Eight Steps You Must Take To Secure Your Network

Introduction
Have you just gotten a network survey done and found that your Fort Knox is more of an Open House? Did you already know that you are playing fast and loose but had no idea how fast and how loose? Well, you can make your network reliable and secure, starting at the perimeter (firewall) and working your way inwards. And you can resolve your worst networking problems, the same way they built the pyramids, one brick at a time. And remember, if it is not automated, it simply will not happen.

1. Secure the perimeter
Securing the perimeter with a good, deep packet inspection firewall is the easiest and most broadly effective step you can take. Just a few years ago, firewalls were very simple devices that simply scanned the headers of data packets (well under one percent by "volume" of data). They simply verified that a request for a certain page was valid and that the response to that request came from the intended target. No attention was paid to the 99 percent of each packet that was the actual data stream.

With everything from viruses to attacks against browser flaws in that data stream, you need more from your firewall these days. You need a device that does deep packet inspection, a device that has the ability to recognize and control specific traffic (i.e., instant messaging or streaming video). You need a "unified threat management" or UTM device, one that can also provide secure remote access and wireless capabilities. ***Ask NSI about easy and affordable UTM Firewall products.***

2. Setup Network Antivirus
The need for reliable network antivirus software is not news. But antivirus threats have grown tremendously in sophistication over the past few years. We still very commonly see sites running a mix of three or four different, unmanaged products on their desktops (or worse, nothing at all). That which you cannot automate does not get done. And that which you cannot get reports on, you will not even know is not getting done. ***Ask NSI about managed network antivirus for your business.***

3. Setup Software Patching/Updating
How many patches did Microsoft release for Windows XP? Thousands. How about Windows Server 2003? Hundreds. What things need patching? Servers, desktops, operating systems, browsers, MS Office, Dot Net Framework, Flash, Java, Adobe Reader, and more. Why do you care? Because every major attack you have heard of for years takes advantage of vulnerabilities that have *already been patched* (or should have been). ***Ask NSI about how to automate your network patch management.***

4. Setup Reliable Data Backups

Nearly everyone has heard of (or experienced) the hardships of getting tape backups to work properly. So why do so many still use tape backup? Because it's fast (LTO is faster than USB hard drives or NAS), reliable (with the right equipment), and cheap (a $50 tape holds 1000G of data). Finally, tapes can easily be stored locally in a fire safe and go home with you for off-site storage as well. But tape is not the only answer you need. ***Ask NSI about a data backup solution tailored to your needs.***

5. Setup Local Disaster Recovery

Think that your data backup is all you need to recover from a loss or theft? What if you had a theft that left you with no servers? Your data is safe on tape somewhere, but what does it take to get back to work: New hardware first, then the installation of your server, email/and or database servers, your backup software and then the recovery from tape of your data. That's two to five days without a network, after you get hardware. What if you could do it one afternoon? How much could that save you? ***Ask NSI about imaging and virtualized solutions for disaster recovery.***

6. True Disaster Recovery (DR) Planning

Want to fall asleep every night knowing your data backup and disaster recovery solutions are truly bulletproof? What if you had actually had a plan for a stolen server, a damaged building or other disaster? Perhaps you had never considered this all before. If so, let's get you sleeping well again. Most of this planning is strategic not technical, and not costly. ***Ask NSI about true DR planning and devices for your business.***

7. Setup Reliable Power Protection

Maybe you know that your UPS can support your servers for no more than about half an hour during a power outage. Maybe you have wondered . . . what happens then? And are all the really important pieces of your network protected from power fluctuation, contamination and loss? Did you know that you can connect all of your networking gear to one monitored device that can handle all your power needs? ***Ask NSI about power backup and monitoring solutions for your business.***

8. Educate and Train

No matter how diligently you protect the perimeter, maintain network antivirus and software patching, plan and execute backups and DR planning, all it takes is one piece of seriously bad judgment to bring it all down. ***Ask NSI about training your staff in the basics of reliable and secure computing.***

Net Sciences, Inc.

Since 1996, 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!