

Network HACKERS

The Hidden Threats

BY BILL BOOTHE

Securing your club's computer network may not be on the top of your to-do list — but it should be. Today's private club systems face a myriad of outside threats: e-mails loaded with deadly viruses, hackers intent on doing damage to your network, and crafty entrepreneurs looking for ways to use your club's network for their own business purposes.

You may already be aware of the more obvious dangers presented by intruders: damage or theft of your club's private data files, system crashes, and e-mail viruses. In this article, we'll focus on less obvious threats to your network — threats that are just now coming into full use by intruders.

Attacks on Other Networks

Hackers can use your club's systems to attack others. A common attack scenario is called Denial of Service (DoS), where one computer sends a barrage of communications to another in an attempt to overwhelm the target computer. A more sophisticated version of this attack is called Distributed Denial of Service (DDoS), where multiple computers (typically thousands) are used to direct a coordinated attack on a target.

Hacker websites provide sophisticated "attack scripts" which are easy to use — even by novice hackers. Plus, these sites promote attack "tournaments," with prizes to those with the most successful attacks. Recently, a hacker site was itself hacked during a tournament in an effort to keep the results from being published (a satisfying turn of events).

This is a popular attack formula for teenaged hackers (millions across the globe) because they are often competing for "bragging rights" on the number of computer systems they have "taken down." Hacker websites provide sophisticated "attack scripts" which are easy to use — even by novice hackers. Plus, these sites promote attack "tournaments," with prizes to those with the most successful attacks. Recently, a hacker site was itself hacked during a tournament in an effort to keep the results from being published (a satisfying turn of events).

What's disturbing about DoS and DDoS attacks is not just that your club's computers could be involved, but that your club could be sued in court by the party damaged by an attack. In some recent court cases, plaintiffs have attempted to assign responsibility to unwitting owners of systems used in such attacks. These owners

were accused as "intermediate sources of damage" and were sued for liability in the attacks. To our knowledge, the courts have thus far taken a lenient approach towards these owners, agreeing that they cannot be held liable for something of which they were unaware. However, industry experts warn that these decisions could begin to turn against unwitting owners as public awareness grows on the subject.

Setting Up Shop on Your Network

Computer processing capability is expensive (especially for a 16-year old). Starting up an online business requires up front capital for computer equipment and software, Internet access fees (bandwidth), office space, equipment maintenance, and lots of other business costs. That's why hackers would prefer to use your club's systems for free!

A favorite of hackers is using resources from unwitting systems owners to operate Web-based businesses. These "spam factories" can send thousands of e-mail advertisements per hour — sapping the resources of your club's network. Equally disturbing, unauthorized spamming can put your club at risk if the spam content is offensive to its recipients (i.e. pornography). Recently we heard from a club whose Internet Service Provider (ISP) threatened to suspend the club's access to the Internet because of numerous complaints from sites in Europe receiving porno spam — with the club's e-mail address as the sender! Needless to say, the club was greatly embarrassed by this incident, and moved quickly to rid their system of the intruder and shore up their security gaps.

Another exploit is to use a vulnerable server as an intermediate storage device for the trading of music and other not necessarily desirable files. In some cases, because of the nature of the files involved, federal and state authorities may launch detailed investigations. Those investigations often involve the internal personnel of the exploited network, who must first be ruled out prior to looking for outside culprits. This can be a time-consuming — and embarrassing — endeavor for a private club.

How Vulnerable is the Club Industry?

Our firm performs more than 150 financial audits each year for private clubs in Florida. Because we are concerned about network security for those clients, we recently added a network security survey to our standard audit approach. The initial results have been an eye opener.

First, we were surprised at the number of clubs with high speed Internet access (mostly DSL) through their networks. Based on the results of the first 40 surveys, more than half of the clubs are "hot wired" to the Internet. However, we were shocked to learn that only a third of those high-speed connections are adequately protected with a firewall. Assuming that these results are representative nationally, the industry has a serious problem.

What Can You Do to Protect Your Club?

Most clubs buy a DSL router and service package from a local provider, hook it up, and head for the Internet. Problem is, many DSL providers do not include

a firewall with their DSL service (or what they provide is insufficient). That means the moment clubs go on-line they become wide open to outside intrusion.

Here's the good news: firewalls are simple to operate and relatively inexpensive to purchase and maintain. Most commonly, a firewall is a software program designed to detect and prevent unauthorized access to your network. Software firewalls are available on the Internet for free, or can be purchased for a few hundred dollars.

In addition, a firewall appliance

Most commonly, a firewall is a software program designed to detect and prevent unauthorized access to your network. Software firewalls are available on the Internet for free, or can be purchased for a few hundred dollars.

A favorite of hackers is using resources from unwitting systems owners to operate Web-based businesses. These "spam factories" can send thousands of e-mail advertisements per hour – sapping the resources of your club's network. Equally disturbing, unauthorized spamming can put your club at risk if the spam content is offensive to its recipients (i.e. pornography).

(electronic box with software) can be added to your network to provide a higher level of protection. If you have any devices available on the Internet such as an e-mail server or website, you should have a true, purpose-built firewall such as those from Cisco, Nokia, Watchguard, and SonicWall. These firewalls are specifically designed to protect networks.

If all you are providing is Internet access for your network, then you can use a device such as a cable/DSL router from such vendors as Linksys, D-Link, and Netgear. Properly configured, these devices can provide adequate protection of a private network that only requires Internet access.

For portable computers, you should consider implementing personal firewall software from Zone Labs or Internet Security Systems (ISS). This software will protect these devices when they are away from your protected network.

The Bottom Line

If your club uses high-speed ac-

cess to the Internet, make sure you have a good firewall. Check with your Internet Service Provider to see if you already have one, and if so, which one. If you don't have adequate protection, get it right away. You can't afford to leave your club's computer network open to intruders. ❏

*Bill Boothe is director of club/resort technology consulting for RSM McGladrey, Inc., one of the nation's largest business services providers. He has assisted more than 300 private clubs and resorts with the planning, evaluation, selection, and implementation of computer technology in all facets of their operations. Bill has published numerous articles, is a frequent speaker at hospitality conferences, and is the author of the national newsletter **Private Club Technology Update**. He can be reached at bill.boothe@rsmi.com, or at (561) 682-1638.*

Jeffrey B. Hall, CISSP, GSEC, manager with the RSM McGladrey, Inc. Integrated Technology Solutions Group, was a contributing author for this article.