



this issue

Practical Security for Your Business **P.1**

Upcoming Events **P.1**

Trends & New Software **P.2**

Upcoming Events CT Laserfiche User Training

Join us for CT Laserfiche User
Training via the web.

Basic User Training

- Basic scanning
- Organizing and Retrieving
- Processing and indexing
- Viewing and printing

Date: Thursday, Feb 18, 2010

Time: 10:30am - 11:30am

Advanced User Training

- Advanced scanning
- Import & Export
- Template Creation
- Keyboard shortcuts

Date: Thursday, Feb 25, 2010

Time: 10:30am - 11:30am

To register:

Email - register@ctaccess.com

Call - 262-789-8210

Computer Technologies of WI, Inc.
740 Pilgrim Parkway L3
Elm Grove, WI 53122
262-789-8210 ph
262-789-7356 fax
www.ctaccess.com

PRACTICAL SECURITY FOR YOUR BUSINESS



Scott
Hirschfeld

None of you will be surprised, if I said that the security is of utmost importance, when evaluating the technology within your businesses. Most of us have spent a fair amount of money to insure that our company data, networks, and related peripherals are secure from the onslaught of nastiness that seems to increase with passing time.

Security is an area where yesterday's "good enough" is just not good enough. New tactics, new technology, and even economic incentives are driving the ethically challenged, otherwise known as hackers, to develop more advanced and more dangerous methods of attacking the legitimate user.

None of us have unlimited budgets, and if we did, we would not choose to spend them on security. What is practical, what has changed, and how do we evaluate our level of risk as it relates to our business technology?

Let's start by breaking the broad "security" concept into a few key areas. First, we must secure ourselves against outside threats like hackers and malicious code. We must also secure ourselves against inside threats like employee misuse and behavior that is conducive to bringing on an outside threat. In addition, we must protect ourselves against technology failure

usually caused by hardware or software malfunctioning. Finally, measures must be taken to recover in the event of environmental or physical disruption cause by things like fire, flood, and other natural disaster.

For purposes of this article, we will take a closer look at protecting ourselves from outside threats. One of the most common reactions I get from small and medium sized business owners and managers when discussing this is something like "I don't have any secrets or anything that would make me a target". Most of the hacking going on out there is not directed at you specifically as a target. Most outside threats are general and focused on your company simply as another company on the Internet who might have valuable data, valuable computing power, or valuable storage space. It is kind of like a terrorist who usually is not specifically targeting one person, but targeting a class of people, in this case, businesses and computer users. Years ago outside threats were sometimes just someone trying to prove his technological prowess. Now the threats are generated by cyber-thieves who are often earning large sums of money by stealing use of your equipment, bank account numbers, or credit card information.

Outside threats can be broken down further into a couple of categories. First, there is malicious code or malware, also known as a virus or





spyware. This code is usually transmitted to us via an email or by visiting a website that has been infected. The user usually notices that there is a problem when their system slows down and becomes less functional. The real problem is that this malicious code does more than slow a machine down. It compromises the security of a system and allows it to be used for other purposes. It may allow a hacker to gain remote access to your system. In fact, this access is often sold to other hackers once it is verified. In addition viruses often transmit data like credit card numbers back to their authors who then sell the information. Your credit card number is worth about \$25.00 on the Internet black market.

The other outside threat is the hacker. He may get into your network through malware, or he may enter your network through an inadequate firewall. The direct hacker attack is actually much more rare than it used to be. It is just easier to gain access through an infected machine. This does not mean that firewalls are not important, in fact, I would say they are more important than ever.

The final type of outside threat is a physical threat. This is someone outside your company gaining control of some physical piece of hardware. For instance, what if your smart-phone, laptop, or flash drive falls into someone else's hands? While the intent of this person may be good, it also could be malevolent. What might it do to your business if a key spreadsheet somehow made its way to a competitor, or some embarrassing correspondence somehow made its way into public media?

Now that we have identified these threats, how do we make sure that we are protected? There are three major areas of prevention: the perimeter, the endpoint, and the policy.

The perimeter is really your connection point to the Internet. This is comprised of a firewall. Most often this is a hardware unit that is one step away from your server. The firewall is like the traffic cop, determining what comes into your network, and what goes out. It was common practice to use the main file server in a small business as a firewall.

This is not good practice. You want your server to be completely inside the perimeter so that it is one step away from any threat.

Firewall technology has changed dramatically in the last 2-3 years, so if your unit is older than this, it is time to re-evaluate. Newer firewalls are able to do application filtering that will block spyware and viruses before they enter your network. This, blended with a higher level of intrusion prevention, really increases your security from outside threats and makes a newer firewall worth its salt.

The second area of prevention is the endpoint. The endpoint is the PC, server, or even the smart-phone. Typically these devices are the target of malicious code like viruses and spyware. It is important to make sure that your devices are protected by a commercial product that is up-to-date with both the latest definition files and the latest version of the software itself. Most virus packages don't do that great of a job in preventing spyware, so in addition to an up-to-date virus package, it is important to use a commercial spyware package. This package could either be a gateway package that runs on your firewall, or a client package that runs on the endpoint device, most often, the PC.

The final area of prevention is policy. This really is comprised of two facets. First, it is key to make sure that you have policies in place to guide your employees in safe email and safe web browsing practices. These policies should cover such things as how to handle emails from unknown or suspicious senders, what the company considers appropriate Internet browsing practices, how to handle a lost or stolen smart-phone, and many more. The second facet of policy is really to have an appropriate maintenance program in place. All of the prevention tools rely on a regular plan of updates and maintenance. We no longer live in a world of "if it ain't broke, don't fix it" when it comes to technology. Proactive, scheduled regular maintenance is essential.

For more information on security in your business, please contact Scott Hirschfeld at 262-789-8210 or scoth@ctaccess.com.

EYE ON IT Industry Trends

It is finally almost here! The iPad 1.0 that is. The first generation of multi-media tablet pcs. Is it going to live up to all the hype? That depends on what your expectations are. The iPad can be used for browsing the web, reading e-books, sending email, watching videos, enjoying photos, playing games and listening to music. It weighs just 1.5 pounds and features a 9.7 inch LED multi-touch display. It runs most of the 140,000 apps from the Apple Store and syncs with iTunes. It has Wi-Fi and an amazing 10 hour battery life. So what is the iPad missing? There is no multitasking, you can only run one app at a time, no flash, which means no video when browsing the internet, no wide screen for viewing, or HDMI output, so you can't hook it up to your tv. It is missing a kickstand, you will need to purchase a dock. No camera which means no video chat or taking a quick pic and uploading it to Facebook. Did I mention no USB, you will need to purchase a iPad Camera Connection kit. The price range is from \$499-\$829 plus the \$30 monthly fee for the unlimited plan. The iPad is set to start shipping in March.

SOFTWARE Monthly



Having trouble with some nasty spyware or malware? Try Combifix. It is one of our techs favorite spyware removal tools and it's free! You can find it at www.combifix.org.