Global Information Assurance Certification Paper

Implementing a Defense In-Depth Strategy in a Non-Profit Organization

GIAC Security Leadership Certificate (GSLC)
Practical Assignment
Version 1.0

Steven K. Troester
Submitted February 5, 2004

Abstract
Many organizations use a firewall as their main (or only) network defense, placed at the perimeter, between their private local network and the public Internet. This is an appropriate first step, but most network perimeters have become very porous and a firewall cannot protect against all the holes in the perimeter.

What holes in the perimeter, you might ask? Think of all the entry points to your network that may or may not go through your firewall. Wireless access points and remote access of many varieties including dial-in clients, VPN clients, and PDA clients. Do you have mobile machines that often connect to your network but sometimes connect to other networks? Each of these types of clients have two subcategories, those managed by the IT department and those that are not.

Layering multiple defenses in addition to a firewall is the strategy of "Defense in-depth" and can provide much better protection for the information assets of an organization. Properly implemented, it can fill many of the holes in the network perimeter. Another advantage of defense in-depth is protection against a "zero day attack", where the vulnerability is exploited before it is widely reported to the rest of the community. While it is difficult to construct a single defense against an unknown attack, a defense in-depth approach can offer significant protection.

This paper will discuss how the strategy of defense in-depth was successfully implemented in a medium sized non-profit organization.

Selection Criteria
According to the CERT Coordination Center, information security incidents have been steadily increasing almost every year since 1988. Beginning in 1999 the number of incidents started to increase by greater than 100%. The CERT statistics also demonstrate a continued increase in vulnerabilities over the same period of time. In a report titled Overview of Attack Trends, CERT identifies the following "trends that affect the ability of organizations (and individuals) to use the Internet safely."[1]

- Automation; speed of attack tools
- Increasing sophistication of attack tools
- Faster discovery of vulnerabilities
- Increasing permeability of firewalls
- Increasingly asymmetric threat
- Increasing threat from infrastructure attacks

This data clearly demonstrates that all organizations using information technology must develop an information security strategy to protect their information assets in order to maintain the financial viability of the organization.

[1] CERT, http://www.cert.org/archive/pdf/attack_trends.pdf, p.1

Although our organization was performing some Internet e-commerce, confidentiality was the main concern in a CIA (confidentiality, integrity, availability) analysis followed by integrity. The “crown jewels” of the organization consists of a large database of contributors that include personal and financial information. A breach of our data could release confidential information that may harm our contributors, our own organization, our reputation, and our future success.

Discussion

Many small business and home networks are built with very little thought to network security. Network equipment and high bandwidth Internet access costs have decreased to the point where most small businesses and home users can easily afford them. Some business networks and most home users have a single layer of security, client side virus protection. If they have any perimeter defense, it is usually only a firewall. When I arrived as CIO at this organization in late 1999 I found an existing medium sized network infrastructure with very little security including:

- No perimeter defenses (firewall)
- No host based or perimeter virus protection
- The entire network accessible to the Internet, including all ports on all desktop computer systems, servers, and network devices
- Client virus protection individually managed with no assurance of scheduled virus definition updates
- Single collision domain, which allows any internal connection to collect all network traffic and “sniff” for sensitive information
- All users with full administrative rights to install any software on a desktop computer
- No detection of network events

The strategy of “defense in-depth” was deployed to mitigate these deficiencies. The following are defenses that were added or strengthened as part of our strategy.

Virus defenses

Not many people today will argue that client-side virus protection is necessary. The question remains, is it enough? In a business with 300 desktop computers using individually managed virus protection, how can the IT department be assured that each computer is running virus protection software and that its virus definition file is the most current? What is the effect on network bandwidth when 300 clients attempt to download an updated definition file from an Internet site? Shouldn’t file servers and email gateways also have protection?

In 1999 our organization had unmanaged client-side virus protection, with no protection on the servers or email gateway. The existing virus software was replaced with a centrally managed suite of virus protection products for servers,

clients and email gateways. One server is designated as the virus definition "master". This server is scheduled to check the vendor's site for definition file updates once an hour. If an update is available, the server downloads the file and makes it available to the desktop computers which then automatically update their own copies of the file. Our IT staff can configure, monitor, maintain, and deploy clients remotely and easily through a web-based management tool.

Firewall

A properly configured firewall is considered by most to be the first step in a network security strategy; however this organization had yet to take that step. Our firewall implementation used the "principle of least privilege", meaning all traffic was initially turned off (default deny), and only if it was identified as necessary for business reasons was it allowed. All Internet accessible machines were placed in the DMZ (web server, email gateway, external DNS, etc.) and access between the DMZ and the internal network was restricted to source and destination IP addresses.

Network infrastructure

Our buildings entire network infrastructure was one collision domain using antiquated 10BaseT hubs. From a security perspective, this situation would allow any internal network connection to easily gather all the network traffic in the building, and sift through it gaining access to sensitive information.

We implemented a complete upgrade of the network using high performance, remotely manageable switches. Each port was individually switched with desktops receiving 100 Mb ports and servers receiving 1 Gb ports. All ports in unused offices and common areas were turned off. Conference room ports were restricted to specific MAC addresses.

Physical security

The physical security in this organization had been well planned. There are limited entry points into building. During normal business hours these entry points are monitored by receptionists as well as being video recorded around the clock. All doors are electronically locked with all access attempts recorded and time stamped.

Hardening Systems

Patch management on a handful of servers can be managed by a system administrator in a manual effort, but add 300 (or more) desktop computers and you have an immediate need for automation. We implemented a server based management tool that could deploy Windows service packs and security updates to our entire desktop population in a single effort. Any software deployment could be scheduled during off business hours using Wake on LAN.

New servers were deployed to increase performance and to allow for separation of services. All unnecessary services were disabled across all servers.

Secure Desktop Policy

In a corporate environment, allowing non-IT staff to have full administrative privileges on their desktop computers is usually a mistake. Granting 300 users these privileges can create a nightmare! Who knows what each user is downloading and installing on their systems (intentionally or not). The CIO of our organization created a policy that was supported by upper level management removing administrative privileges from all users other than IT staff. This reduced Help Desk calls, allowed IT staff to verify accurate licensing of all software products, and provided assurance that only approved applications were installed throughout the organization.

IT Staff with security duties

If no one in an organization is made responsible for daily security tasks, then security will always be secondary to every emergency or high priority item that occurs. If an organization is going to take security seriously, it will be made part (or all) of someone's responsibilities.

Our organization designated two IT staff to be responsible for daily security tasks. These tasks included monitoring firewall and server logs, receiving alerts from automated monitoring software, and vulnerability alerts from external sources. Our CIO also monitored vulnerability alerts from external organizations such as CERT, SANS, and the major vendors used in our operation. The CIO and the two security staff scheduled the installation of updates or patches based on the severity of the risk to the organization.

Vulnerability scanning

How do you know that your systems are patched against the latest known vulnerabilities without scanning? Have you ever thought you had fixed a problem, only to have it reoccur? These are the simple reasons for periodic vulnerability scanning.

Our organization implemented an automated tool to scan all Windows servers and client computers to assess their level of vulnerability, and to deploy the required patches. In addition, we used tools from multiple vendors to double check our servers and to assess our non-Windows based servers and network devices. It is important to note that most organizations will want to restrict the number of tools they use, so that IT staff can become proficient in their use, rather than allow the tools to go unused and become "shelfware".

Wireless LAN

The use of wireless network access (WiFi or 802.11a/b/g) is being demanded by many users in most businesses. If the IT department doesn't supply and support a central infrastructure, those users will do it in isolation without a single thought to security.

Security was planned as part of our initial wireless deployment in 2000. Steps taken to secure our implementation included turning off the broadcast of SSID, enabling 128 bit WEP encryption, and restricting access points to a known set of MAC Addresses.

We understand that none of these steps will make the wireless network completely secure. Given that, we are investigating the additional steps of using RADIUS authentication at the access points and moving the access points into the DMZ. Implementation of these strategies would then require the use of a VPN client to access the internal network.

Security awareness training

Sometimes the user can be the weakest link in the security chain. Security awareness training can help strengthen that weak link. A variety of topics should be covered in this training including:

- Choosing a strong password
- Keeping your password secure
- Using different passwords for different levels of security
- Social engineering techniques used by those with malicious intent
- How to handle strange email

Users should always be alerted to current vulnerabilities and threats with instructions of how they should react.

Applicability

According to anti-virus vendor Sophos, the SoBig virus, Blaster worm, and Nachi worm ranked numbers 1, 2 and 3 on their list of top ten viruses for 2003. Together these three malware totaled 43.4% of all virus reports submitted to Sophos in 2003. All were launched in August of 2003.

Hundreds of thousands of computers were affected worldwide including high profile companies such as the U.S. Federal Reserve Bank in Atlanta, the Maryland Motor Vehicle Administration and government offices in Hong Kong. The large university in our city was one of the organizations hit hard by these outbreaks with over 2500 computers affected. Its IT staff spent weeks recovering.

Because our organization had implemented a strategy of defense in-depth, we were untouched by either the SoBig virus or the various RPC worms. Our IT staff members were able to monitor the external activity while continuing their daily duties without one lost hour of productivity.

References

SANS Institute, Course Material from “Track 12 – Security Leadership for Managers”, 2003.

SANS Reading Room Documents, URL: http://rr.sans.org/index.php , (January 30, 2004).

CERT Coordination Center, “CERT/CC Statistics 1988-2002”, URL: http://www.cert.org/stats/cert_stats.html , (January 30, 2004).

CERT Coordination Center, “Overview of Attack Trends”, URL: http://www.cert.org/archive/pdf/attack_trends.pdf , (February 20, 2002).

Sophos Plc,” Sobig-F wins 2003 war of the worms”, URL: http://www.sophos.com/pressoffice/pressrel/uk/20031203yeartopten.html , (December 3, 2003)

Discovery Channel, “New Web Worm Promises 'Time Bomb'”, URL: http://dsc.discovery.com/news/afp/20030811/webworm.html , (August 13, 2003).