Improved MANRS for Enterprises

JOINING A COMMUNITY FOR GREATER SECURITY

Enterprises face many challenges in running their IT infrastructure, and one of the most significant is the selection of service providers. Assessing provider capabilities and performance can be a complex process. One factor that can aide in this decision is a provider's participation in the Mutually Agreed Norms for Routing Security (MANRS) project. MANRS is a collaborative project that focuses on concrete steps to enhance the security posture of participants and thereby contribute to the overall security of the Internet community. In working with a service provider that is part of the MANRS project, enterprises can establish themselves within the vanguard of those with a security-forward position and join the larger Internet community that is working to improve security and reliability.

THE MANRS PROJECT GOALS

The MANRS project seeks to improve the security and reliability of the global Internet by standardizing the controls and operating principles used by network operators. It lays out a set of four actions that participants put to work as part of their operations and their interactions with others. Collectively, these efforts aim to curb accidental or intentional activities that can damage Internet reliability. The four actions are:

ROUTE FILTERING: Preventing the propagation of incorrect routing information.

ANTI-SPOOFING: Preventing traffic with spoofed source IP addresses.

COORDINATION: Facilitating global operational communication and coordination between network operators.

GLOBAL VALIDATION: Facilitating validation of routing information on a global scale.

Together these actions can help prevent problems and speed resolution when problems occur. Service providers that are MANRS participants have made a commitment to be part of this effort. One of the challenges of the Internet's structure is that it requires larger community efforts such as this in order to be effective. This effort can help in reducing perennial problems, such as traffic rerouting (detouring), denial-of-service attacks (DDoS) and traffic hijacking.

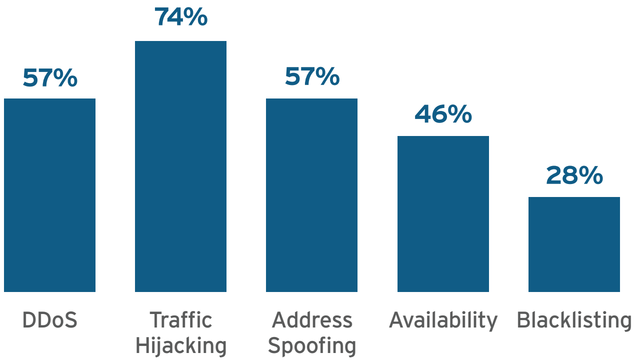
THE MANRS STUDY

In an effort to evaluate and assess the MANRS project and its impact on enterprises and service providers, 451 Research undertook an expansive study, the results of which provide useful peer benchmarking data on the importance and impact of the project for enterprises. Over 70% of study respondents identified that their information security posture was a primary core value to their organization. A big part of any enterprise security environments is their connection to the Internet and the partners they select to deliver it, making MANRS an important qualifier.

The study also explored Internet security concerns for enterprises and sought to quantify how enterprises expected to address them. The greatest concern was traffic hijacking, a problem that has often been in the news, and one that has customer satisfaction implications beyond its security implications.

Figure 1: Internet Security Concerns

Source: 451 Research study: MANRS Perception & Action, July, 2017

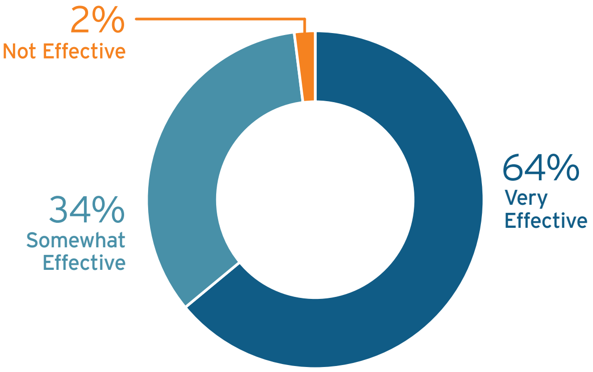


The next two most important concerns have an intrinsic link. While denial-of-service attacks are a concern, address spoofing – the technique that can be used to cloak the origins of DDoS attacks – received an equal measure of concern among study respondents. The MANRS project seeks to address the causes of these concerns through its four actions.

The study also evaluated the responding organizations' thoughts about how effective the MANRS project would be at combating the problems that concerned them. Almost the entire respondent pool reported they felt that, over time, the project would be an aid in addressing Internet security concerns. Almost two-thirds felt it would be very effective.

Figure 2: MANRS Effectiveness

Source: 451 Research study: MANRS Perception & Action, July, 2017



LEVERAGING MANRS FOR ENTERPRISE

One of the primary benefits of the MANRS project for enterprises is the indication that it gives for the attitude and initiative of service providers around operational security. The typical enterprise expends significant effort in selecting IT infrastructure partners, but effective selection criteria can be hard to come by. Service providers that are participating in MANRS have made an effort to improve their security posture, and are working with a larger community to reduce threats to Internet security and stability. MANRS participation can be a reasonable selection metric and can be included in RFP, tender and purchasing processes to improve the understanding of a provider's capabilities. In the 451 Research study, 97% of respondents indicated they would consider including MANRS participation in their selection process.

The MANRS project also provides a means for organizations to join a larger community that's concerned with security. This can help organizations looking to collaborate on addressing concerns. It can be a means to identify ecosystem partners with whom enterprises can join forces to create a stronger foundation for security. In regulated industries, MANRS links can be an additional factor for auditors to consider when assessing the overall security posture of an organization.

MANRS can also strengthen an enterprise's bottom line. As the 451 Research study showed, most organizations are concerned about security, and being part of the MANRS community can strengthen enterprise security credentials. It communicates an enterprise's security investment to its customers. MANRS involvement can be included in marketing materials and could be part of a larger brand statement.

While the MANRS project is targeted at service providers, any organization that has peering arrangements that involve BGP can also become part of the community. Incorporating the MANRS actions into IT operations can add maturity and increase operational efficiency.

CONCLUSIONS

The MANRS project offers a number of benefits for enterprises that are directly attainable. There should be careful consideration given to MANRS participation, not only by an enterprise's service providers, but potentially for the organization itself. The wider Internet community can benefit from the greater security awareness that the project offers, and enterprises play an important role here. Enterprises that join the MANRS community can improve their security posture, as well as their business.

WWW.MANRS.ORG

MANRS