



# WLAN WELL-BEING.

**A PROACTIVE APPROACH PROTECTS SERVERS BEFORE BREACHES HAPPEN.**

In 2005, cyber-criminals penetrated the IT infrastructure of a leading apparel retailer. According to news reports, the perpetrators were able to capture information for as many as 94 million credit card accounts over the following year and a half.

»»»

Incredibly, they did this without physically entering any of the firm's facilities. They gained initial entry by monitoring 802.11 wireless LAN traffic from outside one of the firm's offices. They then broke into the network, still wirelessly, from outside the premises.

Today, Wireless LANs (WLANs) are widely deployed everywhere from conference rooms to coffeehouses. If your company is using a WLAN and hasn't yet secured it properly, now is the time to do so.

## » SPENDING ON SECURITY

It's easy to consider security an expense that doesn't contribute to the bottom line. However, that's an incorrect and dangerous attitude.

Even if it doesn't hit the billion dollar mark, the cost of a security breach to your company is likely to be significant. It can amount to anywhere from tens of thousands of dollars to hundreds of millions of dollars. These costs can include:

- Identifying and correcting security problems, which can include consulting services and new products
- Lost productivity due to missing data, infected systems or employees caught up in fixing security problems or addressing related issues
- Legal fees, notification costs, added call-center requirements, regulatory fines, civil penalties, restitution to impacted parties and paying for credit reports to at-risk customers
- Additional audit requirements
- Additional marketing and PR costs, possibly free or discounted product offers

In addition, a highly publicized security breach may result in, or contribute to, reduced or lost sales, loss of customers and failure to get new ones. And, like any bad publicity, a visible security breach can have a negative impact on the company's stock price.

## » GUARDING THE AIRWAY

Wireless LAN technology is occasionally an afterthought for many companies. "A firm often adds wireless with wired-class security," points out Jon Kuhn, director of product management at SonicWALL.

"There is less oversight on how the wireless product is set up," he adds. "Firms will focus on ease of deployment and fast setup. There is less concern for how employees and others access it, including people outside the building."

A major threat with WLAN technology is that it is so easy to deploy. Therefore, it is also easy to deploy incorrectly, inappropriately and without authorization.

"If someone is doing it officially, within a project, they may look at the security stance and turn on the encryption and authentication," says Bill Jensen, product marketing manager, Check Point Software Technologies. "You want to be sure

that only authenticated authorized devices are taking part in the LAN."

It's easy to buy a WLAN device and install it to provide Wi-Fi capabilities within an office. Therefore, you need a company policy to control what's going on in your network. Make it "automatic" to update your firm's policy when adding to or altering your network infrastructure.

One way to ensure that only authorized devices can access certain elements on your network is to segment your critical data from where people access it. You can do this by having remote users utilize a Virtual Private Network (VPN) for safe network access and communication.

A VPN encrypts data at the sending end and decrypts it at the receiving end. It sends the data through a tunnel that cannot be "entered" by content that is not properly encrypted.

"It is also important to make sure you are using some form of endpoint security," says Jensen. "This should couple with your network security, where you authenticate the device and make sure it has a security posture before access is granted."

SonicWALL network security appliances go beyond the standard authentication steps for wireless users, according to Kuhn. "When a user connects to the WLAN, we run every connection through a series of security engines and do deep-packet inspection on traffic. So if there are any threats, we block them before they go to the main network."

Savvy network security managers also segregate their wireless LAN environments from the rest of the network and interpose additional security in between. "Segment off the WLAN traffic, using VLANs [Virtual LANs] or by hardwiring them on a separate network," Check Point's Jensen says.

## » SECURITY TOOLS

Unlike wired LAN traffic, wireless LAN traffic can be eavesdropped on without detection. As mentioned, these access opportunities can extend beyond physical facilities.

According to published reports, the apparel retailer, noted earlier, was violated by "wardrivers." Wardriving is the act of searching for open Wi-Fi networks by someone in a moving vehicle.

Wireless access points must be protected against "warwalkers" and wardrivers. Dealing with both is essential to securing your WLAN environment.

Data encryption plays an essential role in WLAN protection. Encryption makes security attributes part of the data itself. It protects data while "in motion" and "at rest."

To verify that the WLAN security implemented is actually in place and working, many companies are turning to WLAN monitoring tools. For example, the AirMagnet Enterprise provides a simple, scalable WLAN monitoring solution that enables any organization to proactively mitigate wireless threats.

"Our sensors listen to a wireless network 24x7," says Wade Williamson, director of product management, AirMagnet Inc.

“They proactively look at all traffic to check for threats, and take action if something is found.”

Sensor-based monitoring is essential even when there are no threats, Williamson notes. “You monitor your own traffic to verify your authentication and encryption schemes. The idea is to make sure traffic that should be encrypted is, and to look for vulnerabilities.”

## » SECURING THE SERVERS

Today’s servers hold both important and often sensitive data, as well as applications. Therefore, it’s essential that they be secured. This is particularly true of machines housing mission-critical applications and confidential data.

Securing servers includes keeping out unauthorized users or unauthorized activities by authorized users. It also includes blocking malicious code and hostile programs.

Firewalls can provide a good first line of defense against attacks on servers from outside the network. They are designed to prevent unauthorized access to a private network via the Internet.

Firewalls can be in the form of software or hardware appliances. The firewall examines all traffic as it enters or leaves the network and blocks messages that don’t meet specific criteria set by the user.

Network Access Control is another security approach for controlling an endpoint’s ability to access the network. It works with your network’s directory services to authenticate users and their level of access. And it validates each user’s computer as complying with security policies and configurations.

Some IT experts encourage adding on extra layers of server security beyond antivirus and firewall. “We’re seeing more

companies putting dedicated intrusion prevention in front of their servers,” says Brian Krause, security specialist with CDW.

Krause also recommends looking at event logs on a frequent basis. “Many of the Security and Incident Management [SIM] products, like Cisco Security Monitoring Analysis and Response System [MARS], RSA enVision and Symantec Security Information Management [SIM], give you a centralized source for event logs,” he says.

“By looking at the event logs off the servers, you can see what a problem is,” he adds. “You can then react to it and see what needs to be hardened.”

## » PROACTIVE APPROACH

The changing nature and degree of today’s security threats are causing more companies to take a proactive approach. In short, they are staying ahead of the curve and proactively protecting the organization.

Additionally, customers, business partners and regulatory agencies are demanding greater accountability and compliance. So security now isn’t just an internal concern, it is part of your competitive positioning.

Today, vendors can help calculate your network security risk profile. They can show you ways to overcome vulnerabilities with technology solutions that protect the network and the business.

This can include helping IT with the tools to demonstrate the business value of security solutions to management. It can also help to ensure that security solutions stay comprehensive and up-to-date.

“Our new proactive security approach includes promoting security and vulnerability assessments,” states Stan Oien, sales

## WLAN SECURITY BASICS

Wireless Local Area Networks (WLAN) bring fundamental changes to business data access and communication. It offers convenient alternatives to the way we work. There are, however, a number of issues that anyone deploying a wireless LAN needs to be aware of, according to Craig J. Mathias, a principal with Farpoint Group advisory firm.

1. **Security Policy** — You need to have a security policy that defines what sensitive data is, what data should be protected, who should have access and what to do if you have a breach.
2. **Encryption** — Make sure that any sensitive data is encrypted anywhere it resides, whether on a server or a mobile device.
3. **Strong Authentication** — The user must prove who they are to the device, to the network and to the server that holds the data.
4. **Authorization** — Use Active Directory, Remote Authentication Dial In User Service (RADIUS) or other directory services to control what functions can be executed by an authenticated user.

For wireless LANs and devices, “Always turn on wireless security,” Mathias stresses. “WPA [Wi-Fi Protected Access] or WPA-2 is easy to turn on. In addition, always implement the upper layers of security, like 802.1x and a VPN [Virtual Private Network].”

In buying a WLAN, be sure to get your firm’s operations people involved in the purchase process. “Get them involved in advance,” Mathias advises. “That way they can look at the operational expense, since it’s a lot more than the hardware cost.”

Mathias also suggests the use of firewalls, virus-checking and other standard security products. Follow those general guidelines and keep things up to date.

Other basic, but important, security “to do’s” include:

- Modify default installations, for example, reset admin and other passwords.
- Define clear security policies, including use (and restrictions) regarding personal/appropriate web access, personal use of e-mail and corporate and public messaging services.
- Train users to recognize — and respond correctly to — “social engineering” attacks. Social engineering is the art of manipulating people into performing actions or divulging confidential data.
- Don’t neglect physical security, for example locking doors, video monitoring, securing servers and storage.
- Promote user security awareness and do user training.

manager, CDW. “We work with businesses to design security into their networks.”

Although security is often viewed as an impediment to business, it can just as easily be seen, and engaged, as an enabler. In short, proper security can be used to advance business strategy.

For example, a wireless LAN environment that’s been secured can allow a retail company to provision floor staff with wireless tablet notebooks. The PCs can be used to facilitate the entire purchase transaction, and not just do product information look-up.

A properly secured server, and integrated network environment, can let database managers, application developers, IT hardware admins and others get the appropriate degree of remote access, resulting in greater system availability and staff productivity.

Security tools can also deliver non-security benefits. Web-filtering tools can help with bandwidth management. And wireless LAN monitoring tools can be used for remote performance troubleshooting, thereby reducing the need for onsite diagnosis and repair.

## » USE POLICIES

Just as with other network components, a multilayered security approach to WLAN protection is considered most effective.

“Implement defense in layers,” says Tracy Hillstrom, senior product manager, WatchGuard Technologies Inc. “Be sure you are using an encrypted path from start to finish. Think through your network architecture that way.”

“Segment your servers and put them on their own LAN segment,” suggests Check Point’s Jensen. “And protect this segment with a VPN and firewall.”

“Securing a WLAN against eavesdropping or intrusion isn’t that difficult,” says Martha Vazquez, research analyst with the market analysis firm Frost & Sullivan. “You need to be aware of the security tools and implement them.

“Many of the recent attacks were done to WLANs using older encryption,” she says. “Attackers could read the wireless traffic, get the encryption keys and get the records. And once you get the key, you can get into the back end of the system.

“Use better encryption, and have Wireless Intrusion Prevention Systems [WIPS],” she adds. “Then you know the rogue access devices you were being connected to.”

Businesses are finding that when it comes to security, their work is never done. This is because threats keep changing and multiplying. In other areas of IT, for example, when you install network hardware, you’re done.

“You have to be prepared to deal with new security challenges every day,” says Craig R. Mathias with the Farpoint Group advisory firm. “And remember that while reports can show you’re compliant, there are lots of other things that can go wrong without the monitoring system ever noting it.” ♦



LET CDW HELP WITH A VARIETY OF SECURITY SOLUTIONS GEARED TOWARD CURRENT AND FUTURE NEEDS.