William Cox GSEC Practical Assignment V.1.2e
Submitted by William Lewis Cox

The Most Critical Security Issue

Introduction

We are bombarded daily with reports of varied security weaknesses in our network operating systems, routers, firewalls, and even our PDAs. It can be overwhelming at times and difficult to determine which issue has the highest priority. This practical seeks to suggest which security issue should be addressed before all others and upon which all others depend.

The 3 Aspects of Security

While data security is a very complex field with numerous components, there are three general aspects to any type of data security function for any type of organization or individual:

- Prevention
- Detection
- Recovery

Prevention involves the avoidance of intrusions and related damages, and generally includes the following elements:

- Hardware Protection
- File Protection
- Network Perimeter Protection

Detection involves having the systems in place to provide awareness of intrusions or attempts when they occur in order to reduce their impact. Detection includes the following elements:

- Alerts
- Auditing

Finally, *Recovery* involves having the ability to undo any damage caused by an intrusion and includes these elements:

- Data Backup
- System Software and Application Backup
- Hardware Backup

Overview of The 3 Security Aspects and Associated Elements

Aspect 1 - Prevention:

Element - Hardware Protection (physical security)

Hardware protection, commonly called "physical security", is of vital importance to provide a safeguard against internal security breaches. Denying physical access to servers and network infrastructure equipment is a strong first layer of defense against malicious insiders who would damage storage devices, appropriate unauthorized data, or corrupt data integrity. Additionally, it prevents non-malicious activity that can down equipment such as accidentally overturning equipment, or unplugging power cords.

A recent article on the Netsecurity web site highlights this issue:

> One of the weaknesses of Windows NT is that if you can gain physical access to the computer, you can gain access to the SAM or Security Access Manager file. Once you have the SAM file, any decent password cracker will go to town on it and give you a nice list of the available user names and passwords. To prevent this you must not allow access to the file. If you can't lock up the computer, lock the drive. If we are talking about a server, you obviously can't remove the hard drive, so you must prevent access to the information on the hard drive.[i]

While a serious security issue, hardware protection is not the most important issue to address first.

Element - File Protection (authentication, access control, anti-virus)

If a malicious user or application cannot access data on shared media, they cannot abuse it. By providing for authentication and access control and maintaining up-to-date anti-virus software, malicious activity by casual intruders can be curtailed. Authentication (verifying that the user is who they say they are and that they should be allowed network access) is typically handled by using unique ids and passwords for each user. Once the user is verified, access control determines what resources on the network they have access to and what type of access (read, write, etc.) they should have to those resources. More stringent authentication methods are available and are being developed, including tokens, biometrics, and even using the manner in which users type as an authentication method ("keystroke biometrics")[ii]. Also, methods to strengthen password authentication exist that force hard-to-guess passwords and require that they be changed on a scheduled basis.

Malicious code (viruses, trojans, worms) is one of the most visible security issues regarding file protection, which has generated the most press and has had the most obvious financial impact to corporations. According to the "2000 Computer Virus Prevalence Survey" conducted by ICSA (now TruSecure Corporation):

- The number of corporations infected by viruses has risen by 20% this year alone
- 99.67% of companies surveyed experienced at least one virus encounter during the survey period

- 51% claimed they had at least one "virus disaster" during the 12-month period before they were surveyed
- 80% said the "LoveLetter" virus was their most recent virus disaster
- The monthly rate of infection per 1000 PCs has been nearly doubling every year since 1996
- The reported damage estimate from the "LoveLetter" virus is as much as $10 Billion.
- The reported damage estimate from the "Melissa" virus was $385 Million
- Including hard and soft dollar figures, the true cost of virus disasters is between $100,000 and $1 Million per company [iii]

Unfortunately, creating viruses is not difficult even for inexperienced intruders. Macro capability in several widely used applications (Microsoft Word® and Excel® in particular) has made it extremely easy for the novice intruder to cause annoyance and sometimes real damage. Prime examples are the "Melissa" and the "LoveLetter" viruses which generated high volumes of email traffic by sending itself to recipients in the victim's email address book using easily created scripts.

The term "virus" is often used as a generic term for other maliciously coded applications such as trojans and worms. According to the McAfee Virus Dictionary, the following are proper definitions for each of these types of malicious code:

> Virus:
> A computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies or creates the files.
>
> Worm:
> Worms are parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread via IRC (Internet Relay Chat).
>
> Trojan:
> A Trojan horse program is a malicious program that pretends to be a benign application; a Trojan horse program purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but Trojan horse programs can be just as destructive. [iv]

While a serious security issue, file protection is not the most important issue in data security.

Element - Network Perimeter Protection (firewalling)

Another security element is that of implementing adequate firewalling techniques to protect private networks. Firewalls are often thought to be impenetrable, but without proper configuration do little more than provide a minor annoyance to a determined intruder. The purpose of a firewall is to allow authorized traffic in and out and block all other traffic. These differ from server authentication methods in that the authentication is connection-based rather than user-based. The firewall will typically look at IP addresses and associated ports to identify authorized sources and traffic types.

Network protection is provided through either a software or hardware firewall. A very good primer on firewall technology provided by Vicomsoft can be found at the following address: http://www.vicomsoft.com/index.html?page=http://www.vicomsoft.com/knowledge/reference/firewalls1.html*track=internal

Network perimeter protection, though critical, is not the most important issue to address first.

Aspect 2 - Detection:

Element – Alerts:

Even if care has been taken to provide protection through secured physical access, stringent authentication methods, updated anti-virus software, and properly configured firewalls, the possibility always exists that a way will be found to circumvent these protections. If that does happen, your next layer of defense is to be aware of it so you can react and minimize the damage.

Alerts can be provided through a variety of means, including pop-up messages, email notifications, and text paging. Numerous utilities exist and native abilities are available in network operating systems, anti-virus software, and firewalls to send alerts through any of these methods. Alerts can be triggered by failed or successful intrusion attempts (for example, administrative logon failures) or by the unusual state of a service or performance metric (i.e., is a service stopped that should be running, is CPU utilization above a standard threshold). Any of these events can indicate malicious activity as well as possible system problems.

Several intrusion detection systems (IDS) exist today that can identify unusual or suspect network activity and alert administrators, as well as in some cases take action automatically to stop the attack. Robert Graham explains intrusion detection methods in his FAQ section on RobertGraham.com:

> **network intrusion detection systems (NIDS)** monitors packets on the network wire and attempts to discover if a hacker/cracker is attempting to break into a system (or cause a denial of service attack). A typical example is a system that watches for large number of TCP connection requests (SYN) to many different ports on a target machine, thus discovering if someone is attempting a TCP port scan. A NIDS may run either on the target machine who watches its own traffic (usually integrated with the stack and services themselves), or on an independent machine promiscuously watching all network traffic (hub, router, probe). Note that a "network" IDS monitors many machines, whereas the others monitor only a single machine (the one they are installed on). [v]

Alert mechanisms are crucial, but are not the first issue administrators need to address.

Element - Audit

To further identify unusual activity, regular audits should be performed on each server, router, firewall, or other network device that supports event logging. It is important to ensure that logging is enabled and that the proper level of logging is activated as default logging tends to be minimal. An example of auditing is to use the Security logging of the NT event viewer to monitor activity of administrative ids to determine times and devices at which the id has been used. If this shows activity at a time or location when the administrator was not active, then it is likely an unauthorized user has compromised the id.

In addition, utilities that monitor file integrity are available to identify what data has been compromised. Once again, from RobertGraham.com:

> **System integrity verifiers (SIV)** monitors system files to find when a intruder changes them (thereby leaving behind a backdoor). The most famous of such systems is "Tripwire". A SIV may watch other components as well, such as the Windows registry and chron configuration, in order to find well known signatures. It may also detect when a normal user somehow acquires root/administrator level privleges. Many existing products in this area should be considered more "tools" than complete "systems": i.e. something like "Tripwire" detects changes in critical system components, but doesn't generate real-time alerts upon an intrusion. [v]

Auditing is important, but is not the issue requiring first attention.

Aspect 3 - Recovery

Element – Data Backup

The most important process in LAN management is to maintain complete, current, and verified readable backups of data on media separate from servers. This media can take the form of magnetic tape, optical disks, or disk drives on other servers. The media must be stored in a physically and environmentally secure location and protected from unauthorized access as securely as the original data. At minimum backup media should be stored in a fire *and* heatproof container on-site in a secured safe or locked room away from the servers. To truly guarantee availability of data in case of facility disaster such as fire or earthquake damage, media should be stored at a secure location off-site.

Data backup is critical because without a copy of the uncompromised data it can sometimes be impossible to recreate the data needed for the resumption of production and may result in devastating financial losses.

Depending upon time-sensitivity of the data, backups should be performed so that it is financially or logistically feasible to recreate lost data from the time of the last backup. This period of time can sometimes, though rarely, be as long as one week or in extreme cases may need to be real-time.

Data backup, the most important process in LAN management, is still not the first issue to address for ensuring data security.

Element - System Software and Application Backup

An item easily overlooked is ensuring that backups exist of the system software (network operating systems, router operating systems, etc.) and applications in addition to the data. Without these foundational pieces of the system, the data is unusable. In most cases these types of software can be repurchased or copied from another location, but the amount of time it may take to find and deliver the media may be unacceptable to the organization. The lost revenue may cause financial hardship and the company's image can also be damaged.

In addition to the base software, all tested and applied patches should be available as well. It would be advisable to store these items in a manner similar to data.

Again, system software and application backup is not the item to first address.

Element – Hardware Backup

Finally, data security and recovery plans need to ensure that spare hardware is available to replace damaged equipment. This includes servers, routers, and other infrastructure hardware that is essential to the organization's operations.

The most difficult aspect of this element is funding. It is often difficult to convince those who must pay for this equipment that it is indeed necessary. The cost of downtime must be determined to provide justification for having capital invested in equipment that will not be used on a regular basis. If immediate repair is not required, standard or enhanced warranty terms may be sufficient that can ensure repair will occur within the needed timeframe.

This element of data security, while important to ensure recovery from security intrusions and equipment failure, is still not the first and most critical issue to address.

The Most Critical Security Issue

Many security issues exist that must be addressed. All the items mentioned in this practical are important and should be addressed in any organization. However, it is vitally important that a framework exist within which issues are addressed and security updates are applied. The most critical security issue is not technological. It is a management issue. It is *procedure*.

Without procedure, it is impossible to verify that the technological issues are being addressed properly. Without procedure, security issues are likely to be handled in a random and unreliable manner. Without procedure, there is no consistent methodology that can be measured against generally accepted practices and improved as needed.

Applying well-known patches could have prevented many intrusions that have affected even large organizations. If procedures had existed at the affected organizations to research, evaluate, and apply patches on a regularly scheduled basis, these breaches would not have occurred. Unfortunately, an alarmingly high number of organizations do not have scheduled procedures in place to identify and apply security updates. The recent BIND DNS issue highlights this. Apparently many organizations responded due to media coverage, but even with that more than 10% of large companies had not corrected this well-known issue.[vi] It is likely that smaller organizations with fewer resources and less expertise are even more delinquent in having scheduled procedures to address this or any other security issue.

Procedures can ensure new risks are identified and protected against, but can also ensure that new system installations are created according to adequate security guidelines and are updated with current security patches at time of installation. By consistently configuring server security settings according to a documented checklist, a known level of security can be assured that can be evaluated and which prevents any particular server from being a weak point for intrusion efforts.

Procedure requires discipline. Most security procedures are mind-numbing exercises that most technologists would rather avoid in favor of the more exciting areas. However, these procedures are the underlying foundation for the maintenance of a secure environment. The best way to ensure these are performed in a consistent and timely manner is the assignment of responsibility for each activity to a staff member or group, and to conduct regular audits verifying the accomplishment of these responsibilities.

A schedule of procedures that should be followed at minimum by any organization is provided in Appendix A.

Conclusion

Without standardized processes and procedures in place, it is very difficult to get a handle on information security. Activity as simple yet extremely vital as anti-virus signature updates can be skipped without a set schedule and assigned responsibility. It must be a daily effort, and one for which responsibilities are clearly defined. The key to security is not application of one-time fixes, but consistent and diligent fine-tuning of systems to adapt to changing security threats.

Appendix A - Schedule of Minimum Security Procedures

Frequency	**Activity**	**Responsibility**
Daily	Anti-Virus Signature Update	*Name*
Daily	Audit Dial-In Log	*Name*
Daily	Audit Logon Activity for Admin Ids	*Name*
Daily	Data Backup	*Name*
Weekly	Audit Server Event Logs	*Name*
Weekly	Check for Application Patches/Updates	*Name*
Weekly	Check for Network Operating System Patches/Updates	*Name*
Weekly	Check for Router/Infrastructure Patches/Updates	*Name*
Weekly	Weekly Data Backup	*Name*
Monthly	Audit Backup Selection Lists	*Name*
Monthly	Change administrative passwords	*Name*
Monthly	Monthly Data Backup	*Name*

References:

[i] Williams, Jim. "The Importance of Physical Security." NetSecurity. URL: http://netsecurity.about.com/compute/netsecurity/library/weekly/aa020501b.htm (24 Apr. 2001)

[ii] Fontana, John. "Biometrics software aimed at improving Windows NT security." Network World Fusion. (21 Dec. 2000). URL: http://www.nwfusion.com (12 Apr. 2001)

[iii] Williams, Erik. "The Cost of Malicious Code." SANS Institute Information Security Reading Room. (21 Feb. 2001). URL: http://www.sans.org/infosecFAQ/malicious/cost_code.htm (14 Apr. 2001)

[iv] "Virus Glossary." McAfee.com. http://www.mcafee.com/anti-virus (05 May 2001)

[v] Graham, Robert. "FAQ – Network Intrusion Detection Systems." RobertGraham.com. URL: http://www.robertgraham.com/pubs/network-intrusion-detection.html#1.1 (10 May 2001)

[All rights reserved. This document may be reproduced only for non-commercial purposes. All reproductions must contain this exact copyright notice. Reproductions must not contain alterations except by permision.]

[vi] Joris Evers, IDG News Service, "Study - Many Still Lax On Securing DNS", ComputerWorld.com, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58302,00.html