

Information Security in the Internet Age Securing Wireless Networks

Executive Overview

Wireless networks are becoming more and more critical for business operations. They provide flexible connections that allow users access to crucial information at any time and at any place. The comparative ease of deployment makes them an attractive alternative to the traditional wired network, providing the added benefit of lower installation costs. However, an insecure wireless LAN can create one of the biggest security vulnerabilities in a corporate network. Proper design, deployment and policies are a must.

This paper describes how wireless networks can be a security threat and what measures can be taken to mitigate those threats:

- Assessing the environment for unknown or miss-configured wireless access points
- Establishing a wireless security policy
- Determining wireless requirements and appropriate architecture for your business

Introduction

Wireless networks are an inexpensive method to increase access to your network resources. However, it is an often overlooked fact that the boundaries of the wireless signal do not end within your building. If there is valuable data to be protected precautions need to be taken with the wireless network design.

A recent example: new laptop equipment can come with built-in wireless capability that is part of the default configuration. When added to a physical network connection, an insecure access point in your network may be established. Employees often are not aware of the security risk created by adding a wireless access point to your network and may do so without proper approval or security measures.

Most wireless networks are not adequately protected, as the following excerpts illustrate:

Most people with PDAs and phones don't use built-in security features . . . If a device is lost or stolen, all the information on it can be accessed by someone else.

The 802.11 family of specifications used for wireless LANs relies on a protocol that has been broken. Without the proper security measures in place, a wireless LAN can be accessed by anyone with cheap equipment and hacking skills.

- CIO Magazine

'Flaws in Wireless Security Detailed' Hackers can often park their cars in a company's parking lot and simply "become a node" on the firm's wireless network - known as authentication spoofing . . . Hackers can travel the entire length of Market Street in San Francisco "and basically not lose 802.11 coverage" while picking up wireless LAN signals.

One of the most significant problems found in the WEP algorithm includes weaknesses in the way WEP encrypts packets of data using a stream cipher. Through a series of computations, hackers can eventually uncover the plain text of certain encrypted messages and use those packets to intercept and decrypt messages encrypted with the same key, which is known as an Initialization Vector packet collision.

- Computerworld

Using a technique known as "War Driving", hackers can drive by your place of business and locate your network from a distance, making it unlikely that you will ever notice their presence. In some cases, on poorly secured networks, they can observe network traffic, and interfere with your wired network, while sitting unobserved in a location that is surprisingly distant from your office area.

AsTech Consulting can perform a security assessment that includes scanning for unknown wireless networks and/or determining the level of security present on a current wireless network.

Mitigating the Risk

While there are known security flaws with wireless encryption (WEP), with the right combination of security tools, you don't have to put the brakes on your wireless installation to remain secure.

Security is a critical step in the initial deployment of a wireless network. Without proper attention during the design phase of a wireless deployment, a wireless network can be nearly impossible to secure, as "add-on" security is never truly as effective. Using a number of different risk assessment methods, Astech Consulting can help your business determine what type of security is needed on its wireless deployment. Depending on the type of business, and the amount and classification of data passing over the wireless network, a security design that fits your organization can be created. In some cases it may be sufficient to use standard WEP encryption, while others will require a full VPN/firewall solution. A thorough understanding of your security needs **before purchasing and deploying** will save money in avoiding costly security incidents and redesigns in the future.

The second step in creating a wireless network is getting to know the deployment environment. Signal strength is often an issue, and each location poses its share of challenges, whether it be thick concrete walls, or interference from other sources in the workplace and other equipment nearby. This is where Astech Consulting's experience with wireless network deployment can help. Our familiarity with building networks in

complex, large-scale environments will result in better designs that can simultaneously cut down on the cost of access points and also provide extra security by limiting the wireless signal, keeping it out of reach of insidious hackers.

Wireless Security Tips

- **Disable broadcasting on network hubs**
- **Change default names**
- **Don't give the network a name that identifies your company**
- **Move wireless hubs away from windows**
- **Use the built-in encryption**
- **Disable the features you don't use**
- **Put a firewall between the wireless network and other company computers**
- **Regularly test wireless network security**

Wireless Security Policy

An important final step in a wireless deployment is to update existing security policies to include wireless technology. Provisions pertaining specifically to wireless networking should be included in every security policy, whether a wireless network deployment is planned or not. The low cost, and ease of use make wireless access points a tempting alternative for employees to deploy on their own. Adding a provision to forbid this kind of activity is an important part of educating network users on the danger of a poorly implemented wireless network. Additional considerations for a wireless security policy include key rotation, distribution and strength guidelines. Astech Consulting has years of experience in preparing practical security policies that enhance your company's mission, and can help you design a security policy for your environment that makes sense.

Summary

A wireless network can be a great asset to a company, both in productivity and low cost growth; however, the lack of security inherent in any poorly designed wireless network can be a company's biggest weakness. Hackers are looking for poorly secured wireless networks, just as they search for poorly secured web sites, to gain unauthorized access to a target network. Using a multiple step process of assessment, design and deployment can help customize a wireless network that's appropriate for any enterprise.

Astech Consulting offers a comprehensive wireless network strategy that encompasses not only excellent design, but design with security as a primary focus.