Jan. 01, 2008

From the Jan./Mar. 2008 Issue

Happy New Year! I hope 2008 has started off in a good way for you. For me, it is that annual time of the year where my thoughts turn more to accounting than technology as those of us in public accounting all spend the next three and a half months working like mad to help our clients file their annual paperwork. But even as those of us in public practice start working on our clients' accounting records, we still need to be mindful of the technology threats that face us every day, even during tax season. The hacker never sleeps (he/she uses automated tools for much of their work) and so we, as accountants, cannot be asleep at the switch either. While those of us in public practice tend to put our technology upgrades on hold during this time of year, we need to remember that the hacker or identity thief is still out there breaking into systems and stealing information. We need to remain vigilant this time of year even though we are busy working for our clients. As we go forward into this busy time, we still need to ensure that we are working at peak efficiency to protect our clients' data.

FEDERAL DESKTOP CORE CONFIGURATION

The Federal Desktop Core Configuration (FDCC) was developed under the direction of the Office of Management and Budget (OMB) in collaboration with DHS, DISA, NSA, USAF, and Microsoft by the National Institute of Standards and Technology (NIST). This set of standards provides resources for federal agencies, which allows them to test, implement, and deploy Windows XP and Windows Vista securely.

While this protocol was designed for use within the government, the OMB, through the NIST, has also made this core configuration available to the public. This

provides businesses, nonprofits, and individuals with a process for securely

our country's infrastructure as well as protecting our secrets, have worked with Microsoft to develop this protocol. Irrespective of public opinion about how competent our government is or is not, these guidelines provide exceptional help in securing our computers on our network. By following this standard without deviation, it provides you with a useable defense in the event the firm network is compromised and client data is stolen. The FDCC can be obtained from the NIST at http://csrc.nist.gov/fdcc.

PEER-TO-PEER NETWORKS

In recent months, we have heard more and more discussion about which type of network to implement in a firm. The decision is between a domain-based network and a non-domain-based network, also referred to as peer-to-peer. With all the security threats on the Internet today, the peer-to-peer network has reached the time when it needs to be removed from use as a valid network system for a business and especially an accounting organization. This is not because of the fact that it does not work well for public accounting firms and other small businesses; it does. The issue is how peer-to-peer networks handle authentication. Each machine on the network by default trusts the other machines on the network to which they are connected. To make a peer-to-peer network, the user needs to simply create a set of networked computers with the same workgroup name and then share files on one or more computers. Once the files are shared, any one computer on the network that can be compromised by a hacker now makes the information on all the other computers available to the hacker, as well.

In a domain-based network, many features prevent these sorts of problems from occurring. Domain networks are better because they are:

- Much more secure by using a more robust authentication protocol.

- Microsoft's recommended method for setting up a network.

a peer-to-peer. In fact, there is absolutely no legitimate reason to not use a domain in setting up a network. Should a peer-to-peer network still exist in the firm and be used to store client data, you should talk with your network consultants today about putting together a replacement plan for just after the end of busy season. They can work on obtaining the components now while you are focused elsewhere so when the time comes after busy season, the project can start.

MICROSOFT BASELINE SECURITY ANALYZER

This is a great tool for discovering areas that may need improvement in terms of security. This software tool is free from Microsoft. After it is installed, you should run it on your system. The resulting report will provide a listing of the vulnerabilities found as compared to a database of known vulnerabilities. This may include things that you may not be aware of such as Microsoft hot fixes, patches, and service packs that may not yet be installed on your system. The report may also contain instructions on registry changes or system permission changes to make the computer more secure. Download and run it today on all the workstations and servers in your firm. Search on Microsoft.com for Baseline Security Analyzer to obtain the link to download this tool.

SOME OTHER RESOURCES

Here are some additional resources that are important for accountants to know about and, in some cases, important to visit on a fairly regular basis. Some of these items are tools anyone can install and use. Others contain information helpful in ensuring the ability of firm members to stay current with trends and changes in technology security.

CERT Coordination Center & SANS Internet Storm Center

These two organizations are responsible for two very important tasks on

the

and the SANS Institute can be found at www.sans.org.

WindowsSecurity.com
This is a great website to find information, articles and tutorials on security-related
issues for Windows computers: www.windowssecurity.com.

Microsoft Windows Defender
This is a great tool for finding and removing spyware. Microsoft is certainly going to be adept at removing spyware from Windows because they know what
should be in the system and what shouldn't. In Windows Vista, this comes pre-installed. In prior versions, it is available for download on Microsoft's website at
www.microsoft.com/athome/security/spyware/software/default.mspx.

National Institute of Standards and Technology
Earlier in this column, the FDCC was introduced as an available tool from the NIST. Other tools are available from the NIST related to computers and may be helpful to you. They have guides and helpful information on Cryptographic
Standards, Security Testing, Security Research/Emerging Technologies, and much more. Check them out at www.nist.gov. Note: There are a large number
of other standards promulgated by the NIST so don't get lost reading about all the other interesting stuff on this site. To go directly to the computer-related information, go to http://csrc.nist.gov.

IN CLOSING
Security in a public accounting firm is not just about locking the doors and

setting the building alarm when walking out at night. It is also about securing

bother someone else who is less secure and less knowledgeable.

I want to again wish you a happy and prosperous 2008 and, most importantly, a trouble-free tax season. I look forward to visiting with you again in April as we continue to explore various security issues at the intersection of technology and public accounting. Enjoy!

Digital Currency • Technology