



Three Ways You *Must* Protect Your Network !

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. I also often hear things like “if everything is running just fine” and wonder if those same people would claim that diet and exercise aren’t important until they are seriously ill. It’s easy to be overly dramatic but the bottom line is that your network is under attack and serious problems can remain invisible until it is too late. The answer is to implement a “layered” defense scheme at the perimeter, server(s) and desktop.

Firewall w/Deep Packet Inspection - The Front Door

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, quality firewalls (hardware or software based), have performed SPI, or stateful packet inspection. This means that each data packet is interrogated (the packet 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, DIP 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. However, advances in processing power and design have made very inexpensive, very fast DPI firewalls a reality of late. Ask Net Sciences for more information on DPI.

Network Antivirus (w/Antispyware) - The Back Door

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. As the second layer of your network defense strategy, this sort of protection is like covering the proverbial back door.

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 (because any AV solution is only as good as its last update) can also guard against viruses introduced by users checking their personal email through POP or web accounts. 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 AV.

Windows Updates (Patch Management) – The Windows!

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. These patches are released on a regular schedule by some vendors (such as “Patch Tuesdays” by Microsoft) and much less so by other vendors, and can be hard to manage. 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 fish nets on the Windows!

There are many tools on the market to handle patch management, but one of the simplest and most effective (albeit, covering only Microsoft products) is a freebie known as WSUS (Windows Software Update Services). WSUS provides a good, basic level of patch management and distribution (and even limited reporting) for all Microsoft Windows 2003, Vista, XP and Office applications, as well as other products such as Internet Explorer and Outlook Express. WSUS is just one of many such options, of course. Other options include the ability to patch non Microsoft software and even other operating systems. Ask Net Sciences for more information on Patch Management for your network.

And The Keys to the Kingdom

I am going to briefly discuss now, the “fourth of three” keys to securing your network. We are talking here of the most difficult to manage and potentially threatening component of any network; the people (or carbon units as we security geeks sometimes say). Seriously, educating your end users will go as far as any other single measure you can take, and is probably the most overlooked of all security measures. They say that security is not a product, security is not a job, but that security is a process. And that process hinges upon user education that you should seek out and provide your users.

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, it certainly was not. She was a moment from handing out the keys to the kingdom, all because someone politely asked. Good passwords that don’t get written down on Post-Its left on keyboards are also important. And no network defense is complete without periodic user education.

And Beyond

Security can be thought of as a continuum. Imagine Fort Knox at one end; very secure, very expensive to support and you probably can’t get a pizza delivered. At the other extreme you’ll find the typical small business network, maybe even yours. It’s very easy for anyone to access anything, but that really does mean anyone, which is not ideal. You have to decide where to draw that line and how to trade-off security against ease of access. There are many more ways to protect your network, including antispam and antiphishing (message filtering), dedicated server and desktop antispyware (separate from the AV software) and more.

Call Net Sciences at 266-7887 or visit us on the web at www.netsciences.com to learn more about protecting your network against these and other threats. Net Sciences has been building and securing networks in New Mexico since 1990 and with HP, Intel, Microsoft, Sonicwall, Symantec & Xerox authorizations, NSI is your Small Business Network Expert.