

Analysts expect that, by the end of 2004, there will be more than one billion wireless devices in use, and over 100 million of them will be connected to the Internet. Source: Wireless Business & Technology magazine, Nov 2002



"Between 60 and 80 percent of corporate wireless networks are insecure" Source: Adrian Wright of Secoda Risk Management

You are looking at a "warchalking" symbol. A notice to wireless hackers that your network is not



Has your company been marked for attack?

The Threat

Wireless LANs face all of the security challenges of a wired network as well as all of the new risks introduced by the wireless medium that connects clients to access points. The analogy has often been drawn that if you have a wireless network that isn't fully protected, you may as well have a network drop in your parking lot for anyone to drive up and use. By implementing wireless technology, you may be offering someone who ISN'T EVEN IN YOUR BUILDING access to your company's most private data. From your wireless access point, the insides of your network are completely vulnerable. At this point, your firewall and intrusion detection systems are completely useless unless you've properly integrated your wireless network into your network defense architecture. Your risks?

- Loss of company data to competitors or criminals. This could include private customer data you are required to protect by law or even your company's trade secrets.
- Drive-by spammers commonly use poorly secured wireless networks to send thousands of non-solicited e-mail. Best case, you are losing bandwidth you've paid for. Worst case, you may be accused of sending spam e-mail.
- An open wireless access point is one of the most common backdoors into your normally secure hard-wired network. In addition to stealing your data, a hacker can quickly upload a trojan horse or backdoor that can be accessed at a later date, from another location.

The Challenge

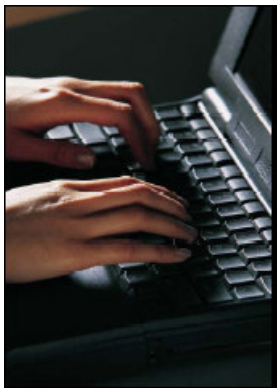
Over the past few years wireless LAN (WLAN) technology has become critical to many business and government IT infrastructures. The freedom afforded by wireless communications, combined with the decreasing costs of the underlying technology, has everyone from CIOs down to network administrators excited about the possibilities offered by wireless. Unfortunately, as that old saying goes "freedom isn't free". The excitement surrounding wireless has led to WLANs being implemented quickly and in most cases incorrectly. Even if some forethought is put into the implementation of a WLAN, current security mechanisms for maintaining the confidentiality, integrity, and availability of wireless communications are insufficient to meet today's corporate security needs. Recent security standards, such as the IEEE 802.1x, attempt to provide solutions to these security defects. However, if improperly implemented, even these new standards are flawed, allowing attackers to perpetrate both active as well as passive attacks.

The Solution

Global Security Consultants offer a wide range of options to aid you in bringing your network to the security posture you require for your business. We use a combination of the latest in commercial and open source technology as well as custom developed software to ensure every aspect of your network is thoroughly tested and evaluated. All of our professional computer security analysts have at least ten years experience in the communications or computer security arena, and all possess advanced degrees in the areas of Computer Science, Computer Networking, and Computer Security.



A firewall costing thousands of dollars can be completely compromised by a single incorrectly configured wireless access point, even when the access point is behind a brick wall.
Source: Network Computing



Anyone with the right equipment and some time to spare can detect and even access your internal traffic
Source: PC Magazine, April 9, 2002

Services Offered

ACCESS POINT DISCOVERY

On site and off site analysis and mapping of all access points and their effective coverages in and around a company's physical premises. This list is compared with a list of company authorized access points to determine unauthorized points of entry into the network. All discovered access points are probed to determine the SSID, MAC address, use of encryption (WEP), and all associated clients.

PENETRATION TESTING

Comprehensive internal and external penetration testing of all wireless networks is conducted in order to identify and document all vulnerabilities and threats. A complete examination of the current security and network infrastructure is also conducted to identify vulnerable areas between wired and wireless networks.

WIRELESS QUALITY ASSESSMENT

A signal strength coverage analysis of the WLAN is conducted in order to ensure maximum performance of the network. Identifies "dead zones" and offers solutions to alleviate them.

SECURITY POLICY REVIEW

A thorough review of the client's overall corporate security policy is conducted in order to identify potential human vulnerability issues.

HARDWARE/SOFTWARE REVIEW

Complete evaluation of current wireless hardware and software setup and configuration is conducted for comparison to industry best practices.

WIRELESS NETWORK / TRADITIONAL NETWORK PROJECT PLANNING

We will provide a detailed project plan outlining expectations, timelines and deliverables to the customer. Customer's current as well as future security requirements are outlined and analyzed.

The Next Step?

Contacting a Global Security Consulting expert is the first step to securing your wireless network. Every customer has different needs and desires. Our consultants will propose an assessment plan based on your current situation. In most cases, an assessment can be scheduled within days. Contact us now for a better piece of mind!

Contact Us

To receive a free quote or for more information about the company, contact us at 888-354-0079 or at info@GlobalSecurityConsultants.net.

