Feature: Delivering Secure Wi-Fi

Submitted by: Nuvias (Wick Hill)
Wednesday, 4 January 2017

Tony Evans from Wick Hill (https://www.wickhill.com/) (part of the Nuvias Group) highlights the risks of Wi-Fi and provides some advice for delivering a secure hotspot

The fact that Wi-Fi stands for Wireless Fidelity hints at how long Wi-Fi has been around, but it was only in 1999 that the Wi-Fi Alliance formed as a trade association to hold the Wi-Fi trademark, under which most products are sold. Today, Wi-Fi is on the top of the list of must-haves for businesses of all types and sizes. People will simply vote with their feet if good and, usually free, Wi-Fi is not available.

But this demand for anytime, anyplace connectivity can mean that some of us are prepared to jump onto Wi-Fi hotspots at cafes, hotel, airports or company guest networks, with only a fleeting consideration of security – a fact that has not gone unnoticed by cyber criminals. There are over 300,000 videos on YouTube alone explaining how to hack Wi-Fi users with tools easily found online.

Risks from unprotected Wi-Fi:

Wi-Fi Password Cracking

Wireless access points that still use older security protocols such as WEP, make for easy targets because these passwords are notoriously easy to crack. Hotspots that invite us to log in by simply using social network credentials are increasingly popular, as they allow businesses to use demographic information such as age, gender and occupation to target personalised content and advertisements.

Eavesdropping

Without encryption, Wi-Fi users run the risk of having their private communications intercepted, or packet sniffed, by cyber snoops while on an unprotected network.

Rogue Hotspots

Cyber criminals can set up a spoof access point near your hotspot with a matching SSID that invites unsuspecting customers to log in leaving them susceptible to unnoticed malicious code injection. In fact, it is possible to mimic a hotspot using cheap, portable hardware that fits into a backpack or could even be attached to a drone.

Planting Malware

There are common hacking toolkits to scan a Wi-Fi network for vulnerabilities, and customers who join an insecure wireless network may unwittingly walk away with unwanted malware. A common tactic used by hackers is to plant a backdoor on the network, which allows them to return at a later date to steal sensitive information.

Data Theft

Joining an insecure wireless network puts users at risk of losing documents that may contain sensitive information. In retail environments, for example, attackers focus their efforts on extracting payment details such as credit card numbers, customer identities and mailing addresses.

Inappropriate and Illegal Usage

Businesses offering guest Wi-Fi risk playing host to a wide variety of illegal and potentially harmful communications. Adult or extremist content can be offensive to neighbouring users, and illegal downloads of protected media leave the businesses susceptible to copyright infringement lawsuits.

Bad Neighbours

As the number of wireless users on the network grows, so does the risk of a pre-infected client entering the network. Mobile attacks, such as Android's Stagefright, can spread from guest to guest, even if the initial victim is oblivious to the threat.

Best practices

There are established best practices to help secure your Wi-Fi network, alongside a drive, from companies such as WatchGuard (https://www.wickhill.com/products/vendors/detail/28/Watchguard), to extend well-proven physical network safeguards to the area of wireless, providing better network visibility to avoid blind spots.

Implementing the latest WPA2 Enterprise (802.1x) security protocol and encryption is a must, while all traffic should, at a minimum, be inspected for viruses and malware, including zero day threats and advanced persistent threats. Application ID and control will monitor and optionally block certain risky traffic, while web content filtering will prevent unsuspecting users from accidentally clicking a hyperlink that invites exploitation, malware and backdoors to be loaded into your network. The use of strong passwords, which are changed frequently, should be encouraged, along with regular scanning for rogue Access Points (Aps) and whitelisting MAC addresses, when possible.

WatchGuard's latest cloud-managed wireless access points also have built-in WIPS (Wireless Intrusion Prevention System) technology to defend against unauthorised devices, rogue APs and malicious attacks, with close to zero false positives.

While WIDs (Wireless Intrusion Detection Systems) are common in many Wi-Fi solutions, WIDs require manual intervention to respond to potential threats. This may be OK for large organisations with IT teams that can manage this, however WIPs is a fully-automated system, which makes it far more attractive to SMEs and organisations such as schools and colleges.

Using patented, Marker Packet wireless detection technology, WatchGuard WIPS differentiates between nearby external access points and rogue access points. If a rogue access point is detected, all incoming connections to that access point are instantly blocked. WIPS also keeps a record of all clients connecting to the authorised access points, so if a known device attempts to connect to a malicious

access point, the connection is instantly blocked. WIPS will also shut down denial-of-service attacks by continuously looking for abnormally high amounts of de-authentication packets.

Wi-Fi as a marketing tool

While Wi-Fi networks have traditionally been viewed as part of the IT infrastructure and the responsibility of the IT department, the latest Wi-Fi systems deliver more than just connectivity, which makes them an attractive proposition for customer services and marketing departments.

For example, the WatchGuard Wi-Fi Cloud provides visibility into marketing data, including insights into footfall and customer demographics and also makes it possible to have direct communication with individual customers in the form of SMS, MMS or social networks. And with customised splash pages, businesses can personalise the customer Wi-Fi experiences by offering promotional opportunities or surveys and promoting all-important branding.

It is clear that Wi-Fi is here to stay and is becoming much more than simply a way to get online. While the rapid speed of Wi-Fi adoption has led to a disconnect between physical and wireless security, this is now changing and there is no longer any excuse for providing insecure Wi-Fi.

ENDS

949 words

About Wick Hill

Established in 1976, value added distributor Wick Hill specialises in secure IP infrastructure solutions. The company sources and delivers best-of-breed, easy-to-use solutions through its channel partners, with a portfolio that covers security, performance, access, networking, convergence, storage and hosted solutions.

Wick Hill is particularly focused on providing a wide range of value-added support for its channel partners. This includes strong lead generation and conversion, technical and consultancy support, and comprehensive training. Wick Hill has its headquarters in the UK and offices in Germany and Austria. Wick Hill also offers services to channel partners in fourteen EMEA countries and worldwide, through its association with Zycko, as part of Nuvias Group, the pan-EMEA, high value distribution business, which is redefining international, specialist distribution in IT.

For further press information, please contact Annabelle Brown on 01326 318212, email pr@nuvias.com Wick Hill https://www.wickhill.com