



ACT Tech Advisor

A quarterly newsletter provided by
ACT Network Solutions of Cary, IL - Delivering Innovative IT Solutions For Over 23 Years

In this issue:

Dealing with Security Breaches

7 Tips for Improving
Wireless Network Security

Terminated employees take
data with them.

Fighting Rootkit Malware

Are Your Terminated Employees Walking Out With Your Data?

A recent survey confirms
exiting workers are taking a lot
more with them than just their
personal plants and
paperweights.

Nearly 60 percent of the
people surveyed admitted to
taking confidential company
information with them,
including customer contact lists
and other data that could
potentially end up in the hands
of a competitor for the
employee's next job stint.

Most of the data takers (53
percent) said they downloaded
the information onto a CD or
DVD, while 42 percent put it on
a USB drive and 38 percent
sent it as attachments via e-
mail, according to the survey.

Eighty-two percent of the
respondents said their
employers did not perform an
audit or review of documents
before the employee headed
out the door and 24 percent
said they still had access to the
corporate network after
leaving the building.

Security Breaches – Protecting your business from hackers and thieves

There's a lot of money to be made hacking computers and so many ways to get away with it! It's the number #1 growth industry in the world. It's not just a bunch of kids working out of their parent's basement anymore. The low cost and high returns of starting such rackets keep the cybercriminals' interest focused on the data that users store on their computers. Because law enforcement almost always stops at national borders, cyber-criminals frequently work with impunity across the globe.

Every type of data has value not just bank accounts and social security numbers. Names, addresses, phone numbers, e-mail addresses, Facebook accounts and even PlayStation information get stolen, sold and then re-sold on the black market.

It's not just criminal organizations from Eastern Europe either. It can be your own employees and trusted partners too. 48% of business security breaches involved insiders and 11% implicated business partners. Everything has a price and if you factor in the quantity and variety of data that's saleable, the dollar figures can be pretty staggering. What's even scarier is that 61% of network intrusions were discovered by third parties NOT the in-house tech staff.

What can you do to protect yourself?

First and foremost, security shouldn't be an after-thought. Unfortunately, too many businesses take the attitude "It won't happen here!" until it does. Don't say you can't afford it. The cost of a breach and the subsequent clean up can dwarf the cost of prevention not to mention the negative blow-back to your reputation in your industry.

Every organization no matter how small should perform security reviews regularly. Don't ever think you're not a target. Everyone is! Whether it's your own information or data you hold about other people, in the business of information theft, everything has value.

Beyond that, your computers could be launching platforms for attacks on other organizations. Industry experts estimate that over 200 million computers worldwide are infected and participating in these networks. What group is the biggest unwitting participant in these BotNets? Not surprisingly, it's schools.

Using your in-house IT staff isn't always the best resource to verify your security because they're too close to the problem. They probably built it. Of course, they're going to say your systems are secure. It's better to have an outsider evaluate your security. They also don't have the breadth of experience to do a proper evaluation.

Where to start?

Two practices that should be in place in your organization are Vulnerability Assessments and Penetration Tests.

Vulnerability Assessments compare all of the intrusions methods available against your ability to react and defend against them. They also determine if you're compliant with security requirements applicable to your organization. Vulnerability Assessments take simple risk analysis further by addressing the ways to reduce any consequences and improving your capacity to manage future incidents.

Penetration Tests put your security to the test by actually trying to get around what you have in place by whatever methods are available. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities. Security issues that are found are then presented together with an assessment of their impact, along with a proposal for mitigation. It's also not just a purely technical project either.

Continued on page 2



Fighting Rootkit Malware

What's a Rootkit?

A rootkit is software that enters your system most frequently from e-mails or via infected web sites. It subverts the operating system functionality to hide and protect itself. Once it is installed, it allows attackers to mask the ongoing intrusion and maintain privileged access to your computer to perform tasks like sending spam, participating in denial of service attacks on other computers or further spreading itself.

It sometimes locks down functions of your computer and makes it nearly impossible to use normally.

Is it different from a virus?

Oh Yes! The way that malware is written has evolved recently and now plays havoc with the anti-virus industry.

Almost all anti-virus software works using a list of "signature files" of known malware. If it finds a piece of code on the list, it attempts to remove or at least isolate it. Now malware can modify itself after every infection to a different signature meaning that a single malware can morph itself thousands of times per day. McAfee recently announced that they find more than 55,000 new malwares each day compared with 5,700 for the entire year of 2007.

How do you fight it?

There's no single anti-malware program that can catch everything so cleaning is very tough. Using a clean-machine specifically designed to isolate infected drives is often the best way to clean off malware and it can be very time consuming.



Security Breaches – cont'd from page 1

A good Penetration Test should include social engineering risk exposures. For example, how easy is it to get information from your employees that might hurt your organization.

Who should perform these tests and evaluations and how often should they be performed? Preferably it should be an outside that provide a fresh perspective. They should have your permission to attack your network with everything that a hacker might use and your in-house staff should not know when the attack will come. It's got to be a surprise to see how your organization will react. There's no point in running a penetration test if everyone is on heightened alert waiting for it to start.

Count on running these evaluations at least every other year if not more frequently.

What are the new hacker targets?

Industry experts believe that portable devices like Smartphones, Tablets, iPads and such are becoming the next big target for hackers. What steps have you taken to secure these devices? If you have to think about it, you're probably already five steps behind in the race to snatch your data. You'd better get busy!

7 Tips for Improving Wireless Network Security

Change Default Administrator Passwords (and Usernames)

This sounds way too obvious doesn't it? You'd be surprised how many times we walk into a new client and discover that all of the wireless settings are still set to the factory defaults.

Change the Default SSID of the access point/wireless router

Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. Change the default SSID immediately when configuring wireless security on your network.

Disable SSID Broadcast

In Wi-Fi networking, the wireless access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may roam in and out of range. It increases the likelihood someone will try to log in to your network once they detect your SSID.

Turn on WPA / WEP Encryption for your wireless network

All Wi-Fi equipment supports some form of *encryption*. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans.

Enable MAC Address Filtering

Each piece of Wi-Fi gear possesses a unique identifier called the *physical address* or *MAC address*. Access points and routers keep track of the MAC addresses of all devices that connect to them. (This may not be practical if you have a large number of users or intend to allow guests to use wireless within your office.)

Assign Static IP Addresses to Devices

Some networkers gravitate toward using *dynamic IP addresses*. DHCP technology is indeed easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from your network's DHCP pool.

Enable the Firewall on the wireless Router

Modern network routers contain built-in firewall capability, but the option also exists to disable them. Ensure that your router's firewall is turned on and properly configured especially if you intend to allow remote access to employees or support staff.

DataVault

Easy to use – Secure 256-bit Encryption - Up to 365 Days of History - Restores lost data in seconds
Secure your critical business data for a little at \$14.95 per month

Try DataVault for FREE for 30 days

ACT Network Solutions
(847) 639-7000

700 Industrial Drive, Suite H, Cary, IL 60013
WWW.WACT4NETWORKS.COM