

# Come proteggere la "spina dorsale" delle reti

Valerio Salvi

I principali temi sulla sicurezza dei DNS (Domain Name System) emersi in un convegno organizzato dalla Fondazione GCSEC. Intervista a Andrea Rigoni, Direttore Generale GCSEC

**S**i è svolto a Roma un Forum scientifico, tenutosi presso la sede centrale di Poste Italiane, socio fondatore della **Fondazione GCSEC**, l'istituzione internazionale pubblico-privata senza fini di lucro che

ha l'obiettivo di offrire occasioni di confronto tra gli esperti e di studiare soluzioni per garantire la massima sicurezza delle comunicazioni via internet a beneficio dei cittadini, dei governi e delle imprese.

La giornata di studio ha visto la parteci-





*Andrea Rigoni*  
Direttore Generale di Global  
Cyber Security Center (GCSEC)

pazione anche dell'AD di Poste Italiane, **Massimo Sarmi**, **Paul Mockapetris**, il padre del DNS e **Paul Vixie**, inventore di BIND il server DNS più utilizzato al mondo. Durante l'evento sono stati presentati i risultati del primo anno di funzionamento della **Response Policy Zone** aperta nel 2010 da ISC.

La Response Policy Zone ha lo scopo di pubblicare informazioni sulla reputazione dei nomi di dominio e sarà uno strumento fondamentale per la sicurezza del

DNS oggi e nel futuro. Abbiamo intervistato su questi temi **Andrea Rigoni**, Direttore Generale di Global Cyber Security Center (GCSEC).

### Ci può precisare innanzitutto cosa è il DNS?

Il DNS (Domain Name System) è la spina dorsale di tutte le applicazioni Internet. Senza il DNS non potrebbero funzionare nessuno dei servizi web ed applicazioni di rete che ciascuno di noi utilizza giornalmente, ad esempio: la posta elettronica, il commercio elettronico, i social network, l'e-banking, i servizi postali, ma anche gli sportelli bancari, il caselli autostradali ed i sistemi di controllo industriali. Il DNS è indubbiamente una delle principali infrastrutture critiche del pianeta, al pari delle reti di distribuzione energetica e di trasporto. Anche se pubblicamente poco dibattuta, la **sicurezza del DNS** è uno dei temi più attuali nel panorama della cyber security.

Da sinistra **Andrea Rigoni**, Direttore Generale GCSEC e **Paul Mockapetris** inventore del DNS



**Ne avete parlato recentemente in un convegno.**

Si, lo scorso ottobre a Roma. Al convegno internazionale **DNS-EASY 2011**, organizzato dalla fondazione di ricerca Global Cyber Security Center (GCSEC), in collaborazione con ICANN e DNS-OARC, le due principali associazioni internazionali che si occupano della gestione ed osservazione del DNS, si è dibattuto sui problemi attuali e futuri del DNS e sono state presentate le soluzioni che ne garantiranno la sicurezza e robustezza oggi e nel futuro.

**Quali sono i temi più importanti e i risultati, emersi durante il convegno?**

La sicurezza prima di tutto. Il DNS, il servizio su cui si reggono Internet e gran parte dei sistemi ICT, siano essi critici o no, non è immune da guasti ed attacchi. Purtroppo ad oggi non è ancora disponibile uno strumento per misurare il suo livello di salute e di sicurezza. Gli incidenti che si verificano sono molti e, come emerso durante il convegno, non bisogna abbassare la guardia. Deve essere fatto uno sforzo maggiore in termini di modellazione, fondamentale per studiare effetto di attacchi e contromisure, ma anche per capire come distribuire appropriatamente sia i server che il carico al fine di aumentarne le prestazioni anche a fronte di nuove applicazioni e degli sviluppi futuri.

Modellare un sistema complesso quale il DNS non è banale, simulazione, emulazione e modelli matematici uniti insieme sono la risposta al problema. La dif-

I dettagli tecnici delle soluzioni proposte dai ricercatori presenti al convegno sono stati raccolti in un volume, edito da GCSEC e distribuito durante la conferenza [disponibile online sul sito [www.gcsec.org](http://www.gcsec.org)].



fusione del **DNSSEC**, non ancora completata su scala mondiale, Italia compresa, deve essere ulteriormente incoraggiata e la sua gestione deve essere automatizzata. Attualmente non esistono regole di governo del DNS, siano esse centralizzate o distribuite. Non esiste un insieme di strumenti per misurare il livello di sicurezza, robustezza, affidabilità e prestazione del DNS. Quest'ultimo punto è di estrema importanza. Come si può controllare un sistema, come si può verificare che siano soddisfatti i requisiti di sicurezza e prestazioni richiesti dall'utente se non è possibile misurare il suo stato di salute? Definire un framework per la misura del livello di sicurezza e di salute del DNS è una delle principali sfide per il futuro. GCSEC sta attivamente lavorando in questa direzione.

**Quali sono i risultati emersi dal primo anno di funzionamento dalla Responce Policy Zone?**

I risultati degli studi, sono stati elaborati in 12 diversi centri di ricerca internazionali dislocati su 9 nazioni e 3 continenti (Olanda, Giappone, Italia, Francia, Stati Uniti, Cecoslovacchia, Cina, Canada e Corea), e sono relativi a tre argomenti correlati:

- modelli per un DNS più sicuro e robusto
- metodologie ed applicazioni per un DNS più sicuro e robusto
- gestione e operatività del DNSSEC.