


Network Security: Problems and Solutions



MIS Topics
Dr. Wang
24 April 2012

Introduction

In today's society, people access networks in a variety of ways and for a variety of reasons. Many are concerned with the way their information is stored and whether or not it is secured from unauthorized access. With this concern in mind, companies must find the causes of security problems and ways to fix those problems. This in turn helps the company's information to be kept private and also the information of other users of the applications. Network security is important for network implementation and applications.

There are a few definitions that must be covered when dealing with the issue of securing networks. All of which combined together help to understand what to look for when finding and solving problems of any potential breaches. First security must be defined. Security can be defined as "the process of maintaining an acceptable level of perceived risk" (Bejtlich 4). In 1998, Dr. Mitch Kabay, a former director of education for the International Computer Security Association, "security is a process, not an end state" (Bejtlich 4). This meant that no organization can be completely secured. Security today is based on what is currently happening on the network and must be checked before one can say that the network is secured. If you were to be asked if the network is secured tomorrow, the best answer would be indefinite because one never knows what new breaches or holes will be found.

The security process

There are four steps involved in the security process: assessment, protection, detection, and response. Assessment is the leader of the process because it helps to prepare for the remaining three components. Assessment deals with any policies, procedures, laws, regulations, budgeting, and managerial duties including technical evaluation of one's security position. A failure to account for any of these can mess up the flow of other operations in the process. Next is protection. Protection is when countermeasures are applied to help limit the likelihood of compromising the network. Protect and prevention may both be used interchangeably. Detection come after protect/prevention in the process. Detection is when policy violations or computer security incidents are identified. The final step in this process is response (Bejtlich 5). "Response is the process of validating the fruits of detection and taking steps to remediate intrusions" (Bejtlich 6).

Causes of network security problems

Having an acceptable level of perceived risks was mentioned in defining what security is. Risks are simply the possibility of suffering from harm or a loss occurring (Bejtlich 6). Potential risks are present when you have assets or something of value. These assets can range from the company's data to the information collected from customers. This is all valuable information, which must be protected by securing the network. The risk equation helps us to begin looking at what causes security problems within a network.

“Risk = threat X vulnerability X asset value” (Bejtlich 6)

Threats are the main causes for network security issues. Information access threats “intercept or modify data on behalf of users who should not have access to that data” (Stallings 18). Service threats “exploit service flaws in computers to inhibit use by legitimate users” (Stallings 18). Both types of threats are extremely crucial to organizations.

There are several other forms of attack on network security. Some of the ones we will discuss are: viruses, “hoaxes,” back doors, and password crack. Viruses or worms attack software and can be introduced to an individual system or the entire network (Stallings 19). If introduced to the network, this becomes a problem of network security and the security process must be handled. Hoaxes are false virus reports, which contain real viruses. Some users are not aware that this is an actual virus and transmit them to other users on the network via email or other electronic mediums. Back doors are holes that are left during the development process. Some of these holes are not intentional while others are purposely left there are traps for coming users. Password cracks are quite common. They are codes used to break or crack user passwords (Whitman, Mattord, Austin, and Holden 24-25). “A cracking attack is a component of many dictionary attacks. It is used when a copy of the hash of the user's password is obtained and is used in search of a match. When a match is found, the password has been cracked” (Whitman, Mattord, Austin, and Holden 25). All of these methods of intrusion are among the most popular and common of attacking networks. An organization is not always able to predict when new attacks may enter the system; therefore, they must continually perform the security process to insure that breaches do not occur.

Prevention and solutions

Firewalls

There are several ways to protect a network from attacks. Without protecting the network, data would run rampant in the hands of the unauthorized. There are several softwares or programs that help with protecting the network. One of these ways is by using firewalls. A network firewall or firewall “is a device placed at the connection point for an internal network to control network traffic to and from the outside world” (Norton and Stockman 49). Firewalls are able to see each packet that comes through the network and has the ability to identify whether the packet stemmed from a trusted internal source or an un-trusted, external source (Norton and Stockman 49). When the correct amount of trust and un-trusted sources are identified, firewalls are the most effective. “The advantage of firewalls is that they can stop unauthorized network traffic from passing into or out of your network” (Norton and Stockman 50). Firewalls have the ability to prevent code crackers that use viruses from accomplishing their goal. “The disadvantage of firewalls is that they are not foolproof. Many Trojan horses can be configured to use ‘friendly’ ports” (Norton and Stockman 50). This is the same with hoaxes disguising themselves as helpers when they really are viruses. Firewalls are not always able to protect against this particular kind of attack, but are one layer of protection.

Firewalls go deeper than the standard norm. There are firewalls that filter packets that follow a particular set of rules that are set up by the user. This type of firewall uses low-level controls when determining which packets to let through. The down side to this is that they may be difficult to configure for maximum security of the packet (Norton and Stockman 52-53). Application proxy firewalls “don’t actually allow traffic directly between networks to which it’s connected. Instead, it accepts traffic from a particular client application on your internal network and then sets up a separate connection on the public network to the server” (Norton and Stockman 57).

Advantages: Specific control over connections, eliminating unnecessary services from your network by restricting outgoing requests, and capability of most proxy firewalls to log all connections.

Disadvantages: Must customize the user’s system to a certain extent, and some applications may not support proxy connections at all (Norton and Stockman 58).

All in all, firewalls allow you to determine how much incoming and outgoing access to allow. When combined with encryption, firewalls help to make the network more secure.

Cryptography

Cryptography is “the science and art of transforming messages to make them secure and immune to attacks” (Forouzan 9). Cryptography use to refer only to the encryption and decryption of messages that were using secret keys. Now It spans into symmetric-key encipherment, asymmetric-key encipherment, and hashing (Forouzan 9). Symmetric-key encipherment uses a secret key that is only known by the parties involved in the message. Asymmetric-key encipherment uses one public key and one private key between the parties. In this method, the sending party uses the private key to lock the message and the receiving party uses the public key (also contained in the sent message) to unlock the message without ever having to know the sender’s private key (Forouzan 9-10). Hashing creates a fixed length digest out of a variable length message (Forouzan 10).

Conclusion

There are many ways to breach a network. It is of key importance to always be testing the network to determine where possible breaches may occur. In accordance with testing, organizations should always have electronic ways to help in detecting system breaches. These electronic sources may be able to catch things the human eyes may have missed. However, the technology cannot always be completely trusted because they are still susceptible to breaches themselves. When organizations do not get comfortable in their network security measures, they have less of a chance of being under attack by malicious behavior.

Having the most advanced technology and experts on the team can help to prevent attacks on the system at all times. Remember, security is indeed a process. Security does not stop when one breach is found and fixed, continual searches must occur to insure no additional breaches are found.

We can all rest assured that our information is protected when we know companies are finding these holes before they occur. Even as consumers, if we suspect a possible problem in our information, it may be a hint to the company that they have a network problem.

Resources

- Bejtlich, Richard. *The Tao of Network Security Monitoring: Beyond Intrusion Detection*. Boston, MA: Pearson Education, Inc., 2005. 3-763. Print.
- Forouzan, Bejrouz A. *Cryptography and Network Security*. Boston: McGraw-Hill Companies, Inc., 2008. 1-685. Print.
- Norton, Peter, and Mike Stockman. *Peter Norton's Network Security Fundamentals*. Indianapolis: SAMS, 2000. 49-67. Print.
- Stallings, William. *Network Security Essentials: Applications and Standards*. 3rd. Upper Saddle River, J: Pearson Education, Inc., 2007. 7-315. Print.
- Whitman, Michael E., Herbert J. Mattord, Richard D. Austin, and Greg Holden. *Guide to Firewalls and Network Security: with Intrusion Detectin and VPNs*. 2nd. Boston, MA: Course Technology, 2009. 24-25. Print.