رقمي

التحديات التي تواجهه أمن المعلومات

د. خالد بن سليمان الغثبر ❖

في عالم رقمي مترابط ويعج بالأخطار والكوارث الرقمية، يأتي أمن المعلومات بمفهومه وتطبيقاته وتقنياته فارساً على خيله للذود عن الأنظمة الرقمية للمنظمات، و لكن التحديات التي تواجه أمن المعلومات كثيرة و بعضها معقدة يعجز الفارس وحده على مجابهتها.

فمن بعض تلك التحديات سرعة الهجوم، ففيروس (أو دودة رقمية) سلامر الذي انتشر في ٢٠٠٣ استطاع أن يصيب ٧٥٠٠٠ حاسوب في أول أحد عشر دقيقة من تفعيله الأولي، بل كان عدد الحواسيب التي تصاب تتضاعف كل ثمانية ثواني، حيث استطاع بعد اثنتي عشرة دقيقة من تفعيله أن يصيب أكثر من مليونين ونصف المليون حاسوب. إنها سرعة هائلة لا تمّكن الشركات المختصة بكتابة خبر عن انتشارها في هذه السرعة، قد تكون هذه الفترة الوجيزة هي وقت احتساء مدير الأنظمة لكوب من الشاي!

ومن التحديات، ازدياد تعقد الهجمات، حيث أصبحت الهجمات بأنواع و ألوان و سمات لم تُعهد من قبل، فعلى سبيل المثال، قد يصلك فيروس و كأنه مجلد و ليس ملفاً مما يجعلك تفتحه لترى ما فيه و إذ بك تفّعل الفيروس، و قد يأتيك على هيئة ملف نصي أو فيديو و هو غير ذلك، و قد يأتيك من زميلك أو أخيك رسالة إلكترونية و بها ملف يريدك أن تراه، وفي الحقيقة أن المرسل لم يكن ما توقعته.

كان المهاجم سابقاً يهاجم ضحيته من مصدر واحد، أما الآن فقد أصبح المهاجم أكثر احترازاً و خطورة، حيث يلجأ أكثر المهاجمين إلى التخفي أو استخدام حواسيب وسيطة لها صفات أمنية ضعيفة و سعة اتصال بالإنترنت عالية (مثل DSL) يملكها أناس عاديون، حيث يقوم المهاجم بتوجيه تلك الحواسيب الوسيطة في وقت محدد لمهاجمة الهدف، مستفيداً بذلك من التخفي وكثرة المهاجمين، مما قد يغرق الهدف و يعطل خدماته.

كذلك من التحديات سرعة اكتشاف عيوب الأنظمة الحاسوبية ليس من قبل المصنعين بل من قبل المهاجمين أو الهواة، و اكتشاف تلك العيوب قد ينتج عنها اكتشاف ثغرات أمنية يمكن للمهاجم استغلالها للولوج للأنظمة بطريقة غير نظامية مما يعرض المنظمات للخطر.

ولحل مشكلة الثغرات الأمنية فان الجهات المصنعة أو المطورة تقوم بإصدار رقع لسد الثغرات و تلك الرقع عبارة عن تعديلات دقيقة في الأنظمة لتلافي الخطر الناتج عن الثغرة.

يبدو للقارئ أن خطر الثغرات أصبح ضعيفاً، لكن واقع الحال ينفي ذلك حيث إن هناك معضلتين للثغرات و الرقع، الأولى تكمن في أن بعض الثغرات المكتشفة معلومة فقط للمهاجمين دون المطورين، أو أن الرقع لتلك الثغرات لم يتم إصدارها بعد، وفي هذه الحالة فإن الأنظمة التي تحتوي على ثغرات تكون عرضة للخطر سواء علم بها مدير النظام أم لم يعلم. أما المعضلة الأخرى فهي أن إصدار الرقع ليس نهاية الخطر؛ لأن الخطوة الثانية و هي إنزال تلك الرقع على الأنظمة ذات الثغرات لا تتم على جميع الأنظمة، وذلك ناتج عن تكاليف إنزال الرقع على جميع الأنظمة أو انشغال أو تجاهل مدير النظام. فعلى سبيل المثال، بالرغم من صدور رقعة لفيروس سلامر قبل ١٨٥ يوماً قبل صدور الهجوم الأول، إلا أنه انتشر بشكل سريع كما ذكرنا آنفا.

وما دام أن هناك مهاجمين محترفين و على درجة كبيرة من المهارة، و ما دام أن هناك أنظمة حاسوبية تُطور دون الالتزام بمعايير أمن المعلومات، فإن التحديات والأخطار لن تزول.

جامعة الملك سعود

ksaksu@gmail.com