

Wireless: The Airborne Killer

Digital security concern and uncertainty are commonplace in today's times. Technology is advancing rapidly and regulations are trying to play catch-up. Amidst this fast-paced environment of growth, it can be both confusing and difficult for organizations to protect their information assets. As a result, the basics of security are often neglected. A good example of this can be seen in wireless networks today.

Wireless networks are flexible, transparent and portable. The wireless market today offers price-flexible options for all possible business needs ranging from speed to coverage-area.

There is, however, no such thing as a free lunch. With all its attractive advantages, wireless networks are today the Achilles Heel of organizational security. The wide and transparent availability of wireless networks means that the attack surface, for an attacker to exploit, is that much more. Essentially, an organization's wireless network can become the realm for a perfectly silent attack which could affect reputation, bring lawsuits and eventually put the organization out of business.

There are some vivid examples of security incidents where wireless protection was compromised. Some of them that were widely made public are (*references: Chris Waters, NetworkWorld.com and The Wall Street Journal*):

- **SAM's Club**, where hackers utilized the wireless network to cause a security breach that exposed credit card information belonging to an unspecified number of customers who purchased gas at the wholesaler's stations for almost 2 months.
- **BJ's Wholesale Club**, where the store agreed to implement a comprehensive data-security system and undergo biannual security audits for the next 20 years under a settlement with the Federal Trade Commission (FTC). The FTC found that the company did not use readily available security measures to limit access to its computer networks through wireless access points on the networks.
- **PG&E**, where a consultant utilized the wireless network to gain unauthorized access to obtain sensitive computer files related to a contentious battle with a municipality.
- **Lowe's**, where hackers utilized the wireless network from the store's parking lot to obtain customer credit card numbers.
- **Wake Forest University School of Medicine**, where a hacker was able to obtain confidential patient files via its wireless network.
- **GE Money**, where a bank employee utilized his unauthorized access to the wireless network to steal funds from online bank accounts.

So how do wireless networks really work? Wireless networks use radio signals that carry data through the air. Wireless nodes communicate with devices on the network, and with each other, by periodically announcing their signal. Clients wishing to connect to the network latch on to this signal and existing clients on the network refresh their signal.

Mitigating the risk of wireless attack

Let us discuss some of the bare-minimum measures that can significantly reduce the risk of your organization falling prey to a wireless attack –

- 1) **Use wireless ONLY IF really needed:** Sure, wireless networks are relatively inexpensive, easy to install and more portable than a wired network, but unless your organization really needs it, use a wired network.
- 2) **OK, so you need it; well take care of the basics:** These are basic elements that any wireless network, independent of size and scope should first address:
 - **Infrastructure vs. Ad-Hoc mode:** A wireless network can exist in either ad-hoc (peer-to-peer connection) or infrastructure (clients connecting to a central access point) mode. The ad-hoc mode allows any wireless connection, while the infrastructure mode demands connection configurations to a network name, or SSID. Ad-hoc mode is almost never recommended, due to the fact that any client that can see that wireless communication can establish a connection with it.
 - **Lock down and manage Access Points:**
 - **SSID:** While utilizing the infrastructure mode, proper configuration of the Service Set Identifier (SSID) should occur. Disable the broadcasting feature so that random network searches cannot be performed. Allocate non-significant names, particularly not the default ones, as the SSID so that clients will need to know the specific SSID in order to connect.
 - **Filtering Client MAC Address:** Filtering the MAC addresses of the client stations determines who can connect to the access point of the network. A downside is that on large networks, administration of the excessive MAC address lists makes it almost impossible to manage. In addition, a MAC address can also be sniffed and acquired by attackers, who can then impersonate access. For larger companies, a more complex filtering and authentication service is recommended, via the implementation of RADIUS, which is covered below.
 - **Implementing RADIUS (Remote Authentication Dial-In User Service):** RADIUS is a client-server protocol that enables remote wireless clients to authenticate in a central database, thus making it more viable and efficient to manage policies and authorization schemas. A downside of RADIUS is its implementation complexity and associated effort.
 - **Enable Encryption and Authentication (at least WEP - Wired Equivalent Privacy):** WEP is a standard that offers optional password authentication while establishing a connection using a network's SSID. In other words, if the SSID is WEP-enabled, the client will need to first authenticate with a 40 bit – 128 bit encryption pass-phrase. However, contrary to common misconception, WEP just offers the same security as *unencrypted* data over a wired network. It only operates on the data-link and physical layers of the OSI (Open Systems Intercommunications) Model and hence does not provide end-to-end security. There are many ways to crack WEP pass-phrases; however it is better than no encryption at all.

3) **Establish Policies and promote Awareness and Training:** After covering the basics and deciding on the encryption method, it is necessary to implement and enforce specific policies that address access and deployment procedures, physical and logical security, incident management, password policies and user management. Conduct regular security awareness and training sessions for both systems administrators and users. An educated user will often be a compliant one, not to mention a less-protesting one.

4) **Monitor your network:** An organization needs to keep an eye on its wireless traffic and ensure proper protection against potential breach attempts.

- *Deal with the Rogue Access Points:* A basic mitigation control for this would be to conduct extensive site surveys regularly to determine the location of all access points. Additionally, control radio frequency with directional antennas and ensure that all SNMP (Simple Network Management Protocol) community passwords are disabled on access points. Finally, implement a forced periodic re-authentication for connected users.
- *Intrusion detection:* WLANs should have their wireless-specific IDS (Intrusion Detection System) in place, one that is specifically designed to identify attacks to the networks. There are a number of good wireless-IDS products available in the market today.

5) **Don't underestimate Physical Security:** Due to their size, wireless network access points and client devices are prone to theft, often exposing sensitive information and even configuration information that can further expose your wireless network. It is a good idea to enforce adequate physical security on such devices by controlling and monitoring inventory, and also utilizing device-independent authentication in order to control a lost/stolen device's authentication to the network.

6) **Assess and test your network periodically:** Like any other system or network element, wireless infrastructures should be periodically assessed for vulnerabilities. Doing this will keep your network up-to-date on the latest threats and exploitation routes. Also conduct periodic network penetration testing and ensure that the administration team promptly addresses any issues found.

Wireless networks are soft targets for hackers today. Flexibility comes at a cost. Securing wireless networks is essential if you plan on using them. Don't be the next victim to feed the headlines on a wireless network compromise!

Georgios Mortakis, CISSP, CISA, QSA, is an Information Security Consultant Manager with Enterprise Risk Management, one of the leading providers of IT Security, Risk Management and Compliance services to local, national and international businesses. He can be reached at gmortakis@emrisk.com.