Minimal steps required to secure a Local Area Network

By: Richard A. Bassett, Asst. Professor – Western CT State University

---

A local area network (LAN) supplies networking capability to a group of computers and related devices that share a common communications link and can share the resources of one or more processors or servers within a small geographic area (for example, within an office building, a school, or a home). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users or thousands of users.

Most LANs connect workstations and personal computers; these systems are also known as network nodes. Each node in a LAN has its own CPU in which it can execute programs or access data and devices anywhere on the LAN. LANs give users the ability to share expensive devices, such as laser printers, as well as access to critical data. Users can also use the LAN to communicate with each other, through a corporate Intranet, by sending e-mail or engaging in chat sessions. LANs are especially useful for sharing files, providing access to printers and access to the Internet.

The diversity of users needs, software applications, hardware profiles and access to the Internet all create significant complexities and challenges to the System and Network Administrators who are charged with the responsibility of ensuring the availability and proper functioning of LANs to their user communities. The following are the areas which LAN Administrators should evaluate when considering which steps to take in securing their local area network:

- **Access Controls** should be defined for and assigned to specific data files, utilities, resources and other system privileges.

- **Auditing & Logging facilities** should always be turned on for auditing and should never be turned off for any reason. Auditing your LAN will enable you to enforce policies and standards associated with the use of software as well as to ensure that any security standards required for the LAN are not being compromised or circumvented.

- **Backup and recovery** of databases in the mainframe environment is mostly an automated process. Backup and recovery standards for mainframe environments have evolved over a number of years and now follow generally accepted standards. The standards for backup and recovery are not as clear cut in the LAN environment. A file server backup regime should exist with backup tapes being securely stored and off site copies of backup tapes maintained.

- **Data Confidentiality:** Data entered at a workstation attached to a LAN is typically transmitted in clear text over the network. Any user on the network is able to use a "sniffer" program to view and capture data transmitted over the LAN. The security policy for an organization needs to define the acceptable use of sniffer programs.

- **Dial-Up Security:** When implementing dial-up software products on your LAN, consider products that offer security features such as password protection for dial-up users, host screen protection, keyboard options (e.g., disable input from the host or remote keyboard), callback, call logging, and session record and playback functions. Also look for forced timeouts when inactivity occurs for extended periods of time.

- **Documentation:** LAN security controls must be adequately documented to allow for effective security and use of the network. The documentation should cover the security features built into each component of the network and how the components interact with each other.

- **Firewall deployed behind the server:** This is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

- **Guest Accounts:** Guest Account is an account set up to provide individuals with temporary and restricted access to the LAN. The administrator should evaluate the security needs of the network and determine whether to install the GUEST account and, if so, what rights temporary users may exercise and what information they can access. No obsolete user accounts should exist on a LAN, it is recommended that an employee's account be removed upon their termination.

- **Hardware Failure Recovery:** Redundancy is a technique, which enables the LAN administrator to provide for continuing service in case of failure of critical components. There are a number of techniques used to provide hardware redundancy, including: Disk Mirroring, Disk Duplexing, Drive Arrays and Hot Backup.

- **IDS deployed behind Server, but prior to the LAN:** An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

- **Inventory:** An up-to-date inventory of all hardware and software associated with the LAN, including software installed on individual workstations should be maintained.

- **Media Protection:** It is quite easy to damage diskettes, tape cartridges, and other magnetic media, or to lose the data stored on such media. Users should be instructed on the proper use, care and storage of magnetic media.

- **Network Management/Protection Controls:** Network management controls include resource accountability, errors and omissions, reporting malfunctions, and preventive maintenance. Some of the questions included in this section may also appear in other sections.

- **Patches & Fixes:** Software publishers are constantly tweaking their products to combats the constant and evolving onslaught of security threats. A patch is a general-

purpose fix that is an entirely new executable module that replaces the old one. In the contexts of LAN security patches can be applied to Operating Systems, Browsers, Email Software, Switches, Routers or System Boards for the purposes of closing up holes that intruders can use to violate LANs.

- **Power Protection:** The LAN servers, routers and switches should have uninterruptible power supply protection installed.

- **Physical Security:** Physical security of the LAN, including the server and workstations, is critical to the security of the LAN, but is often overlooked. It is important that access to critical system components (such as the server) is restricted to a small number of individuals (usually the administrator and his/her backup.) Other considerations should include protection of equipment against theft, fire, and electrical hazards. Put servers and important equipment in a secure location wherever possible. Keep important network equipment (such as servers, routers, hubs, and switches) in a secure, locked room that only trusted personnel can access.

- **Recovery Planning Considerations:** Since many businesses and users now rely on LANs to conduct their business, it is imperative that LAN owners plan for emergencies, contingencies, and disasters. A well thought out plan which is maintained and tested on a regular basis can go a long way in conducting "business as usual" following any kind of contingency.

- **Security Administration:** Assigning administration responsibilities for the LAN is absolutely necessary in order to maintain LAN security. The responsibility for the administration of the LAN, including security administration, should be assigned to an knowledgeable individual. The administrator should be aware of his/her responsibilities vis-à-vis administration of the LAN as well as the security and integrity of the data and information stored and processed on the LAN.

- **Security Policy:** The LAN security policy is the total set of security rules enforced by the network. The policy should be documented, and the documentation should be available to individuals with a need to know the policy. This should include the LAN administrator and his/her backup, the owner of the LAN, users of the LAN, Internal Audit and Computer Security Administration.

- **Server Security Considerations:** A LAN file server can be exposed to many risks, such as software and hardware crashes, theft, power failures, disk drive failures, circuitry failure, and memory or interface cards failure. S proper backup scheme is one of the foundations of an effective LAN management strategy. In addition to backup procedures, it is possible to increase the chances that a server will continue to function in case of a contingency. This can be accomplished by hardware redundancy (i.e., duplicating certain or all hardware elements.)

- **Transmission Backbone:** The LAN cabling should be secured against unauthorized access or tampering, especially when the cabling must traverse shared areas in office buildings. Every effort should be made to encrypt any LAN traffic that is sent in an unconnected wireless format.

- **User Identification and Authentication:** User identification and authentication is the ability to identify the user to the system and to confirm the claimed identity of the users. The user identifies him/herself to the system by entering a User/Logon ID, usually consisting of his/her name. The user's identity is authenticated when the user enters a valid password.

- **Use strong passwords:** Force users to use strong passwords (i.e., passwords that contain a mixture of different character types). Unfortunately, you can't set this policy from the User Manager Account Policy dialog box: You have to install the passfilt.dll file, which comes with SP3, on all your network domain controllers. Although you need to add this file only on the Primary Domain Controller (PDC) to implement strong passwords, I suggest you also add it on your Backup Domain Controllers (BDCs) in case NT needs to promote a BDC to be the PDC at some point.

- **Virus Protection:** Virus infections are becoming increasingly widespread. A virus infection may be at a minimum, an annoyance to the users of a personal computer. In a number of situations a virus may end up costing the user a lot of time through destruction of data or by preventing the user from being able to access the data stored on a hard drive. The file server should be regularly scanned for viruses and imported diskettes are virus checked before use.

- **Weak passwords** - Companies must teach employees how to employ good password practices as weak passwords can easily be cracked.. Password management presents one of the biggest problems when it comes to security. Users should take care to include both upper and lower case letters, numbers, and punctuation when permissible in their passwords. Ideally passwords should be six characters or more. Unique passwords should be used for each account. Most networks and applications can be set up to prompt users to change their passwords on a regular and prescheduled basis.

Conclusion

The functionality of LANs and the benefit that they serve to businesses have increased steadily in the past several years. The exposure to security risks in LANs has also increased with the increased dependence on them by their users.

Before the widespread deployment of shared high-speed Internet connections, when LANs were private systems, the risk of intrusion was considerably smaller. While adding tremendous value to LAN user, the Internet has also greatly contributed to the risk of being hacked by unauthorized outsiders. With the Internet has come the need for encrypting data, installing firewalls, maintaining system logs and intrusion detection systems to name just a few areas. Wireless networks are also contributing to the need for heightened security amongst LAN Administrators.

The simple file & print sharing days of LANs appear to be gone as the technology moves forward. The complexity in installing and maintaining secure LANs is also increasing with the technological innovations that the user community desires. LAN Administrators must stay apprised of current possible threats and continually update their skill set to combat these threats.