When Corporate Network Safety Starts at Employees' Homes

Protecting Your Network from Home Wireless Hackers

August 2008

Introduction

Remember the good old days of wireless Internet, when we boldly broadcast our SSIDs and happily shared our bandwidth with our neighbors? Sadly, that modern-day Mayberry is gone, as hackers and criminals alike discovered the open back door into our systems and began to relieve us of our personal and business data, email communication, and bandwidth or CPU cycles for their own evil exploits. They even banded together to advertise the open door with "war-chalking" and other types of public notification.

Today, as the lines between home and business computing continue to blur, even enterprise IT administrators need to be concerned with their employees' security practices on their home wireless networks. The last thing you want is for a hacker to compromise an employee's computer via an under-secured home wireless connection, and then quickly and efficiently travel down that handy remote user VPN tunnel straight into your business's network. Not surprisingly, enterprise IT managers are now deploying training on wireless security, specifying wireless router hardware and/or configuration settings, and in some cases, providing firewall/VPN endpoint appliances (managed from the data center) for key employees' in-home use.

Educating employees on the secure use of wireless home networks can be as simple as reviewing the practices of "SAFE WIFI."

SSID Broadcasting "OFF"
Activate WPA2 encryption & authentication
Firewalls (and especially proxy-based firewalls) are best
Employ strong passwords

Web controls
Inactivate "automatically connect to non-preferred networks"
Filter MAC addresses "ON"
IPSec VPN as remote connection to the office

1. SSID Broadcasting "OFF"

There is really no reason to broadcast your home wireless network SSID. Liken it to the risk you take when you put a sign outside your house with not only your last name, but the first names of all who live there. In providing your name and address, and given the ease by which criminals can obtain additional information about you on the Internet, you make a good identity theft target.

It can be helpful to broadcast your SSID during the setup process, especially in more densely populated areas where you may be able to pick up a large number of wireless signals and need to initially distinguish your router's signal from the masses. But most of the time, you'll know yours by signal strength even without SSID broadcast. However, we do expect this situation to get worse once more 802.11n wireless devices make their way into your neighbors' homes, their range can be longer and stronger than the technology being used by most people today. Therefore, once you've associated your computer(s) to the router and set them up to automatically connect to your network, turn your SSID broadcast off immediately to tighten your wireless security. It's a much more daunting task to try to guess your SSID and password, and hackers would be more inclined to pass you up in hopes of finding an easier target.

2. Activate WPA2 encryption & authentication

You will have three standard choices for securing your wireless communications. They are, in order of increasing security: WEP, WPA, and WPA2. Also, of course, you could choose to not enable any of these, and then all it would take is someone with the right "tuner" to pick up your radio signal and "listen in" on all of your communications; or worse yet, to use your wireless signal to hack into your computer and other connected networks.

WEP provides very little protection. It was developed during a time when it was difficult to "tune in" to these wireless networks, and so it did not secure the initial negotiation, making it ineffective in today's wireless world. WPA and WPA2 offer encryption for the initial negotiation as well as the later communication packets, with WPA2 offering stronger encryption. It is generally thought that this encryption is likely to be hacked at some point in the future, but for today's home user, it's a good security option for now.

3. Firewalls (and especially proxy-based firewalls) are best

Most are relying on VPNs and client-based anti-virus (AV) solutions in the home, but they take you only so far in terms of network security. VPNs provide "privacy" but not protection – so unless your packets are getting a good scrubbing by a firewall somewhere in the communication stream, you are unprotected. And, client-based AV is limited in that it is OS-based and as a result is often "turned off" by today's sophisticated malware.

More and more, we are seeing firewalls employed in home networks as an effective way to beef up security. Check to make sure that your wireless router has firewall capabilities, or better yet, add a firewall device in-line for better security. Looking to tighten the wrench one more turn for increased home network security? Then, your firewall should offer "proxy-technology" for true application layer security – a step above standard packet filtering.

4. Employ strong passwords

As processors get faster, passwords need to get longer and utilize more of the standard character set in order to have greater resistance to hacker programs. Today's strong passwords are at least 13 characters, they use upper case, lower case, numbers and symbols; they use nonsense words, and have no direct connection to the user. One example of a strong password would be "When U W1sh upon a St@r"

5. Web controls

Today's hackers aren't just adolescent pranksters anymore. Hackers include organized crime and its big business. Their tactics are sophisticated and they make special efforts to get victims to go to web sites that look real but are fake. Once there, they get you to enter personal information so that they can either steal from you directly or under your name. In addition, you may land on a legitimate web site that has been hacked and installs malware on your computer in a "drive-by download." Almost immediately, the malware disables your client-based AV software, and then it converts your computer into a botnet – using your processing power and information to fuel criminal activity. For all these reasons, it just makes sense to limit where you and family members visit on the Internet.

There are known bad "blacklisted sites," regions of the world and IP addresses, and you can set up your firewall to not allow communication from these places. In addition, some UTM appliances offer URL filtering services that allow you to limit the scope of Internet activities by categories. This is particularly helpful when there are impressionable young minds in the house. Any way that you are able to limit Internet activity to known good areas, will help you to achieve a secure home network.

6. Inactivate "automatically connect to non-preferred networks."

Another way that criminals can gain access to privileged information, and then use it to hack into your wireless network, is by setting up a rogue access point. They place an access point in range of your home and then try to get you to log on to the rogue AP. Usually, if they can reduce the signal of your wireless router enough, and you have "automatically connect to non-preferred networks" activated, then you will likely connect to the rogue without even knowing it. Therefore, to reduce threats from rogue access points, you need to inactivate this setting.

7. Filter MAC addresses "ON"

Another option you have is to set up your wireless router to only allow known computers to connect to the network. It is still possible to "spoof" a MAC address, but again, it's one of those things that makes it just that much harder for someone to hack into your wireless network. You get enough of these annoyances, and you are just too much trouble for the average hacker.

8. IPSec VPN as remote connection to the office

You might ask why hackers would have any interest in your home wireless network at all. It depends. Some specialize in identity and consumer theft; others are after bigger fish – namely, your employer. As more and more employees are working from virtual or remote home offices, and it is perceived that the remote network connection has more lax defenses than other network interfaces, criminals see this is a new opportunity to penetrate the corporate network perimeter in order to reach a bigger payoff. Entire botnet armies are set up to recruit until they find the right path into a target company. For this reason, your home network wireless security and your VPN connection to the network resources both contribute to a safe computing environment. Given the choice between a standard VPN, SSL VPN and IPSec VPN – the IPSec VPN will support the strongest security.

While there is no guarantee for 100% hacker-free security, the "SAFE WIFI" practices package some of the best security that is commonly available with today's commercial products, to make your home wireless network a less attractive target for criminals. However, this is a rapidly changing environment, and you will want to keep the lines of communication open with reputable resources and your corporate IT manager so that you can enjoy the convenience of wireless communication in the home now and in the future.

For more information about WatchGuard security solutions, visit us at www.watchguard.com, or contact your reseller. Better yet, hand this white paper over to your company's IT or Internet security professional and ask them to help you work from home more safely.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

U.S. SALES:
1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD
Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. All products are backed by LiveSecurity® Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.