Routing Resilience Manifesto & MANRS

ION Romania | Bucharest | 12 October 2016

Mind Your MANRS:
Mutually Agreed Norms for Routing Security

BGP is based on trust – no validation of routing updates

- Announcement of prefixes not belonging to network (e.g. impersonating a network)

- Route leaks (e.g. traffic intercept)

- Source IP address spoofing (e.g. reflection DDoS attacks)

- Contactability of network operators (e.g. how to mitigate a DDoS attack)

MANRS is building a community of security-minded operators to promote collaborative responsibility through four concrete actions.

Good MANRS

Filtering – prevent propagation of incorrect routing information by defining clear policies, and implementing systems to ensure correct announcements of their own and their customer announcements

Anti-spoofing – filtering to prevent traffic with incorrect source IP addresses leaving the network

Coordination – Facilitate global operational communication and coordination between network operators by maintaning globally accessible up-to-date contact information
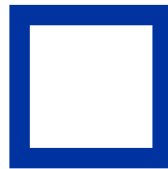
Global Validation – Facilitate validation of routing information on a global scale through IRR and RPKI

Internet Society™
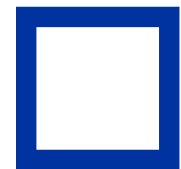
Are you interested in participating?

Filtering	Anti-Spoofing	Coordination	Global scale
☑	☐	☑	☐

Routing Manifesto - https:/www.routingmanifesto.org/

MANRS website - https://www.manrs.org/

Internet Society

The MANRS manifesto is not just a document – it is also a commitment

1) The company **supports the Principles and implements at least one of the Actions** for the majority of its infrastructure. The Action "Facilitate global operational communication" cannot be the only one and requires that another Action is also implemented.

2) The company becomes a Participant of MANRS, helping to **maintain and improve** the document. For example, by suggesting new Actions and maintaining an up-to-date list of references to BCOPs and other documents with more detailed implementation guidance.

Discuss!

Kevin Meynell

Deploy360@isoc.org