6

أمن ومراقبة الشبكة

يسهل التحكم في الوصول إلى الشبكات السلكية التقليدية نظراً لضرورة الوصول فيزيائياً إلى حاسب أو مجمّع متصل بهذه الشبكة قبيل التمكن من استخدام (أو إساءة استخدام) موارد هذه الشبكة. مع أن آليات الحماية البرمجية تتمتع بأهمية كبيرة في مجال أمن الشبكات فإن التحكم بالوصول الفيزيائي يعتبر أفضل وسائل تأمين الشبكة. أي أنه إذا افترضنا بأن جميع أجزاء وتجهيزات الشبكة متاحة فقط للإستعمال من قبل أشخاص موثوقين فإننا سنتمكن على الأغلب من الوثوق بالشبكة بأكملها.

لكن هذه القواعد لا تنطبق على الشبكات اللاسلكية، فعلى الرغم من أن مدى تغطية نقطة الولوج العادية قد لا يتجاوز عدة مئات من الأمتار إلا أنه بإمكان شخص ما يقطن في حي بعيد نسبياً الوصول إلى هذه الشبكة من خلال هوائي ذو ربح مرتفع. عدا عن أنه يستحيل في حال اكتشاف مستخدم غير مخول بالولوج إلى الشبكة تقفي أثر هذا المستخدم لمعرفة موقعه الجغرافي. يمكن أيضاً لأي مستخدم أن يقوم بتجميع كافة المعلومات المنقولة عبر الشبكة اللاسلكية وتخزينها لاستخدامها لاحقاً لتوجيه ضربة إحترافية لهذه الشبكة. لذلك ينبغي عليك ألا تعتبر بأن الأمواج اللاسلكية تتوقف عند حدود المباني الخاصة بك أو بمؤسستك.

يستحيل طبعاً أن تثق ثقة عمياء بجميع مستخدمي الشبكة حتى في حالة الشبكات السلكية. قد يتسبب الموظفون الغاضبون والمستخدمون المبتدئون والأخطاء غير المقصودة من قبل المستخدمين الأمناء بأضرار جسيمة للشبكة. تقع مهمة تسهيل الإتصالات الخاصة بين المستخدمين المخولين للشبكة على عاتقك أنت باعتبارك مصمم هذه الشبكة. سيحكم على مهمتك هذه بالفشل إذا واجه هؤلاء صعوبة في استخدام الشبكة للتواصل فيما بينهم.

هل سمعت بالمثل القديم القائل بأن الوسيلة الوحيدة لتأمين حاسب ما بشكل تام تنحصر في فصله عن الشبكة ووضعه في خزنة مقفلة ثم إتلاف مفتاح هذه الخزنة ودفنها ضمن كتلة من الخرسانة المسلحة؟ مع أن نظاماً كهذا سيتمتع بأعلى درجات الأمن إلا أنه عديم النفع للتواصل والعمل. تذكّر دوماً عند اتخاذ قرارات تأمين شبكتك بأن الهدف الرئيس من وجود هذه الشبكة