

Project:	Document:	Date:
CIL	White Paper	05/10/2000
Security Audit & Its Importance in E-Business		Author: Srinivas

SECURITY AUDIT & ITS IMPORTANCE IN E-BUSINESS

A BACKGROUND....	2
INTERNET SECURITY POLICY:	3
HOW SECURE IS YOUR ORGANIZATION?	3
WHY DO U NEED A SECURITY AUDIT?	4
SECURITY AUDIT FROM CYBERMATEINFOTEK™	6



Cybermate Infotek Limited

11, Sripuri Colony, Kakaguda, Secunderabad 500 015, A.P. INDIA

Tel: +91-40-55326447/8

Fax: +91-40-55486446

URL: www.cybermateinfotek.com

Electronic Business and communication over the Internet offer tremendous market potential in today's highly interlinked world. The Internet is an ideal channel for electronic businesses offering an inexpensive, flexible, and efficient way for entities to trade and communicate with each other. For an organization to succeed in this new economy the level of security is crucial in this very large but albeit a dangerous network. This document focuses on Security auditing as a first step in the process to ensure that your guard is up round-the-clock and you are always one-up on those unscrupulous elements lurking in the dark corners of the web.

We at CybermateInfotek™ believe "No system can ever be error proof - therefore systems have to be designed that are failure proof!" as said by Dr. Dennis L. Meadows, Club of Rome and provide necessary Security awareness to your business and help design your system to be failure/error proof.

A Background....

In 1960 Department of Defence, USA in association with Bell Labs designed Arpanet to communicate within themselves. The Communication used to take place in packets. After a decade as the traffic over this has increased in leaps and bounds the packets were incorporated into communication protocols, which is now called as Internet. Internet is just a huge collection of networks spanning the whole globe.

Over the Internet the information that is transmitted passes through numerous systems before it reaches

the intended destination. As the Internet was never designed for security and due to its open architecture there will always be unscrupulous people on the look out to intercept, tamper and replace the data. As the global village is increasingly moving towards E-Business, the level of security of your system determines your organizational success, as half of the Internet users are corporate entities. Internet security has become so vital that now companies have started appointing Security Managers to look after their systems and applications just like they do to safeguard their physical assets.

Internet, which is interconnection of networks, runs on protocols that are determined by W3c. A protocol is a set of rules for communication. The basic protocol used in Internet is TCP/IP, which was formulated in 1969.

TCP - Transmission Control Protocol establishes a connection between two computers and provides reliable end-to-end communication and packet acknowledgement.

IP - Internet Protocol performs addressing, routing, forwarding and packet management

UDP - User Datagram protocol is used primarily for broadcasting information that need not be acknowledged.

Other protocols include NETBEUI, NETBIOS and IPX/SPX etc.

Internet Security Policy:

As the Internet offers various benefits in terms of increased access to information, in volumes of business it has, security plays a vital role as internet connectivity is volatile for sites with low standards/levels of

security which if ignored can prove disastrous for an organization. Inherent problems with TCP/IP, complexity of host configuration, vulnerabilities in software development process make the site more open to intruders/hackers *.

To overcome this W3C has formulated an Internet Security policy that helps the organizations to protect themselves from these intruders.

The Internet security policy is divided into two parts

- 1) General policy, which sets the tone for the overall approach of the organization
- 2) Specific rules which is an equivalent of a system specific policy

These rules define what is to be allowed and what is not to be allowed.

Policy Types:

Computer Security Policy means different things to different people. For senior managers it means to design a computer security program, establish and assign responsibilities. For middle level managers it can mean decisions regarding security and privacy of data. For low-level personnel it can mean security rules for systems. Internet security policies are classified into three types basically

Program policy: Sets organizational objectives for security and assign resources for implementation.

Issue specific policy: For specific issues of concern of the organization

System specific policy: This policy focuses decisions taken by the organization for protecting a system.

How Secure is your Organization?

When you provide service to users/customers over the net you expose your organization to unscrupulous people. An organizations success depends on how secure are they to these attacks. How secure is your business from these people depends on the following:

Web Servers:

A web server is a program that uses the client/server model and HTTP to retrieve web pages to the Internet users. Every organization that has a web site on the Internet has a web server program. Most popular web servers are Microsoft Internet Information server, Apache web server etc. how secured are these determines the security for your organization.

Firewalls:

Firewall is an approach to security. It acts like a mirror between the user and your organization protecting your data from the users misusing it.

**For More Information on Internet security policy please visit: <http://www.w3c.org/>*

Firewall system is a router, a personal computer, a host, set up specifically to shield a site or subnet from protocols and services. The main purpose of a firewall system is to control access to or from a protected site/network, implementing security policy by evaluating it. A firewall system is usually located at a higher-level gateway, such as a site's connection to the Internet

Application Servers:

Application servers act as an interface between the database, data and the client. In a 3-tier structure they form the middle tier and the business logic is embedded into this.. As the Internet Revolution increased the concept of web application servers increased because of high scalability and reliability required. Application servers are more exposed to intruders /hackers and hence securing application servers is vital.

File Transfer Protocol:

File transfer protocol is a method of transferring files over the Internet between two or more computers.

Operating Systems:

Operating systems act as interface between the system and the user. They manage your file structure.

Databases:

A database can be defined as a collection of related data in a pre defined form. A database management system is a computerized record-keeping system that stores, maintains and provides access to information. A database has a three-tire architecture. Data in a database is stored in the form of entities and attributes. Databases are available on any machine, from small micros to large

mainframes, and can be single or multi-user.

Type of Database Systems:

Centralized Data systems:

This type of database stores the data in a single location. They are basically single user database systems.

Distributed Database Systems:

A Distributed Database systems can be defined as consisting of a collection of data with different parts spread across locations. All the computers are interconnected through a network and each system operates under autonomous processing capability serving local requirements.

A database forms the backbone for an organization as it stores the information related to that organization. As today's world is moving into mainly distributed database from centralized database systems. Securing your database is just securing your organization.

The basic architecture of the database makes it available to the knowledge-based intruders.

Why do u need a Security Audit?

Today, most businesses are connected to the Internet, and have taken appropriate actions to protect themselves from attack by hackers outside the network, by using firewall products and other security measures. Yet this addresses only a portion of a vast majority of problems that affect your information technology (IT) infrastructure.

According to various reports your IT is far more likely to be attacked or compromised by sources inside your firewall. Your internal IT can be at risk, even if you have all the right technology, if your company's security policy and procedures are poorly implemented or outdated

A few software vulnerabilities account for the majority of successful attacks because attackers are opportunistic – taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, by scanning the Internet for vulnerable systems.

The information security community is meeting this problem head on by identifying the most critical Internet security problem areas – the clusters of vulnerabilities that system administrators need to eliminate immediately.

Bind Weakness:

Berkeley Internet Name Domain is the widely used Domain Name Service (DNS). This helps in locating a system without knowing its IP address. According a survey conducted by an independent organization in 1999 about 50 % of all the DNS are using vulnerable BIND versions making it open to Intruders/Hackers. In a typical Bind attack Hackers/Intruders erase

Unauthorized users to gain administrator privileges.

Sendmail buffer overflow weaknesses, pipe attacks and

the system logs, and installs tools to gain administrative access to the site. Mostly Systems running on Unix and Linux were affected

Vulnerable CGI Programs and Application Extensions Installed on Web Servers:

Most of the web servers interact with Web pages using CGI interface for data collection and verification. Many CGI programmers fail to consider how their programmers may be misused or subverted. Vulnerable CGI programs provide intruders to easily locate and operate with the privileges of the Web Server. Intruders vandalize a the web pages, steal credit card numbers and set up back doors to future hacking.

RPC Weaknesses:

Remote procedure calls allow programs on computer to execute on the other computers. There is compelling evidence that the vast majority of the Distributed Denial of Service (DDoS) attacks launched during 1999 and early 2000 were executed by systems that had been victimized because they had the RPC vulnerabilities. Mostly Linux and Unix based systems are affected.

RDS Security Hole In Microsoft IIS:

Many of the sites use Microsoft Internet Information Server as the web server and are deployed on WindowsNT and Windows2000 servers. Programming flaws in Remote Data Services are being employed

MIMEbo, that allow immediate root compromise:

Most of the Unix or Linux based systems use Send Mail Program to transmit electronic mail that has

several flaws making it vulnerable to intruders.

Sadmind and Mountd:

Sadmind offers remote administration access to Solaris systems with a graphical access to system administrative functions. Mountd controls and arbitrates access to NFS mounts on UNIX hosts. Buffer overflows in these applications can be exploited allowing attackers to gain control with root access.

Global file sharing and inappropriate information sharing via Net BIOS and Windows NT ports or UNIX NFS exports or Macintosh Web sharing or Apple Share ports:

File sharing ports on these systems when misconfigured give critical access to file system or full access to the file system

When file sharing is enabled on Windows machines they become vulnerable to both information theft and certain types of quick-moving viruses.

The same Net BIOS mechanisms that permit Windows File Sharing may also be used to enumerate sensitive system information from NT systems

User IDs, especially root/administrator with no passwords or weak passwords:

IMAP and POP buffer overflow vulnerabilities or incorrect configuration:

IMAP and POP are popular remote access mail protocols, allowing users to access their e-mail accounts from internal and external networks. The "open access" nature of these services

makes them especially vulnerable to exploitation because openings are frequently left in firewalls to allow for external e-mail access. Mostly Linux and Unix systems are affected.

Default SNMP community strings set to 'public' and 'private':

The Simple Network Management Protocol (SNMP) is widely used by network administrators to monitor and administer all types of network-connected devices ranging from routers to printers to computers. Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely

Security Audit from Cybermate Infotek™

Security audits provide you with the information on what services are made available by your network. Even the best-secured systems need to be evaluated for effectiveness and efficiency. These audits detect and alert you about the potential loopholes in your network by performing various scans and vulnerability tests.

A security audit is classified into two categories:

External Audit:

Security audit done remotely "off-site" from the outside of the fire walled environment. This is done to determine the extent of risk of an external attack. This audit performs all the port scans and vulnerability tests, hacking of web servers, application servers, subnets etc.. Subject to legal terms and conditions and limited disclosure.

Internal Audit:

Security audit done from the site of the fire walled environment. This is done to determine the extent of risk of an external attack. This audit performs all the port scans and vulnerability tests. The whole internal audit program is compliance with the audit checklist and have course the organization's information security policies

Types of Audit :

Basic Audit:

A basic audit performs port scans of TCP port of 2000 ports ranging from 0-1999. It also checks for the vulnerability identification of Firewalls, routers.

An External basic audit takes anywhere from 1-24 hours and an Internal basic audit takes anywhere from 1 - 12 hours.

Standard Audit:

A standard audit comprises of basic audit and port scans of TCP port from 2000 - 12000. A standard audit also performs 1000 vulnerability test on FTP, Application servers, Web servers.

Advanced Audit:

An Advanced audit comprises of Standard audit and port scan of TCP ports from 12001 to 65356 ports, all the UDP ports and 3000 vulnerability test on FTP, Application servers, web servers, Database servers including CGI.

Corporate Audit:

A corporate audit comprises of Advanced audit and 4030 vulnerability

test and Ethical hacking subject to Legal terms and conditions.

Ethical Hacking:

Ethical hacks are custom, hand crafted attacks on your sites, servers, databases upon your request. This is a specialized service to tangibly demonstrate system vulnerabilities.

No client information will be kept online or offline by Cybermate Infotek Limited or any employee or sub-contractors after the contract. All data will be returned to the client or destroyed