

هل الإنترنت آمن؟

أ. د. علي المشاط

2015-03-02

يعتبر الإنترنت العمود الفقري للحياة الحديثة ولكن أمنه (أمن الإنترنت) يكتنفه الغموض. وفي هذا المجال من المهم معرفة ان الإنترنت بطبعه معرض للإختراق بسبب أنه أصلا صمم ولم تكن الناحية الأمنية إحدى اهتماماته. صمم الإنترنت ليكون وسيلة لتسهيل التعاون البحثي بأقل تعقيد ممكن. ولذلك هو سهل الإستعمال ومستجيب لمطالب المستعمل. إستجابته والمهارة التحليلية اضافة الى الذاكرة وسهولة الربط تطورت وأصبحت غير باهضة الثمن بحيث أصبح بمتناول الجميع خصوصا في استعمال الهواتف الجواله التي تمتلك امكانية ارسال واستلام المعلومات. بيد أن خصائص الإنترنت التي تجعل منه أداة ذات منفعة عظيمة هي نفسها التي تجعله معرضا للإنتهاك.

من أولى سمات الضعف في الإنترنت هي دلالة الشخصية للمخاطب والمخاطب على حد سواء. كما أن غالبية مستعملي الإنترنت لا يعلمون حقيقة فيما اذا كانوا يستعملون الإنترنت بأمان أو لا. هذا من جانب ومن الصعوبة بمكان فهم المشاكل الفنية المتعلقة بمنظومات مكوناته سواء المنظومات أو المواد الإلكترونية أو البرمجيات أو الرقاقات أو غيرها من جانب آخر. بكل بساطة، ما أن يتم ربط الحاسوب بالإنترنت حتى يستطيع (المهاجم) أن ينفذ الى منظومة (المهاجم) بإدخال برمجياته والإستحواذ على مايريده بما يسمى بيوم الصفر (zero-day). وهذا الأسلوب يعتمد عادة من قبل مهاجمين بإمكانات عالية على أهداف مهمة. أما أكثر الحالات شيوعا فهي أبسط من ذلك بكثير. فلاختراق منظومة أو حاسوب كل ما تريده هو قيام الضحية بالكبس على موقع أو فتح مرفق ما فيتيح ذلك تحميل برمجيات موبوءة تعين المهاجم على دخوله وتحقيق أهدافه. ومن الطرق البسيطة الأخرى هي اغراق منظومة الضحية بكميات هائلة من الأوامر التي تطلب معلومات لا معنى لها مما يؤدي اشباع المنظومات ومن ثم تعطل عمل الإنترنت.

الطريقة التي ننظر بها الى الحواسيب والمنظومات هي من حيث مواصفاتها وسعرها متناسين موضوع خصائصها الأمنية. ان مجرد التفكير بأننا يمكن أن نحاسب على عدم استخدامنا للحواسيب بشكل منضبط يولد صدمة لنا. ولكن حينما لا نستخدمه بما يلزم من حيلة وانتباه ونجعله عرضة للإستغلال

والإختطاف من قبل الجواسيس والمجرمين والعابثين يجعلنا مشاركين معهم في أعمالهم السيئة وما يتبعها من احتمال تحطيم علاقات وانهيار اقتصاد وحتى أمن قومي. منظومة الإنترنت تجعل من الموقع الجغرافي لا معنى له. فكل مستعمل معرض لهجوم سايبري اينما كان موقعه. وحينما يحصل هجوم يؤثر الشخص أن لا يتكلم عنه لأنه يؤثر سلبا على سمعة عمله. لذلك ينبغي لمن يكون مسؤولا عن سياسة العمل السايبري ان يسن ضوابط للعمل في مثل هذه الحالات مثل ذلك كمثال الحجر الصحي على بعض الأمراض وهنا يجب أن يمنع الذي تعرضت منظومته لفيروسات يمكن انتشارها أن يستمر بالإبحار عبر المحيط السايبري حماية للمستعملين الآخرين.

وبتفكير شبيه بالحجر الصحي يمكن معاملة مشكلة الإختراقات الفايروسية في الفضاء السايبري. المشكلة الرئيسية تكمن في أننا لم نتطور بما فيه الكفاية للتعامل مع التطور في الإلكترونيات والإتصالات. خلال الألفية الماضية تكون للإنسان العديد من المهارات للموازنة بين التعرض للخطر والأمان والتمتع بالفوائد المرجوة من كل أمر يقدم عليه. لذلك فإننا مبرمجون لمساعدة الآخرين والثقة بهم. كما إن حواسنا كالعينين والأنف والأذنين تعلمنا بأننا في خطر أو في أمان. وماذا علينا أن نعمل وأين ومتى. أما الآن فما أن ندخل في عالم الأنترنت فكل مناعات الإنسان المشار اليها تختفي من تفكيرنا وممارساتنا.

ذلك لأن حواسنا تتعطل وكل ما نملكه ونعول عليه هو ما يظهر لنا على الشاشة وما نسمعه من مكبرات صوت صغيرة في الحواسيب. وهذا شبيه على ما يبدو بالعالم الخارجي ولكن بشكل خادع. فبالرغم من ثقتنا بما نقوم به على النيت من تسوق وتصفح وبيع واستعمال مواقع التواصل الإجتماعي إلا اننا في الحقيقة بلا حماية وغير متهيئين ومعرضين للصوم النيت والمستغلين والأعداء. لأننا لا نرى من نتعامل معهم، لا نستطيع الحكم عليهم من خلال أصواتهم ونبراتهم ولغة سلوكهم وتعابير وجوههم. ولا نستطيع شمهم أو لمسهم. كل هذا ولكن علينا التعامل معهم. وباستعمال تكنولوجيا لا نفهمها حقيقة. لذلك فإن استعمالنا للحواسيب في تزايد وبنفس الوقت امكانية صد المهاجمين لا يتحسن. فإذا لم يتحسن سلوكنا الحاسوبي وطريقة تفكيرنا سنكون أكثر عرضة للإختراق وفقدان الحرية والصحة والسعادة.

من أهم ما يجب أن ينحو اليه تفكيرنا أن الأمن السايبري ليس بمشكلة فنية. شأنه في ذلك شأن سلامة الطريق فهي ليست مشكلة هندسية. كما أن السلامة البدنية لا تعني بالضرورة إلحاما بالطب. المهم أن علينا اعادة النظر في سلوكنا في التعامل مع مخاطر العمل السايبري الحي، سواء كنا أفرادا أو كمؤسسات أو كمجتمعات. هذه مشكلتنا كبشر لا كمكائن.

البريد الإلكتروني للكاتب: rafidian@gmail.com

Arab Scientific Community Organization (ARSCO) · arsko-ai.org