



January 10, 2007

Rapid Growth Of Municipal Wireless Deployments Opens Back Doors To Corporate Data

Atlanta, GA - AirDefense, the innovator that launched the wireless LAN security market, recently warned corporations that record numbers of municipal wireless deployments across the United States have opened a back door for hackers and unauthorized individuals to access corporate data, files and proprietary information because of sub-par security policies currently in place.

Corporate network administrators face a variety of challenges. Not only do they have to enforce their own wireless network policy to keep hackers off their corporate network, but they also have to deal with employees who intentionally or unknowingly log onto municipal access points in violation of a company's wired/wireless access policy.

Recent data from industry analyst firm Allied Business Research (ABI) suggests an explosion in wireless deployments is occurring. ABI recently reported that municipal Wi-Fi network coverage worldwide will increase to 126,000 square miles by 2010, representing an 84x increase from the 2005 coverage of 1,500 square miles.

“Today, more and more corporations find their airspace invaded by free, unsecured and pervasive Wi-Fi offered by a growing number of cities across the country,” according to Dr. Amit Sinha, chief technology officer, AirDefense. “For all the advantages that municipal Wi-Fi offers, any employee can bypass wired security and policy enforcement mechanisms by simply connecting to the internet through a readily available municipal Wi-Fi access point. This simple fact makes protecting corporate information extremely difficult.”

Network administrators can take the following precautionary and preventative steps to help protect corporate data:

- Think Defensively About Muni Wi-Fi Networks – Muni Wi-Fi networks with free access are breeding grounds for hackers looking to get into a corporate network by linking to the laptop of an unsuspecting user. Security should never become an afterthought at any level and it is critical to take all necessary steps to keep proprietary information in the hands of employees and not hackers.
- More is Better Than Less - Corporate firewalls, personal firewalls and VPNs do not provide enough protection against municipal Wi-Fi attacks because they are designed to protect data in transmission or against a direct attack on a computer. Municipal Wi-Fi attacks are similar to Phishing attacks in that the user is tricked into believing they are dealing with a reputable dealer online. In the case of municipal Wi-Fi attacks, users believe they are using legitimate access points when in fact a fraudulent access point has been created. More intensive security measures such as wireless intrusion protection systems

and end point security and policy enforcement steps should be taken to prevent corporate data from falling prey to hackers.

- The Weakest Link – Laptops and other wireless devices provide the least amount of security and are typically the weakest link in a corporation's security infrastructure. It is essential to realize that these mobile devices are extending the edge of a corporate network making it appealing to a hacker. Ensure that all wireless devices have activated their internal firewall and wireless access policies are monitored and enforced centrally.
- Restrict Access on the Corporate Wireless Network - To prevent other wireless devices from connecting to your network, specify what devices are allowed on the network and restrict all others using centralized wireless monitoring.
- Enforce A Strict No Muni Wi-Fi Policy – Employees will try skirting the no municipal Wi-Fi policy in place at their company by looking for municipal access points from which they can day trade, play or shop online, or send corporate information over private email accounts – reducing productivity and opening a back door to corporate secrets. It is critical to enforce a strict employee policy against using municipal Wi-Fi service during work hours or while traveling on company business using any wireless devices. Such enforcement is only possible through the use of dedicated wireless monitoring and intrusion prevention systems.
- Install Free Software from Wireless LAN Intrusion Prevention/Detection Vendors - Several products are available from software companies such as AirDefense that centrally monitor the airwaves for wireless risks and can be used to effectively define and enforce wireless access policies. To download a free version of AirDefense Personal Lite, log onto: <http://www.airdefense.net/products/adpersonal/index.php>.