Information By Design
Technology for Business Performance

Protecting against the stealth hacker

Network security should be paramount on your mind. Try this one on for size. The cyber criminals are now collaborating to create networked (combined) and persistent (stealth) threats. They are getting paid by 'bad guys' based on the number of infections and the persistent (undiscovered) nature of their malware. The greater the number of infected hosts, and the longer the infection lasts, the more money that hacker can reap. The malware, of course, is designed to provide some avenue of revenue generation for the 'bad guys'. An example is the ability to capture the administrative login ID and password for your SQL Server (the database that holds your company data).

We've just finished reviewing Cisco Systems Mid-year Security report (http://cisco.com/web/about/security/intelligence/midyear_security_review09.pdf) and VeriSign's white paper on the state of phishing. These reports describe the increased sophistication of hackers to penetrate the standard firewall, anti-spam, anti-virus configurations found on most SMB (small and medium sized business) networks. While you're feeling comfortable with these basic security building blocks, the 'bad guys' have found numerous methods to circumvent this architecture.

Phishing — luring unsuspecting users to provide sensitive information for identity or business theft — is a serious threat. This fraud method has been growing rapidly, with one estimate citing approximately 8 million daily phishing attempts worldwide. To increase success rates, some attacks combine phishing with malware for a combined attack model. For instance, a potential victim receives a phishing e-card via email that appears to be legitimate. By clicking on the link inside the email to receive the card, the person is taken to a spoofed Web site which downloads malware to the victim's computer.

As the hacker community becomes more sophisticated 'breaking and entering', you have to be more diligent in your approach to IT security. The best run companies practice a layered approach to IT security. By implementing the appropriate tools, technologies, training and process, you can make it almost impossible for even the most experienced hacker, to penetrate your defenses and wreck havoc with your most valuable company asset – your data.

IBD has recently partnered with Perimeter USA, a global leader in security tools, to craft the most cost effective approach to implementing layered security. Contact us to discuss how IBD can help protect your future.

The author, ***AJ Walters*** is a principal consultant for Information By Design, LLC.