Running Head: NETWORK SECURITY

Network Security: Methods and Practices

Jered McClure

Walden University

Network Security: Methods and Practices

A network is more than its component parts. It is built for the distribution and sharing of information for the betterment of the organization. As such, a key focus should be on securing the data contained on that network. Therefore, all systems should be patched and updated to the latest firmware/software at all times, antivirus should be installed locally on all machines, and a gateway filter should be implemented at the router to scan all packets for malicious intent. This will ensure the integrity of all information more than the security, but in a corporate environment, this is what is needed.

Other methods of securing the network are:

* A directory services structure, such as LDAP or AD, in order to secure all user accounts and workstations.
* Group policy scripts which automate network security rights every time a user boots up a workstation or logs in to their machine.
* White hat scanner services that allow system administrators to check for security flaws on the network.
* Staff training to understand malicious intrusion through social engineering so as to avoid network breeches from staff giving out sensitive information.

While each of these methods are a step in the right direction, they are not always the catch all, in and of themselves. A directory structure is only as good as the administrators that maintain it, and only as secure as the password to the administrator’s account. Too many people with access to the administration of the directory can lead to serious security gaps.

Similarly, group policy scripts are only so good as long as they are run on a regular basis. If the system in question is compromised, an intruder can generally bypass any group policies which should have kept them out. An internal scanner service is only as good as the software it runs on. Additionally, if a network is compromised and the intruder gains access to the scanner service, half their work is done for them.

Finally, staff training is only as good as the trainers. If the instructors who give the courses do not understand the problems and issues which cause a network to become vulnerable, how are they themselves supposed to explain it to people who do not know an IP address from a post box. Post training, a culture must be maintained by managers across the organization, as well. Otherwise, staff will simply ignore what they were taught and continue with their work as usual.

Reference

Dhillon, G. (2007). *Principles of Information Systems Security: Text and Cases.* John Wiley & Sons, Inc.

Meyers, M. (2009). *CompTIA Netowrk+ Guide to Managing and Troubleshooting Networks* (2nd ed.). McGraw-Hill.