MANRS

Mutually Agreed Norms for Routing Security

How Can Policymakers Improve Global Routing Security?

INFORMATION FOR ICT AND TELECOMMUNICATION POLICYMAKERS

Several recent Internet routing incidents have caused real-world problems, including lost business revenue, misdirected Internet traffic, and DDoS attacks. As a result, more governments are investigating how they can clean up their networks and the global routing system.

Because the Internet is a collection of interrelated networks, solving systemic issues like routing security requires global collective action, such as the actions called for in Mutually Agreed Norms for Routing Security (MANRS) - an industry-led initiative to reduce the most common routing security threats. Governments and policymakers can help facilitate MANRS best practices in their own networks and across their regions.

Policymakers must work with network and infrastructure operators, critical infrastructure protection agencies, and standards bodies, among others, to improve global routing security while preserving vital system aspects that have allowed the Internet to be open and universal.

What Role Can Policymakers Play?

Whether through government procurement policies or working with the private sector to improve routing security, governments have a crucial role in creating a safer Internet routing ecosystem.

Avoid regulatory barriers: Improve market incentives for better routing security by avoiding regulatory barriers and facilitating cooperation and collaboration.

Encourage good practices: Facilitate initiatives in a way that preserves the Internet's strengths, including its overall resilience, ease of use, flexibility, and scalability.

Promote common guidelines: Support the use of common guidelines that facilitate industry best current practices for routing security.

Grant incentives: Motivate local operators to use best practices in routing security through incentives such as grants and tax rebates.

Encourage information sharing: Identify and eliminate legal barriers to information sharing and responses to routing incidents. Network and infrastructure operators and security researchers must be able to work together to disclose routing security incidents and threats. Providing safeguards for them can help ease such concerns.

Lead by example: Invest, improve, and maintain the Internet infrastructure reliability and security of your own government networks by using MANRS best practices.

Governments Are Acting

The United States and the Netherlands offer two recent examples of governments addressing routing security.

On 31 July 2023, the United States Federal Communications Commission held a Border Gateway Protocol Security Workshop highlighting the importance of addressing BGP vulnerabilities and securing Internet routing.

Also in July, the Biden-Harris Administration published the National Cybersecurity Strategy Implementation Plan, which identifies "collaborating with key stakeholders to drive secure Internet routing" as a critical action item.

The U.S. Federal Government is also considering how to improve the routing security of its own networks.

In the Netherlands, the Dutch government's "comply or explain" initiative requires governmental departments to deploy a routing security best practice called RPKI, or adequately explain why they cannot comply.

Similarly, a Dutch public-private partnership has developed a gold star program, providing private sector network operators a service (internet.nl) to show that they comply with routing security best practices.

Balancing Government Interest is Challenging

As governments attempt to improve routing security, they must uphold the globally distributed and decentralized nature of the Internet.

There is no single point of failure or single controller, so the routing system is difficult to break on a global level. In fact, the routing system's architecture contributes to the Internet's resilience, scalability, and ease of adoption.

Top-down efforts to centralize the routing system undermine the qualities that have made the Internet successful and increase the risk of security attacks. Government and industry must work together on solutions that prioritize the distributed nature of the Internet routing system while increasing the use of best practices. MANRS participants are well placed to advise governments trying to tackle this issue.

FIND OUT MORE AT MANRS.ORG