PROCESSOR

Tech & Trends

Click To Print

General Information

October 15, 2004 • Vol.26 Issue 42
Page(s) 31 in print issue

Are You Paranoid Enough?

Security Testing & Auditing Keeps IT Resources Safe & Sound

If there is an IT department on the face of the planet that doesn't understand the need for tight security, it must be living in a cave—probably one without Internet connectivity. With denial of service attacks, viruses, and malicious malware just waiting to penetrate the corporate firewalls, security is often the No. 1 priority for a CIO.

But once all the firewalls are installed, the virus scanners humming, and the VPN bridging your home users, how do you know that you've really locked out all the bad guys? When downloading an image can spread a virus, what does it really mean to be secure?

Designing a security policy and performing a gap analysis is something that a company can tackle by itself, says Ross Armstrong of Info-Tech Group. Armstrong, who is currently in the middle of an in-depth analysis for Info-Tech, says that competent HR and IT managers can work together to determine where the company is lacking as far as security policies and procedures go. But when it comes time to put these policies to the test, it's time to look outside the company. (*Disclosure: Info-Tech analysts write a twice-monthly column for* Processor.)

■ The View From Outside

"For example, it's a good idea for any medium-sized company to conduct a penetration test once in awhile," Armstrong says. "It's almost a fundamental requirement that you hire somebody else to do it. Hire a third party to do it whether or not you have the expertise in-house to do it. Hiring your own network administrator to do a penetration test on your network is like hiring yourself to break into your own house."

Armstrong states that security testing needs to be done from the standpoint of an outsider trying to break in. This means the tester should have essentially zero knowledge of the network at the start. "You've got to make sure the consultant or consulting group hasn't had any direct contact with anyone in your company nor has any inside information regarding your network because, again, it's supposed to be an external penetration test. If they have any inside information, that can skew the results of the test."

Conversely, auditing requires a firm to dig deep into the details of current infrastructure and policies. For that reason, Armstrong doesn't believe that a single small firm can perform both duties. Larger outfits can separate their roles sufficiently so that a separate group can handle each function without sharing information that would give the testing team unfair information.

Similarly, Armstrong warns against giving your IT staff any heads-up notice that testing is going to occur. “It’s one thing if they’re coming in to check the physical building and they’re going to be checking out alarm codes and that sort of stuff—then you’re going to want to give them a heads-up. But when it comes to straight-up network testing, you want them to be able to try and hack into the network as if it were any normal day. And if you tell your staff, they might get reactive and then it won’t be a normal day.”

The Human Factor

In addition to purely electronic testing such as port scanning, Armstrong is a believer in testing human assets, as well. “That’s usually a good thing to try and test; have [the tester] call up the IT help desk or something like that and pretend to be a user and try to get a password. That’s actually an excellent way of assessing internal security because then you find out that not only are [users] susceptible to social engineering, but if you do get a password, then you can see if the employees are using strong passwords or not.”

Testing isn’t a one-time endeavor, either. Depending on the industry, it needs to be repeated on a regular schedule. “There’s really no hard-and-fast rule that I’ve ever come across saying how often you should have the testing done,” explains Armstrong. “A lot of it’s going to have to do with what type of business model you have. For example, if you’re an ecommerce company, then you’re going to want your Web servers tested pretty frequently, like maybe a couple times a year, because everything depends on the revenue being generated from your site. For a company that’s more bricks and mortar, it might only be necessary every 18 months.”

He also points out that with new regulations such as Sarbanes-Oxley and Gramm-Leach-Bliley, a company may find itself required to perform tests on specific schedules. “There might be some new piece of legislation out there that says you have to get testing done every 12 months, without exception.”

Ask The Right Questions

Finding a credible firm to conduct auditing and testing requires that you look at several factors. One important question to ask is whether the company is certified for the networking hardware and applications you own.

“You’ve got to make sure that the consultant has the skills to navigate your network without interrupting the service in any way or crashing the server,” comments Armstrong.

Cost is another factor to consider. Armstrong believes that this is one expense that doesn’t make sense to skimp on. “You do get what you pay for, so if a consultant becomes so cheap it’s too good to be true, then it probably is.” ■

by James Turner

Auditing vs. Testing

A comprehensive analysis of your company's security requires insider knowledge of the company, as well as the kind of inquiry that only an outsider can conduct. Here's a brief summary of both kinds of analysis.

Auditing

- Provides a detailed gap analysis of what policies and procedures are outdated or missing.

- Should do a physical inventory of equipment and determine what resources may be on the network but unmonitored or unprotected.

- Should ensure that all procedures are in conformance with industry regulations.

- Requires in-depth knowledge of the company.

Testing

- Intended to probe the defenses of the company.

- May include "human engineering."

- Should have zero knowledge of the company resources except for publicly available information.

Some Auditing Resources

Information Systems Audit and Control Association
www.isaca.org

The Institute of Internal Auditors
www.itaudit.org

Generally Accepted Information Security Principles
www.issa.org/gaisp/gaisp.html

Federal Financial Institution Examinations Council
www.fdic.gov/regulations/examiner/index.html

Health Insurance Reform: Security Standards Final Rule
a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03-3877.htm

Source: Burton Group