Audit servizio DNS registrazione domini

RHX srl

2018

Indice

1 Premessa

RHX è una società che svolge registrazioni di *nomi a dominio*, questo servizio richiede una corretta configurazioni dei name server autoritativi dei domini. RHX è Registrar accreditato presso il registro dei nomi a dominio dal 2004 con la sigla RHX-REG.

2 Obiettivi

RHX ha verificato la qualità del servizio reso con un'analisi automatizzata di tutti i domini registrati al fine di evidenziare anomalie o difetti nella configurazione nel servizio DNS.

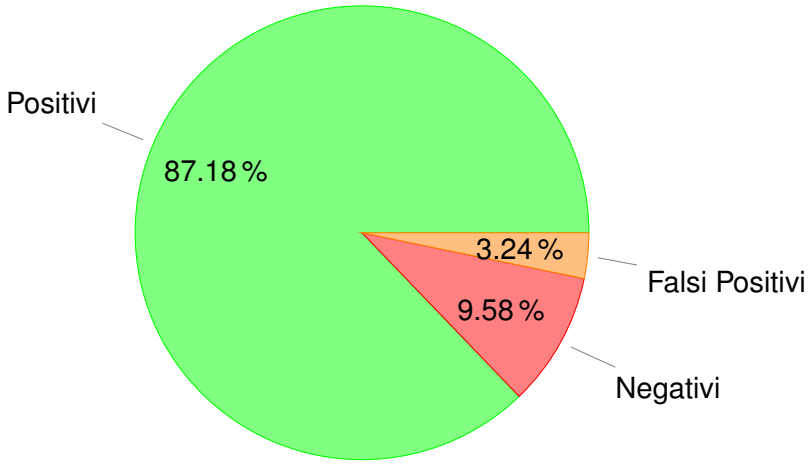
3 Analisi

Per l'analisi è stato utilizzato il tool zonecheck [1] che svolgerà una verifica del dns alla ricerca di eventuali errori di: connessione TCP/UDP, lista NS, record SOA, mappatura inversa dell'indirizzo IP, record MX, e-mail ecc.

Questo controllo verrà effettuato su tutti i domini di competenza dell'azienda, quest'ultima operazione verrà svolta grazie all'ausilio di uno script bash che esegue il comando zonecheck per ognuno dei omissis domini registrati da RHX, lo script filtra i risultati su un file *results.log* e se il risultato è stato positivo scriverà il nome del dominio con un OK seguente sennò con un KO. Successivamente a quest'ultima operazione se il risultato è stato negativo su un file di nome *errori.log* ne scriverà l'output d'errore.

4 Risultati

Risultati OK sono stati	87.18 %
Risultati KO sono stati	12.82 %

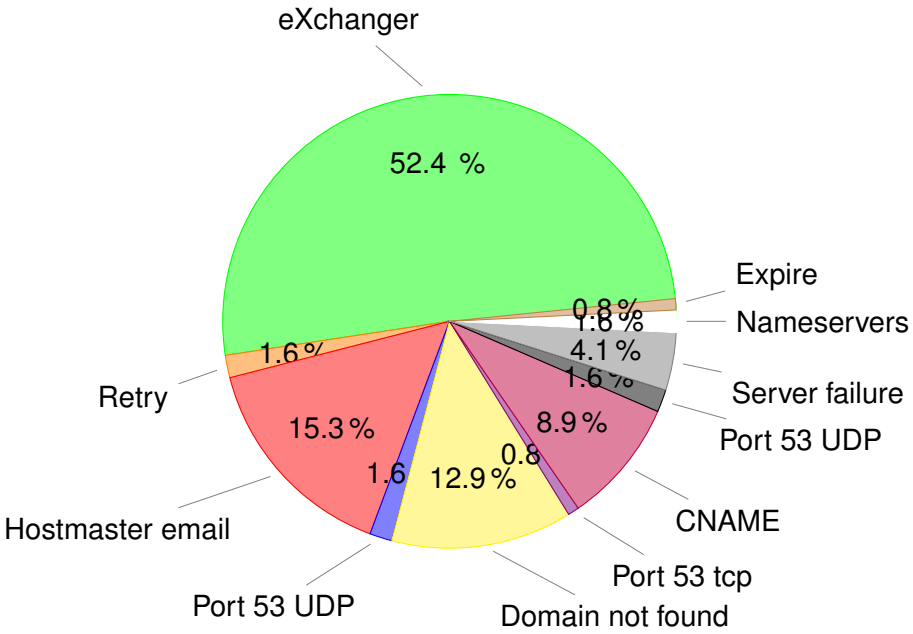


4.1 Tipologia di errori rilevati

I tipi di errori rilevati sono stati:

[1] https://www.afnic.fr/

- *The IP address of the Mail eXchanger can't be resolved*
- *SOA and ANY request disagree*
- *The hostmaster can't be contacted by email*
- *The domain has not been found through the local resolver*
- *MX is not allowed to point to a CNAME alias*
- *[TEST loopback is resolvable]: server failure: (PTR 1.0.0.127.in-addr.arpa)*
- *The 'retry' period must be lower than the 'refresh' period*
- *Server doesn't listen/answer on port 53 for UDP protocol*
- *At least two nameservers are necessary*
- *Server doesn't listen/answer on port 53 for TCP protocol*
- *The 'expire' period should be between 1W and 6W*



4.2 Approfondimento e azioni correttive

4.2.1 The IP address of the Mail eXchanger can't be resolved

L'errore riguarda la dichiarazione di MX record non risolvibili da DNS.

Buona parte degli errori riguarda un una configurazione errata da parte di un cliente che dichiarava due record MX ma in effetti utilizza soltanto un mail server, al cliente è stato richiesto di rimuovere il secondo record MX. Altri casi riguardavano una intenzionale dichiarazione di MX non risolvibili.

Altri casi sono stati segnalati ai clienti che hanno effettuato configurazioni customizzate del DNS.

4.2.2 SOA and ANY request disagree

Questo errore si rileva su domini che utilizzano i DNS di CloudFlare, in breve i DNS dichiarati non restituiscono risultati per una interrogazione ANY, da verifica con comando *dig* la risposta è

```
"ANY obsoleted" "See draft-ietf-dnsop-refuse-any"
```

Pertanto viene considerato un "falso positivo" e non viene intrapresa nessuna azione correttiva in quanto CloudFlare per scelta non risponde alle interrogazioni con tipo di record ANY [2]

Il caso è stato segnalato come Issue al progetto Zonecheck [3].

4.2.3 The hostmaster can't be contacted by email

Si tratta di un errore di raggiungibilità dell'email dichiarata nel record SOA del dominio. In tutti casi segnalati i DNS erano di terze parti, pertanto il problema non può essere risolto da RHX.

4.2.4 The domain has not been found through the local resolver

Questo errore indica in varie forme che i DNS autoritativi per il dominio non sono dichiarati o non rispondono.

Sono emerse varie casistiche: domini cancellati e dismessi ma ancora in anagrafica, domini con DNS di terzi che non rispondono (probabilmente intenzionalmente), domini in stato di clientHold per mancanza di validazione mail secondo le regole ICANN.

Sono state poste azioni correttive per i domini in clientHold e rimossi dall'anagrafica dei domini attivi i domini dismessi.

4.2.5 MX is not allowed to point to a CNAME alias

Questo errore indica che sono dichiarati dei record MX come CNAME e non come atteso record A.

In alcuni casi è stato effettivamente evidenziato questo problema, in altri casi l'errore riguarda i clienti che utilizzano il servizio di posta di mail.protection.outlook.com

[2] https://blog.cloudflare.com/deprecating-dns-any-meta-query-type/

[3] https://github.com/icann-dns/zonecheck/issues/2

sul quale non abbiamo approfondito la questione essendo un servizio fornito da terzi.

4.2.6 [TEST loopback is resolvable]: server failure: (PTR 1.0.0.127.in-addr.arpa)

Pochi casi, servizio erogato da terzi.

4.2.7 The 'retry' period must be lower than the 'refresh' period

Pochi casi, servizio erogato da terzi.

4.2.8 Server doesn't listen/answer on port 53 for UDP protocol

Questo errore indica che i name server non sono accessibili tramite protocollo UDP su porta 53, riguarda solo i domini del TLD .tel che usano DNS dedicati.

4.2.9 At least two nameservers are necessary

Questo errore riguardava soltanto due domini, per i quali nonostante la delega sia stata fatta su due dns, da interrogazione su name server primaria per record NS risultava solo un record.

E' stato aggiunto il secondo record NS.

4.2.10 Server doesn't listen/answer on port 53 for TCP protocol

Questo errore indica che i name server non sono accessibili tramite protocollo TCP, riguarda domini con DNS di terzi.

4.2.11 The 'expire' period should be between 1W and 6W

Pochi casi, servizio erogato da terzi.

5 Conclusioni

Nonostante in prima battuta gli errori riguardanti i domini appaiano in grande numero, nel momento in cui si va ad analizzar i singoli problemi si evidenziano tanti errori della configurazione da parte dei clienti e/o servizi d'hosting gestiti da terzi non imputabili ad un mancato controllo e gestione dell'azienda RHX. In conclusione i veri problemi di competenza aziendale sono rilevati di bassa gravità e in numero molto ridotto.