An Ounce of Prevention

Because broadband has become an essential utility, network operators must prepare to deal with threats to system reliability – including malicious attacks.

By David Daugherty / *Clarus Broadband*

My article "Broadband Do-It-Yourselfers," published in the October 2018 issue of Broadband Communities, discussed several developers of master-planned communities who were considering building their own fiber networks. These developers know that rock-solid, future-proof networks will be necessary to attract residents and support smart-community applications. They began to consider the DIY alternative when they could not obtain commitments from service providers to build and maintain state-of-the-art networks.

However, building such a network is not straightforward, and operating it is even less so. Would-be do-it-yourselfers must understand what it takes to design and operate a stable, reliable network.

In this year's hurricane season, buildings were flattened, bridges washed away and communications networks destroyed. A few well-built structures survived where others didn't. Clearly, an ounce of planning could have prevented considerably more than the proverbial "pound of trouble."

The internet, much like the weather, is unpredictable – with one notable exception.

Malware, just like internet services and commerce, is becoming more integrated and complex.

Providers *know* that future demand will present unanticipated design and operational challenges, so why use design and operating standards tuned to today's needs? Why not take a hint from Mother Nature and pay for an ounce of protection?

CYBERSECURITY

One type of storm network operators will have to prepare for is malicious disruption. It turns out that the U.S. government is good at planning for inclement weather, at least as far as the internet is concerned. Despite the recent concern over international hacking, the federal government is pretty well prepared. It has been gearing up for "future" cyber threats since 2014. This is apparently not true for state and local governments.

The internet is changing commerce in new and unexpected ways. "Alexa, mute the TV" has become an hourly refrain for many telecommuters. However, advertisements on streaming services can now instruct Alexa to make purchases on a credit card. What's next?

This is just the tip of the iceberg. The last Pinterest image my wife clicked on activated embedded malware that quietly installed a Trojan designed to record keystrokes and transmit them to China! As internet-based services and commerce become more integrated and complex, malware is undergoing a similar metamorphosis.

The standard solution to this problem – subscription-based antivirus software resident on subscriber devices – is not sufficient to address and eliminate the rapidly growing universe of

cyber threats. The most likely solution to this problem must incorporate active, 24/7 live monitoring, complete with interdiction and remediation services. This type of support operates in parallel with the network operating center (or NOC) and is called a security operating center (or SOC).

From an operating perspective, the addition of a SOC approximately doubles the operating cost of a NOC. This has necessitated industry soul-searching about how internet services are packaged and priced. The requirement for active security services, combined with the avalanche of new internet-of-things technology, drives up operating costs and related contingent liability.

Clarus Broadband's chief security and information officer, Scott Blackard, has been involved in several notable cyber projects over the last 20 years, including threat modeling for Fortune 100 organizations, threat modeling and cyber operations support for the U.S. Department of Defense, support for academic organizations and more. He explains that the DoD's Cyber Protection Team, which is charged with mission assurance and threat mitigation support for U.S. critical infrastructure, provides security services in sequential layers: identification, protection, detection, response and recovery.

These services have matured over the years and provide a solid foundation for the development and support of commercial and residential infrastructure.

Most currently available forms of cyber protection fall within identification and protection. Much as a help desk uses "run books," passive forms of cyber protection use whitelists and blacklists to identify, protect and respond to known forms of malware. A SOC also uses "run books" and knowledgeable security service personnel to help respond to and recover from new and ongoing security threats.

"One of the more insidious characteristics of evolving cyber threats," Blackard notes, "is that cyber threat also includes real-time attacks from bad actors. These attacks employ the orchestrated application of both passive and active malware and real-time hacking to break into your network." The only way to protect networks from this kind of attack is with the use of good actors known as "white hackers" and "counter hacking."

> To ensure stability, a network requires a security operating center to work in parallel with the network operating center – for roughly the same cost.

White hackers and defense perimeter network administrators work as a team to control the security domain in a cost-effective manner for each network defended.

Identify. The first phase of protection is the identification of known, common cyber vulnerabilities. This information is typically updated and provided through third-party virus protection software. These lists are provided through subscription services, and cyber specialists continually add new threats to the lists.

Protect. Hardening an enterprise infrastructure is a large, time-consuming task that typically takes a week or two. For vulnerable networks, hardening steps should be taken in prioritized order to ensure the threats can be detected, isolated and mitigated. All steps in the hardening process are important, but the order in which they are executed is critical. During the hardening process, the infrastructure can typically be defended if the attack can be detected. This makes detection the first and most important element of protection.

Detect. The most important element of detection is the ability to characterize normal and abnormal users, devices, software and configurations. Everything must be analyzed as "known good," "known bad" or "unknown." Unknown threats must be analyzed to determine the danger they pose.

Respond. If a new and unknown cyber threat is detected, damage is occurring. Every minute the threat goes unaddressed increases the cost of recovery. Damage includes the time required for cyber operatives to terminate the attack, assess and correct the damage, as well as the costs of implementing security provisions designed to prevent similar attacks in the future.

Recover. After identifying and terminating a previously unknown cyber threat, cybersecurity operatives restore normal network operations and fully document the new threat. This information is also used to update passive forms of cyber protection.

SUMMARY

Maintaining reliable internet access is already sufficiently difficult, and rapidly maturing cyber threats have added a new, expensive dimension to customer support. The good news is that the vast majority (99 percent) of cyber threats are quickly and quietly dealt with through passive support systems. The bad news is that the last 1 percent easily accounts for 99 percent of the cost of and related damage to modern network operations. It is no longer a matter of whether you will suffer a cyberattack but a matter of how much identifying, terminating and recovering from an attack will cost.

Cybersecurity is just one of the many reasons broadband do-it-yourselfers need to ally themselves with professional service organizations that can help maintain stable broadband systems. ❖

David Daugherty is the chairman and co-founder of Clarus Broadband. Clarus is dedicated to the development and marketing of broadband in underserved markets. Contact David at david@clarusbroadband.com.