STEVEN ALEXANDER

the importance of securing workstations

Steven is a programmer for Merced College. He manages the college's intrusion detection system.

alexander.s@mccd.edu

SECURING WORKSTATIONS IS AS important as securing servers. Even so, the security of workstations is often ignored, because servers are individually more important.

Eyes on the Prize

Most of the attention given to computer security by system and network administrators focuses on servers and network devices. Allocating the bulk of a network administrator's resources to these systems makes sense, since a failure or security breach in one of them has the furthest-reaching consequences. Some recent privacy laws (such as SB 1386 in California) require the disclosure of security breaches where personal information may have been disclosed. Such laws are likely to reinforce the focus on server security. It is important, however, to implement and maintain comparable security measures for workstations.

Much of the attention given to PC security has focused on viruses, worms, and spyware, since such malware can affect productivity. Unfortunately, too many organizations fail to consider the other threats to PC systems and the consequences of a successful security breach by a person, rather than by a random automated attack.

Some of the most lucrative targets for data thieves are large database servers, but workstations also contain valuable information (including passwords for servers). It is important to note that not all workstations (or servers) are created equal. It may only be necessary to implement minimal security measures in a computer lab at a college or university—provided, of course, that the lab machines are kept separate from the rest of the network. The machines in a computer lab have little information that is of value to an attacker. Of course, an attacker can still use the machines to launch other attacks, trade pirated software, or snoop on a student checking his email. On the other hand, a workstation belonging to someone in the human resources or payroll departments might be a worthwhile prize by itself. Such systems often contain an abundant amount of valuable information which, if compromised, might lead to an embarrassing public disclosure with financial consequences.

Employees in different areas of an organization might have many sorts of valuable information on their workstations, including payroll and tax information, company financial data, strategic and planning information, confidential memos, and more. To make matters worse, access to this data is harder—if not impossible—to audit than is access to a centralized database server. Encouraging employees to store as little as possible on their own workstations might have a small positive effect, but such efforts can be obstructed by real-world needs, as well as by the fact that an attacker is likely to gain access to the same centralized resources as the owner of a compromised machine.

IT departments can also pose a major risk. Not only do programmers and other IT employees often have valuable data on their machines, their other duties often introduce extra security risks. It is not unusual for IT staff to run a wide variety of applications, test out new third-party software of various sorts, and test internally produced software. This software, particularly if it is a networked application, can be a security risk. In larger IT departments, the job responsibilities of individual employees might be well separated (though not necessarily), but in small departments employees are often required to take on responsibilities that might properly belong to several different positions. Part of this problem can be alleviated by using separate machines to test software, but too often this is not an option.

The security of an individual workstation is unlikely to be as important as the security of many of the servers in an organization. The security of all workstations together, however, might be as important as the security of all servers. While an individual server can hold more data, breaking into a workstation is often easier and may provide a larger reward for the effort expended. It may also be used as a foothold to a larger system.

Building Secure Systems

It is essential to secure new machines and to put management and patching procedures into place before giving the machines to employees or connecting them to the network. The folks at the San Diego Supercomputing Center have done some admirable work in this area. Abe Singer's "Life Without Firewalls" discusses this work and is required reading.[1]

All new systems should be fully patched, and automated patching should be set up. Windows Automatic Update can be useful, but many administrators (particularly in larger organizations) would do well to use Microsoft's SUS (Software Update Services) or SMS (Systems Management Server). Antivirus software should be installed on all Windows machines; it is less of a concern for other platforms. Anti-spyware tools should be used as well.

Additional security measures must also be put into place on each workstation. Unnecessary services should be turned off, default accounts should be disabled or the passwords changed, etc. Most of the "best practices" applied to servers apply to workstations. The Center for Internet Security has published useful guides for Linux, FreeBSD, Solaris, Windows, and other systems.[2]

Open source systems should use buffer overflow protection. Many books and articles about security say little, if anything, about this. They should! The amount of protection used depends on the requirements of the system and on considerations such as performance. Compiler patches such as StackGuard and ProPolice/SSP provide good protection with a minor performance impact. The addition of OS-level protection such as PaX and W^X provides much better security but at a higher performance cost. The SmashGuard Web site has information about several buffer overflow protection mechanisms.[3] Information about W^X is available from the OpenBSD site.[4]

The NSA has produced guidelines for Windows 2000 and XP.[5] The recommendations are somewhat restrictive, so most administrators would do best to study the NSA and CIS suggestions and then develop their own policy. Pay attention to network logon rights, terminal services access, and remote registry access even if host firewalls are used. Windows administrators should also study the new features available in Windows XP Service Pack 2. The Windows XP firewall is not very flexible but is adequate for many networks and, if manageable, it should be used. Once a reference system has been constructed, new machines can be built using tools such as Ghost or Altiris to clone them. Reference configurations can be maintained on UNIX using cfengine.

In most circumstances, users should not be given full administrative rights to their own machines. The more privileges a user has, the more likely that person is to use those privileges to circumvent security measures. What an administrator sees as necessary the user may see as irksome. If users must be given local administrative rights (more common in academic than business environments), measures can be taken to restrict certain prohibited software (such as Kazaa or edonkey). There are a number of ways this can be accomplished; for instance, software can be restricted directly using MS Group Policy and indirectly by preventing network traffic using firewalls. Tools such as Altiris can be used to inventory the software installed on workstations throughout the organization.

Data loss is important to consider. It can come about through an intelligent attack or by simple hardware failure. Network storage can be used to mitigate this problem. Each user should have his or her own folder on the network, which can be used as a repository for important documents and data. The user folders should be backed up regularly.

Network Security

Firewalls have taken a beating at the hands of several security experts in the past few years. One of the major reasons is that many people (technical folks as well as managers) think that firewalls are a cure-all; instead, because of the way they are used, they become a palliative. Many people think it is okay to put a firewall on the border of a network, ignore everything on the inside, pat themselves on the back, and announce, “We’re secure. We have a firewall.” Shame on them! May they find themselves in the company of a BOFH and an empty tape safe.

Firewalls do not (and never will) block out all of the bad traffic while allowing well-intentioned, legitimate users to access the network. Firewalls can be used to restrict the types of traffic that are allowed through, though, thus narrowing the window of vulnerability. By enforcing certain restrictions, firewalls require attackers to have a greater degree of skill or luck in order to launch a successful attack. Often, as is the case for much of what I discuss here, the firewall is a router with packet-filtering capabilities.

Firewalls should be used at the border of a network to prevent or hinder reconnaissance and to prevent access to services and machines that should not be accessed from outside the network (such as internal DNS and FTP servers). Most (but not all) ICMP traffic should be blocked, thus preventing a lot of reconnaissance activities. Unfortunately, blocking all ICMP breaks things. For instance, many administrators have caused problems by blocking the “fragmentation needed” ICMP packets that are required by Path MTU Discovery.[6] Certain services that must be accessible to the outside should be placed on a screened subnet so that a compromise of one of them poses less of a threat to the rest of the network.

Critical divisions within the network should be separated from each other. Departments should be logically separated and traffic between them controlled. Whenever possible, a user should be unable to use his or her workstation to access workstations of users in other departments. If collaboration is required between departments, shared storage should be set up on a server that members of both departments can access.

Separation can be achieved in a number of ways. VLANs can be used but have a number of issues.[7] Firewalls are more flexible but can be difficult to configure correctly. The problem with firewalls is that IP addresses are unauthenticated. Just because an incoming IP address matches the one used by Debbie Sipiyae in Accounting doesn't mean that the packet wasn't generated by Joe Student in the computer lab. Vulnerability to IP spoofing can be mitigated by using ingress and egress filtering. This filtering should be used at the network border and between segments within the network. This won't prevent all address spoofing, of course; a user in Accounting will still be able to spoof the address of someone else in Accounting, but he shouldn't be able to use an IP address that belongs to Marketing, HR, or IT.

System administrators may need to access workstations throughout the organization. If possible, this access should be restricted to certain administrative workstations and servers rather than allowing all IT personnel to have this network access. Because administrators require such open network access, system administrators (and possibly support staff) should be placed on a different network segment from other IT staff (such as programmers), who do not need unfettered access to the rest of the network.

When a workstation is compromised, the accounts of the users who use that workstation are usually compromised as well. Furthermore, access to one system on a network is often used to gain access to others systems and accounts. These risks are greatly reduced by not using plaintext passwords and by using solid password encryption. Abe Singer wrote a *;login:* article about eliminating plaintext passwords,[8] and I talked about password encryption in another *;login:* article.[9] Many system administrators still seem to believe that sniffing is difficult or impossible on switched (as opposed to hub) networks, but this is not so.[10]

Conclusion

The importance of information does not vary according to the machine the information resides on. A file containing names and social security numbers is just as valuable whether it is stored on a highly secure file server or a Windows PC. Owing to the fact that administrators do not know in advance what information will be used or stored by each of the users of an organization, the security of each user's machine should be as strong as possible.

REFERENCES

1. Abe Singer, "Life Without Firewalls," *;login:*, vol. 28, no. 6, December 2003, pp. 34–41. See also Singer's "Tempting Fate" in this issue.

2. Center for Internet Security, *http://www.cisecurity.org/*.

3. SmashGuard, *http://www.smashguard.org/*.

4. OpenBSD, *http://www.openbsd.org/papers/*.

5. NSA Information Assurance, *http://www.nsa.gov/ia/*.

6. Richard van den Berg and Phil Dibowitz, "Over-Zealous Security Administrators Are Breaking the Internet," *Proceedings of the 16th Systems Administration Conference (LISA '02)*, November 2002, *http://www.usenix.org/publications/library/proceedings/lisa02/tech/vanderberg.html*.

7. Rik Farrow, "Network Defense: VLAN Insecurity," March 2003, *http://www.spirit.com/Network/net0103.html*.

8. Abe Singer, "No Plaintext Passwords," *;login:*, vol. 26, no. 7 (November 2001), pp. 83–91.

9. Steven Alexander, "Password Protection for Modern Operating Systems," *;login:*, vol. 29, no. 3 (June 2004), pp. 23–33.

10. Dug Song, "dsniff," *http://monkey.org/~dugsong/dsniff/*.