A Network Security Checklist You Can Really Use

BY BILL BOOTHE
DIRECTOR OF CLUB/RESORT TECHNOLOGY CONSULTING
RSM MCGLADREY INC.

Many of you may know that our affiliate firm, McGladrey & Pullen, LLP, performs financial audits each year for more than 150 private clubs. As part of our service to those clients, the audit staff administers a "Network Security Checklist" designed to quickly identify any significant security issues associated with a particular client's PC-based computer network. Each year we review the responses from our private club clients — and the results are nothing less than shocking! Less than 20 percent of the clubs surveyed with this tool get a clean bill of health. In many cases, we must serve up a lengthy list of "Management Letter Comments" with our audit report, pointing out serious deficiencies in the club's network security.

To assist you in measuring your own club's network security health, we've included below our actual checklist for your use, along with the explanations provided to our audit staff for each checklist question. We recommend that you apply the checklist at your own club, and where appropriate, take immediate corrective action.

PC-Based Computer Network Security Checklist

1. *Is the client's network connected to the Internet via DSL, cable modem, or some other "always on" connection?* DSL and cable modem are the most popular methods used by our clients to achieve a high-speed connection for Internet and e-mail access. If the client is using DSL or cable modem, they are vulnerable to hacker attacks — especially

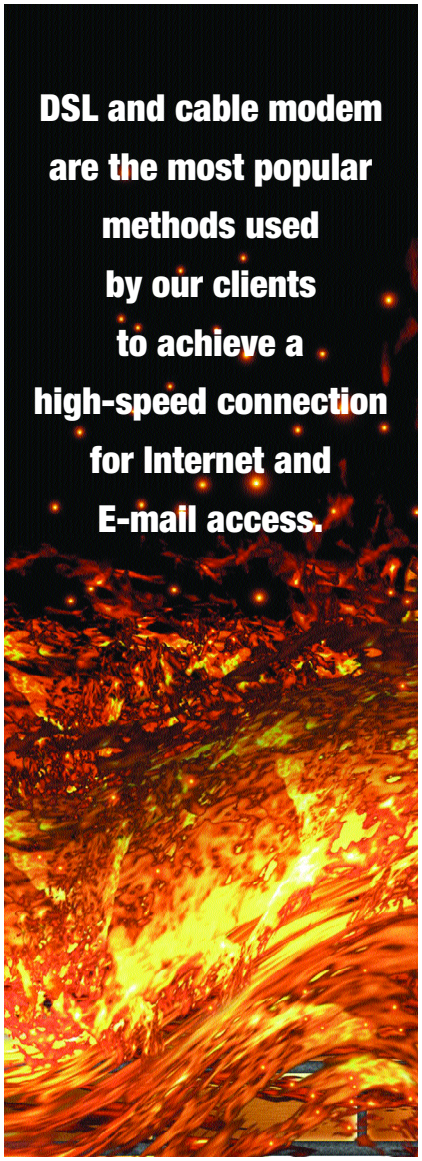
since their connection is "always on." These connections place all of the clients computers on the Internet unless the client has implemented other appropriate security measures discussed below.

2. *Does the network have a firewall product (software or firmware) installed and operational at all times?* Firewalls can take the form of a software program such as BlackIce or ZoneAlarm, or as an electronic appliance such as Watchguard, Sonicwall, Nokia/Checkpoint, or Cisco PIX. Firewalls are designed to keep outside intruders (hackers) out of the client's network. Once inside the network, hackers can do great damage to the client's systems. They can steal or destroy information, crash the network, or use the system to attack other networks. We need to assure that our client networks are secure from hacker damage, and firewalls are an important part of that security.

If so, what brand and version? We need to know specific information about the firewall in use. Different firewalls provide different levels of protection. To make sure the client is adequately protected, we need to know the following: the name of firewall's manufacturer (e.g., Cisco, Nokia, Watchguard, etc.), product name (e.g., PIX, Firebox, etc.), model number (e.g. 515, 330, etc.), version, date installed, and date last updated.

3. *Does the network have an intrusion detection/prevention system installed and operational at all times?* Intrusion detection/prevention systems represent an additional step above firewall protection. These systems look closely at all network traffic, seeking to identify any suspicious files or activity as they occur. They pick up where firewalls leave off, helping to identify attacks that may have already breached the firewall. Most of our clients can be adequately protected without the need for intrusion detection/prevention. However, for systems that store highly sensitive data (e.g., credit card numbers, social security numbers, etc.) or for systems that have been repeatedly compromised, intrusion detection/prevention may be needed.

4. *If so, what brand and version?* (Same as question 2 above.)



5. *Has an independent source been contracted to test the network's vulnerability from outside intrusions?* Periodic security testing of the network is the only practical way to know if the network and related systems on the network are reasonably protected. Such testing is carried out by network security specialists using some of the same tools employed by hackers. Remarkably, a large percentage of clients who believe they are adequately protected are rather easily compromised through this testing technique. Once the testing is completed, appropriate recommendations can be implemented to insure that satisfactory security is implemented. Because of the complexity, sophistication, and ever-changing nature of network security testing, outside organizations are inherently more capable of conducting such testing.

If so, how recently and what were the results? Network security changes on a daily basis, as hackers learn new ways to compromise systems and vendors react with upgrades and fixes. If outside testing has been performed, we need to know how recently the testing was conducted, to assure that the network and systems are satisfactorily protected. The more outdated the testing report is, the higher the risk that the client's systems could be susceptible to attack.

6. *Has the client's network or systems been attacked or compromised?* If so, please describe the attack or compromise and the outcome. It is especially important to know if the client's network or systems have ever been attacked or compromised, when they were attacked or compromised, what was attacked or compromised, and what was done to prevent future attacks and compromises. Often clients may discover an attack, install a firewall (or enhance an existing firewall) and assume they are safe - only to find out later that the attacker has left a "back door" open for unauthorized entrance at a later date. Networks or systems that have been attacked, and especially those that have been compromised, should have a security assessment to assure that they are satisfactory to operate.

7. *Have network devices such as routers, switches, and servers been security hardened as per their vendor's published security guidelines?* Cisco, Microsoft, Novell and other vendors offer detailed specifications on how to security "harden" their devices — making them harder to compromise. Failure to follow these guidelines puts a client's network and systems at much higher risk.

8. *Are passwords required and are they periodically changed?* Passwords are a relatively simple — and surprisingly effective — security measure. Unfortunately, most clients do not use an effective password system. Many clients assign the same password to multiple users, or allow users to keep passwords in use for many months or

years. We need to know the status of the client's password usage to determine if enhancements are needed.

9. *Does the system maintain a user access log that tracks user access to the core applications and network servers?* Advanced networks can track all user activity if system logging is enabled. Unfortunately, most clients do not review these reports and are thus not aware of obvious security breaches - from within or outside the organization. We need to know if these reports are being reviewed regularly, and by whom.

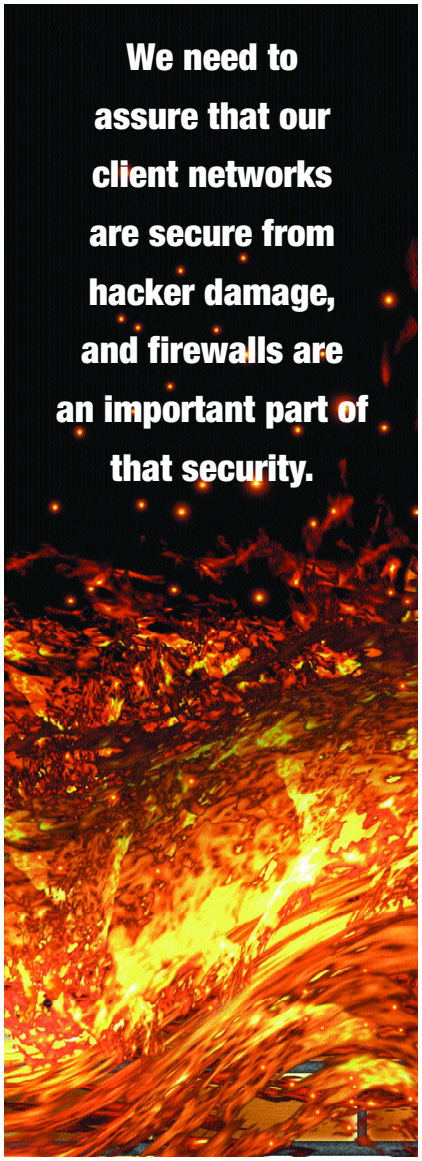
10. *Are the critical data and applications backed up on a daily basis?* This is another area where many clients do an inadequate job. All critical data should be backed up every day, using a 30-day tape rotation system.

Are back-up media taken offsite? A copy of the backed-up data should also be stored offsite every day. Generally, the offsite media is from the previous day. There is no way to predict when a disaster might strike, so a daily offsite backup routine is an important measure to safeguard the club's data.

Are the on-site backup media securely stored? All back-up media kept on site should be stored in a fire/water proof cabinet or safe. Access to this media should be limited, and the cabinet/safe should be locked.

11. *Is the operating system software of all network devices such as routers, switches and servers periodically updated to be current with the latest patches released by the devices' vendor?* Cisco, Microsoft, Novell, etc. continually release updates to their operating system software. Many of these updates are security-related, designed to strengthen the security of the network. Often clients are remiss in applying these upgrades in a timely manner, and thus their networks are at a higher than acceptable risk to the threats. We need to know that the client is keeping the network software up to date.

12. *Does the client have anti-virus software installed on all servers and PCs?* Viruses are the most common source of attacks on networks and their systems. Viruses can damage



or delete data, copy sensitive information, and send it to an outsider, or crash the network altogether. Anti-virus software is an important part of a network's security defenses, and should be installed on all servers and PCs.

If so, what brand and version? We need to assure that the client is using the latest version of a recognized anti-virus product such as Symantec (Norton), McAfee, Trend Micro, or Computer Associates (CA).

13. *Does the anti-virus software automatically scan all files added to the system — including e-mail?* Automatic scanning is the key to early identification and eradication of viruses. Unfortunately, many clients do not employ automatic scanning, but instead rely on employees to execute their own scans on a periodic basis. Delays in scanning are just what viruses and worms are counting on as they send themselves to attack networks.

14. *How often are anti-virus definition files updated?* As stated above, the world of computer security changes daily. It is estimated that about 10 new viruses appear each day to attack unwitting systems, the majority of which are focused on Microsoft Windows. Anti-virus software includes a library of virus definition files, which are used during scanning to identify and destroy viruses. Obviously, if these definition files are not regularly updated, they will present opportunities for newer viruses to slip through the scanning.

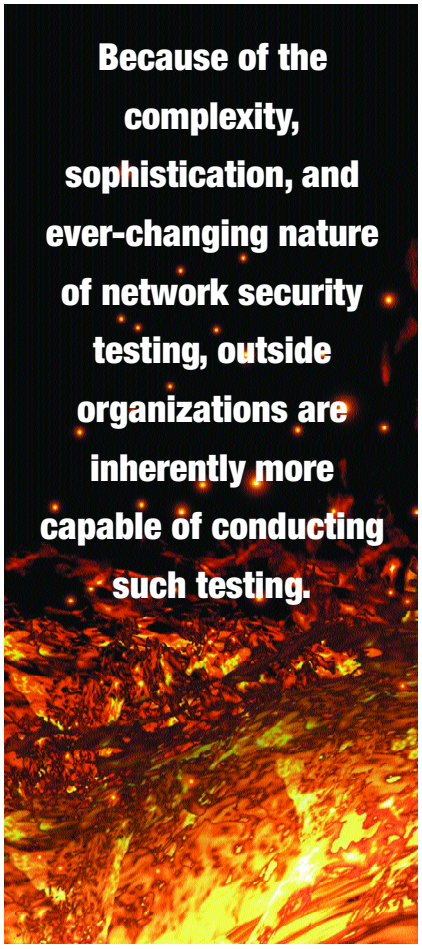
Is it a manual or an automatic process? Most clients require employees to update their virus definitions on a regular basis. Unfortunately, such a volunteer process typically means that anti-virus definitions are not updated often enough to ensure reliable protection. To eliminate this problem, virus definitions should be updated automatically from the anti-virus software provider at a minimum of once per day.

15. *Does the network use a wireless method of communications to attach PCs and printers?* If yes, is Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access v2 (WPA2) configured and fully operational? Wireless technology is becoming more popular with organizations. Some examples of wireless uses are: to connect one or more users located in the main clubhouse to the main computer server, without installing cabling; to connect golf or tennis shop PC's to the main network server, when the shop is in a separate building nearby; to connect hand-held POS devices to the main network server. Wireless can be a great tool for connectivity, but it brings with it significant security risks. In essence, wireless systems broadcast a signal outwards 150 to 300 feet in every direction.

If this signal is not protected, it can be picked up by any nearby wireless PC. Once the signal is acquired, the outsider can attach to the club's network and operate as a

normal user. Hackers dubbed "war drivers" drive through office parks and neighborhoods looking for wireless networking signals. "War drivers" then post their lists of wireless networks for others to use and abuse. To eliminate this threat, Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access v2 (WPA2) should be used. WEP and WPA2 configure the wireless transmitter to only accept PCs that use an assigned system identifier and key, thus keeping unauthorized persons off the wireless network. Properly configured, WEP and WPA2 also encrypt wireless communications. WPA2 was introduced in late 2004 and is designed to be significantly more secure than WEP. It is recommended that client's implement the WPA2 standard in place of WEP to ensure the highest level of wireless security.

16. *Is a formal disaster recovery plan in place for critical systems and operations?* Most of our clients do not have a formal disaster recovery plan — not even a simple one — for their computer systems. Once disaster has struck (in the form of hacking, theft, vandalism, or natural disaster), it's too late to start thinking about what can be done to recover. We need to know if a plan is in place to assure that our clients are prepared to handle a disaster if it occurs.



If yes, has the plan been tested recently? Some clients have disaster recovery plans that are many years old, and are no longer applicable to current conditions. Disaster recovery plans should be tested on a periodic basis to assure they are still adequate to the task.

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, (561) 682-1638, or at www.rsmmcgladrey.com/privateclubs.*