Il Routing Resilience Manifesto

Raccomandazioni per il routing globale

Marco d'Itri
<md@seeweb.it>
@rfc1036

Seeweb s.r.l.

TOP-IX technical meeting - 10 dicembre 2015

Routing Resilience Manifesto

Come migliorare la sicurezza e resilienza del sistema di routing globale?

Mutually Agreed Norms for Routing Security (MANRS)

- Prima raccomandazione pubblicata nel settembre 2014.
- Best practices minime da implementare per migliorare affidabilità e sicurezza del routing globale.
- Dimostra un impegno a seguirle da parte dei leader dell'industria: sponsorizzato da ISOC, tra i fondatori ci sono NTT, Level3, Comcast, CERNET.
- Seeweb aderisce nel febbraio 2015, prima rete italiana.

seeweb

Obiettivi

Dimostra la capacità dell'industria di autoregolamentarsi e crea consapevolezza grazie alla partecipazione dei leader.

- Promuove raccomandazioni minimali, adottabili facilmente da tutti e non controverse.
- Non pretende di risolvere tutti i problemi del routing e ci si aspetta che una rete ben gestita adotti misure più rigorose.
- Ogni piccolo passo aiuta.

seeweb

Le azioni raccomandate

- Impedire la propagazione di informazioni di routing non corrette.
- Impedire il traffico con IP sorgente falsificato.
- Facilitare le comunicazioni e il coordinamento tra gli operatori.
- Facilitare la validazione su scala globale delle informazioni di routing.

Nessuna di queste regole è innovativa: Seeweb ha potuto aderire immediatamente senza dovere modificare in alcun modo le proprie configurazioni o procedure.

seeweb

Informazioni di routing non corrette

Validare le informazioni di routing ricevute dai propri clienti, per impedire l'utilizzo non autorizzato di reti di terzi (per errore o per frodi...).

Esempi:

- Filtrare i propri clienti con prefix-list (non basta filtrare l'as-path!).
- Verificare la legittimità di ciascun nuovo prefisso annunciato prima di accettarlo.

Non richiede di validare le route dei propri peer, ma rimane comunque un'ottima idea...

seeweb

Traffico con IP sorgente falsificato

Impedire ai propri clienti diretti di falsificare gli IP sorgente del traffico che generano, il cosiddetto IP spoofing.

È indispensabile che il traffico generato dai propri utenti sia filtrato da meccanismi che permettano di utilizzare solo gli IP a loro assegnati.

Esempi:

- BCP 38 (RFC 2827): maggio 2000!
- ACL antispoofing
- `ip verify unicast source reachable-via rx`

seeweb

Comunicazioni e il coordinamento

Pubblicizzare i propri contatti H24 per essere prontamente rintracciabili dagli altri operatori in caso di necessità.

Esempi:

- Un oggetto role nel database whois di RIPE.
- Il sito del MIX.
- PeeringDB.

seeweb

Validazione delle informazioni di routing

Rendere possibile agli altri operatori la validazione delle proprie informazioni di routing, pubblicando l'elenco delle proprie reti e di quelle dei propri clienti.

Esempi:

- Pubblicare oggetti `as-set` e `route`/`route6` per le proprie reti.
- Richiedere lo stesso ai propri clienti.

Questo permette ai propri peer di validare i propri annunci.

seeweb

Domande?

`http://www.linux.it/~md/text/routing-manifesto.pdf`

(Google . . . Marco d'Itri . . . I feel lucky)

seeweb