أمان الشبكات اللاسلكية

كيف تعمل الشبكات اللاسلكية؟

هي الشبكات التي تتيح للاجهزة الاتصال ببعضها البعض و بالانترنت بدون الحاجة إلى استخدام الكوابل والأسلاك، ينتشر استخدام هذه النوع من الشبكات في المكاتب و البيوت و المطارات و حتى في المقاهي و المطاعم و ذلك لسهولة نشرها ة تنصيبها و أيضاً لسهولة الاتصال بها. كما أنه يمكن الوصول إلى هذه الشبكات من أي مكان طالما أن هذا المكان يقع ضمن تغطية الشبكة اللاسلكية.

تعتمد الشبكات اللاسلكية على موجات الراديو لارسال البيانات كبديل عن الكوابل، و لكي يتم الاتصال اللاسلكي، فإنه يجب توفير الجهاز المُرسل (Transmitter) و الذي يعرف باسم البوابة (Gateway) أو نقطة الاتصال اللاسلكي (Wireless Access Point - WAP) و هذا الجهاز المرسل يتصل سلكياً مع مصدر الانترنت الفعلي و لكنيتصل بمستخدمي الانترنت و الشبكة بصورة لاسلكية. هذا التشكيل بشكله الكامل (نقطة الاتصال اللاسلكي + اتصال انترنت فعلي) يُعرف باسم النقطة الساخنة (Hotspot). تشتمل النقاط الساخنة على معلومات مميزة مثل مُعرّف الخدمة (Service Set Identifier) و يختصر غالباً بـ SSID و هذا المعرف يساعد المستخدم على تمييز الشبكات اللاسلكية ومصادرها عن بعضها البعض. و لكي يتم الاتصال اللاسلمي من قبل المستخدم، يجب أن يحتوى جهاز الحاسوب (المكتبي أو المحمول) على بطاقة اتصال شبكة تدعم الاتصال اللاسلكي المستخدم، و بعد ذلك يقوم جهاز الحاسوب بالبحث الآلي على النقاط الساخنة المتوفرة أو قد يتم البحث بصورة يدوية.

التهديدات الأمنية المرتبطة بالشبكات اللاسلكية

تعتبر سهولة الاتصال بالشبكات اللاسلكية و عدم استخدام الكوابل للتواصل بين أجهزة الشبكة عاملاً مساعداً، ليس فقط للاستفادة و انما أيضاً للتخريب. فهذه السهولة تتيح لأي شخص بنوايا سيئة اكتشاف كافة الشبكات اللاسلكية أو النقاط الساخنة المتواجدة في الجوار. يعرف هذا النشاط عادةً باسم Wardriving و هو عبارة عن قيام بعض الأفراد بالتجوال و في حوزتهم حاسوب أو هاتف محمول يدعم الاتصال اللاسلكي و أيضاً برامج خاصة باكتشاف الشبكات اللاسلكية و تحديد مواقعها عبر النظام العالمي لتحديد المواقع GPS، هذا النشاط بحد ذاته غير مؤذ لأن طبيعة الشبكات اللاسلكية تتطلب نشر معلوماتها ليتمكن المستخدمون من الاتصال بها و لكن هذا النشاط يقوم به عادةً الأفراد الذين لهم نوايا سيئة و ذلك عبر اعتراض الاتصال أو تخريب موجة الاتصال أو حتى عبر نشر شبكات لاسلكية مزيفة بنفس الأسماء المستخدمة. و لمواجهة هذه التهديدات و غيرها يمكن استخدام عدة أساليب كما هو مبين في الجزء التالي من النشرة.

الوسائل اللازمة لتقليل مخاطر الشبكات اللاسلكية

هذه الوسائل تهدف بالأساس إلى حماية الشبكات اللاسلكية المنزلية، و لكن يمكن استخدامها لحماية الشبكات اللاسلكية الأكبر حجماً و التي تكون في بيئة قابلة للتحكم مثل الشبكات المكتبية. بعضها قد لا يصلح لحماية الشبكات العشوائية كتلك المنتشرة في المطارات و المقاهي و الأماكن العامة.

- **تغيير كلمات المرور الافتراضية** – فأغلب نقاط الاتصال اللاسلكي (WAP) تأتي مصحوبة بمجموعة من الإعدادات الافتراضية و التي تشتمل على كلمة مرور

خاصة بإدارة نقطة الاتصال، و يمكن الحصول على كلمات المرور الافتراضية لأنواع معينة من هذه الاجهزة بسهولة عبر الانترنت، و لهذا فإن تغيير كلمات المرور الافتراضية سيعقد امكانية تغيير الإعدادات و التحكم بنقطة الاتصال اللاسلكي.

- **تقليل الصلاحيات** – بحيث لا يتم السماح إلا للأشخاص المخولين بالوصول للشبكة اللاسلكي، و هذا الأمر يمكن أن يتم عبر العنوان الخاص ببطاقة الاتصال و هو العنوان الذي يعرف باسم MAC address، و للقيان بذلك يمكن من خلال إعدادات نقطة الاتصال اللاسلكي نفسها تحديد قائمة بعناوين الـ MAC المسموحة للاتصال على الشبكة، إذا لم يوجد مثل هذا الخيار في إعدادات نقطة الاتصال اللاسلكي فإنه بالتأكيد سيكون موجوداً في نقطة اتصال أحدث من تلك التي يتم استخدامها.

- **استخدام آلية خاصة بتشفير حزم البيانات** – يوجد عدة بروتوكولات تستخدم لتشفير البيانات في الاتصالات اللاسلكية و منها WEP أو Wired Equivalent Privacy و WPA أو Wi-Fi Protected Access، و هذين النوعين يقومان بتشفير البيانات المرسلة بين جهاز المستخدم و بين نقطة الاتصال اللاسلكي، إلا أن البروتوكول الأول يعاني من عدة نقاط ضعف تجعله أقل فاعلية من WPA، و لهذا فمن الضروري عند شراء نقطة اتصال لاسلكي اختيار النوع الذي يدعم بروتوكول WPA و حديثاً WPA2، يفيد تشفير البيانات في منع المتطفلين من اكتشاف محتوى البيانات المرسلة.

- **حماية اسم معرف الخدمة SSID** – و ذلك عن طريق عدم نشر اسم المعرف و جعله ظاهراً عند البحث على الشبكات للاسلكية و هذا يفيد لتجنب اتصال الغرباء بالشبكة اللاسلكية المنزلية، يمكن الاستعانة عادةً بالكتيب الخاص بنقطة الاتصال لمعرفة كيفية تغيير اسم المعرف إلى اسم يصعب استنتاجه و أيضاً عن كيفية إعداد أجهزة المستخدمين للاتصال اليدوي بهذه النقاط.

- **استخدام جدار حماية ناري** – و هو من اجراءات الأمان المستحسنة أيضاً، راجع النشرة الخاصة بالجدر النارية

- **استخدام نظام حماية من فيروسات الحاسوب** – و هو أيضاً من اجراءات الأمان العامة و المستحسنة، كما يمكن مراجعة النشرة الخاصة ببرامج الحماية من فيروسات الحاسوب للتعرف على هذه البرامج و كيفية عملها.

دائرة أمن المعلومات