The Michigan Association of MACPA Certified Public Accountants

the BusinessEdge Inside Technology

Oct. 31, 2008
Volume 5, No. 11

In this issue...

Words from the Wise

"The secret to creativity is knowing how to hide your sources."

- Albert Einstein

Network Security Audits: Every Three Months or 3,000 Miles

Printer Friendly

By Lee Barken

Taking care of an automobile is a concept that we can all understand. Like the old saying, "an ounce of prevention is worth a pound of cure," paying attention to vehicle maintenance is a way to prevent little problems from becoming big problems. Does this type of mindset translate easily when you consider your company's operations and the Internet? When it comes to Internet security, what steps are you taking to protect your network and prevent a crash?

According to the 2007 CSI/FBI Computer Crime Survey, more than 80 percent of organizations conduct regular security audits. Who's watching *your* network? The answer may surprise you.

Every device on the Internet is scanned hundreds of times each day, but most of this traffic is harmless probing. It's up to companies to be vigilant about network security threats and plug the holes before the attackers find them.

A *network security audit* is a review and assessment of a company's network security protection. It's like having a police officer walk around your house to help you understand the most likely points of entry by a criminal. The idea is to learn from an expert before an attacker exploits a point of weakness. In fact, network security audits frequently use many of the same tools that the attackers use. The primary difference is that you get to discover the vulnerabilities (and fix them) before any actual damage happens to your company's assets and reputation.

Network security audits can be performed from an "external" perspective (outside the network perimeter) or from an "internal" perspective (inside the network perimeter). Given that network threats exist from both internal and external sources, a review of both should be considered.

It's important to remember that the goal of network security is not necessarily to provide absolute assurance against future network attacks. Rather, security professionals recommend an approach based on "security in layers." Why? The objective is to prevent the most common attacks, thereby encouraging attackers to move on to other,

easier targets. Like the old joke, "I don't need to be faster than the bear. I just need to be faster than you."

For example, if you ask yourself what steps you can take to defend against an attack on your car's security and protect against theft, the most common answer is to lock your car doors when you leave the vehicle. Will this stop 100 percent of all car thieves? Probably not. A determined attacker will likely find a way to exploit door lock vulnerability. How about if you add a steering wheel locking device? It won't stop everybody, but statistics tell us that most attackers will simply move on to the next, less protected target.

You can extend this analogy as far as you'd like. Would you hire armed guards 24 hours a day, seven days a week for your car? Would you deploy Patriot missiles? Of course not; this is an extreme. However, your actions will be based on whether you're driving a Pinto or a Porsche. Ultimately, a cost/benefit analysis will determine how far you will go to protect your information assets (or your car). While each company will answer this question differently, the point remains the same: New vulnerabilities are discovered on a daily basis and network security is an ongoing battle. So every now and then, somebody needs to check if the doors are locked and the steering wheel locking device is securely in place.

For wireless networks, once you "cut the cord" and experience the pleasure of uninhibited roaming (and increased productivity), it's impossible to go back to the mundane era of tethered PCs and work environments that require you to be "chained" to a desk.

The great thing about radio frequency wireless networks like Wi-Fi is that the signal goes through the walls. The bad thing about wireless networks is that the signal goes through the walls. An attacker could be in your parking lot or even 25 miles away. With specialized wireless gear, he or she can pick up your company's wireless network signal and attempt to gain unauthorized access. This means that your company's investment in perimeter security—network firewalls, door locks, key cards, cameras, guard stations—can be circumvented by an improperly configured wireless network. Therefore, wireless networks should be included in all network security audits.

About the Author

Lee Barken, CPA, CISSP, CISA, CCNA, MCP is an IT practice leader with the CPA firm, Haskell & White, LLP, located in Irvine, Calif. Lee can be reached at lbarken@hwcpa.com.