Four Basic Tenets of Network Security

Introduction
I speak with business owners all the time that say things like, "but my data isn't valuable to anyone." This usually leads me to ask them whether they think that vandals that "key" cars do it because they need the paint. The bottom line is that your network is always under attack, whether it be targeted or more commonly, simple Internet vandalism. ***The answer is to implement a "layered" defense scheme at the perimeter, server(s) and desktop.***

Secure the Front Door (Firewalling)
Every Internet connected network needs good perimeter defenses. In other words, you need to cover the front door. Firewalls serve as the first layer of your defense system and stand between you and the outside world of the Internet. For many years, firewalls simply performed SPI, or stateful packet inspection. This means that each data packet's header is examined to verify its validity. Unfortunately, this is roughly akin to asking people at the front door if they are carrying a weapon of any sort before allowing them in the door, without verifying the response in any way. Your network needs better protection than that.

That is where DPI, or deep packet inspection, comes into play. Unlike SPI, where just the packet header is examined, DPI scans the entire packet (each of the billions of them that comprise a day's work) for "signatures" of known attacks of every kind. Since virtually all attacks are identifiable in this manner, DPI firewalls are capable of searching packets for viruses, spyware, trojans, and many other network attacks. Their traffic scanning abilities are vastly superior to that of old school SPI firewalls. The downside to this is performance. As anyone who has spent time in airline security lines knows, thorough examinations take longer. Fortunately, fast DPI firewalls are now affordable for every business. ***Ask Net Sciences for more information about the Sonicwall line of DPI firewall/UTM devices.***

Secure the Back Door (Antivirus)
The next layer of your defense functions at the server. It probably goes without saying that every network requires comprehensive antivirus protection nowadays. This means running antivirus at the server and at the desktop. Any truly effective network antivirus software will include spyware and other "malware" protection as well. Network managed antivirus software can also alert you to problems and produce status reports on demand as well. This is what you want protecting your network.

Networked antivirus stands as a second line of defense against front attacks, but also covers intrusions from within. Networked antivirus can stop attacks that do not originate from outside the firewall. Desktop AV clients, managed and updated regularly by the server (any AV solution is only as good as its updates) can also guard against viruses introduced by users (on USB keys, checking their personal email, etc.). Just remember, a locked front door really cannot protect your business from attacks that come in through a missing back door. ***Ask Net Sciences for more information on networked antivirus for your network.***

Secure the Windows (Patching)

The third layer of your complete network defense is at the operating system and application level. It is probably not a surprise any more that Windows itself (and nearly all other software) requires patching to keep it secure. They are vital to your network's security though. Even with the other layers in place, many of today's most effective attacks happen at this level and without successful patch deployment and management, you will end up with bank vault doors front and rear, but screen doors everywhere else!

There are many tools on the market to handle patch management, but one of the simplest and most effective is a freebie known as WSUS (Windows Software Update Services). WSUS provides a good, basic level of patch management and distribution for all Microsoft products, including Windows Servers, Exchange and SQL Servers, Windows XP, Vista and Windows 7, Office applications and many others. WSUS is just one of many such options, of course. ***Ask Net Sciences for more information on Patch Management for your network.***

The Keys to the Kingdom (People)

This is the final key to securing your network. We are talking here of the most difficult to manage and potentially threatening component of any network; the people that actually use the systems. Educating your end users is the single most important measure you can take and is probably the most overlooked of all security measures. Remember, security is a process that hinges upon user education, so schedule an hour of basic security training at least once a year for your employees, and more often if you can.

Learning how to avoid becoming victims of "social engineering" is paramount. One day, standing at the front desk of a small law firm here in town waiting to come in to work on their firewall, I heard a receptionist say to a caller on the phone that she would be right back with the network password. I asked to whom she was talking and she replied that it was "the guy that does our network," which she suddenly realized, was actually me. She was a moment away from handing out the keys to the kingdom, all because someone politely asked. ***And again, there is no security without periodic user training.***

And Beyond

In addition to the above, there are other security products out there (such as antispam software and hardware, critical file protection products, and more). The issue is what level of commitment you can afford to make (in terms of both money and time). Security can be thought of as a continuum. Imagine Fort Knox at one end; very secure, but you probably can't get a pizza delivered. At the other extreme you find typical small business networks, maybe yours; easy for *anyone* to access anything, which is not really ideal. ***Ask Net Sciences to help you figure out how much security is right for your business and how to get there.***

Net Sciences, Inc.

Since 1995, Net Sciences has been building reliable, secure networks for our New Mexico customers. On networks of three to 300 computers, supporting law firms, architects, engineers, scientists, accountants and nearly every other profession, Net Sciences is the complete solution to your business network equation. Net Sciences designs, builds and supports networks, keeping them running smoothly, and protecting your data so that you can focus on taking care of business!