TECHNOLOGY

The eSecurity Advisor

Column: The eSecurity Advisor

Jan. 01, 2007

From the January-March 2007 Issue

Last month, we began a multi-part series on confidentiality. We started first by reviewing the pillars of security — confidentiality, integrity and availability. We then discussed the importance of identifying all critical data and reviewed a number of steps users could take to help safeguard the confidentiality of their information, focusing first on physical access. We then discussed the importance of backing data up and, finally, previewed some promising new hard drive protection technologies that should afford further protection. With that as the back drop, I wanted to continue our discussion on safeguarding our valuable data, especially when users take their show on the road!

Unprotected Shares

Way back in the early days of Windows (*Windows for Workgroups* to be specific), Microsoft provided a means for users to easily and conveniently share file folders and printers with each other. These shared resources were simply called "shares." And when users shared resources, they would typically allow anyone and everyone to connect, without the need for any type of authentication
or password. This was referred to as an "unprotected share." And while these shares made it fast and easy to access common files and connect to networked printers, they present a notable security challenge in today's

more mobile and complex connected environments. Let's put it together and see why.

- To share a folder or printer in the Windows operating environment, a user need only right-click on the desired folder or printer, select "Sharing and Security" from the pop-up menu, then click the box entitled, "Share this folder on the network," from the Sharing tab. Voila! The folder or printer is now accessible by others. Note: This procedure varies slightly depending on the version of the Windows operating system being used. It is also worth noting that while newer versions of the Windows operating system have tried to improve the security surrounding this ability to share folders and printers by providing better Help and walking the user the through the process in attempts to help limit unauthorized access, the process and end results remain largely unchanged.
- The user may further designate whether other users are limited to only "reading" files within a folder, or whether they can "change and update" documents. Users will often give "full rights" to shared resources on their system so they can save any changes back to the original folder.
- Windows indicates that a folder or printer has been "shared" by changing the icon to show a hand beneath the shared resource.
- Once a resource has been shared, other users on the network are now able to access the contents of a folder accordingly.

This all sounds simple so far, but what happens when a user leaves the trusted environment of the hard-wired office network with their laptop and begins making connections on other networks, wired or wirelessly? The user may have been completely
comfortable providing full access to the contents of selected folders on their laptop drive with other users in their home or corporate office, but that is not likely what they intend once they are connected to client, hotel and/or coffee shop networks with other unknown users. Yet, that's exactly what takes place.

Okay, so now you're scared! What to do? Well, in most cases we recommend turning off file sharing altogether (i.e., don't share files on local drives, especially laptops or other machines that may leave the office). We also recommend turning off the Windows "Guest" account. This can be inactivated under Start | Control Panel | User Accounts. That way, in the

event you find yourself sharing a network wire with someone who is looking to gain unauthorized access to your machine, they can't login as a "guest!"

In the end, if you wish to share files with other network users, it's best to place them in a shared location on a network server, where a login name and password authentication are required to gain access.

Wireless

While I have talked at some length previously regarding the importance and specifics of 802.11 wireless security — i.e., use WEP at a minimum (WPA or WPA2 preferred), turn on MAC address restrictions, etc. — I wanted to share a slightly different perspective on the use of wireless given its potential impact on confidentiality. More and more of today's devices are arriving with wireless capabilities turned on out of the box. Whether it's PDAs, notebooks or printers, these devices are often pre-configured to make instant connections to the closest available wireless access point. Unfortunately, this can be one of the most dangerous security policies (i.e., connect with whatever you can find, whenever you can find it). As a result, I have often encountered situations where users find themselves wirelessly connected to the Internet but have no idea how or where they are connected! And once connected, the user is now sending and receiving data right alongside other unknown users. Given that, we recommend the following:

- Turn off wireless, except when it's needed (i.e., don't leave it set for "always on — connect when you can").
- Install and/or turn on a personal firewall on all desktop and laptop machines to help better protect them from inbound attacks from other users on the same network. That way, when wireless is turned on, users have one more layer of protection against outside attackers.
- Be mindful of what programs are communicating over the wireless connection, and understand that some data may in fact be transmitting in clear text (i.e., unencrypted). For example, one thing users should never do is access their POP3 e-mail accounts over a wireless connection since POP3 connection information
  is transmitted in clear text. This point was never more clearly made to me than when I was giving a talk on security in Las Vegas a few years back, and a student shared that by the end of my presentation, he had successfully captured login names and password information for more than 50 other users in the room who were using their laptops to connect to their e-mail accounts via POP3

... all done via simple packet sniffing tools (available for free on the Internet) and the wireless connection provided by the hotel where the seminar was taking place. Talk about scary!

Based on the security issues surrounding wireless connectivity, we now recommend that unless a user is confident that they have a secure connection and that they can transmit data securely, then they should consider not using wireless at all! Users must think about security first and convenience second!

VPN

So what happens when a user needs to securely send and receive information between a remote location and the main office? Is it even possible? That's where Virtual Private Networks (VPNs) come in. A VPN creates a highly secure connection between two end points by encrypting the information passed between them. And VPN connections can be established in one of several ways:

- **Software** — This method uses software at each end to encrypt/de-encrypt the traffic moving between. This approach is reasonably straightforward now that many organizations have standardized on the Windows Server operating platform (i.e., Windows Server has the necessary functionality to support software-based VPN connections on the server side). And the VPN client software required by end users is a part of the Windows XP desktop operating system.
- **Hardware** — Hardware-based VPNs actually use hardware at one or both ends to help speed the encryption/de-encryption process. Depending on the amount of information traveling between two locations and the latency end users experience, a hardware-based VPN may be worth considering.
- **Third Party** — If all this talk of VPNs gets you woozy, then you may want to consider outsourcing the process to a third party instead. This approach involves registering the host or head office end of the VPN with a third-party service. Then, when an end user needs to make a secure connection back to the office, they actually connect with the third-party service instead that then tunnels all the traffic securely for them. This spells secure connectivity with far less hassle.

In the end, there are so many ways our critical data may be placed at risk, but using the various techniques and technologies we've reviewed, there's

absolutely no reason a user's data can't remain secure and confidential. Until next time, safe computing!

David Cieslak is a Principal in Information Technology Group, Inc. (ITG), a computer consulting firm with offices in Simi Valley and Huntington Beach, Calif. He is currently an instructor for K2 Enterprises and a frequent speaker on technology issues. He also currently chairs the AICPA IT Executive Committee and serves on the Information Technology Alliance board of directors and CalCPA Council.

Technology • Article