Global Information Assurance Certification Paper

Are Firewalls Enough?
Peter Giannoulis
September 11, 2000

Overview

How many times have you heard, "We already have a firewall, we're secure." Working in the consulting field for the last while I have heard that expression more times then I would like to admit. It's actual a scary thought if you think about it. At one time, some system administrators viewed firewalls as their only line of defense for network security. More and more system administrators are starting to realize that firewalls are only one of the many tools that they can use to defend their networks properly. Another issue to take into consideration is that most companies do not realize is that 90% of the attacks that are performed on the systems they try so hard to protect are the result of 'inside jobs.' So, what if your internal users are the ones causing all the grief? With this document I am going to examine a few of the tools and procedures we as IT Professionals can take in securing and monitoring our network systems.

First Line Of Defense

What is a firewall? A firewall is more or less a security host sitting in between you company's internal network and the Internet. Firewalls are typically a company's first line of defense against attacks that form from the outside. There are a few different types of firewalls on the market today. I will briefly discuss the two most popular. These include Packet Filtering and Proxy Servers. Both types of firewalls have different capabilities. Packet Filtering firewalls allow or deny traffic based on the IP address or source and destination ports. Proxy firewalls use proxies based on the specific application that needs to be used. For example, http, telnet, and ssl traffic will be checked at the firewall with the specific rules you apply for these applications. The type of firewall you chose to deploy in your organization will depend on your security profile.

Deploying a firewall is a necessary step in any organization. I have performed many firewall installations in large organizations that simply thought that they didn't need one. Here's an example of one case: One morning, the IT staff comes in and realizes that two production file servers have been taken off line for some apparent reason. These specific servers were sitting right on the Internet for everyone to see. After bringing the boxes back up, they realized that a lot of data had been erased. Now, you may think, well that's okay, I have backups. Well, backups are great to recover your information, but the thing many company's overlook is that the data stolen could be confidential company data that could be used against them. In this case, it wasn't. The moral of the story is that if you are going to connect your company to the Internet, you need to deploy security tools for the proper protection and monitoring of your network. A firewall is just the beginning.

Intrusion Detection

Have you ever thought of what might happen if an intruder somehow bypassed your firewall and you didn't have the proper monitoring tools in place? Can you imagine the damage that can and will be done if you are not prepared? A skilled hacker could get through certain firewalls without you noticing. Deploying intrusion detection tools at the perimeter of your network is just as important as deploying a firewall. You must couple these two technologies together at network boundaries. If a hacker happened to penetrate your firewall and gain access to you network, wouldn't you like to know? Using these tools will give you the capability of performing real-time monitoring, which can send off an alert to the proper authorities. This will allow you to take the appropriate actions you need to take to protect your valuable data. If you wanted to go an extra step further you would probably want to deploy a firewall with intrusion detection tools between most departments in your organization. The benefit of doing this is that all accounting, sales, and/or management data is protected from prying eyes. This leads me into my next topic.

The Insider Attack

"Hackers and crackers aren't the only threats to your enterprise's valuable data." According to *InformationWeek's* recent Global Security Survey (http://www.informationweek.com/743/security.htm). In a recent survey conducted, 41% of the IT Managers claimed that most of their security problems were caused as a direct result of their employees. That is a significantly large number. Let's think about that for a second. 41%. What can be done to prevent this? What exactly are the employees doing that could cause a vulnerability in the organizations network? Are the employees purposely or accidentally doing this? The answer to those questions lie in the tools and procedures you take.

One of the things I like to stress to all companies that I have dealt with is end-user training. This is a very important

measure to take. We do not have to be reminded that our end-users have access to some or all of the company's data. Accidents do happen, over and over and over again. In order for us to eliminate the chance of accident, we must put aside the time and investment in our employees training. Simple training programs that will properly train the end-user on the operating systems and applications they need to perform their job duties is a start. Some people may be saying, "Well that sounds great, but the company's budget does not allow it." Well, why don't you ask the powers that be how valuable the data that sits on your network is. This should get them interested in the topic.

What are you to do if the internal attacks on your systems are purposely done? Well, this is where intrusion detection software tools come into play again. Monitoring your users is a normal precaution taken in many organizations. I personally would like to know where my employees are utilizing their time. Are they using company resources for company related activities or for personal use? The placement of intrusion detection software will help you monitor the environment that you work in.

Conclusion

In conclusion, you should never rely on one software or hardware device to protect you from the danger outside. I'm not saying that firewalls are not doing a good job, but I am simply stating that they are not enough. Coupling different technologies such as firewalls and intrusion detection systems are definitely one of the more secure ways to go.

Resources

When Passwords and Firewalls Aren't Enough
http://www.3com.com/news/vpk/march1500a.html

Global Security Survey – Amy K. Larsen
http://www.informationweek.com/743/security.htm

Firewalls: The First Line Of Defense – Brian Robinson
http://208.201.97.5/ref/hottopics/security/firewalls.html