Kim Freeman
Version# 10
SANS Security Essentials Network Security
Kfreema001

Network Security Survival

Kim Freeman

September 22, 2001

Computers and networks have changed the way people live, play, and work. It has become a very complex environment with change as the only constant. The computer environment has evolved rapidly, as has network security and IT responsibilities of its professionals. Network security has become increasingly complex creating many challenges in the attempt to keep intruders out. IT professionals realize that the network they support is never safe from intruders. One may ask how can an organization survive security threats with unrelenting changes taking place? One way to answer the difficult question is to review the past and present of network security.

In the past, the primary security concern was intruders physically breaking into facilities and stealing confidential information. Computer systems were huge machines behind locked doors, cameras, and guards. Someone would have to penetrate the building and security system to steal confidential information. Computers systems usually had one password and were located in a secure area. The workstations were "dumb" terminals. These "dumb" systems didn't allow users to locally store any information. Backups were made several times a day, and backup tapes were stored in a secure location both on and off the premises.

Computer hardware and software began to evolve, which brought on new challenges to the network security system. Users started having their own personal computers at their desk and home, which allowed them to store information locally. Operating systems began to standardize; the operating system they used during working hours was the same operating system they used at home. This newfound freedom presented an increase in vulnerability to networks, which had never been encountered. Confidential information could now leave the building, be printed by other systems. Users could take work home with them bringing about new security concerns.

New technology continues to compound security issues. Historically, IT professional were trained on mainframe systems. Their jobs had always been concerned with securing only the data and keeping the mainframe system running within the computer center. Now they were being forced to manage multiple personal computers. Network infrastructure began to make major changes. Wire was pulled to every station to allow access to the new server technology. Wiring closets were built to allow hubs and switches to be placed within them. Fiber optic cabling became the backbone of this new infrastructure. Routers were placed as gateways to the Internet. IT professional anxiety and stress level grew because they realized that once the organization is connected to a network and the internet, it is in no longer secure. Network security vulnerabilities multiplied with all demands of change.

Network security issues became a driving force of software vendors to provide products that would diminish the vulnerabilities of networks. Firewall, encryption, and anti-virus solutions became the improved resolution to secure the perimeter. At the same time when new and improved resolutions were being implemented, hackers' tools became more sophisticated. This meant that IT professionals had to learn to support, implement, and protect the new technology, and keep the old systems running until the overall conversion was completed. The circle of change never stops for IT professional. The only thing that is constant has become change.

At present, network security has grabbed the attention of practically every user. Security is viewed not only as a technology issue, but one that directly affects the ability to conduct business. Technology is evolving so rapidly that securing the perimeter becomes a constant pursuit to handle complex technical issues. As an organization grows, networks have to expand to support the growth. As this growth occurs, so do security risks. Society is demanding Internet connectivity with mobility. Building infrastructures are required to provide freedom and mobility to travel floor-to-floor or office-to-office with ease. Every wireless connection represents a possible vulnerability to unauthorized entry. These changes are complicated and demanding.

The World Wide Web is becoming an essential business communications tool. It supports intra- and inter-enterprise research, collaboration and accelerated business processes. The Web brings with it vulnerabilities to infection, intrusion, and tampering via files such as cookies or other active content, which can be downloaded, often without the user's knowledge. Each and every day hackers' tools become more sophisticated, and instances of network intrusion become more widespread. This issue is one of the main reasons why computer crime has risen to an all time high and is growing every year. Organizations must strengthen their security measures to reduce the risk of attacks.

The 2001 Computer Security Institute/FBI Computer Crime and Security Survey shows a dramatic increase in computer crimes and the resulting financial losses suffered by businesses. One hundred eighty-six respondents to the survey reported $377,828,700 in collective financial losses. Also, the FBI/CSI study (Computer Security Institute, 1999) indicates that nearly 70 per cent of break-ins are not reported because if crime is reported, businesses may find themselves rebuilding consumer confidence.

There are many things that can be done to lessen the likelihood of an attack. The key is to address and define the risks, and then do what you can to minimize them. The cost of safety measures, along with the cost of potential losses, requires us to take the approach of defense-in-depth. No single mechanism should be entrusted with the total responsibility for security. A layered system of defenses must be designed incorporating various barriers, including risk analysis, tools, policies, procedures, and training. These defenses should work together to make the intruder's job as hard as possible.

- **Risk Analysis –** Is determining the risks that the organization could encounter, figuring out how to reduce risk to an acceptable level, and taking prudent steps to avoid unnecessary risks that might damage the organization. Determining an acceptable level of risk is very important. Acceptable risk must be defined within the context of an organization and the legal environments in which they operate. Only when the risks are understood can they be minimized. Once the risks are measured for severity, countermeasures can then be developed. Hackers are not the only threat. Other factors such as unanticipated demand, natural disaster, equipment failure, and software bugs, etc., all add to the overall risk that key processes will not perform as expected.

  The best time for risk analysis is before you have been hit! Senior management plays a large part in when a comprehensive risk analysis is forced. Sometimes senior management doesn't understand the importance of risk analysis until there has been a hit. A meeting should be scheduled with IT professionals and senior management to determine the needs and scope of the risk analysis. There are several questions that need to be addressed:

  - What resources need to be protected?
  - What or who do they need to be protected from?
  - What is the cost of loss or compromise?
  - What is the cost of protection?
  - What is the likelihood of loss and compromise?
  - What is percentage of vulnerability? Is it acceptable?
  - What is the balance between risks and costs?

  Once the answers to these questions are determined, it is time to analyze appropriate countermeasures. Unfortunately, there is no proven, easy way to make decisions. Drawing conclusions on how countermeasures will help to secure the network is a good start. For example, what are the costs of the compromise, of protection, and of the probability of the compromise? How will having firewalls at each site, auditable analog lines, web surfing filters, special logins, and developing security policies and procedures help minimize intrusion? Considering all of these issues will assist in building a foundation while continuing to analyze the risk and forming the team's intuition to improve security.

- **Tools**

  - **Firewalls –** are devices that act as a buffer between a network and the Internet. They perform a critical function at the perimeter of an organization. They have four main categories:

    - **Packet filtering** is the most basic element of firewall technologies. This examines the header of each packet it encounters and decides whether to let that packet precede or stop. The IT professional determines this decision.
    - **Stateful Packet Inspection (SPI)** takes the concept of packet filtering to the next level. It uses packet filtering, and it keeps track of the larger context, or 'state,' of specific transmissions. By maintaining a table of current connections and their most recent events, it moves beyond the network layer.
    - **Application-level proxies** inspect packets at the application level. They essentially execute a stripped-down version of the application to determine whether the behavior of the packet is acceptable. The network session is broken between the host in the trusted network and the entrusted network. Both sides believe they are communicating with each other, but they are actually communicating with the proxy. This is very tight security and increases overhead cost.
    - **Circuit-level proxies (SOCKS)** are between the application-level proxy and the SPI. It works at the session layer and requires a special functionality to be added to each system. This process is known as socksification. It distributes the workload so the firewall will not have high overhead cost associated with application-level proxies.

    It is important to recognize the capabilities and weaknesses of firewalls. They can provide a degree of isolation by controlling the traffic on the network. One goal is, of course, to stay away from undesirable packets while not hampering the flow of acceptable network traffic.

- **Policies and Procedures**

  - IT security policies and procedures are the foundation, the guideline, and the bottom line of security within an organization. Developing basic security policies and procedures should be effective, realistic, and manageable to attain the security goal. Without security policies and procedures, the organization is exposed and unprotected. Policies and procedures establish protection for the users, data, systems, IT professional, and the organization. Listed below are security policy objectives:

    - To protect the organization's business information and any client or customer information by safeguarding its confidentiality, integrity and availability.
    - To establish safeguards to protect the organization's information resources from theft, abuse, misuse and any form of damage.
    - To establish responsibility and accountability for Information Security in the organization.
    - To encourage management and staff to maintain an appropriate level of awareness, knowledge and skill to allow them to minimize the occurrence and severity of Information Security incidents.
    - To ensure that the organization is able to continue it's commercial activities in the event of significant information security incidents.
    - To provide suitable coverage of International Standards ISO 1779 and BS 7700.
    - To force the staff to familiarize themselves with the organization's Information Security policies and the related responsibilities, which are critical to their job functions. They must understand the specific information security measures they are expected to observe if Information Security is to be effective.

- **Training**

Training is the most power weapon that can be used in securing a network. The best security administrator, the best intrusion detection software, the best policies and procedure and the best hardware are worthless if one user disregards or is not aware of security policies and procedures. The implication of this concept conveys the importance of developing an efficient, ongoing training program.

Initiating and developing a training program will take substantial effort by the IT professional. He or she will have to show strong leadership, patience, and be a good listener. A strong focus must be retained on educating employees on security concepts and issues by making all employees aware of the threats and safeguards.

Educating users and senior management will make enforcing policies and procedures easier. Senior management can make the training and implementation difficult to enforce, or they can make it effortless. To ensure that every effort is taken toward a smooth implementation of policies and procedures, IT professionals should start by meeting with senior management.

The first meeting with senior management should bring them up-to-date illustrating the changes, which have occurred over the last few years, and then show where the organization stands with security at the present time. At this time, briefly review security concerns and explain what Trojans, viruses, and worms are, and how they can affect the network and how time consuming they are to repair. Give examples of how intruders have harmed other organizations, and what they had to do to overcome the invasion. End the meeting with the importance of ongoing training. Hopefully, senior management will realize the importance of being proactive in security training.

With senior management support, the training process should include all staff, for example, senior management, middle management, staff, or any other user (guests, students, vendors, etc.). Each level should be handled differently by recognizing what the varying needs are. For instance, it may be necessary to over prepare for senior management because they will question every aspect of security and cost associated with it. Also, getting the users motivated to except the changes will help with the ongoing training. There are books that are short and to the point about handling change and keeping a good attitude. Who Stole My Cheese, written by Spencer Johnson, M.D., is a good example. One of the most important processes of the training is to help the user to understand why access may be taken away from them.

Understanding the past and the present will be helpful to defend against hackers and intruders in the future. Being aware of weaknesses, realizing training needs, accepting and enforcing security policies and procedures are steps that will help toward meeting the challenges in attending to secure a network. But to put it simply, the job of securing a network is quite difficult because networks are complicated, and there are too many variables in terms of hardware, firmware, operating systems, applications and networking, not to mention human behaviors, for anyone to prepare adequately for all possibilities. Also having insight that the inability to break into a computer system or penetrate a network doesn't prove it's safe from intruders, it only proves that it isn't vulnerable at that point in time to a specific set of attacks. More likely, it only proves that an intruder didn't try hard enough to break in. In fact, the only secure system is one that is switched off, and then; of course, it's not good to anyone. Understanding the task and having determination to tackle each and every situation will help to handle the obstacles of securing a network.

References:

1. **The Sans Institute**
Essential Security Actions:
Step By Step
http://www.sans.org/newlook/resources/esa.htm

2. **Microsoft Security**
Security Strategy
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/secstrat.asp

3. **Symantec**
Information Protection – Why Bother?
SEP 5, 2001 ARTICLE ID: 855
http://enterprisesecurity.symantec.com/article.cfm?articleid=855
The Importance of Layered Security
JUN 14, 2001 ARTICLE ID: 769
http://enterprisesecurity.symantec.com/article.cfm?articleid=769&PID=8405845
Internet Security Training for Employees
FEB 21, 2001 ARTICLE ID: 613
http://enterprisesecurity.symantec.com/article.cfm?articleid=613&PID=8405845
Information Protection-Why Bother?
September 5, 2001 Article ID: 855
http://enterprisesecurity.symantec.com/article.cfm?articleid=855
Securing the Perimeter, Part 1
http://enterprisesecurity.symantec.com/article.cfm?articleid=743&PID-na

4. **Computer Security Resource Center**
http://csrc.ncsl.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf

5. **SearchSecurity.com**
Http://searchsecurity.techtarget.com/originalContent/0,289142,sid 14_gci538854,00.html

6. Harold F. Tipton "Information Security Management." 1999

7. Computer Security Institute (1999) 1999 CSI/FBI Computer Crime and Security Survey. Computer Security Issues & Trends, Winter, Vol V, No. 1.