



BUSINESS TECHNOLOGY QUARTERLY

Brought to you by *The Technology Group, LLC*

(860) 524-4400 www.TheTechnologyGroup.com

The Need for Security Procedures



By Greg Rothausser, MCSA

For any given security issue, there are both procedural and technical solutions. Too often, companies focus on the technical side and implement either insufficient policy and procedure controls or none at all. By looking at a few common security issues, we can see how technical solutions while helpful and necessary, still leave gaps in protecting your network, business or organization that only proper procedures can alleviate. We'll look at how protecting your network from Internet hackers, viruses and loss of data on a mobile device, such as a laptop, requires both technical and policy controls.

(Continued on page 2)

Should I upgrade to Office 2007?



By Gregory Robinson

If your company relies on Microsoft Office for crucial day-to-day tasks, you may be wondering about the recently released Office 2007 suite's new features, potential impact on your budget, and whether upgrading now makes sense. To help you decide whether

(Continued on page 4)

Sentinel Offers New Levels of Security

By Ian Apruzzese

Sentinel – a new way of thinking about client networks and what keeps them running.

The Technology Group has launched its Sentinel brand of products. The Sentinel brand is designed to give our clients the highest levels of protection and security, 24 hours per day, 7 days a week.

Our specially designed Sentinel products are tailored to offer our clients just what they need for their specific network and business needs.

The Sentinel line includes 24x7 network monitoring and secure offsite backup. The laser focus of these products is to deliver just what the client needs without the additional cost or hassle of complicated in house systems. Future Sentinel products will include hosted SPAM protection.

Sentinel 24x7

A monitoring system that continuously reports network and server system health status

(Continued on page 6)

Join Us!

Upcoming Sage MIP and Sage FR50 Seminar

Thursday April 17, 2008

Bridgeport Holiday Inn
1070 Main Street, Bridgeport, CT

Breakfast & a Free Demonstration of Sage MIP Fund Accounting & Sage Fundraising 50

(Continued on back page)

INSIDE

Security News	pg. 3
In-House News	pg. 4
We'd Like to Hear From You!	pg. 5
MIP Tips & Tricks: "SQL server failed" during v9.0 upgrade	pg. 6
A New Breed of Laptops	pg. 7

Security Procedures

(Continued from page 1)

Internet hackers are often the first security breach organizations think of when discussing network security. The idea of a teenager halfway across the world trying to break into your network is certainly sobering. When we discuss keeping the outside world out of your network, we are talking about "perimeter defense."

Generally speaking, the solution to this issue is to implement a firewall and possibly an Intruder Detection System (IDS).

A firewall, means you are fully protected, right? Not exactly. Just like any other computer system there are ways to attack it. In order to be as secure as possible (nothing is ever 100% secure) the firewall should be upgraded periodically with the latest fixes and software. That means having a policy and procedure that defines how often it should be upgraded.

Similarly, an Intruder Detection System only does any good if someone is reviewing the logs periodically; the frequency depending on the policy and needs of the organization. Without that policy-driven review, the IDS is essentially a useless piece of equipment.

Virus protection is very similar. Even given a best-case scenario of a corporate-level anti-virus package with a

centralized method of updating definition files, human intervention is necessary. As an example, a recent new-client-visit uncovered a number of PCs that were no longer updating their definitions. They were using a corporate anti-virus solution that provided a single "dashboard" to view all of the PCs' definitions.

"...users are not even aware of the risk to which they are exposing your company."

However, the company had no policy for actually visiting each workstation on a periodic basis to verify that they were indeed still updating. In this case the computers "lost" their connection to the dashboard thus no "red flag" was raised and those two computers went months without being protected and exposed the company to unnecessary risk.

Finally, let's look at the prevalent issue of losing sensitive data on a laptop. The news has been filled with reports of various organizations or governmental agencies "losing" laptops with private information on them. The data could be protected health information of patients, confidential HR data of employees, financial records, etc.

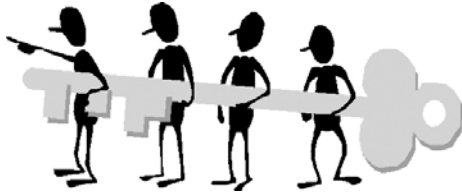
If an employee's job function requires that data of a sensitive nature be carried on a laptop, it needs to be protected. The industry accepted method of protecting this data is "whole disk encryption", as a previous Technology Quarterly issue

discussed. This has generally been considered to be "bulletproof" protection.

However, security researchers proved in February that a PC left on, whether it is in suspend mode, logged off or just "locked", is vulnerable to the encryption key being stolen right from running memory. There would be no need to know the password at all – the thief would be able to read the entire contents of the "protected" drive. This same vulnerability could apply to digital keys used for secure transactions at websites such as online banking. Therefore, in this case, the best current protection would be to adopt a policy that requires all users to completely shut off a laptop when they are done using it and when left unattended rather than merely suspending, locking it or logging off.

Certainly, there is always the possibility of a user not complying with the policy, but without it the users are not even aware of the risk to which they are exposing your company.

Whether it is users properly taking care of mobile equipment like laptops, IT staff stopping viruses or a security officer reviewing intrusion logs security requires the human element. In order to provide your employees and contractors with guidelines to help keep the network secure policies and procedures need to be implemented to complement and enhance the protection that technical solutions can provide. ■



SECURITY NEWS

TEEN PLEADS GUILTY IN BOTNET SCHEME

(Feb 19, 2008 Sans Institute)

A US teenager has pleaded guilty to using botnets to place adware on hundreds of thousands of computers. The unnamed teen worked with Jeanson James Ancheta, who is currently serving a 57-month sentence for his part in the attacks. The teenager will face a prison sentence of between one year and 18 months when he is sentenced in May. The pair infected computers at the Defense Information Security Agency (DISA) and Sandia National Laboratories.



We will not be hiring Mr. Ancheta for our open Security Engineer position at TTG.

MORE THAN 50% OF COMPANIES HAVE FIRED WORKERS FOR EMAIL AND INTERNET MISUSE

(Feb 28, 2008 Sans Institute)

More than half of 304 US companies surveyed said they had fired employees for email and Internet misuse. Of those managers who fired employees for Internet misuse, 84 percent said the employees were viewing inappropriate content, and 34 percent said they had fired people for excessive

personal use of the Internet on the job. Of managers who fired workers for email misuse, 64 percent said workers had violated company policy and 62 percent said the emails contained inappropriate or offensive language. Twenty-two percent said they fired people for breaching confidentiality rules in email, and more than 25 percent said they had fired workers for excessive personal use of email.

IMPROPERLY CONFIGURED SERVERS AND NETWORKS CREATE LARGEST SECURITY RISKS

Mar 7, 2008

Mark Torello, CISA, CPA, CFE

Security experts, including those from my firm confirm that "IT guys" should be more concerned about the security risks created by miss-configured networks than by all the flaws and exploit code that is known today.

If servers, firewalls, routers, and other systems are not regularly patched, maintained or upgraded, organizations risk greatly exposing the company attackers. At a minimum, a solid patch management system should be in place.

"COLD BOOT ATTACK" HIGHLIGHTS ENCRYPTION WEAKNESS - SHAKES THE SECURITY INDUSTRY

Mar 7, 2008

Mark Torello, CISA, CPA, CFE

The news that disk encryption technology used by the highest levels of government can be compromised has shaken the technology and security industry. Encryption products

such as ssh-agent and PGP software use DRAM memory on a pc to store their encryption keys. In a paper published Thursday February 21st, a team of security researchers affiliated with Princeton University announced they had discovered a way to leverage the inherent characteristics of DRAM found in all computers to circumvent various disk encryption products.

Makers of these systems rely on encryption keys that get stored in RAM that get erased when the system is turned off. But newly published research shows that the hardware isn't behaving like we thought, and that memory modules, even removed from the motherboard can retain data for seconds to minutes allowing retrieval of the cryptographic keys. Leading manufacturers of this software were quick to respond with guidance and best practices to mitigate or eliminate this risk.

The "Cold Boot Attack," is dependent upon the attacker having physical access to the computer either while it is running or within a few minutes of shutting down. Details of how the Cold Boot Attack works have been published on C|Net and can even be viewed on YouTube.

What should you do? Rely on the "layers of security" concept by strengthening controls over physical access to systems. That is, make sure that only authorized individuals can gain access to pc's and systems.

More security alerts at www.TheTechnologyGroup.com

Office 2007 Upgrade?

(Continued from page 1)

moving to Office 2007 is right for your organization you might want to know about what the new version has to offer.

While Groove and OneNote are the only two new applications that have been added to the Office 2007 suites, Microsoft has made significant changes and added new features to a number of other Office programs. The biggest and most noticeable change concerns the way it looks. Microsoft has abandoned the traditional menu found in past Office applications in favor of a design scheme it calls the "Ribbon". Rather than requiring the user to browse through several menus, the ribbon interface arranges all of its options under a few basic tabs; clicking a tab brings up a selection of related tools. For instance, in Word 2007, choosing the Insert tab on the Ribbon brings up a toolbar containing all available tools, such as those for inserting tables, headers and footers, graphics and page numbers. Another advantage to using the ribbon is that when you make a change you are able to preview the change immediately without having to wait for closing out the options panel.

The ribbon interface also pops up certain toolbars when it thinks you might need them. For instance, when you highlight a block of text in Word 2007, a small formatting

toolbar will appear with options for changing font styles and applying italics and bold to text.

Though the user interface is the most obvious change in certain Office 2007 applications, Microsoft has also added a variety of less noticeable features. For instance, you can now save Word, Excel, PowerPoint, and Access files as PDF documents.

Keep in mind that since certain Office 2007 applications have radically redesigned interfaces, you may want to consider what kind of impact upgrading will have on your staff in terms of how much training they'll need to become proficient with the new applications.

In the 2007 versions of certain Office applications — including Word, Excel, and PowerPoint — Microsoft has introduced a new file format that's designed to help keep file sizes small. This new format adds the letter "X" onto the end of Microsoft's existing file format extensions. So while a document created in Word 2003 might be called "fundraising_goals.doc", the same document created in Word 2007 would be called "fundraising_goals.docx." By default, Office will save your documents in this new file format. If someone else needs

to open or edit the file using a previous version of the Office application, they will have to install a special piece of software in order to do so. However if you want to avoid

"...you may want to consider what kind of impact upgrading will have on your staff in terms of how much training they'll need to become proficient..."

this small problem, because you don't know if the other person you are sending the file to has this 2007 compatibility pack installed on

their older version you can choose the Save As option to save the file in an older version format.

In-House News



The Technology Group, LLC unveiled its new suite of Sentinel (TM) Products.

These products have been developed and are offered to meet the growing demands of our clients.

They include:

- Sentinel™ 24x7 Remote Monitoring
- Sentinel™ Remote Backup
- Sentinel™ Incident Management

We welcome the following new client additions:

- Aquarion Water Company
- United Way of Eastern Fairfield County
- Meriden Wallingford Chrysalis
- YMCA of Greater Springfield

**Do you know if your network is in trouble?
RELAX... We know!**

Sentinel 24x7

24 hours/day

7 days/wk

If you have ever asked...

- ◆ Are we ready for full time IT attention?
- ◆ Can I reduce downtime, poor performance and increase IT security without paying too much?

You are not alone.

Sentinel Monitoring Benefits:

At The Technology Group, we believe in proactive monitoring and preventative maintenance. We work toward making your systems work optimally. It sets you free from all the worries of cost and downtime and allows you to focus on your core business.

What we offer:

Feature list

- ◆ 24x7 Critical event monitoring
- ◆ Reduced downtime
- ◆ Automatic issue alerting
- ◆ Peace of mind

If there's a problem we're alerted and working to fix the issue!

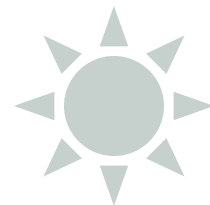
The Technology Group provides top-class IT services and a sophisticated set of IT management tools, currently available only to Fortune 1000 companies.

You gain all of this without a huge up-front investment or committing to long term contracts.

Our technology allows us to proactively fix issues before they turn into problems and instantaneously attend to a problem to prevent disasters.

Experience a higher level of service with...

**Sentinel Monitoring
Rely on us!**



We manage everything related to your network and servers.

The Technology Group performs specialized database monitoring, e-mail protection and management, network management, server maintenance, desktop support, performance monitoring, patching, anti-virus updates, software deployments and much more. We utilize a team of certified engineers, delivering high levels of personal IT support on 24x7 basis.

Special Non-Profit Pricing Available

Call us at 860-424-4400



MIP Tips & Tricks "SQL server failed" during v9.0 upgrade

By Camille Livsey

Version 9 of Sage MIP Fund Accounting (MIP) product was shipped in November of 2007. We have received a number of calls from MIP clients who have attempted to install it on the server and are getting an error message saying "SQL server connection failed." For those MIP users who have not already installed, we wish to share the resolutions so you are able to be up and running on the new version quickly and easily.

Please note: if you are logged into the server as an Administrator, you are not likely to encounter this error. Please verify your log in before installing and proceed as follows:


If the error occurs and you are logged into the server as an Administrator, then the likely cause is that an older version of the Microsoft Data Engine (MSDE) is still being utilized from version 6.x (or earlier) of MIP. To determine if you are using an older data engine, go to Control Panel > Add or Remove Programs and look for "Microsoft Data Engine for MIP (SP3)" or "Microsoft Data Engine (Build 194.05) for MIP". If either of these show up, then you are using an older data engine.

There are two options to resolve this:

1. If you know the password for the SQL Server administrator

account (sa), then install using the "SQL Authentication".

2. If you do not know the password for the SQL Server administrator account (sa), you will need to download a script which will update authentication in your older data engine. This will allow you to install normally.

Full details are provided in knowledgebase Article 268875. The online knowledgebase is located in Sage Software Online. After logging in, click the green "SUPPORT" button to be directed to the main support page which contains a link to the knowledgebase. 

Just for Nonprofits Contacting Support at Sage Software

On March 3, 2008, Sage NonProfits eliminated their "Authorized Contact Policy".

When someone from your organization needs assistance, you no longer need to be concerned about whether that person is already on your Sage Nonprofit Solutions contact list. The support analyst will add the person immediately, if necessary, and then proceed to assist.

All you need is your client ID and call 1-800-945-FAST.



Sentinel

(Continued from page 1)

back to a central network operations center 24 hours a day. This gives us the ability to service our clients better by reducing downtime associated with system failures and to proactively assess potential problems, often before they have had a significant impact on business operations. Sentinel 24x7 stands guard watching for problems that would normally have a significant impact on operations and alerts our engineers quickly so that we can begin recovering from these problems and keep their business up and running.

Sentinel Remote Backup

An offsite backup and storage solution that protects critical client data; by backing up to a secure offsite facility. This scalable offsite backup system protects clients by backing up their most business critical data to secure offsite servers. This protects the business from failed tapes, incomplete backups, and total loss of data from disasters at their offices like fire or flood. By storing this critical data offsite we are able to ensure that the data they rely on for business operations is available even if their offices are physically destroyed.

The Sentinel products by The Technology Group offer a new level of service to our clients, making The Technology Group a truly superior technology firm. 

Product Review A New Breed of Laptops

By Eric Stoltz

In case you haven't noticed, there's a new breed of laptops hitting the market. They're fast, light, and most of all, stand out in a boardroom. These new laptops are employing new technology such as solid state hard drives, extended batteries, touch screens (also known as tablets), built in web-cams, and built in wireless using the new 802.11n standard. There are many choices out there, so here are a few to consider when shopping for a new laptop:

Apple MacBook Air



If you're not an Apple person, and don't feel like having to learn a new operating system on your laptop, please skip to the next model below. For the rest of you that are seasoned Apple OSX users, or those of you daring enough to try something new, this is the system that everyone is talking about. The entire laptop is less than one inch in thickness when closed, weighs only three pounds, and still employs a 13.3" screen (not to mention the shiny silver anodized aluminum case). There are no on-board drives for removable media (DVD,

floppy, etc), but utilizes USB ports for external devices. It's the ultimate road warrior's choice with its light weight and extra tough exterior, and it can still run Microsoft Office applications such as Word, Excel, and PowerPoint.

Asus Eee PC



Many of the hardware manufacturers are now offering systems with alternatives to Microsoft Windows, by pre-loading their laptops with different versions of Linux. One of the great advantages of an alternative operating system is cost savings. The Asus Eee PC is available for under \$400, with built in wireless and half a gig of RAM. These systems are not the fastest laptops on the market, but they can fit the need for an internet station that is extremely portable and affordable.

Lenovo Tablets



You may know this one by its old company name "IBM", but don't be scared by the change, these systems can still deliver. The Lenovo tablets offer high speed processors, built in wireless, long lasting batteries, and the ability to write on the screen with the special pen that comes with the system. These systems also offer the ability

to translate your hand written documents from the screen into text, which comes in very handy in offices where speed is always needed.

Dell XPS

If you're into gaming, then you know how important performance is. Many laptops sacrifice hardware speed for weight, and try to keep their systems as portable as possible. If you don't mind carrying around a slightly larger system, and you need high end processor speed and video performance, then you should check out the Dell XPS line. These systems offer many of the same options as desktops, but still have the portability of a laptop.



With so many different options available now with laptop computers, it can be challenging to decide what model is best for your needs. Some systems may seem fun and portable, but may lack the ability to interface with your company's systems. Others may work perfectly with your network applications, but give you a back-ache carrying them back and forth to the office each day.

Don't let these choices take the fun out of a new laptop, give The Technology Group a call and let us help you find the best fit.



Sage MIP and Sage FR50 Seminar

(Continued from page 1)

8:30 – 10:00 am: Sage MIP Fund Accounting Software

The Oct. 2007 issue of the CPA Technology Advisor awarded Sage MIP Fund Accounting version 8, five out of five stars overall, in the publication's annual review of "Not-for-Profit" accounting systems.

10:00 am – Noon: Sage Fundraising 50

The most cost-effective and complete fundraising management tool. Powerful, yet easy-to-use

Register today by calling Camille Livsey at (860) 524-4465 or via email at clivsey@ttgct.com



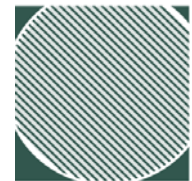
The Technology Group, LLC is proud to be allied with:



Authorized Partner



**SPRING 2008 EDITION OF
BUSINESS TECHNOLOGY QUARTERLY**



at Whittlesey & Hadley, P.C.
147 Charter Oak Avenue
Hartford, Connecticut
06106-5100



PR SRT STD
U.S. POSTAGE
PAID
Hartford, CT
Permit #2639