THINGS THAT GO BUMP ON THE NETWORK

By identifying what went wrong, FIA tools help companies recover from disasters

By W. Wyatt Starnes, CEO, Tripwire Security Systems Inc.

Whether you're a network manager or CEO, stories of computer-system disaster are the stuff of nightmares. And a steady stream of new statistics tells us that the familiar boogeymen—fires, human error, faulty backups, power outages—have been joined by even more devious demons: sophisticated attackers intent on damaging businesses, especially those based on e-commerce.

In a recent survey, the Computer Security Institute (CSI) found that 30 percent of respondents reported system penetration from outside their companies, and 55 percent suffered attacks from inside. Over half said their Internet connection was the point of attack.

So we know attacks are on the rise, but the real financial impact remains a mystery. The 1998 CSI / FBI survey concluded that less than a third of the victim companies could even put a pricetag on their losses. But for those who could quantify the damage, the trend is alarmingly clear—monetary damages have more than doubled in the past year, to more than $136 million just among the knowledgeable respondents.

Today, hacking is one of the Internet's most common forms of disaster and often involves Trojan horses, viruses, active attacks and buffer overflows. The attacker usually has a goal of either shutting the system down or obtaining remote access in order to sniff passwords to open a channel so that information can be viewed at any time or exploit other trust relationships on the target network.

Having a disaster response and recovery plan is essential. Beyond specifying who is responsible for which corrective actions and chain of command issues, you need to ensure that the proper technologies are in place to enable a quick and complete recovery. Fortunately, tried-and-proven methods, such as system redundancy, are being bolstered by tools providing what network managers need most: accurate damage detection and the ability to restore system integrity.

As a sign of the times, case histories are accumulating that prove the value of tools, such as File Integrity Assessment (FIA) software, in helping businesses that suffered potentially disastrous intrusions get back to business quickly, thus minimizing financial loss.

Real-Life Nightmares

The very nature of E-commerce presents new and complex system vulnerabilities. No longer is the damage as trivial as the security of a credit card transaction. If you're an airline, it means your entire reservation and ticketing systems are grounded. If you're an online stock trader, it means fines, penalties and a potentially fatal loss of reputation.

Consider the plight of the system administrators in these three recent incidents:

- An attacker penetrates an online stock-trading site with 10 web servers connected to a central database server. The administrator could not contain the damage by disconnecting the servers from the network. Disconnecting would constitute a "trading halt," subjecting the company to review by the SEC and possibly fines. Such downtime would stop the business in its tracks and destroy its trust reputation, perhaps permanently. Every second spent looking in the wrong place allows the attacker to burrow deeper into the network. Which servers have been compromised? To what extent?

- A hacker attacks all critical machines on an online E-commerce company's 100-server network. Everything is compromised, from access-control mechanisms to passwords, to internal operations. Reinstalling the OS on every machine is simply not feasible.

- An engineering firm terminates an employee and soon afterward detects evidence of repeated attacks. No intrusion-detection software is installed that can tell what files have been altered or what methods the intruder employed. What to do?

Detecting the Attack

One of the first considerations in your disaster plan is how to prevent small incidents from exploding into disasters. An Intrusion Detection System (IDS) can serve this purpose by providing critical notification of an attack.

A network-based IDS relies upon an attack signature database to recognize incoming exploits. They are especially effective against "script kiddies," publicly available attack scripts used by less sophisticated attackers. The shortcoming is that new attacks are developed every day, and the **best**-case scenario is that network-based IDS will always be one step behind.

An anomaly-based IDS, however, utilizes known facts about your system files to detect any alterations to those files. When it detects a deviation, it alerts you. Anomaly-based IDS can also monitor your software's system calls, because any deviation may indicate an attack, such as a buffer-overflow attack. Anomaly detection can also flag deviations in network communication channels, which is an effective way to monitor internal networks.

FIA is a type of anomaly-based IDS gaining prominence for its effectiveness in disaster recovery. FIA tools compare system "snapshots" before and after an incident. For example, it will check access control lists and registry keys, in addition to file permissions (almost any attacker will modify files or registry keys somewhere on your system as part of the attack).

Identifying the Damage and Recovering

When confronted with a system attack, the ability to compare pre-attack system data with the system's current state is the key to successful recovery. Remember the three nightmare incidents earlier in this article? All are testimonies to the value of effective IDS tools:

- In the case of the stock-trading firm with the 10 web servers, the system was equipped with an FIA package, called Tripwire® from Tripwire Security Systems, Inc. Immediately after discovering the intrusion, the system administrator checked the integrity of each of the 10 web servers. Within minutes, she found that only three of the web servers had been compromised. She disconnected those three from the network and was able to keep the site running until the end of the day's trading. Over the weekend—using the database Tripwire created prior to the attack—she was able to fully restore the three compromised web servers in time for Monday trading. The administrator estimated that 260 hours were saved because of Tripwire.

- The online E-commerce company with 100 servers did not have the right tools installed prior to the attack. They immediately brought in a system consultant who reinstalled the OS on one machine to create a baseline database. The consultant then progressively determined what had been changed on the other machines, and was able to restore them using Tripwire. The company estimates that manually comparing and reinstalling all servers would have taken three man-years. With the right tools, it took less than three man months.

- The engineering firm also did not have an FIA tool installed, but the system administrator was able to create a baseline database on a clean machine, and then copy it to a compromised machine. At that point, the company ran a scan with Tripwire, which detected root kits and trojans in several user home directories. The firm removed these backdoors to prevent future attacks.

Lessons Learned

Every organization hopes they will never need to use their disaster plan. But, just like planning fire escape routes and knowing where the fire alarms or fire extinguishers are located, knowing how you will proceed if confronted with a system disaster is half the battle. To conclude, your first priority after any intrusion is to determine the damage.

You need to know what is damaged, what can be repaired, and what is still clean. An FIA tool enables you to quickly make these assessments.

The key to making FIA effective is being proactive. Before bringing systems or servers or workstations online, take "snapshots" of them in pristine form to create a baseline database. If you're attacked, you can quickly determine which files have been altered. Make sure to run the tool at regular intervals so you can detect intrusions before they reach nightmare proportions.

With the proper precautions and some forethought, addressing disaster in the digital age does not have to spell disaster for your organization.