FIVE WIRELESS SECURITY BANDITS

A common vulnerability in wireless networks is in their ability to create unexpected connections that can result in security gaps. Here are five common wireless security bandits to watch out for:

1. **The rogue access point (AP).**

   A rogu is an unauthorized access point connected to your wired network, generally connected by someone in your organization trying to set up do-it-yourself wireless service. Although rogue access points are usually installed innocently enough, they can provide an unsecured gateway right into the heart of your network.

2. **The ad-hoc client.**

   Ad-hoc mode is the ability of wireless devices to connect directly with other wireless devices without accessing an access point. If a computer on your wired network sets up an ad-hoc wireless connection to another computer, that other computer can gain access to your network through the ad-hoc computer.

3. **The out-of-compliance access point.**

   Older access points that have not been updated to the latest firmware release may open your network to hackers. Keeping all the equipment on your network up to date with firmware releases will protect your network from attack to known vulnerabilities. Not doing this can weaken security and reduce network performance. Out-of-compliance access points tend to be a problem in organizations that do not have a security policy that addresses keeping all equipment up to date on their firmware releases.

4. **The mis-associated client.**

   This is a problem, not with your wireless network, but with nearby wireless networks. When a wireless client has more than one wireless network to choose from, it may accidentally connect to the wrong network. This kind of mis-association, especially if it’s by a laptop also connected to your wired network, creates a security breach. Although mis-association is usually accidental, a hacker may deliberately create a decoy wireless network that looks like yours in order to fool users into logging on. This connection then allows the hacker to steal passwords and attack your wired network.

5. **The non-traditional wireless device.**

   It's easy to focus on laptop computers and forget about other wireless clients such as personal Bluetooth® devices, cell phones, bar-code readers, and printers that may also use your wireless network. All these devices are vulnerable to cracking and may present an entry to your network to an enterprising hacker.

Your best defense against these common security bandits is a that includes network access control, regular site surveys, and a consistent, up-to-date security policy. A makes planning and enforcing network security far more efficient than in "traditional" wireless networks with autonomous access points. Managed systems can often be set to independently handle tasks such as network access control and rogue mitigation, making life far easier for time-stressed IT managers.

Source: https://bboxblog.wordpress.com/2011/10/06/five-wireless-security-bandits/#more-1656