

Have the Security “Willies?” Build a Safer Network

By Sharon D. Nelson and John W. Simek

© 2007 Sensei Enterprises, Inc.

Can you really design and build a safe network? The short answer is no. Nothing's perfect, no matter how hard you work at it. We've all known the local health nut who was felled suddenly by a heart attack or mysterious illness. He should have eaten the gooey chocolate cake once in a while, done a few tequila shots and had some fun, right? Well, we can't be so cavalier with networks. Absolute safety is the Holy Grail, and you're just about as likely to find it. But if you realize that security is an ever-shifting target and you're receptive to monitoring events and making adjustment, the good news is that you can get very, very close to being well secured.

Microsoft will of course tell you, “trust me, I'm the sheriff in these parts.” Hah. It would be nice if Microsoft could simply wipe out the bad guys in the red sashes, a la Wyatt Earp and Doc Holiday, but the truth is the bad guys just keep coming. Mow six down and sixteen thousand take their place, all with the goal of getting your data. Though Microsoft has indeed paid increasing attention to security, it can never get away from its own prominence. You want to boast that over 90% of the world's computers use your operating system, you have to live with the fact that 90% of the pasty-faced, living on coke and delivery pizza, hackers, crackers, and business espionage experts are coming after you.

So what drives a network design?

Sometimes, regulatory measures or laws. As an example, you may have to take steps to retain, log and secure instant message communications if you are subject to SEC regulations. There are now over 14,000 federal and state statutes and regulations dealing with the preservation of data. This is one of the prime factors in network design. So, of course, are cost, performance and capabilities. And they all have an impact on security.

What should give you the willies in the middle of the night? (Hint: look over the cubicle wall)

The folks you see every day at work. Whether they are for sale for a few million rubles or seriously ticked off at management, the number one threat to data security is internal threats. A recent survey, conducted by the Ponemon Institute, of the IT departments for 461 U.S. organizations reports that the average annual cost of managing data security from inside threats is \$3.4 million per organization. Most of us are not at this level of expenditure, but we should be aware that the first step in securing our data is to address inside access. Roughly 70% of data breaches stem from an internal source. Seriously, keep an eye on the woman in the next cubicle!

Something to consider, which is standard fare for government entities, are background checks as part of the hiring process. As a minimum, you should verify the accuracy of the information on the employment application or resume. Also, there should be some

document or contract that defines the employee's obligation regarding confidentiality and non-disclosure of sensitive data. Should you monitor employees? Of course you should, and most large companies do. The point is not to invade anyone's privacy, but to protect your network. If you have an appropriate Internet and e-mail use policy in place, there should be precious little private materials to stumble on to in any event. For heaven's sake, pay attention to access rights. Does the receptionist need access to your law firm books? No, no, no. Consider carefully who needs to have access rights and develop a policy. Who do you watch most carefully? The folks who can do you the most damage, your IT folks.

You'd be amazed at how often employers fire employees and forget to "yank the plug" on their access to the network. This is a critical step, and failure to do this is often the reason employers get burned by former employees. No one who is terminated is in a happy frame of mind, and these unhappy campers frequently find that revenge seems, at least at the time, like a splendid idea. They may become guests of the state at a later stage, but if your data is already gone or compromised, you're going to have some serious explaining to do about the absence of good security and good policies.

Besides the human element of securing data, there are several technical alternatives to provide for a safer network. We'll identify techniques that can be applied in a wired and wireless network environment. There are specific security and design measures that are only used in a wireless network design, which will be identified later in this article.

Switches/Hubs

Hubs were used in the most basic of networks, but their day is past. A hub is a network device used to aggregate the connections for all of the computers. In the early days of Ethernet, all of the computers were connected using coaxial cable in a daisy-chain arrangement. With the usage of unshielded twisted pair (UTP) cable, hubs were used to provide the necessary connectivity. The first step in securing your network is to have the hub installed in a closet or area that can be physically secured. If the hub is sitting on someone's desk, then it is very easy to tap into the network or disconnect a critical computer, thereby disrupting service to the firm.

Hubs connect all computers into a single network where all devices "see" the traffic for everyone on the network. This is not a very secure or efficient way to communicate. Switches are now used as the replacements for hubs. Switches set up a very fast communications connection between two devices at the time that it is needed. This means that the network traffic moves between the originator and recipient and is NOT "viewed" by all of the other computers on the network. This makes for a more efficient and secure communication environment. Switches are much more intelligent than a hub and can provide for some level of network traffic segregation.

As with all critical computing components, switches should be physically secured. Switches can be viewed as the core connection component for the computers on the network and should be protected from tampering or compromise.

VLANs

Virtual LANs (VLANs) have been around for many years. You normally see VLAN implementations in larger firms, but they can be effectively used in small offices, especially in a shared office environment, where many people need to share a common Internet connection. Switches that support VLANs are more expensive than those that don't. Simply stated, VLANs are a way to virtually define which ports participate in a particular LAN. Network traffic is only allowed to communicate between those devices that are configured for the same VLAN. This means that you can define multiple VLANs to a single switch and restrict traffic to selected groupings of ports on the switch.

It is very common to have multiple law firms share office space so as to reduce the overall cost to the individual firms. VLANs are an excellent way to provide network traffic isolation yet allow usage of a common communication connection such as a high-speed Internet link.

Routers

It really doesn't matter if you only have **one** computer connected to the Internet via a broadband connection - it should be connected through a router. Routers are relatively inexpensive and provide a very good first line of defense. Of course, you can buy a router for several thousands of dollars, but that expense is usually left to the mid and large size firms.

By default, most small office routers will use a process called Network Address Translation (NAT). This creates a private internal network and does not advertise your real IP address to the outside world. When you connect the router to the Internet, whether it is via a DSL (Digital Subscriber Line), cable modem or some other method, the registered IP address for the Internet connection is translated to a private address on the local network. This means that the outside world only sees the address for the Internet connection and not the internal address. This method of translation also allows for multiple computers to share a single IP address for the Internet connection.

Another default operation is to block all unsolicited traffic from coming in to your network. Communications are allowed if initiated from a device internal to your network, but requests from the "outside world" are blocked. This operation acts as a type of firewall, preventing "snooping" of your network resources. Of course, you will have to override some of these defaults if you host your own e-mail or web server. You have to allow unsolicited connections to your mail server since you don't know when someone may want to send an e-mail message. There are other TCP/IP ports that you may need to allow through as well. As an example, you may need to allow the inbound traffic for access to your Exchange server when you are using a browser. This is normally known as Outlook Web Access (OWA) and is very common in Exchange mail environments. Since we're speaking of OWA, consider changing the default TCP port 80 to something else.

There are constant scans on the Internet for port 80 devices and moving the port number will reduce the potential for attack and compromise.

Larger and more expensive routers will have increased capabilities and features. As an example, you may be able to connect multiple internal networks to the router, thereby providing some internal level of isolation. Large firms will use these higher end routers to provide fault tolerance, alternate network paths and faster handling of traffic routing decisions.

Firewalls

Another consideration for network security is the installation of a firewall. The usage of NAT is a quasi-firewall type of implementation since it does restrict traffic. Firewalls can be of the hardware or software variety. Software firewalls are typically installed on a single computer and are used to protect the individual computer from external attacks as well as some operating system compromises. The firewall will look to see if an application is trying to send data out (perhaps as a spam engine) without user intervention.

Hardware firewalls are more expensive and more complicated to implement. They are also more costly. It would not be unusual to spend thousands of dollars on a hardware firewall. The hardware firewall is a specialized piece of equipment that runs a very specific software application, which is designed to rapidly investigate each packet of data and make decisions as to whether or not to allow the data to enter or leave the network.

UTMs

Another serious consideration should be given to implementing a UTM (Unified Threat Management) device if there is no firewall, anti-virus protection or intrusion detection already installed. A UTM device is a single device that can handle all of the traffic decisions for your network. It can contain anti-virus and anti-spyware software so that you don't have to have it installed on each computer. A UTM provides firewall functions and can also be used for detecting intrusions and attempts at intrusions for your network. The UTM is a very specialized device and is probably most cost effective if you don't have any security systems currently in place. Because UTM's are a combo-solution, some components are often better than others, and our choice, frankly, is to take the best-of-breed and make custom solutions for clients rather than installing a UTM.

What's that in the air?

As promised, wireless networking brings along its own special considerations. We could write an entire article (and we have) on wireless network security. There are some basic techniques to consider with all wireless networks. The first configuration change should be to disable the broadcasting of the network presence. This is done by disabling the broadcast of the SSID (Service Set Identifier), which is nothing more than the name of the network. Two other changes are encryption of the data transmissions and restriction

of the devices that can connect to the network. Encryption of the data transmission can be done using WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access). Restricting those computers that can connect to the wireless network is done through MAC (Media Access Control) filtering. Each computer has a unique MAC address associated with its network connection. The MAC filter will only allow connections for computers that are listed in the MAC table.

So how are those willies?

Nothing about network security is simple. It will in fact, inevitably become more complicated along with the increasingly complexity of the technology itself. It will never remain static. The average lawyer has not a prayer of remotely understanding network security. Lawyers as a rule will remain dependent on in-house IT or outside consultants. Since you can't be your own Wyatt Earp, your best bet is to be savvy about hiring a good one, one who is flinty-eyed and watches all horizons. If you're lucky enough to have a Doc Holliday as well, you are twice-blessed – when it comes to security experts, it helps to have both keenly skilled and gut-intuitive guardians on your side. And don't fret about having those willies – it is the complacent who most often get nailed.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com