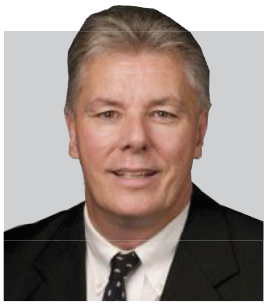
IT Intelligence

5 STEPS TO SAFEGUARD AGAINST CYBER THREATS

by Bob Stockwell



Bob Stockwell is Chief Technology Officer for STANLEY Security. From 1997-2012, he was Niscayah's Director of Systems Operations.

bob.stockwell@sbdinc.com

Beyond making sure a project is completed correctly and on time, security integrators must be wary of virtual threats to a customer's system. With most of today's devices connected to data networks, it's imperative that integrators are diligent about protecting the customer's infrastructure as well as their own.

A single virus or worm can wreak havoc. Other ways to cripple a network or compromise data include denial of service (DoS) attacks, keyloggers, rootkits, spyware and adware. Let's look at how integrators might guard against them.

ENTIRE NETWORKS FACE RAPID COMPROMISE

Most viruses are designed to replicate themselves into other files to consume hard-drive space, corrupt files or produce malicious code. If a virus penetrates an access control system, this may allow protected areas to become vulnerable to outside threats and unauthorized individuals. Viruses called *dialers* reroute a system's phone dialers to other numbers; these open a backdoor into the system or route calls.

Worms are similar in that they replicate themselves, but are network-aware. After a worm infects a system, it searches for other connected systems. This can bring down a whole system in a very short time. Additionally, it's very difficult to get rid of worms, because as it's deleted, the worm continues to reinstall itself unless protection is immediately put in place. For instance, an infected video server farm would be rendered useless until the worm could be removed. In some cases, worms are designed to delete files, causing a loss of video that could take hours or days to rebuild.

Malicious attacks don't have to come from the Internet, and can even come from well-meaning or disgruntled employees.

One of the most dangerous threats is a *keylogger*, usually combined with a remote-access virus. Keyloggers capture every keystroke typed and report them to the controlling system, granting remote access to the system's information. This compromises the system and confidential data.

STRINGENT POLICIES ALSO NEED ENFORCING

It's essential to have trained personnel working on and monitoring a system. Clicking on the wrong link can bring down an entire system or delete critical data, setting up both the customer and integrator for serious liabilities.

Protecting customer site information is critical. For many businesses, it's not unusual for employees to keep backup copies on their company laptops. While this can be immensely beneficial for quickly restoring a crashed or infected system, it can also expose customer configuration and information to others if not properly protected.

This is why it is so important that company computer policies are always enforced. Most companies have these policies in place, but they are not monitored or regularly carried out. Consider these scenarios:

Scenario 1: An employee takes a company laptop home to do some after-hours work. While at home, he remembers that he wanted to look up an item for a birthday gift. Rather than going to his personal computer, he uses the company laptop. The site he visits is infected with malware, subsequently infecting the laptop. The next day, the employee connects to the corporate site and security network with the same laptop, thus infecting it.

Scenario 2: An employee takes a company laptop home, and connects to her network. Her kids have been downloading music, unknowingly infecting the home PC and network with a worm. The worm registers the new laptop on the network and infects it. She then uses the laptop at work and infects the rest of the company's networked computers.

Malicious attacks don't have to come from the Internet, and can even come from well-meaning or disgruntled employees. Sometimes an act as simple as deleting a critical file can take a system down.

Though no solution is bulletproof, critical steps can be taken to prevent these problems:

(1) Start with a strong, company-wide computer use policy that is meticulously monitored and enforced.
(2) Install antivirus and malware protection software on all company computers and servers.
(3) Have firewall and DoS applications in place on the corporate network.
(4) Scan incoming E-mails for potentially virus-infected attachments.
(5) Monitor Web traffic.

Every day, new attacks are created and released. You must be vigilant in helping customers identify weaknesses in their systems. Implementing as many walls of protection and preventative policies as possible will help to diminish the threats — and to protect the liability of both you and your customer. SSI