Single layer of security not enough

IN MY OPINION

SATNAM PUREWAL

The Internet is growing at a phenomenal rate and along with it are growing security risks to business information systems.

In a recent test conducted by the U.S. defence department, 7,860 of 8,932 random attacks launched on systems on the Internet were successful. What's more frightening is that only 390 attacks were detected and only 19 eventually reported.

In a survey published in the October 1996 issue of *Information Week*, nearly 70 per cent of respondents felt the increase in security risks to information and data matched or exceeded the growth in computing resources. Yet most companies continue to take an ad hoc approach to security.

The responsibility for security is all too frequently delegated to junior staff members who don't have the authority to implement or enforce security policies. This sends a clear message that not only is security unimportant, it is not a serious concern of the organization.

One of the most important steps in establishing a security infrastructure is to establish a security policy. Only 50 per cent of the businesses responding to the *Information Week* survey said they had one.

Senior management must establish a solid information-security policy that leaves no doubt as to what is required and expected and who is responsible.

A complete security policy for a company connected to the Internet should address access control and authentication, monitoring, incident response and reporting, data classification, business continuity planning, and non-disclosure agreements.

This will not only protect the company, but also establish the rights of the employees.

When moving to the Internet, companies must be aware that the control techniques used with their current systems will need to be enhanced. A single layer of security isn't enough.

The traditional ID and password approach with passwords expiring after 60 days is no longer sufficient. Passwords can be stolen and distributed over the Internet within minutes. With a little help from technology, malicious eavesdroppers can pick up a user's ID and password, so there is a much greater requirement for encrypted communications once an Internet connection is made.

Regular monitoring of the system is critical. Often, system administrators only discover a security breach from their counterparts at other sites, by which time the intruder may have been on the system for an extended period.

Never assume you know what's happening on your system. Tools that immediately notify appropriate personnel of intruders on the system are critical for the early detection of problems.

Stronger authentication is also necessary. Computers are configured to accept certain types of connections from other external or internal computers or servers. An individual bent on mischief could impersonate another server or person with privileged access — a technique known as "spoofing."

Technology changes quickly and it is important to remain up to date. In-house staff or hired consultants who install security in your systems should be experienced, professional and certified by an appropriate information-system security organization.

Ongoing training is also a necessity to ensure that new security trends, tools, and techniques are understood. If in-house staff are implementing new technology, you may want to consider including an experienced security professional in the project team. This will enable potential weaknesses to be identified at the planning stage.

It's important to remember that security is only as strong as the weakest link. Potential disaster is brewing for the many business connected to the Internet without appropriate security controls.

Satnam Purewal is a senior consultant specializing in systems and Internet security in the management solutions department of the Vancouver office of Deloitte and Touche. She can be reached at spurewal@dttus.com