آراء خاطئة عن أمان أجهزة الحاسوب

1- مهما كانت اجراءات الأمان على الحاسوب، فإنها لن تمنع المخترقين من الوصول للحاسوب:

من المرعب عادةً تصور أن هناك أشخاصاً يعملون ليل نهار لاختراق حاسوبك والوصول لملفاتك الخاصة، ولكن واقع الأمر حالياً هو أن أغلب عمليات الاختراق التي تتم عبر الانترنت لا يكون مصدرها أناس حقيقيون ولكن عبارة عن برامج آلية (robots) تقوم بمحاولة اختراق أكبر عدد ممكن من الأنظمة عبر وسائل آلية تتم بأنماط ثابتة كأن تكون استغلالاً لثغرة أمنية حديثة تم اكتشافها في أحد الأنظمة. قد يراود المرء شعوراً بالعجز عن مواجهة المخترقين وأنه من غير الممكن الحفاظ على جهاز الحاسوب آمناً بشكل كامل، ولهذا فليس من الضروري اتخاذ أي تدابير أمان.

من المعلوم أن اتخاذ أي تدابير أمنية لحماية المنزل من السرقة، لن تمنع اللص المثابر من سرقة البيت ولكن قد تعيقه، ولكن هذا لا يعني أن يُترك أبواب المنزل أو نوافذه مفتوحة عند مغادرته. ولهذا فإن استخدام برامج الحماية المختلفة سيكون له التأثير الايجابي بكل تأكيد، فأغلب برامج الحماية توفر آلية تنبيه معينة للابلاغ عن أي محاولات تسلل تتم للحاسوب حتى يمكن بعدها اتخاذ الاجراءات المناسبة لمنعها كلية.

2- لا يحتوي حاسوبي على أي ملفات هامة ولهذا فأنا غير مُضطر لحمايته:

من المُفيد استخدام الأرقام لتفنيد هذه المقولة، فنظام التشغيل العادي على أجهزة الحاسوب الحديثة وبدون تثبيت أي برامج اضافية عليه، يحتوي تقريباً على 100,000 ملف مختلف، وهذا الرقم لا يشمل المستندات الشخصية والملفات المحفوظة من قبل المستخدم ولا يشكل أيضاً المواقع المفضلة أو الملفات المرفقة مع رسائل البريد الالكتروني أو سجل

المحادثات أو الاختصارات المختلفة أو الصور أو الملفات الصوتية أو أي إعدادات مُخصصة قد يقوم بها المستخدم لتسهيل استخدامه للحاسوب، وفي حال كونك مستخدماً عادياً فإن عمر نظام التشغيل قد يتراوح بين 1 – 3 سنوات من الاستخدام ولهذا فإن عدد الملفات قد يتجاوز الـ 300,000 ملف.

فكيف يمكن لأي شخص أن يُحدد الملفات الهامة وغير الهامة؟ كما أن أغلب مستخدمي الحاسوب لا يقومون بالاطلاع على الملفات المُخزنة لتصنيفها إلا إذا تعطل النظام بشكل كامل، ولهذا فإن البديل الأمثل هو القيام باجراء نسخ احتياطي للحاسوب كما لو كانت كافة الملفات "هامة".

3- لا أقوم بتطبيق أي تحديثات للحاسوب، فهي لا تُسبب سوى المشاكل:

أجهزة الحاسوب هي عبارة عن آلات، وهي تحتاج إلى عمليات صيانة باستمرار أسوةً بباقي الآلات. قد يكون صحيحاً أن بعض التحديثات تُسبب عدم استقرار للحاسوب وربما تعطيله بشكل جزءي أيضاً ، إلا أن أغلب هذه التحديثات المُسببة للمشاكل يتم سحبها أو الغاؤها بمجرد اكتشاف أضرارها ويتم غالباً استبدالها بتحديثات أخرى وبشكل سريع أيضاً، ولهذا فإن تطبيق التحديثات التلقائية يظل ضرورياً جداً وهاماً لحماية الحاسوب وضمان استقراره على المدى البعيد ، فهي تقوم بانهاء وجود الثغرات الأمنية والأخطاء الفنية في تصميم النظام ليتم منع استغلال هذه الثغرات من جهات خارجية.

في كثير من الأحيان لا يدرك المستخدم العادي أنه تم اختراق حاسوبه والسيطرة عليه إلا بعد وقت طويل وبعد أن تبدأ بعض المظاهر بالاتضاح، كأن يُصبح النظام غير مستقر أو عندما يبدأ المستخدم بفقد بعض الملفات الضرورية أو حتى عندما يشتكي بعض معارفه أنهم يستقبلون رسائل مزعجة من جهازه الشخصي أو بريده الالكتروني. تطبيق التحديثات سيساعد المستخدم لتجنب الكثير من هذه المظاهر في المستقبل.

4- لنفترض أن الحاسوب يحتوي على بعض البرامج الخبيثة، إذا لم تؤثر على حاسوبي فأين المُشكلة؟:

يقوم العديد من مبرمجي الفيروسات والبرامج الخبيثة عموماً بكتابة ونشر الآلاف منها وتصنيفها تحت مسمى "Zombies" و "botnets". أما الـ "botnet" فهي تعبر عن مجموعة من أجهزة الحاسوب الحاوية على البرامج الخبيثة وهذه الأجهزة بدورها تُعرف باسم "Zombies". هذه البرامج الخبيثة يمكن التحكم بها غالباً من خلال كاتب البرنامج الأصلي نفسه بدون علم صاحب جهاز الحاسوب المحتوي عليها. إذا كانت حالة الحاسوب الخاص بالمستخدم ينطبق عليها مفهوم الـ Zombie، فإن المستخدم قد لا يشعر بأي اختلافات أو أي مظاهر غريبة مُطلقاً، باستثناء أنها قد تكون ذات أداء بطي نسبياً وهذا البطء قد يعزوه المُستخدم غالباً إلى كونه ناتجاً عن كثرة البرامج أو لأن الأجهزة المتصلة بالانترنت تكون أبطأ من غيرها. قد لا ينزعج المستخدم من هذا البطء ولكنه قد يكون مسئولاً عن اصابة العديد من الأجهزة الأخرى بالبرامج الخبيثة بدون علمه.

دائرة أمن المعلومات