How Secure Is Your Enterprise?

To Avoid Data Breach, Assess Your Current Security Situation

by Jean Thilmany

• • •

ENTERPRISES SPEND THOUSANDS of dollars on the latest lines of security defense, but they are still vulnerable to data breaches and failed audits due to areas that are often overlooked.

IT managers can never really be assured their IT operations are 100% secure, but by assessing their security methods and taking into account areas perhaps overlooked in the past, Chris Boyd, senior threat researcher at GFI Software (www.gfi.com), says they can get a better understanding of just how secure their enterprises are, he says.

"Personally, I'd start with the assumption that everything has been compromised—whether that's the physical building security, firewall policies, malware on the network, or data leaks—then [ask]: 'What's the most damage that could come out of this?'" Boyd says. "Once you know the worst that can happen, you can take steps to lessen the damage."

Evaluate Your Security Setup

Begin with a security assessment, says Upen Sachdev, senior director at technology services provider Allied Digital Services (www.allieddigital.us). Look at the firewall first, which is usually the top line of defense against hackers at SMEs, Sachdev says. Every day, hackers run massive network scans across the Internet in their search for vulnerable firewalls.

Key Points

- Assess current security measures throughout the enterprise and identify any security holes.
- Keep in mind that any changes you make to the network may open up your enterprise to security threats.
- Social networking sites can lead to security breaches; some vendors make technology that analyzes and stops such leaks.

"Monitoring a firewall and reviewing its logs will tell you how often your network was under attack and how successful

Go to Page 10

> "Small businesses usually run very lean IT operations, which means network changes are a lot more on-demand and tactical rather than strategic. So network changes can often lead to security lapses [or backdoors left] open."
>
> *- WaterlooSecurity Ltd.'s Fernando Duran*

Continued from Page 1

your firewall was in keeping hackers at bay," Sachdev explains.

IT managers with limited security staff could choose to hire a third-party security company to conduct vulnerability scans against the firewall, says Fernando Duran, CTO at WaterlooSecurity Ltd. (www.waterloosecurity.com). "There are several vulnerability scanners, but their reports can be overwhelming to interpret if you are not an expert," Duran says.

Even with contracted security help, however, IT managers must be aware of all enterprise hardware—such as the Web server or database servers—that has contact with the Internet and the business reason for that contact. To avoid security woes, if there's no business reason for the contact, the server shouldn't be linked to the Internet, Duran says.

Network Changes

IT managers will also need to assess security when instituting network changes, which can impact overall enterprise security, Duran says.

"Small [and medium-sized] businesses usually run very lean IT operations, which means network changes are a lot more on-demand and tactical rather than strategic," he says. "So network changes can often lead to security lapses [or backdoors left] open for intruders and hackers."

One common mistake is that temporary access provided for a particular reason isn't revoked, Sachdev says. "For example, a lot of administrators disable certain firewall rules as a troubleshooting step, but [they] forget to enable those rules again leaving open access to vulnerable targets," he says.

Whether they are intended or not, network changes can expose new services and network devices to the Internet, thereby introducing a new area for hackers to attack, Duran explains.

Network design plays a role in keeping enterprises secure, as well, Duran adds. Design flaws, such as allowing for local network congestion or failing to separate local networks, can also expose the networks to security compromises.

On The Defense

In addition to monitoring for threats against the firewall and assessing changes to the network, enterprises can take a number of other defensive measures to protect against security threats, Duran says. IT staff should assess those measures regularly to ensure that they will still be up-to-date and pertinent, Duran adds.

IT managers must also ensure that a good recovery plan is in place. Duran says this can be accomplished with backups. A good backup system should back up data automatically at set intervals and should be located offsite, to protect it from theft or natural disasters. You will also want to schedule the backup to run frequently so that a minimum amount of data would be lost if an outage were to occur.

"Check your backup periodically. You don't want to find out after a disaster that the [data] cannot be recovered," Duran says.

In addition, Andrew Wyatt, COO at security software maker Clearswift (www.clearswift.com), explains that IT managers need to stay on top of trends and changes, such as the use of social networking tools.

Social networks aren't going away, and, in fact, more enterprises are coming to rely on them for their marketing efforts, Wyatt says. For that reason, IT departments can't just lock down Facebook, Twitter, and similar social networking sites to keep their employees from accessing the sites and potentially sharing secure data.

Wyatt recommends that managers also investigate third-party Web and email software that automatically scans outgoing messages sent via email, social network sites, and other methods for information that violates security rules, as specified by IT managers.

The most important security measure an IT staff can have in place is a clear security policy that all employees understand and comply with. Wyatt says IT staff should refer to the policy often, to ensure it is as current as possible within this quickly changing IT landscape.

Before The Breach

Detecting security compromise after the fact can be tricky and time-consuming, says Joe Fisher, president of Affinity IT Training (www.affinity-it.com). He recommends both intrusion detection and prevention software. The prevention software can stop a breach before it happens or alert IT staff to suspicious activities, which is cheaper than plugging a hole after it's detected and important data breached.

Fisher says to keep in mind that the effectiveness of even this type of software can be compromised if it's installed into an environment that is already compromised.