MANRS

Mutually Agreed Norms for Routing Security

Routing Security Makes Good Business Sense

INFORMATION FOR BUSINESS EXECUTIVES

Businesses increasingly rely on the Internet, from online services and customer support to storing digital assets and information in the cloud. All that data has to move across the Internet without being intercepted, changed, redirected, or blocked.

Your business may be susceptible to these risks if your Internet connectivity, cloud, and CDN providers are not actively mitigating them with proper routing security best practices.

Is Your Connectivity Provider a Threat Vector or a First Line of Defense?

Over the last 12 months, there were around 2,500 major attacks on the global Internet transport and routing systems. These incidents, called 'route hijacks' and 'route leaks,' can:

- Strain infrastructure
- Result in dropped traffic
- Allow unauthorized traffic inspection
- Lead to Denial of Service (DoS) attacks

The most effective way to tackle routing security threats is to choose Internet service providers and cloud and CDN providers that follow established best practices outlined via Mutually Agreed Norms for Routing Security (MANRS).

By choosing service providers who are MANRS-compliant (and joining MANRS if you operate a network), you can improve your company's security and encourage other providers to improve their infrastructure.

An independent study by 451 Research, commissioned by the Internet Society, found that:

- 94% of enterprises would be willing to pay more for a vendor who is a MANRS participant.
- 97% of enterprises were interested in putting MANRS participation in RFP and tender requirements.

How can MANRS help your organization?

Ensure business continuity and prevent reputational damage: Every enterprise should know whether their providers implement Internet routing best practices as part of their business continuity program. MANRS actions offer an effective way to prevent network security mishaps that can cause significant reputational damage to any business.

Qualify vendors or partners: MANRS compliance can help you choose an appropriate network or cloud partner without having to undertake an extensive or complex assessment process. Multiple key vendors are already MANRS compliant, which significantly simplifies the process of auditing their security capabilities.

Security as a differentiator: If you operate networks, implementing MANRS actions allows you to communicate to your customers that you are serious about your network infrastructure's security. This can serve as a critical differentiator for your organization.

Resolving network security incidents: Adopting MANRS actions on your networks helps you mitigate immediate and severe impacts of network security incidents. Left unresolved, these can disrupt your ability to operate, and damage customer confidence in your business.

Threat intelligence: You may be looking to improve your situational awareness and be interested in incorporating intelligence feeds into your operations. The information and event streams that MANRS actions can generate will therefore hold value.

A checklist for auditing infrastructure robustness: The actions highlighted by MANRS can serve as a useful checklist to ensure the robustness of your internal IT infrastructure. Incorporating the MANRS actions into internal IT operations can help you to increase operational efficiency.

Community support for security issues: Joining MANRS gives you access to a larger community that's concerned with security and addressing the issues surrounding it. The community can also serve as a way to identify ecosystem partners with whom to join forces to create a stronger foundation for security.

FIND OUT MORE AT MANRS.ORG