

SNMP's real vulnerability

In-band network management, by its very nature, poses business continuity issues that need to be addressed.

There has been a lot of publicity lately about security vulnerabilities in the simple network management protocol (SNMP). SNMP is used for the monitoring and management of network elements across the Internet, as well as for every service provider and enterprise network. That's what made security holes in the protocol so scary for the entire industry.

But there's a much bigger problem with SNMP-based management than some esoteric code-hole. And it's not a problem that's taken some hacking genius years to discover. Many of us have known about it for years, but a general indifference to infosec issues has kept it out of the limelight. Now

may be the time for that light to shine.

The real security concern with today's SNMP-centric approach to network management is that it's almost entirely based on an "in-band" architecture. That is, network managers monitor and administer network elements via the same network that those elements support.

There are two major problems with this. First, if the network is disabled because of an element failure, then network management is often crippled, as well. This is one of the reasons that IP networks have remained so flaky (relatively speaking) over the years. When a remotely located network element such as a router or switch fails, it is often impossible for a network technician to get fast, effective access to it via in-band communications. So, time-to-fix is often dependent on getting a technician on-site as quickly as possible.

The alternative, of course, is out-of-band management. In the out-of-band scenario, a technician gains access to a network element via another network—typically the PSTN. That way, when the network is down, the element can still be easily accessed, diagnosed and serviced.

Naturally, out-of-band management has its own potential security downside. Dial-up access to a port on a network element creates a "back door" that could be exposed to intruders. Such an exposure is something that any right-minded infosec manager should fear.

One way that organizations protect themselves against such back-door exposure is through the use

of the same RADIUS, security tokens and/or other authentication tools that are commonly used for securing dial-up access to enterprise information systems by regular end-users.

But this presents another problem. How do you get access to the RADIUS server user database if the network is down? In fact, how do you apply any network security system—including intrusion detection—to out-of-band management when you can't be sure that those networked systems will be accessible at the moment they're needed most?

The answer, it turns out, is to interpose a simple but sophisticated little device between the managed network element and the PSTN that provides all the authentication and encryption capabilities necessary to protect the network. Such a device enables fully secure out-of-band management that can be utilized even during the most disastrous network failures. It also eliminates any concerns about the security vulnerabilities associated with SNMP, since it encrypts communications between the managed element and the management console as it traverses the PSTN.

Several companies are in the business of producing these devices—most notably Communications Devices (www.commdes.com), which provides built-in support for RSA's SecurID tokens, as well as an intuitive console for simplifying the management of multiple out-of-band security devices across the network.

As simple and cost-effective as such an out-of-band management solution may be, not every company will be ready or willing to buck conventional in-band wisdom. Some companies still cling to the hope that in-band SNMP-based management consoles will give them a single point-of-control for all the devices on their networks—including routers, switches, firewalls, load balancers, servers and even printers.

But for the majority of companies that still practice network management as an independent, specialized discipline, new business continuity concerns should renew interest in secure, out-of-band monitoring technologies. It's probably not a good idea to depend on your network when you have to fix your network. And it's definitely not a good idea to depend on your network's security when your network is down. □

It's probably not a good idea to depend on your network when you have to fix your network.



Liebmann is an independent consultant specializing in the application of networking technologies to strategic business challenges. Send comments to liebmann@comnews.com