HOUSTON
BUSINESS JOURNAL
Strictly Houston. Strictly Business.

Vol. 37 No. 3 Week of May 26 - June 1, 2006 houston.bizjournals.com

Unsecured wireless networks create a new frontier for hackers

WIRELESS

TONY MICKLE

Going wireless is a freeing experience, but surprisingly, few businesses take the proper safeguards to protect their data. And the bad guys are good at staying one step ahead in technology.
Already, wireless networks are a goldmine for hackers. Cybercrime cost companies and individuals about $400 billion in 2004, according to the FBI. But just 5 percent of cyber criminals are caught. Just how do hackers go wireless?

They look for an opportunity, and they exploit it. For example, "wardrivers" are people who drive around specifically looking for unsecured wireless networks to access.

If they get within the signal range of your wireless network, they can steal your private business data (such as account numbers and customer records), record the keystrokes you type on your computer, read your e-mail --without getting out of their cars.

What's more, hackers could use your wireless network to illegally download copyrighted music files, send spam (illegal in some countries), or commit other crimes. And if a crime is traced to your network, you could be held responsible.

Experts predict that in the next four years, everyone in the country will either be a victim of ID theft or know somebody who is a victim of ID theft.

AHEAD OF HACKERS

Like any security measure, your plan should always be focused on the proactive. Listed are the top 10 steps businesses can take to make their wireless connection more secure:

Store your data in an offsite datacenter. This is especially important if your business relies heavily on offsite users. The industry-standard is 128-bit encrypted communication. Currently, there is no set security standard for securing wireless networks. One up-and-coming foolproof solution for securing information is called "IsUtility" computing. IsUtility not only uses 128-bit encryption but also never transmits your data (only screen shots at 28 per/second) outside of the datacenter. The formula is simple: If the data never leaves the datacenter hackers cannot gain access to it.

Get help if you need it. Many businesses don't always have the resources needed to maintain a secure wireless network. You can choose from a plethora of IT outsourcers to help you design, implement and maintain security for a wireless network. Who can you trust? The single most important factor when seeking outside help -"A proactive approach." Choose a vendor that is recognized on preventing security breaches from ever occurring in the first place, rather than just a "troubleshooter" that relies on solving problems.

Disable Bluetooth Features. As user-friendly features such as ID broadcasting and "Find Me" features become more prevalent, so will hacking attempts. Like many of today's new mobile advancements, Bluetooth is in its infancy with no real set security standard. The best option to keep your data secure is to tum off unnecessary features or the Bluetooth functionality all together. Few companies look at Bluetooth security seriously. Lack of intemal policies and regulations opens doors for hackers to access sensitive personal data.

Beware of "Remote Access" Solutions. The growing popularity of remote access solutions like VPNs has made accessing the office workstation easier, but not necessarily safer. These technologies give businesses access from outside the office, but create attractive holes in the network for hackers. It's not enough to set up a firewall. Hackers will use any openings in a network they can find to launch attacks and possibly share illegal information using your infrastructure.

Change your device's default password. Wireless access points/routers come with default passwords set by the factory. Once entered, the password gives you access to change the device's settings. Hackers know these default passwords and can use them to access your network and change its settings. To prevent unauthorized access, change the device's password to something difficult to guess, preferably an alphanumeric combination longer than 8 characters.

Change the default SSID. A service set identifier (SSID) is the name used to identify your wireless network. Your wireless access point/ router came with a default, preset SSID. Hackers often look specifically for these preset SSIDs when scanning for networks, because they're considered easy targets. Change the default SSID to something unique right away, and change it regularly.

Never broadcast the SSID. By default, wireless access points/routers broadcast SSIDs, making it easy for legitimate users –as well as hackers --to find and join a wireless network. Configure your wireless devices that require access to the network to automatically connect to your network's SSID without broadcasting it.

Use most current encryption. Encryption is a security feature in your wireless network equipment that can be tumed on or off in software. In essence, encryption translates data into a secret code only the intended recipient can understand. Encryption prevents data from being altered during transmission between a wireless computer or other device.

Configure your wireless access point. This is done by enabling MAC address filtering. A media access control (MAC) address is a unique series of numbers and letters assigned to every network device. This may make it more difficult to give wireless network access to clients, partners or others visiting your offices or locations but makes it much more difficult for hackers to access your network.

Set a wireless policy. Create a clear but simple wireless network usage policy for all your employees. The policy should include guidelines on the use of passwords, personal devices, such as wireless PDAs, and public Wi-Fi hot spots.
A wireless network is only as good as its security. To keep your business growing today and tomorrow, make sure your wireless plan is secure, comprehensive and ***proactive***.

Tony Mickle is Senior Systems Engineer of Houston-based Xvand Technology, provider of IsUtility® (www.isutility.com.) a fully-managed virtual IT department.

This article appeared on page 6 of the TECH-HOUSTON section of Volume 37, No. 3 of the Houston Business Journal on May 26—June 1, 2006. Copyrighted 2006 by the *Houston Business Journal*, 1233 West Loop South, Suite 1300, 713 688-8811, http://Houston.bizjournals.com.