How can enterprises improve global routing security?

Information for business executives

Today, the Internet plays an essential role in our increasingly digital societies around the world. From banking to education, health to logistics, just about every sector relies on Internet-based applications and services to function.

Our increased dependence on digital technologies brings with it growing concerns around Internet security. While there are many dimensions to Internet security, it's critical we secure the key building blocks of the Internet's infrastructure.

The Internet's routing system enables data to flow from one point to another. Ensuring that this data flows correctly, to its intended recipient, is at the foundation of Internet network security.

Thousands of Internet routing incidents occur every year, leading to economic harm by:

- making key services unreachable
- disrupting e-commerce
- allowing malicious actors to spy on users and with it, the potential to compromise systems.

While existing security measures can help address many of these routing incidents, the solutions they provide are often limited. The interconnected nature of networks means that many solutions only work when other networks make the same improvements.

We need collective action to make real change.

To contribute to efforts to secure the Internet network, enterprises should work with network and infrastructure operators, critical infrastructure protection agencies, among others, to ensure your providers implement routing security best practices while also preserving vital aspects of the system that have allowed the Internet to be open and universal.

What is MANRS?

The Mutually Agreed Norms for Routing Security (MANRS) is a community-driven initiative supported by Internet Society. MANRS provides a set of best practices based on existing norms for network operators to improve the security of the global Internet routing system.

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

MANRS defines four simple but concrete actions for network operators to implement to greatly improve Internet security and reliability. These include:

1. **Filtering** – defining a clear routing policy and implementing a system to ensure that announcements to adjacent networks are correct.
2. **Anti-spoofing** – enabling source address validation (SAV) and implementing anti-spoofing to prevent packets with incorrect source IP addresses from entering and leaving the network.
3. **Coordination** – maintaining globally accessible up-to-date contact information to assist with incident response.
4. **Global validation** – publishing data that enables other stakeholders to validate routing information on a global scale.

The first two, filtering and IP source validation, address the root causes of common routing incidents. The second two, coordination and global validation, help limit the impact of incidents and decrease the likelihood of future incidents.

The MANRS actions define outcomes rather than specific methods. This allows implementation to change with technology and helps establish MANRS actions as best practice.

Alongside routing incidents, MANRS seeks to address ecosystem challenges in the global routing system.

MANRS improves economic incentives for routing security by allowing network operators to demonstrate their commitment to:

- Security – by securing core Internet infrastructure for greater global Internet security.
- Customers – by ensuring the services they provide adhere to routing security best practices.
- Competitors – by ensuring routing security incidents don't have a cascading effect on other network operators.
- Policymakers – by ensuring a robust and resilient national Internet infrastructure in support of the larger Internet security agenda.

An independent study by 451 Research[1], commissioned by the Internet Society, found that traffic routing, hijacking and interception were the leading security concern for enterprises. Distributed denial of service (DDoS) attacks and address spoofing came in second.

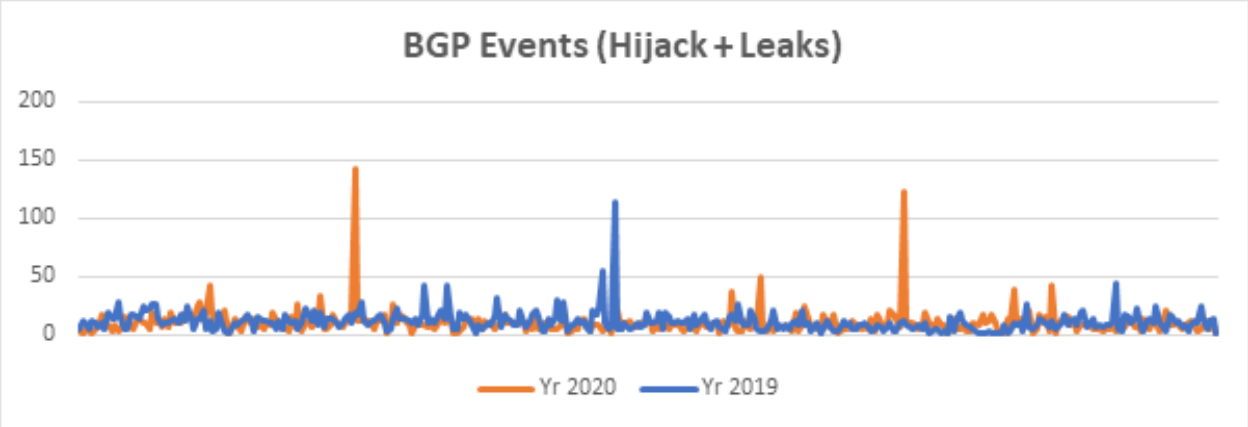
94% of enterprises said that they'd be willing to pay more for a vendor who was a MANRS member in a competitive situation.

This highlights the importance of MANRS implementation as an indicator of a network operator's sound security practices.

[1] MANRS project study report: https://www.manrs.org/wp-content/uploads/2017/10/MANRS-451-Study-Report.pdf

Why does MANRS matter for enterprises?

In 2020, there were a total of 3,873 major network incidents that involved border gateway protocol (BGP) related attacks. Of these, 64% were hijacks and the rest were route leaks.



In 2019, there were 4,232 major network incidents that involved BGP, of which:

- 3.8% of all networks were affected by a routing incident
- 2% of all networks were responsible for the 4,232 routing security incidents.

These incidents can:

- create a serious strain on infrastructure
- result in dropped traffic
- allow for unauthorized inspection of traffic
- be used to perform Denial of Service (DoS) attacks, which threaten business continuity

In July 2020 there were two significant routing incidents in the global BGP routing system[2]. This highlighted the need for network operators to implement good routing security practices. These incidents impacted major North American network providers including TWC, Rogers and Charter, among others[3].

The only effective way your enterprise can tackle routing security threats is by choosing service providers that follow an established set of guidelines, like MANRS. By choosing providers that adopt these measures, you can drive the market to build more resilient networks which, in turn, make the global network infrastructure more secure.

[2] Big route leak shows need for routing security https://www.manrs.org/2020/07/big-route-leak-shows-need-for-routing-security/

[3] Another border gateway protocol Incident Impacts TWC, Rogers, Charter and others https://www.manrs.org/2020/07/another-bgp-incident-impacts-twc-rogers-charter-and-others/

How can MANRS help your organization?

1. **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 your enterprise an effective way to prevent network security mishaps that can cause significant reputational damage to any business.

2. **Qualify vendors or partners:** MANRS can help your enterprise's leadership to choose an appropriate network or cloud operations 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.

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

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

5. **Threat intelligence:** Your enterprise may be looking to improve its 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.

6. **A checklist for auditing infrastructure robustness:** The actions highlighted by MANRS can serve you 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.

7. **Community support for security issues:** Joining the MANRS initiative gives your enterprise 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.

Given the significant impact of routing incidents on critical networks, we need to give high priority to protecting and improving our network infrastructure. However, research shows a general lack of understanding of the fact that simple steps can dramatically reduce such incidents.

Some of the measures outlined above aren't entirely new and some organizations may be working to integrate such measures in the near future. To ensure a healthier and more robust network infrastructure, we must prioritize the measures highlighted in this document, and back their implementation with adequate resources.

- Find out more about MANRS: manrs.org
- Read about the Internet Society's work: internetsociety.org