

I Record DNS per una posta più "deliverabile"

I server di posta di WhiteReady supportano:

- DKIM
- SPF
- DMARC

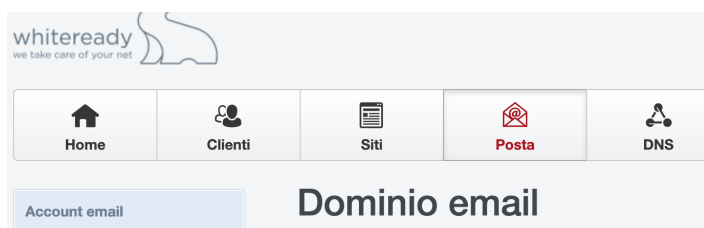
Si tratta di tre record DNS (e qualche "cosa" aggiuntiva).

Il record DKIM:

DKIM (acronimo per **Domain Keys Identification Mail**) è un metodo utilizzato per impedire ai malintenzionati di falsificare la propria identità via email. Analizzando la parte del dominio dell'indirizzo di spedizione, il sistema DKIM verifica se il messaggio giunge dalla fonte dichiarata oppure no e se il suo contenuto (firmato digitalmente) è stato alterato. In sintesi, si tratta di un servizio di "certificazione" del messaggio.

DKIM **viene implementato inserendo alcune informazioni nel record DNS** del proprio dominio, in particolare nel campo CNAME; il mittente ottiene una firma digitale che ne garantisce identità e provenienza. In questo modo è possibile prevenire il phishing che tenti di abusare del proprio dominio o intercettare e manipolare il contenuto del messaggio, incrementando invece la deliverability delle email legittime.

Per attivare il DKIM, sul pannello di controllo è sufficiente andare su "Posta"



quindi cliccare sul proprio dominio e attivare il DKIM cliccando sul tasto apposito

Dominio email

Dominio

Server: condor.whiteready.com

Cliente: WhiteReady :: Xarface (XarFace)

Dominio: whiteready.net

Filtro Spam: Normale

Attivo: ☒

DomainKeys Identified Mail (DKIM) - Chiave di identificazione dominio mail

abilita DKIM: ☒

Selettore di chiave DKIM: default

Chiave privata DKIM:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDFBf2HJtqn5o8zciO9JXOkmge/4
wBjZqCwZ0C+0V6yzv12cp75d9niQMA4rJ/4cFrQelr
V6mMJ1AzwZm5BXhVWEt9i+6m0ad1Al4/DikHx0Jz
AoGAb+Kb/AE7kLekwMFjvEklZ+c02Wny3pXhpyTct
bQ6Q+66D2a+EstWB19gCY82dRpUR8TURhfuG3X:
pB4XQ+vePruglg5M/hlxpz9zqsPRRev1pBldwC47rk
aMrfBFgve8LJxae30PdsiF9/ktSjbjQrbj4RCdVxvyG4l
CNX5hPx1AkEA2wWkqkVTt9VFfSJGaGn+uEXEcc3l
o9HC1O2Tu4qmlI6JGuhm3lr5EIVSP5GQQwJASXQl
-----
```

Genera chiave DKIM Privata

DNS-Record: default._domainkey.whiteready.net. 3600 IN TXT "p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKp3gnfYiewBjZqCwZ0C+0V6yzv12cp75d9niQMA4rJ/4VWEt9i+6m0ad1Al4/" "DikHx0JzynIKmc2MqWFI5RT"

Il sistema provvederà automaticamente a modificare il record DNS e a inserire i dati e i record necessari.

Il record SPF:

Il Sender Policy Framework è un ulteriore metodo utilizzato per prevenire la contraffazione dell'indirizzo del mittente, ovvero l'uso di indirizzi falsi da parte di terzi. Consente al server di posta di verificare che le email in ingresso da un dominio provengano da uno smarthost autorizzato dall'amministratore di tale dominio. In pratica, il proprietario del dominio dichiara che tutte le sue mail sono trasportate dallo smarthost X, e che dunque qualsiasi mail che viaggi per altri canali è da considerare falsa.

Similmente a DKIM, anche il protocollo SPF viene implementato tramite modifiche al DNS del dominio.

Per implementare il record FTP, dal pannello di controllo è necessario andare su "DNS",



clicare sul proprio dominio quindi cliccare sul pulsante verde "SPF" ed editare opportunamente il campo.

DNS SPF Record

DNS SPF

Hostname:

SPF-Record:

Meccanismo SPF:

Consenti ai server elencati come
MX di inviare email per questo
dominio: ☒

Consenti all'indirizzo IP del
dominio di inviare email per
questo dominio: ☒

Indirizzi IP aggiuntivi in formato
CIDR che consegnano o rilanciano
mail per questo dominio:

(Sepearare gli indirizzi IP con spazi)

Qualunque nome server che può
consegnare posta o rilanciare
posta per questo dominio.:

(Sepearare i nomi con spazi)

Qualunque dominio che può
consegnare o rilanciare posta per
questo dominio:

(Sepearare i domini con spazi)

TTL:

Attivo: ☒

Salva

Modifica come record TXT

Annulla

DNS TXT Record

DNS TXT

Hostname:

Testo:

TTL:

Attivo: ☒

Salva

Annulla

Salvo diversa indicazione, i valori corretti sono i seguenti

```
v=spf1 mx a include: wrdns.it include: whiteready.com ~all
```

Il record DMARC:

DMARC (Domain-based Message Authentication, Reporting and Conformance) è una tecnologia che standardizza i metodi SPF e DKIM e ne estende la funzionalità. Il criterio DMARC definisce come il destinatario deve gestire i messaggi email a seconda dei risultati di verifica di DKIM e SPF; anch'esso richiede la configurazione di un record sul dominio. In altre parole, DKIM e SPF indicano se il messaggio è legittimo (o quali parti del contenuto o del suo trasferimento non è possibile garantire); DMARC indica al server di posta del destinatario cosa fare del messaggio in base ai risultati.

Il record DMARC, per i nuovi domini registrati dal 1 gennaio 23 in poi, viene aggiunto automaticamente con impostazioni predefinite (che possono essere modificate) e deve essere solo attivato

DNS DMARC

Dominio: whiteready.it

Politica di ricezione
mail: quarantena

Come devono essere gestiti i messaggi che non hanno superato SPF or DKIM (DMARC).

Indirizzi di invio dei
report di dati
aggregati: abuse@whiteready.it

Indirizzi Email cui notificare i report dagli ISP riguardo i messaggi che non hanno superato la verifica DMARC per il dominio (separare gli indirizzi da spazi).

Indirizzi per i report di
dati Forensi: abuse@whiteready.it

Indirizzi Email cui notificare i report dagli ISP riguardo i messaggi che non hanno superato la verifica DMARC per il dominio (separare gli indirizzi da spazi).

Opzioni di report
Forense:



Generare report se tutti i meccanismi di autenticazione non producono un risultato di 'pass' alla verifica DMARC



Generare report se qualunque meccanismo fallisce.



Generare report se non supera la verifica di firma DKIM.



Generare report se fallisce SPF.

DKIM identifier
alignment:

rilassata

'esetta' richiede l'esatta uguaglianza tra il dominio DKIM e il campo 'da' della email

SPF identifier
alignment:

rilassata

'esatta' richiede l'esatta uguaglianza tra il domini SPF e il campo 'da' della email

Formato Report:



Formato del reporto di mancata autenticazione



Formato di scambio della descrizione del problema accaduto

Applica la politica
con questa
percentuale:

100

% (100 default). Numero di Messaggi in percentuale dal dominio per il quale vuoi che gli ISP eseguano la verifica.

Intervallo di Report:

86400

Secondi (default=86400). Tempo in secondi per aggregare i dati del report da generare (86400 rappresenta 1 giorno).

Politica per i
sottodomini (Default
la stessa dei
Domini):

Stessa dei domini

TTL: 3600

Attivo: ☒

Salva

Annulla

Revision #4

Created 16 February 2023 16:19:03 by Fabio

Updated 16 February 2023 17:47:27 by Fabio