SYRINX
TECHNOLOGIES
MOBILE.AGILE.FOCUSED

Why Simple Can Be Secure

I'm often asked why security has to be so expensive. A lot of my time is spent preaching to clients about the need for increased security. Every day brings another new vulnerability to our computing infrastructure. Hardly a day goes by when we are not bombarded with headlines claiming that another famous company has been hacked, or that our credit card numbers have been stolen by anonymous cyber thieves. My immediate answer to that opening question has always been, "Security doesn't have to cost a lot of money. Simple can be secure."

In the information security industry, there is a concept known as FUD. Fear, Uncertainty and Doubt sells a lot of products. FUD can be a useful concept when applied in the right areas. When convincing IT departments to spend money on security-related expenses, FUD is often used to scare network managers into purchasing hardware and services. Occasionally, FUD is used to sell products and services that might not be needed. Before we think of security companies as total crooks, realize that FUD is used to sell all sorts of products, from all forms of insurance to alarm systems for your house.

My reasoning for the "Why Simple Can Be Secure" title of this article has been formed over many years of working with clients of all sizes. Too often bad things happen when simple policies and procedures would have eliminated the opportunity for things to go wrong. In the information security industry, several years ago there was a strong push to sell firewalls. A firewall is a device, usually consisting of a hardware appliance running special software designed to protect your network. At the time, the thought was that if you purchased a firewall you would be safe. As one infomercial says, "Just set it and forget it."

The problem with that theory was clearly demonstrated during the CodeRed and Nimda attacks a while back. These two worms caused extensive damage throughout the Internet. What was the root cause of the vulnerability? Why didn't the firewalls protect us? These worms propagated through the Internet because overburdened network administrators had not applied patches released by Microsoft many months before the attacks began. The firewalls provided no relief because the attacks didn't violate any network protocol rules. In other words, the CodeRed and Nimda attacks looked like valid web traffic.

There are lots of examples of similar problems with vendor patches not being applied. Several recent examples are the SQL Sapphire worm, the Microsoft IIS WebDAV vulnerability and other known issues with Apache web servers. All of these examples could have been solved by applying the vendor patches that have been supplied months before any publicly known exploits were released. The problem isn't the fact that vendors didn't know about the issues, but that the poor network managers are getting these types of alerts daily. With 10-15 known problems at any one time, how do you prioritize the patch process?

My point in bringing up these examples is to reiterate my earlier point. With all of the FUD being served up by security vendors, the best solution is often the free or nearly free solution. Don't get me wrong, I'm not trying to talk anyone out of purchasing a firewall, VPN or intrusion detection system. These devices are important pieces of an overall security solution. However, I am advocating starting with the basics, such as policies and procedures, which can be developed for relatively low costs. Without enforceable policies, purchasing lots of security hardware and software might not be the best approach.

When performing vulnerability assessments, I often find vulnerabilities that could have been prevented by simple, low-cost solutions. Something as simple as having your users log out of their PC when they go home can be extremely effective in preventing unauthorized access. The use of screen savers when away from your office is another free way to greatly increase the overall security posture of your organization. An entire article could be written about password policies. Anti-virus software can be expensive depending on the size of your organization, but its use has become critical to the security and management of most companies.

In conclusion, when you think of security, remember that sometimes the best approaches to security cost very little money. Developing strong policies and procedures is a great start. Implementing simple security policies involving screen savers and strong password policies can go a long way to securing your network. You will certainly want to look at other security products, but before you spend your hard earned money, make sure you have implemented the low-tech solutions first.