Manager's Guide to Wi-Fi security policies

By SearchCIO.in

SearchCIO.in

The wide-spread adoption of Wi-Fi networks and their growing demand despite their misuse by terrorist groups has placed a significant importance to Wi-Fi security policies by the enterprises and mid-sized companies in India.

This Manager's Guide to Wi-Fi security policies covers the following topics:

- **Legal implications of leaving Wi-Fi unsecured**
- **Wi-Fi security policies: Key aspects to incorporate**
- **Wi-Fi encryption standards**
- **Wi-Fi security tools**
- **Common Wi-Fi encryption terms**
- **Further reading**

Legal implications of leaving Wi-Fi unsecured

When an organization leaves its Wi-Fi network unsecure, the most obvious outcome can be loss to its business and damage to its reputation. But there are legal implications too.

The following examples can illustrate why having rugged Wi-Fi security policies is a must for every organization.

In 2010, a Wi-Fi user in Germany was fined because his unsecured connection was used to illegally download music while he was away on vacation.

In Britain and Finland, among others, new laws are being proposed that can make the user responsible for any illegal use, particularly illegal downloads, made using their Wi-Fi connection.

In March 2010, a court in Netherlands dismissed criminal charges against a hacker on the grounds that he had hacked into the Wi-Fi router, and not a computer.

An organization, which has not implemented appropriate Wi-Fi security policies, may be held responsible by courts in case

any component of its Wi-Fi network is hacked into and misused.

The threat of legal action, thus, makes it imperative that Wi-Fi security policies be formulated and implemented with seriousness by every Indian business, small or large.

Wi-Fi security policy: Key aspects to incorporate

Wi-Fi is an evolving technology and hackers continue to experiment with new methods to infiltrate wireless networks. A number of security policies have been identified to keep Wi-Fi security risks to the minimum.

Monitor the network for intrusions:
As Wi-Fi evolves, hackers remain on the lookout for new bugs to exploit and new methods for breaking into secured networks. It is important to constantly monitor the network for hacker activity, including scanning for rogue access points and brute force attacks, as part of your company's Wi-Fi security policies.

Use encryption:
A number of encryption protocols are available to scramble messages and make them unreadable to humans. Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are encryption protocols promoted by the Wi-Fi Alliance. Note that all devices on the network will need to use the same encryption protocol to make the Wi-Fi security policies work for you.

Use strong login passwords:
As simple as it may sound, a strong password is an effective

guard against basic ‘brute force’ hacking techniques. Brute force hacking involves repeatedly entering simple passwords (first names, birth dates, telephone numbers, words from a dictionary, etc.) to break into a user account. Note that simple passwords remain popular among users, despite the known risks.

Control Wi-Fi signal spillage:
Ensure that your Wi-Fi network signals don’t spill out of the premises into the street or surrounding buildings. Split signals can potentially allow anyone in the vicinity to access your corporate Wi-Fi network, and thus compromise the Wi-Fi security.

Restrict internet use on public Wi-Fi networks:
Advise your employees not to use public Wi-Fi services on company provided laptops / PDAs. Endpoint protection must be incorporated as a critical aspect of your security policies. Online transactions, instant messages, emails, and other documents sent over the net are all open to eavesdroppers and phishers.

Other precautions:
If it is absolutely necessary for any of your employees to use a public Wi-Fi network for business transactions, they must make sure that the websites used are encrypted (they use

the HTTPS protocol), and that the firewall security is turned on at all times.

As a policy, turn Wi-Fi off when not in use. Shutting down Wi-Fi networks avoids the need for constant monitoring and strengthens security by reducing the risk of attack. Turning Wi-Fi off on Wi-Fi enabled devices when not needed keeps the device safe from intrusions.

Wi-Fi encryption standards

Data encryption is a necessary security step when sending data over a network. The Wi-Fi data encryption standards are listed below.

WEP

Wired Equivalent Policy (WEP) was the original encryption created for Wi-Fi devices. It is the most common, but least secure encryption available. It is supported by a wide range of devices, particularly early Wi-Fi devices, and continues to be popular. It is unsafe even when properly configured and set up. The use of WEP is not recommended.

WPA

Wi-Fi Protected Access (WPA) was introduced to remedy the weaknesses in WEP. WAP uses the TKIP protocol. WPA-TKIP remains secure and reliable, although over time vulnerabilities have been found in TKIP.

WPA2

Wi-Fi Protected Access II (WPA2) is the most secure Wi-Fi encryption available currently. It uses a new algorithm based on AES which is considered much more secure than TKIP.

Both WAP and WAP2 can be implemented in PSK mode for personal and home use, and EAP/RADIUS mode for enterprise use. Note that PSK is not adequate for business or enterprise use.

WEP is now considered outdated and is not recommended for use. WPA and WPA2 remain in use, with the latter being preferred. Note that WPA2 will not work with hardware manufactured before 2006.

Wi-Fi security tools

Wi-Fi security can be compromised at many different touch points, and a number of tools have been developed to guard these different vulnerabilities.

The major categories of Wi-Fi security tools include AP discovery tools, connection managers, traffic analyzers, packet sniffers, intrusion detection and prevention systems, Wi-Fi site survey tools, endpoint security clients, vulnerability scanners, assessment tool kits, and more. Make use of appropriate options to make your Wi-Fi security policies work.

Wi-Fi security vendors include AirMagnet (Fluke Networks), AirTight Networks, Bluesocket, Cisco Systems, HP, and Motorola, among others. The major vendors package many of the security tools mentioned above into their Wi-Fi security suites.

Apart from these security tools, a number of Wi-Fi security auditing or penetration testing tools are available. They simulate hacking / attacks to detect vulnerabilities in a given Wi-Fi network to help frame the appropriate security policies. These include devices such as the Silica Immunity

and Portable Penetrator, and software tools such as CORE IMPACT Pro and Ethereal.

A number of pen drive or LiveCD Linux distributions have also emerged for penetration testing. They come with pre-installed penetration testing tools. Examples include BackTrack, PHLAK, Pentoo, nUbuntu, Puck, and others.
As a policy advice, it is recommended to run a security audit on your organizational Wi-Fi network to ensure that it can stand up to a hacking attack.

Common Wi-Fi encryption terms

AES: Advanced encryption standard. Used in WAP2.

CCMP: Counter mode with cipher block chaining message authentication code protocol (A derivative of AES).

EAP: Extensible authentication protocol. A number of variations exist, such as EAP-TLS, EAP-SIM, LEAP, etc.

LEAP: Lightweight extensible authentication protocol, a variation of EAP developed by CISCO Systems.

RADIUS: Remote authentication dial in user service.

TKIP: Temporal key integrity protocol

Further reading

Definition from whatis.com: What is wireless protected access?

Tutorial: Guide to wireless security

News: Mumbai's Wi-Fi enabled businesses have no security policies

Tip: Demystifying wardriving

Tip: Advice on Wi-Fi network security policies

Tip: Enabling the best WiFi security for SMBs

Tip: Controlling embedded Wi-Fi device access

Tip: How to counter wireless threats and vulnerabilities

Answer: Be aware of Wi-Fi security to deal with Firesheep at public hotspots