2006

Securing Networks of Information Age

Bilge Karabacak
Franklin University, bilge.karabacak@franklin.edu

Mert Uneri

Securing Networks of Information Age

Mert UNERI, *

Bilge KARABACAK **

* Chief Researcher, National Research Institute of Electronics and Cryptology (UEKAE) – Scientific and Technical Research Council of Turkey (TUBITAK)

** Senior Researcher, National Research Institute of Electronics and Cryptology (UEKAE) – Scientific and Technical Research Council of Turkey (TUBITAK)

Abstract

Internet and IT devices are being used for business and entertainment more frequently. Internet has been becoming a vital part of social fabric. Threats to Internet and other complex commercial networks are solid and growing. Globalization and the need for interoperability complicates security of IT Networks and Internet. Cyber threats have an important potential damage capacity. Proactive security methodologies are needed to protect valuable information.

According to the situation described above, the purpose of this paper is to examine the current trends in network security, and to propose a roadmap for protecting information from cyber threats. The roadmap consists of the following phases:

Analysis phase

- Risk analysis of the network and assets,

Design phase

- Establishing the security policy,
- Designing the network using security-tested products with proper configurations.
- Establishing a proper perimeter protection structure, securing operating systems, application software and protocols.
- The usage of the proper crypto devices with the proper key management systems in WANs,
- Reviewing the design with system security concepts in mind (hacker view)

Operation phase

- Monitoring and logging the network,
- Establishing a CERT team,
- Performing periodic system security tests and audits.

Securing Networks of Information Age

1. INTRODUCTION

As of 2003, the Internet connected an estimated more than 100 million computers in more than 200 countries on every continent. The Internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways, including gateways, routers, dial-up connections, and Internet service providers. The Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries or time of day.

However, along with the convenience and easy access to information come new risks. Among them are the risks that valuable information will be lost, stolen, corrupted, or misused and that the computer systems will be corrupted. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home, and may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. They can create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

Today, information technologies have been used widely at almost every commercial, official and educational organization. Most of the organizations today are connected to Internet, which is the largest wide area network composed of a number of computers, routers, servers, ISPs, gateways etc. Everyday, new information technology products have been produced for all type of businesses and offered to the use of people and organizations.

Among these information technology products, security tools have an important place. This is so because, even two computers, which are connected to each other, expose new security risks. The largest wide area network, Internet, is the most dangerous network. A computer virus may spread all over world via Internet infrastructure and cost billions of dollars.

The website of the SANS institute, which is the most powerful security institute of USA, was hacked in 2001. The security breaches like this show us that, it is not an easy task to make networks and products secure in the complete life cycle. Network protocols, operating systems and applications are called software in general. Software produced by vendors and people definitely contains coding and configuration errors. This is unavoidable because of the human nature. These coding and configuration errors are

revealed by skilful people and coders, called hackers. After revelation of the errors, crackers exploit these errors. The motivation behind this exploitation may be fame, financial benefit or mostly just enjoyment. Even when absolute secure coding and configuration is performed, intentional threats, natural disasters like fires will be always in agenda. At this scenario, it should be said that, absolute security is an impossible thing to perform.

Because there is no absolute security, there is always a risk that affects the information system. The purpose should not be to eliminate this risk. Risk elimination is impossible because of financial and technical difficulties. There is no technology that eliminates the risk in an information system. It will not be a rational approach to apply a more expensive countermeasure than the cost of asset just in order to eliminate the risk of the asset.

It is more than a realistic approach to live with the risk rather than try to eliminate it. In order to achieve this, a tool is required, which makes comparisons, interpretations, calculations. A sample comparison is between the cost of countermeasure and the cost of asset itself. If the cost of countermeasure is more than the cost of damage comes to the asset, there is no need to apply countermeasure. Risk management is the tool that makes all these comparisons, calculations, interpretations.

The impossibility of absolute security and ubiquitous risk eliminates to see the security as a result. Today, security of information technologies is the real time risk management process. Briefly, security is not a technology concept but it is a business concept. Risk management is the core of this concept and it is the main decision point for the selection and development of security measures.

2. RISK ANALYSIS OF THE NETWORK AND ASSETS

Five important concepts are commonly used in the context of risk management. These concepts are asset, vulnerability, threat, countermeasure and risk. Asset is everything that has a value and that needs to be protected. Hardware, software, data, staff and policy and procedures are all assets. Vulnerabilities are errors and weaknesses in assets. For example, vulnerability in software may be caused by coding errors or configuration errors. All assets types may have vulnerabilities. Vulnerabilities are the main reason for the risk. Threats are the factors that exploit the vulnerabilities in assets and give damage to systems. Basically, there are three types of threats, which are intentional, unintentional and natural threats. Threats are the potentials that have the possibility of giving damage to at least one of the confidentiality, integrity and availability mechanisms. Countermeasures are precautions to minimize the damage that comes from the threats. So, countermeasures decrease the level of risk as a result. To do this, a countermeasure may decrease the value of an asset, the level of vulnerability or the damage potential of threat.

Four factors, namely assets, vulnerabilities, threats and countermeasures, determine the level of risk in an information system. Risk analysis process mainly deals with these four factors. The constructed risk model in the risk analysis process manipulates these factors and estimates the risk.

Risk is the probability of the exploitation of vulnerability in an asset by a threat. Because risk is a probability, risk analysis process is not a well-defined task. There are many uncertainties that risk analysis have to deal with.

After the definitions of the basic concepts, it is more suitable to define the risk management process in depth. As said before, there is no technology and budget to eliminate the risk. That is why; there is always risk when we deal not only with information systems but with everything in our lives. But, the complete acceptance of risk without performing anything has certainly many damages. So, it is necessary to manage the risk by using risk management. Risk management is the mechanism that estimates the risks and proposes the countermeasures basically. Estimated risk amount, cost of countermeasures and security requirements are three main inputs while suggesting the countermeasures.

Risk management is divided into two sub processes, which are risk analysis and risk mitigation processes. Risk analysis is the first process in which risk is estimated. Risk mitigation is the second process in which necessary risk controls are made according to the risk amount (estimated in risk analysis), cost and security requirements.

Risk analysis may be either quantitative or qualitative. Quantitative risk analysis methods use mathematical and statistical tools to represent risk. Qualitative risk analysis methods does not use any mathematics, instead risk is stated with the help of adjectives. Risk model is the heart of the risk analysis process. Risk model converts the information about

assets, vulnerabilities and threat into risk value. The only and most important outcome of the risk analysis process is the estimated risk obtained from risk model.

Risk mitigation process does not just decrease the risk. The basic action, which is performed inside the risk mitigation process, is the control of risks according to risk amount, cost and security requirements. The control of the risk may include the reduction of risk, the acceptance of risk, the transfer of risk and even the escalation of risk actions. If too many countermeasures are used, both cost and difficulties of using the information system increase. This requires the elimination of the some of the countermeasures. This is just an example of why escalation of risk is required sometimes.

Risk management process is not performed just once. Risk management is not a result. Risk analysis and risk management processes form a risk management cycle. Risk analysis process establishes the basis of a cost effective risk mitigation process. This cycle should continue periodically since information technologies have always been changing. That means, assets, vulnerabilities, threats have been changing. Moreover, more cost effective countermeasures may be produced. All these factors require performing risk management cycle periodically. The period of this cycle should be determined by the management of organization.

The dynamic structure of information age certainly affected risk management process. A number of information security risk analysis methods became obsolete because of the profound changes in information technologies. Revolutionary changes in information technologies have converted many risk analysis methods into inconsistent, long lasting and expensive instruments. Therefore, risk analysis methods should be adaptively modified or redesigned according to the changes in information technologies and today's needs. The tools and methods used in risk management processes of 1980s should different from today's tools, so that they meet the information security requirements of the organizations today.

The risk analysis methods that were designed for yesterday's simple information systems are complex in nature. Complicated mathematical and statistical instruments are the main components of these risk analysis tools. Thus, applying these complex risk analysis tools into today's complicated information technologies has become infeasible.

Because the success and continuity of organizations vastly depends on the availability of information technologies, the responsibility of protection of information technologies increased. In 1980s, the responsible staff for protection of information technologies was the head of computer systems department of organization. Today, the company managers are taking this responsibility. Thus, managers of organizations have to understand the risk analysis process that directly affects the protection of information technologies. Moreover, managers may desire to participate in risk analysis process. Yesterday's complex risk analysis methods are not in a structure that may allow the participation of managers.

As said previously, basically there are two types of risk analysis methods according to tools used inside them. Quantitative risk analysis methods use mathematical and statistical tools to represent risk. Qualitative risk analysis methods does not use any mathematics, instead risk is stated with the help of adjectives. Risk analysis methods that use intensive quantitative measures will not be suitable for information security risk analysis. On the contrary of the past decades, today's information systems have a complicated structure and their use is widespread. Therefore, intensive mathematical measures to model risk for complex environments will make process difficult. Calculations performed during the risk analysis process will be very complicated. Quantitative methods may not be able to model today's complex risk scenarios. Risk analysis methods which use qualitative measures are more suitable for today's complex risk environment of information systems. But, one important drawback for qualitative risk analysis methods is their nature that yields inconsistent results. Because qualitative methods does not use tools like mathematics and statistics to model the risk, the result of method is vastly depended on the ideas of people who conduct the risk analysis. There is a risk of giving subjective result while using qualitative risk analysis methods.

As two examples, TUAR is a quantitative tool which uses fault trees and fuzzy logic to express the risk. RaMEX is a qualitative tool which does not use any mathematical or statistical instruments.

Both qualitative and quantitative risk analysis methods may be supported by software. On the contrary of this, risk analysis methods which are executed without assistance of software are called paper based methods. There are a number of risk analysis methods that are supported by software. The risk analysis methods that are supported by software have some certain disadvantages. Firstly, the cost of method will be usually high. Secondly, the main frame of risk analysis process is drawn by software. Thus, some necessary variations during risk analysis process may not be achieved. Paper based risk analysis methods consist of meetings, discussions and working sheets. Paper based methods are more flexible than the methods supported by software. One important drawback for paper based method is their duration. Because of nature of meetings, paper based methods may take a long time to give the risk results.

The Buddy System and Cobra are the examples of risk analysis methods supported by software. The Buddy System is quantitative, Cobra is qualitative in contrary. European Security Forum is an example of paper based method.

Both quantitative and qualitative risk analysis methods may be supported by standards like Common Criteria Framework, ISO 17779 and the other ISO standards related with information technologies. These standards put forward robust and well-defined risk analysis methods. However, these methods require the participation of expert risk analysts because of complexity and formality of methods.

As an example, CRAMM is a quantitative, software-based risk analysis method that is compatible with standards.

By taking the today's information technology environment into consideration, risk analysis method should allow effective participation of manager and staff to the process. In today's technological environment, the risk analysis method for information systems should not contain complicated mathematical and statistical instruments. This will cause a long and complex process. Also, the risk analysis process should not contain pure qualitative measures. This may cause subjective results. The information security risk analysis of today should not extent the risk environment. This causes costly, long lasting and complicated risk analysis process. Also, the risk analysis may give inconsistent results. Risk analysis methods which do not have these properties may not meet the requirements of organizations. In today's situation, public opinion should not be disregarded while performing risk analysis. Public opinion may be obtained by conducting survey. Survey is composed of questions and answer choices related to the specific information security problem. Manager, directors, technical personal and ordinary staff may be the candidates for answering the survey questions. The profiles of survey participants may change according to the information security problem. The aim of the survey should be to understand the effect of information security problem on the system or the organization. In other words, conducting a survey is somewhat making an as-is analysis. The main advantage of survey will be the ease of use. In today's technological arena, risk analysis methods that contain complicated mathematics and statistics may give inconsistent results, take a long time and be costly. Because the qualitative risk analysis methods may give subjective results, these methods may require expert participation. For today's information systems, a quantitative method which does not contain complicated mathematical and statistical instruments is necessary. Therefore, manager and the staff may effectively participate in risk analysis process. A survey may satisfy this requirement. In a survey, simple mathematical weight values for questions and answer choices may be designated. After the conduction of survey, answer choices may be assesses according to their values.

The most important output of risk management is countermeasures. There are vast amount and type of countermeasures to decrease the risk to the desired level. Security patches, secure design of networks, secure configuration of systems, and software like firewall, hardware, technical training, crypto equipment, monitoring, policies and procedures are all examples of countermeasures.

In today technological environment, the most important countermeasures are operational countermeasures like policies and procedures. Security is not a technology concept but it is a business concept. Namely, ensuring and maintaining security is not a technological concern. It is more related with business than technology. Security maintenance is mostly succeeded by policies and procedures. Policies and procedures are not static documents. They always change and develop along with the technology. Risk management has an important support to policies and procedures during this continuous process. Risk management contributes to the policies and procedures during all the period of technology development. Therefore, it is not expected to see a mature and complete policies and procedures from an organization that does not perform risk management periodically. As said previously, security of information technologies is the real time risk

management process. Real time risk management ensures up-to-date policies and procedure.

3. THE SECURITY POLICY

A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues.

A security policy covers the following (among other topics appropriate to the organization):

- high-level description of the technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy
- risk analysis that identifies the site's assets, the threats that exist against those assets, and the costs of asset loss
- guidelines for system administrators on how to manage systems
- definition of acceptable use for users
- guidelines for reacting to a site compromise (e.g., how to deal with the media and law enforcement, and whether to trace the intruder or shutdown and rebuild the system)

The minimal set of documents that should exist in the security policy is:

1. Anti-virus and Worm Incidents policy
2. Password assessment policy
3. Backups policy
4. Incident Handling policy

Security policy protects both people and information. It sets the roots for expected behaviors by people, system administrators, management and security personnel. It authorizes security personnel to monitor, probe and investigate in ways that might be indistinguishable from a hacker were it not for the policy.

A security policy establishes what must be done to protect information stored on computers. A well-written policy contains sufficient definition of “what” to do so that the “how” can be identified and measured.

It is critical to write down in a clear manner what is expected of anyone in the organization when it comes to security. It is also helpful to inform people what is expected of them, what the organization is going to do and what others in various roles within the organization are going to do.

There are three types of policies. These are

1. Program policy: This high level policy sets the overall tone of the organization's security approach. It is usually brief, just long enough to establish direction. Typically guidance is provided with this policy to enact the other types of policies and define who is responsible. This policy may provide direction for compliance with industry standards from organizations such as ISO, as well as with the law and government regulations.
2. Issue specific policy: These policies are intended to address specific needs within an organization, such as password procedures and Internet usage guidelines.
3. System specific policy: For a given organization there may be several systems that perform different functions, and the use of one policy governing all of them may not be appropriate. It may be necessary to develop a policy directed toward each system specifically.

A policy typically includes the following titles:

1. Purpose: reason for the policy
2. Related Documents: lists any other documents that affect the contents of the policy
3. Background: provides information of the need of the policy
4. Scope: states the range of coverage for the policy (to whom and what does the policy apply)
5. Policy Statement: actual guiding principles or what is to be done.
6. Action: specifies what actions are necessary and when they are to be accomplished.
7. Responsibility: states who is responsible
8. Ownership: identifies who sponsors the policy and from whom it drives its authority, as well as defines who may change the policy.

Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users. Management assigns responsibility for security, provides training for security personnel, and allocates funds to security. Technological support for the security policy moves some responsibility for enforcement from individuals to technology. The result is an automatic and consistent enforcement of policies, such as those for access and authentication. Technical options that support policy include (but are not limited to)

- challenge/response systems for authentication
- auditing systems for accountability and event reconstruction
- encryption systems for the confidential storage and transmission of data
- network tools such as firewalls and proxy servers

There are many books and papers devoted to site security policies, including requests for comments RFC 1244 (6) and RFC 1281 (7), guidelines written by the Internet Engineering Task Force.

Security-Related Procedures

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring.

Security Practices

System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. Below are examples of commonly recommended practices:

- Ensure all accounts have a password and that the passwords are difficult to guess. A one-time password system is preferable.
- Use tools such as MD5 checksums (8), a strong cryptographic technique, to ensure the integrity of system software on a regular basis.
- Use secure programming techniques when writing software. These can be found at security-related sites on the World Wide Web.
- Be vigilant in network use and configuration, making changes as vulnerabilities become known.
- Regularly check with vendors for the latest available fixes and keep systems current with upgrades and patches.
- Regularly check on-line security archives, such as those maintained by incident response teams, for security alerts and technical advice.
- Audit systems and networks, and regularly check logs. Many sites that suffer computer security incidents report that insufficient audit data is collected, so detecting and tracing an intrusion is difficult.

Based on the risk management process results, the security policy is the key element in the design process which is covered in the next section.

4. DESIGN PHASE

Designing secure networks is the vital step for protecting valuable information. Designing a secure network is not only performed with technical measures but also with operational ones. A network is composed of hardware, software, data and people who use hardware and software and process data. Therefore design of secure systems should cover all these objects.

Design process can span the whole system, or just a small part of the system. So, the design does not necessarily cover the whole system. For example, one design process may suggest a completely new DMZ structure, new software, new hardware and training programs. On the other hand, another design process may suggest only the reconstruction of a firewall. One design process may deal only with people, and another with just operating systems.

Design is not made just once. Secure design of networks is a countermeasure that is suggested by risk management. Therefore, an information system is always needed to be redesigned periodically. The period of redesign is basically determined by risk management process.

With all these important points in mind, the countermeasures listed below should be considered at the design of secure networks:

- Using security tested products and boxes
- Using perimeter protection devices and constructing a DMZ
- Using crypto equipment and software
- Establishing policies and procedures
- Configuring securely operating systems and application
- Managing the network
- Establishing PKI

a. Using security tested products and boxes:

All of the software and hardware that are considered to be used at the network should be certified if possible. There are three nationally accepted test standards which are ITSEC, TCSEC and CTCSEC and one internationally accepted test standard which is Common Criteria. Common Criteria represents the outcome of efforts to develop criteria for evaluation of IT security. It is an alignment and development of a number of source criteria (ITSEC, TCSEC and CTCSEC). Common Criteria is an international initiative by the following organizations: DSD (Australia), CSE (Canada), SCSSI (France), BSI (Germany), CESG (UK), NIST and NSA (US).

b. Using perimeter protection devices and constructing a DMZ:

Perimeter devices are the most vital part for the security of a network, if the network is connected to another less secure network.

Perimeter devices control the flow of information between less secure outer network and inner network. It protects the information at production system of inner systems.

There are three types of perimeter devices: Firewalls, intrusion detection systems and content inspection devices.

c. Using crypto equipment and software

Crypto equipment and software directly concerns with information itself. Thus, at the information age, crypto equipment certainly has certainly an important place at the design process. Crypto equipment simply decreases the value of information by encrypting it. Crypto equipment can be used along with firewall and routers. So, all the data or desired data between inner and outer network can be encrypted. This is an example of WAN usage of crypto equipment. Apart from this, crypto software can be used inside a trusted network. Some examples of this situation is local drive encryption and file encryption.

d. Establishing policies and procedures

Policies and procedures are very essential operational countermeasures of the information age. Policies and procedures contain and organize all technical countermeasures and their usage.

e. Configuring securely operating systems and application

Operating systems and applications are the main processors of information. Therefore, a problem with operating systems and applications will definitely effect the information. Secure configuration of software is an important aspect, which should not be discarded during a design process. Almost all software comes with default settings that pose security risks. All operating systems and application should be hardened with the guidance of accepted step-by-step checklists.

f. Managing the network

Management of assets at the networks of information age is very important for the sake of security of information. Without management of networks, it will be a very burdening task to control the information. Management of the network includes patch management, configuration management, remote management, asset management and security management.

g. Establishing PKI

Public key infrastructure is an important countermeasure that provides an infrastructure to the certain security services. Four security mechanisms are ensured by using PKI. These are confidentiality, integrity, authentication and non-repudiation. All these services are important for the protection of information.

By considering all these countermeasures during possible design processes, protection needs of information can be satisfied.

At 1970s and up to early 1980s, computer-processing department was an important but completely independent entity in the organization. Few of the other organizational departments depended directly on the activities of the computer-processing department. So, any failure in computer operations had little effect on the organization. This era was computer-centric era.

After early 1980s until early 1990s, organization became more dependent on information technologies. During these years, computer-processing departments turned into IT departments. On the contrary of computer-processing departments, IT departments performed multi-tasking, real time and distributed processing. This era was information technology centric era.

After early 1990s up to today, we entered into another era, which is information centric era. We live more and more information depended day by day. In this era, effective utilization of information is the most vital task. Having the right information at the right time can make difference between profit and loss, success and failure in today's business environment.

Availability of information is a daunting task to perform. Availability is always inversely proportional to the security. Availability is an important information security mechanism along with confidentiality and integrity. It is imperative to supply availability of information especially at this age. So, availability of information should always be in mind at the design phase of networks and information systems, and while proposing the listed countermeasures like crypto devices, firewalls etc.

In the information age, both the security and the availability of information became vital for organizations. These two important and opposite concepts should be profoundly considered during design process.

With these goals in mind, the next step in the roadmap of securing network will be to operate the secure networks.

5. OPERATION PHASE

Three types of actions are necessary for a secure system in the operations phase: system penetration tests and audit, monitoring and logging the system, incident handling. These are explained in detail in the next sections.

System Penetration Tests and Audit Process

The tools available to launch an attack have become more effective, easier to use, and more accessible to people without an in-depth knowledge of computer systems. Often a sophisticated intruder embeds an attack procedure in a program and widely distributes it to the intruder community. Thus, people who have the desire but not the technical skill are able to break into systems. Indeed, there have been instances of intruders breaking into a UNIX system using a relatively sophisticated attack and then attempting to run DOS commands (commands that apply to an entirely different operating system).

Tools are available to examine programs for vulnerabilities even in the absence of source code. Though these tools can help system administrators identify problems, they also help intruders find new ways to break into systems.

As in many areas of computing, the tools used by intruders have become more automated, allowing intruders to gather information about thousands of Internet hosts quickly and with minimum effort. These tools can scan entire networks from a remote location and identify individual hosts with specific weaknesses. Intruders may catalog the information for later exploitation, share or trade with other intruders, or attack immediately. The increased availability and usability of scanning tools means that even technically naive, would-be intruders can find new sites and particular vulnerabilities.

Some tools automate multiphase attacks in which several small components are combined to achieve a particular end. For example, intruders can use a tool to mount a denial-of-service attack on a machine and spoof that machine's address to subvert the intended victim's machine. A second example is using a packet sniffer to get router or firewall passwords, logging in to the firewall to disable filters, then using a network file service to read data on an otherwise secure server.

The trend toward automation can be seen in the distribution of software packages containing a variety of tools to exploit vulnerabilities. These packages are often maintained by competent programmers and are distributed complete with version numbers and documentation.

A typical tool package might include the following:

- network scanner
- password cracking tool and large dictionaries
- packet sniffer
- variety of Trojan horse programs and libraries

- tools for selectively modifying system log files
- tools to conceal current activity
- tools for automatically modifying system configuration files
- tools for reporting bogus checksums

Penetration tests to the system can be performed with a typical tool package given above.

Audit is mainly a comparison tool. It compares the systems, networks and the objects that compose a system with previously defined security criteria. More generally, audit is essentially a measurement against a standard. The aim of audit is to protect the systems within the audit scope.

Auditing is closely related with policies and procedures and risk analysis. While auditing is measurement against a standard, assessing is generally going to be a risk analysis, and an assessment of how effective a policy is.

Audit is an essential process for the protection of information essentially at the information age. Audit should be performed periodically. Within these periods, systems can be audited separately or along with the risk analysis process. Audit and risk analysis processes help mature policies and procedures, which are imperative for protection of information at this age.

Like testing standards, there are also auditing standards, which are effectively used for systems. The most important of these standards is Cobit, which is a standard of ISACA. Cobit attempts to provide an IT oriented checklist for the overall control and management of an enterprise. FISCAM is another set of auditing standards with a very different goal. While COBIT focuses on best business practice and line of business accountability, FISCAM is focused on IT management and auditing in connection with financial auditing.

Monitoring and Logging the System

Continuous monitoring of network activity is required if a site is to maintain confidence in the security of its network and data resources. Network monitors may be installed at strategic locations to collect and examine information continuously that may indicate suspicious activity. It is possible to have automatic notifications alert system administrators when the monitor detects anomalous readings, such as a burst of activity that may indicate a denial-of-service attempt. Such notifications may use a variety of channels, including electronic mail and mobile paging. Sophisticated systems capable of reacting to questionable network activity may be implemented to disconnect and block suspect connections, limit or disable affected services, isolate affected systems, and collect evidence for subsequent analysis.

Tools to scan, monitor, and eradicate viruses can identify and destroy malicious programs that may have inadvertently been transmitted onto host systems. The damage potential of viruses ranges from mere annoyance (e.g., an unexpected "Happy Holidays" jingle

without further effect) to the obliteration of critical data resources. To ensure continued protection, the virus identification data on which such tools depend must be kept up to date. Most virus tool vendors provide subscription services or other distribution facilities to help customers keep up to date with the latest viral strains.

Incident Handling

Incident handling is the action or plan for dealing with intrusions. The best way to act on an incident is by having procedures that are well documented in place. Being able to rely on solid documentation will help in minimizing the chance that a crucial step in the process will be forgotten.

The five steps listed below can be used as a roadmap to incident handling.

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery

1. Preparation

When it comes to incident handling, planning is everything and preparation plays a vital role. It is very important to have a policy in place that covers the organization's approach to deal with an incident. The policy usually covers the following items:

1. If an incident occurs will the law enforcement officials be notified or will the company be silent?
2. If an incident happens will the company cleanup the effects of the incident or continue as nothing happened in order to catch the intruder?
3. Direction for intra organizations and other companies on that incident.

The people working in the incident handling team should be chosen such that

1. Smart and experienced
2. Team player
3. Can work in immense pressure

Training is critical for each member of the incident handling team.

Reaction time to an incident is absolutely critical. One way to minimize the reaction time is using *jump bags.* This bag should be easily accessible and should contain everything needed to respond an incident, contact numbers, checklists, network cables, hard drives, hubs and a PC with the necessary tools.

2. Identification

Possible signs of an incident are listed below:

- IDS Alert
- Unexplained entries in a log file
- Failed logon attempts
- System reboots
- Poor system performance

3. Containment

In containing an accident, the first thing to do is to secure the area, and then a backup should be made of all infected systems. Also passwords should be changed as soon as possible to make sure a compromised account could not be used for reentry into the system by a remote hacker.

4. Eradication

Before the system goes back online an incident handler must make sure that the problem is fixed and the vulnerability that the attacker used to compromise the system is closed. It is not enough to simply recover the system put it back online, the underlying security mechanisms of the affected systems must be altered, fixed or upgraded to accommodate any new vulnerabilities.

Once the system is recovered, it is a good idea to run a vulnerability scanner aainst the affected system to see if the problem is, indeed, fixed and no new holes are opened up in the process. There are a number of commercial products in the market such as NAI Cybercop and ISS Internet Scanner, but the open source tools like NESSUS, and SAINT should not be overlooked

5. Recovery

The key point to consider in the recovery phase is to ensure you are not restoring vulnerable code that has already proven itself to be exploitable by any number of attack methods. If you restore the system form tape backup, then you should be restoring a previos state which contained the vulnerability.

Before the system can be brought back into production, the incident handler needs to validate the system. Removing the vulnerability could have affected other functions of the system that are critical by the business.

There is always a possibility that a reinfection could occur. Therefore the system should be monitored closely for the first few hours of operation

6. CONCLUSION

Internet and applications running on Internet are growing fast so are the flaws or vulnerabilities of the tools. In this paper, In order to build a secure computer network (system) a roadmap is proposed. The roadmap consists of the following steps:

Analysis phase

- Risk analysis of the network and assets,

Design phase

- Establishing the security policy,
- Designing the network using security-tested products with proper configurations.
- Establishing a proper perimeter protection structure, securing operating systems, application software and protocols.
- The usage of the proper crypto devices with the proper key management systems in WANs,
- Reviewing the design with system security concepts in mind (hacker view)

Operation phase

- Monitoring and logging the network,
- Establishing a CERT team,
- Performing periodic system security tests and audits.

References

1. Jacobson, R.V.: CORA. Cost of Risk Analysis. Painless Risk Management for Small Systems, International Security Technology, Inc. (1996)

2. Owens, S.: Information Security Management: An Introduction, British Standards Institution (1998)

3. Bilbao, A.: TUAR. A Model of Risk Analysis in the Security Field", CH3119-5/92, IEEE (1992)

4. Kailey, M. P., Jarratt, P.: RAMeX: A Prototype Expert System for Computer Security Risk Analysis and Management, Computers & Security, Vol. 14, No. 5 (1995) 449-463

5. Gordon, J.: Security Modeling, Risk Analysis Methods and Tools, IEE Colloquium on (1992)

6. Spinellis, D., Kokolakis, S., Gritzalis, S.: Security Requirements, Risks and Recommendations for Small Enterprise and Home-Office Environments, Information Management & Computer Security, 7/3 (1999) 121-128

7. Security Risk Analysis and Management, A White Paper by: B. D. Jenkins, Countermeasures, INC., 1998

8. COBRA Consultant Products For Windows, An easy to use guide and evaluation aid, 2000

9. Business Risk Analysis: Establishing a Risk Analysis Method which is easy to understand and simple to apply. European Security Forum, from Coopers and Lybrand, Europe

10. Toval, A., Nicolas, J., Moros, B., Garcia, F.: Requirements Reuse for Improving Systems Security: A Practitioner's Approach, Requirements Engineering, 6 (2002) 205-219

11. United Kingdom Central Computer and Telecommunication Agency, CCTA Risk Analysis and Management Method, CRAMM User Guide, Issue 1.0, 1996

12. Gerber, M., Solms R.: From Risk Analysis to Security Requirements, Computers & Security, 20/8 (1999) 577-584

13. URN 76/702, The Business Manager's Guide to Information Security, Department of Trade and Industry, 1996

14. Hoelzer, D.: SANS Audit Track, Auditing Principles and Concepts, Version 1.1a, 2002

15. www.sans.org

16. www.securityfocus.com

17. www.commoncriteria.org

18. www.cert.org