**Compliance Within the LAN Domain**

Users generally use their workstations to access other resources that are connected to an organization’s local area network (LAN). A LAN is a network that covers a small physical area, such as an office or building. Resources that are connected to a LAN are potentially available to users using workstations also connected to the LAN. Because LANs increase the number of potential users that can access any resource on the LAN, it becomes even more important to control access to resources and monitor LAN activity to ensure controls are doing their job.

Devices and Components Commonly Found in the LAN Domain :

**•Connection media**—This includes the adapters and wires (sometimes) that connect components together in the LAN Domain. Not all connection methods use wires. Wireless devices use radio waves to transmit data instead of wires. So, connection media includes wireless adapters.

**• Networking devices**—This includes the hardware devices, such as hubs, switches, and routers, that connect other devices and computers using connection media.

**• Server computers and services devices**—This includes the hardware that provides one or more services to users, such as server computers, printers, and network storage devices.

**• Networking services software**—This includes the software that provides connection and communication services for users and devices.

**Maximizing C-I-A**

Maximizing Confidentiality

Ensuring confidentiality in the LAN Domain is one of the simpler tasks. There are

basically four steps to ensuring only authorized users can see confidential data:

1. Identify confidential data.

2. Require positive identification for all access requests and define strict access controls for all confidential data identified in Step 1.

3. Use encryption to store all confidential data identified in Step 1.

4. Use encryption to transfer all confidential data identified in Step 1.

You should already be enforcing identification and access controls in the LAN Domain. The new controls involve using encryption. Encryption is the process of scrambling data in such a way that it is unreadable by unauthorized users but can be unscrambled by authorized users

to be readable again. Specifically, encryption takes cleartext data and turns it into ciphertext through the use of an algorithm and a key. Cleartext data is simply human-readable data. Ciphertext is the resulting unreadable output.

Maximizing Integrity

LAN nodes are just as susceptible to malicious software as any other computers. As LAN nodes become more powerful and based more on standard operating systems, they become

more attractive targets. A compromised LAN node can be just a starting point. Once an attacker gets a foothold in your network, it becomes far easier to compromise other parts of your infrastructure.

Malware is not the only integrity concern. Users can also violate data integrity. Users can be malicious or unaware of their actions. Either way, it is important to control changes to critical data. Good access controls should stop any data changes by unauthorized users. You

can also audit changes to critical data by authorized users. Audit data can provide valuable audit trails for later analysis. Good audit trails can help trace unauthorized changes back to

their source. Getting to the root of unauthorized changes should provide the input needed to modify or add controls to keep the damage from happening again.

Maximizing Availability

It is important to develop and maintain a comprehensive recovery plan to replace lost or damaged data. As you use LANs to store more information in central repositories, it becomes more important to ensure the data is available when users request it. A crucial part of your

security plan is creating secondary copies, or backups, of your data in case the primary copy is damaged or deleted. Because more users are sharing the same set of data, any loss affects a

larger portion of your organization.

Most backup and recovery solutions target networked computers. Don’t forget to include any network devices with valuable data in your backup and recovery plan. Some network devices store configuration settings and performance data. Backing up these devices can save valuable log and performance data and make reconfiguring a device after a failure much faster. In nearly all cases, it is faster to load backed-up configuration data than to re-

enter it manually. Make sure your backup plan includes any devices with data you’ll need if a device fails.

Another important aspect of availability is ensuring your users can access LAN resources in an acceptable time frame. If the network is too slow, users can’t get to their requested information and you are not supporting data availability. In some cases, this problem is just due to excessive network use or a lack of network capacity for normal use. In both cases, you

must examine the behavior and reduce the load on your network, increase its capacity, or both.

In other cases, a lack of availability results from an attack. Suppose your organization

sells automobile insurance. You attract new customers by offering to analyze their existing coverage and providing a competitive quote showing how your coverage saves them money. You depend on your database of coverage costs to generate the analysis report. You cannot

conduct business if you cannot access your database. In this case, an attacker that renders your network unusable effectively stops your ability to conduct business. The type of attack that denies access to a critical resource or service is called a denial of service (DoS) attack.

The best defense against DoS attacks is to aggressively enforce access controls and

monitor your network for unusual or excessive traffic. You’ll need to provide evidence that you’ve implemented both preventive and detective controls to combat DoS attacks.

Managing the Vulnerability of LAN Components

Attackers never stop exploring new ways to compromise information systems. You must constantly make efforts to stay ahead of the attackers. As soon as new attacks surface, most hardware and software developers make changes to their products to address the new attacks. Nearly every hardware and software vendor releases updates to address vulnerabilities in their products. You should establish procedures to ensure all components in the LAN Domain are up to date.

Operating System Patch Management :-

Because operating systems play such a crucial role in granting or denying access to resources, they are a prized target for attackers. If an attacker can compromise the operating system, many attacks are possible. To keep your operating system as secure as possible, you should acquire and install all security-related patches, updates, and service packs. All current

operating systems provide methods for automatically identifying, downloading, and installing updates.

Application Software Patch Management :-

Applications are also prime targets for attackers. Database management systems and document management systems commonly control access to critical data through application access controls. Attackers who compromise applications can often bypass these controls and compromise your data. Just as with your operating systems, you should

establish procedures to frequently identify any security updates and install those on your applications to keep your LAN Domain as secure as possible.