatario non esegue alcuna azione;
  quarantine: indica al destinatario di identificare come spam le email;
  reject: indica al destinatario di rifiutare i messaggi.

- Il tag "**rua=**mailto:INDIRIZZO_EMAIL" invia i rapporti di stato aggregati all'indirizzo indicato come "INDIRIZZO_EMAIL".

  > I rapporti di stato aggregati contengono informazioni sintetiche (data e arco temporale di riferimento, dominio e IP utilizzati per l'invio, risultato delle verifiche SPF e DKIM, la politica DMARC utilizzata, il dominio associato ai record SPF e DKIM). Questi rapporti vengono mandati una volta al giorno (è possibile modificare questo periodo con l'apposito tag che vedremo sotto) e contengono le informazioni relative a tutte le email inviate in questo arco di tempo.

  Avremo ad esempio:

  ```
  v=DMARC1; p=quarantine; rua=mailto:esempio@esempio.com;
  ```

  Il record DMARC configurato in questo modo farà in modo che il destinatario dell'email, che supporti DMARC, riconosca come spam i messaggi che non superano i controlli SPF e DKIM. Il sistema invierà successivamente un rapporto aggregato all'indirizzo definito nel record, in questo caso esempio@esempio.com.

Il record DMARC può essere migliorato utilizzando altri tag, che ne definiscono il funzionamento sotto vari aspetti differenti. Di seguito trovate la loro descrizione:

- Il tag "**ri=**VALORE" definisce il numero di secondi trascorsi tra ciascun invio dei rapporti aggregati al mittente. Il valore predefinito indicato dalla variabile "VALORE" (se non indicato nel record DMARC) è 86.400 (24 ore), ma può essere personalizzato con frequenze maggiori (48, 72 ore)

  Ad esempio:

  ```
  v=DMARC1; p=quarantine; rua=mailto:dmarc@dominio.tld; ri=172800;
  ```

  In questo caso i rapporti di stato aggregati verranno inviati ogni 48 ore, anziché ogni 24

ore.

- Il tag "**pct=**VALORE_PERCENTUALE" (visto nel primo screenshot di esempio) definisce la percentuale di email da trattare con l'azione definita da "**p=**" (visto in precedenza). Il "VALORE_PERCENTUALE" può essere specificato indicando una cifra compresa tra 1 e 100, ma quello predefinito (se non indicato nel record DMARC) è 100. Nel caso si definisse un valore differente da 100 la parte esclusa verrebbe trattata con l'azione di livello inferiore (se p=reject, la percentuale esclusa verrebbe trattata come p=quarantine; se p=quarantine, la parte esclusa sarebbe trattata come p=none).

  Ad esempio:

  ```
  v=DMARC1; p=reject; pct=70; rua=mailto:dmarc@dominio.tld;
  ```

  In questo caso il 70% delle email inviate dal dominio verrebbe tratta con l'azione reject, mentre il 30% verrebbe trattata con l'azione quarantine.

  > Consigliamo di non specificarlo o di definirlo a 100, in quanto valori diversi possono essere utili solo per un test graduale della configurazione.

- Il tag "**sp=**VALORE" definisce l'azione da eseguire se email con indirizzi corrispondenti a sottodomini falliscono i controlli SPF o DKIM. La componente denominata "VALORE" segue i criteri del tag "**p=**" indicati in precedenza.

  Avremo ad esempio:

  ```
  v=DMARC1; p=reject; rua=mailto:esempio@esempio.com; sp=none;
  ```

  In questo caso il record DMARC, in aggiunta a ciò che abbiamo indicato prima, segnalerà al destinatario di non eseguire alcuna azione se il messaggio è stato inviato da un sottodominio attivo sul dominio su cui è stato configurato il record DMARC.

- Il tag "**ruf=**mailto:INDIRIZZO_EMAIL" invia rapporti forensi di eventuali fallimenti all'indirizzo indicato come "INDIRIZZO_EMAIL".

  > Differisce dal tag "**rua**" visto in precedenza in quanto invia subito rapporti dettagliati per ciascuna email che dovesse fallire i controlli SPF, DKIM e DMARC, permettendo di recuperare tempestivamente l'indirizzo IP di un eventuale invio fraudolento o identificare eventuali errori da correggere; tuttavia non tutti supportano questa opzione, è possibile quindi non ricevere questo rapporto dal destinatario.

- Il tag "**fo=**VALORE" definisce il tipo di fallimento da segnalare per i rapporti forensi. La componente denominata "VALORE" può essere:

  fo=0: genera un rapporto di errore DMARC se tutti i meccanismi di autenticazione (SPF e DKIM) non riescono a produrre un risultato "passato". Questo è il valore Predefinito (se non indicato nel record DMARC);
  fo=1: genera un rapporto di errore DMARC se un meccanismo di autenticazione (SPF o DKIM) ha generato un risultato diverso da "passato";
  fo=d: genera un rapporto di errore DKIM se il messaggio ha una firma che non supera il controllo di verifica;
  fo=s: genera un rapporto di errore SPF se il messaggio non superato la verifica SPF.

  > Questo tag è opzionale e dev'essere utilizzato con il tag **"ruf"** visto nel punto precedente, in quanto definisce che tipo di rapporto forense inviare.

- Il tag "**adkim=**VALORE" definisce il grado di corrispondenza con il record DKIM. La componente denominata "VALORE" può essere:

  r: verrà accettato qualsiasi sottodominio valido;
  s: le intestazioni delle e-mail devono combaciare con il dominio negli header delle e-mail.

- Il tag "**aspf**=VALORE" determina quanto i messaggi devono corrispondere alle firme SPF. La componente denominata "VALORE" può essere:

  r: verrà accettato qualsiasi sottodominio valido;
  s: le intestazioni delle e-mail devono combaciare esattamente con il dominio nel comando "SMTP Mail FROM".

  Avremo ad esempio:

  ```
  v=DMARC1; p=reject; rua=mailto:dmarc@dominio.tld; adkim=s; aspf=s;
  ```

  In questo caso il record DKIM si comporterà come indicato in precedenza, indicando in

aggiunta che il record DKIM e SPF configurati sul dominio che invia l'email debbano combaciare perfettamente con quelli riportati nell'intestazione dell'email inviata.

Se il dominio viene utilizzato anche per l'invio di email tramite servizi esterni (come ad esempio piattaforme per l'invio di newsletter o l'invio di fatture) è necessario configurare:

- il record SPF aggiungendo l'IP del server utilizzato per spedire;
- il record DKIM fornito dal gestore del servizio.

Senza questi accorgimenti le email inviate dai servizi esterni potrebbero essere gestiti in modo indesiderato, a seconda del record DMARC impostato sul dominio, e riconosciute come spam dai server dei destinatari delle email.

Per qualsiasi chiarimento o richiesta di supporto per la configurazione del record DMARC potete contattare il nostro supporto aprendo un ticket dalla vostra area riservata admin.artera.net oppure scrivere una email a support@artera.net.

Revision #32
Created 10 June 2022 14:58:24 by Jacopo Re
Updated 10 February 2023 09:48:49 by Paolo Dainotti