25/04/2015 تكنولوجيا

الفضاء الإلكتروني.. قنبلة موقوتة ستفجر كل خصوصيات الإنسان

«الإنترنت» ستتوسع بشكل هائل لخدمة تواصل المليارات من الناس والأشياء من دون تأمينها ضد الاختراقات

مارك غودمان خبير التقنيات في إدارة الشرطة بمدينة لوس أنجليس الأميركية المتخصص في الجرائم الإلكترونية يحذر من «المساحة المظلمة المريعة للتقنيات الرائعة التي تعمل سريعا على تغيير وتشكيل حياتنا». وهو ينذرنا باقتراب عاصفة من الجرائم الإلكترونية.

ويقول غودمان مؤلف الكتاب الجديد «جرائم المستقبل»: إن «العالم سيشهد توسع الإنترنت بشكل لا مثيل له. والأمر يشبه الأيام الخوالي عندما نفدت أرقام الهواتف لدى لندن أو نيويورك وكان لزاما إنشاء أرقام هاتفية جديدة للمناطق. وهذا بالضبط ما نفعله بالإنترنت حاليا، ولسوف يكون التأثير مهيبا».

*** «الإنترنت» الجديدة**

الإنترنت القديمة تدعم نحو 4.5 مليار اتصال متزامن، ولكن نظام العنونة الجديد المزمع الإعلان عنه قريبا تحت مسمى بروتوكول الإنترنت السادس سوف يدعم حتى 79 اكتليونا (واحد وبجانبه 27 صفرا) اتصال في وقت واحد، أي ما يقابل خدمة 78 مليار مليار مليار من الأشياء التي يمكن وصلها على الإنترنت في نفس الوقت. لذا، إذا كانت الإنترنت في يومنا هذا بحجم ملعب للغولف، فإنها في خلال الأعوام القليلة القادمة سوف تنمو حتى تقارب حجم الشمس ذاتها. وكل حبة رمل على كوكبنا سوف يكون لها عنوان على الإنترنت متضاعف تريليون مرة.

ويضيف: «في السابق، لم يكن يساورني القلق حول التلفاز القابل للقرصنة، أو منظم دقات القلب القابل للقرصنة، أو السيارة القابلة للقرصنة، أو حتى الحيوان الأليف القابل للقرصنة. ولكن الآن صار كل ذلك ممكنا.. لقد تمكنا من

وصل العالم ببعضه البعض، غير أننا فشلنا في تأمينه»، كما يقول في حديث لمجلة «نيوساينتست» البريطانية.

في الماضي، كان بإمكانك شراء مسدس أو سكين، ثم تختبئ في زقاق مظلم حتى يمر بك أحد البلهاء فتبرز إليه وتقول «أعطني حافظة نقودك، غير أنك لن تستطيع سرقة إلا 4 أو 5 أشخاص باليوم الواحد. إلا أننا الآن نشاهد نقلة نوعية في عالم الجريمة، ففي قرصنة إلكترونية واحدة تعرضت لها شركة (تارغيت) للتجزئة في الولايات المتحدة عام 2013، وقع أكثر من ثلث المواطنين الأميركيين ضحايا لتلك الهجمة، ومن بينهم عشرات ملايين المواطنين الذين سرقت بياناتهم المصرفية. ولذلك، يمكن لشخص وحيد اليوم سرقة مائة مليون شخص في اليوم الواحد. لم يكن ذلك ممكنا أبدا في الماضي نظرا لاتصالنا جميعا عبر تقنيات ضعيفة.

*** تقنيات المجرمين**

وكان غودمان على دراية باستخدام أدق تفاصيل التقنيات، وعمل مع الإنتربول لمدة 10 سنوات، في مساعدة قوات الشرطة حول العالم على مواجهة الجرائم الإلكترونية. ويقول إنه تعرف على قيام الأشرار باستغلال التقنيات الحديثة، ففي أواخر الثمانينات وبداية التسعينات، حينما لم تكن أجهزة (بيجر) للتراسل شائعة الاستخدام كان يرى أفراد العصابات وتجار المخدرات يحملونها ويتواصلون من خلالها.

تحمل البرمجيات الحديثة رموزا للقرصنة بين طيات البرامج، فإذا ما كنت تريد تنفيذ قرصنة على أحد البنوك قبل 20 عاما مثلا، كان لزاما عليك أن تكون من خبراء القرصنة المعدودين. أما الآن، فما عليك إلا دفع مقابل مادي معين إلى أحد الخبراء الذين يدرجون معرفتهم التقنية العالية في برمجياتهم الإجرامية. ومعظم هجمات القرصنة الحالية لا يشرف عليها البشر، فحادثة القرصنة على شركة تارغيت نفذها صبي يبلغ 17 عاما من عمره يعيش في موسكو كان قد ابتاع بعض البرمجيات من على الإنترنت مكنته من الولوج إلى شبكة الشركة المذكورة.

*** اختراقات إلكترونية**

إن كل جهاز متصل بالإنترنت يعد هدفا للمجرمين، إذ لم يتمكن أحد قط من بناء نظام حاسوبي ضد الاختراق والقرصنة. ويقول غودمان إننا نسابق الزمن وبسرعة فائقة لوصل كل جهاز لدينا بالإنترنت وكلها أجهزة غير آمنة تماما. ينبغي علينا التوقف للحظات. إذا ما اخترق أحدهم تلفازي، فهل سوف أعير الأمر أي أهمية؟ ولكن كل الخدمات العالمية الحساسة تديرها الكومبيوترات، وإننا نرى تلك الكومبيوترات عرضة للهجمات والقرصنة أكثر من ذي قبل. يسعى الناس جميعهم نحو السلطة. والآن، إذا ما سيطرت على الرموز ن فإنك تسيطر على العالم.

إن الأدوات التي نستخدمها في حماية أنفسنا يمكن تخريبها واستخدامها ضد مصالحنا. وهذا ما يمكن تسميته «نموذج الجودو من الأمن الإلكتروني» – بمعنى استخدام قوة خصمك في هزيمته. فلا يمكنك التأكد أنه حينما تنتشر 300 كاميرا مراقبة مثلا شوارع لندن، أو في أي مدينة، أن الحكومة فقط هي من تراقب تلك الشوارع.

كما لا يمكن لأحدنا الوثوق فيما تعرضه علينا الشاشات. كلنا نتلقى رسائل وهمية على البريد الإلكتروني تبدو وكأنها قادمة من البنوك التي نتعامل معها. ولقد انتقل ذلك الأمر إلى مستوى جديد تماما مع هجمات دودة ستوكسنت الإلكترونية التي تعرضت إليها إيران في عام 2010. فلقد كان المهندسون النوويون يطالعون الشاشات التي تعرض لهم حالة أجهزة الطرد المركزية العاملة على تخصيب اليورانيوم. وكانت الشاشات تشير إلى أن كل شيء على ما يرام في الوقت الذي كانت أجهزة الطرد المركزية تخرج عن السيطرة. والحقيقة، أن أحد المتسللين قد تمكن من اختراق المساحة الفاصلة بين ما يجري في الواقع وبين ما تعرضه الشاشات. بالتالي، ووفقا لذلك المثال، صرنا مقطوعو الصلة بالواقع المادي، بهذه الطريقة.

*** حافة الخطر**

غالبا ما يقال إننا على حافة الخطر إذا ما تحدثنا عن الأمن الإلكتروني، فهل ذلك معقول؟ إذا ما كنت راضيا بجهلك التام حول التكنولوجيا وتسعد كثيرا ببعض النقرات البسيطة على هاتفك الآيفون، فإنك بالتأكيد في خطر كبير. فهناك شخص ما في الخارج يدرك تماما كيف يعمل ذلك الهاتف ولسوف يستخدم معرفته تلك ضدك في يوم ما. علينا أن نتيح للناس نوعا من الصحة التقنية.

في عالم الواقع أغطي فمي إذا ما عطست، لكن ليس لدينا أي فكرة عن شكل النظافة على الإنترنت، لذا نستمر في نشر «المرض»، وإرسال ملفات ملحقة برسائل بالبريد الإلكتروني تحتوي على فيروسات، وندخل وحدات ذاكرة محمولة لغرباء في أجهزة الكومبيوتر الخاصة بنا.

مع ذلك من أسباب المخاطر الرئيسية التي نواجهها اليوم هي البرامج السيئة. صحيح أن عملية التشفير معقدة، لكن شعار موقع «فيسبوك» مثلا هو «تحرك بسرعة واكسر الأشياء». بعبارة أخرى، السرعة بالنسبة إلى السوق أهم من الأمان. ومن السخف إلقاء اللائمة على البشر عوضا عن الالتفات إلى مدى سوء فعالية تصميم العنصر الأمني في النظم والبرامج.

*** روبوتات معادية**

وإذا أصلحنا عنصر أمن الإنترنت، هل يمكن ألا نقلق؟ إن التهديدات التي نتحدث عنها تقبع وراء شاشات الكومبيوتر. إذا سرق أحدهم 50 دولارا من حسابك المصرفي، فلن تتضرر بدنيًا، لكننا قد نتضرر مع انتشار الأجهزة الموصولة بالإنترنت.

ونحن الآن أمام واقع جديد إذ إن نسبة كبيرة من الأجهزة التي سنستخدمها قريبا في الاتصال بالإنترنت ستصبح روبوتات تستطيع التحرك. لقد اقتربنا من اختراع ملايين من أجهزة الكومبيوتر التي تسير، وتزحف، وتتدحرج، وتسبح. إنها ستحلق مثل الطائرات التي تعمل من دون طيار، وتلاحقنا في أسراب، وتتبعنا في الشوارع. تستطيع الروبوتات الركل، وتسديد اللكمات، والتصويب.. وكذلك يمكن اختراقها.

ولقد شهدنا بالفعل أمثلة لأشخاص يستخدمون طائرات تعمل من دون طيار. وألقى مكتب التحقيقات الفيدرالي القبض على شاب يدعى رضوان فردوس كان يخطط لوضع متفجرات على طائرات صغيرة تعمل من دون طيار وتوجيهها نحو مبنى وزارة الدفاع الأميركية، والبيت الأبيض. وفي سياتل كان هناك سيدة تغير ملابسها دون إسدال ستائر غرفتها في الطابق الخامس والعشرين في أحد المباني، وهو أمر لم يكن يثير قلقها في الماضي، لكنها عندما نظرت من النافذة وجدت طائرة صغيرة من دون طيار تصورها. وإذا اتصلت بالشرطة وقلت: «هناك طائرة من دون طيار تحلق خارج شقتي»، ماذا ستفعل الشرطة؟ لا توجد أي وسائل متاحة.

*** أسلحة بيولوجية**

* ماذا عن علم البيولوجيا الصناعية؟ على الأرجح هناك مشكلات في هذا المجال أيضًا. من أين نبدأ؟ إذا كنت بمقدورك تسجيل مكونات الحمض النووي، فبإمكانك أيضا اختراقه. ومكونات الأسلحة البيولوجية مثل الإيبولا، والأنفلونزا الإسبانية، متوفرة على الإنترنت. وقد انخفضت تكلفة تصنيعها كثيرًا، وقدرتنا على فك شفرة الحمض النووي تزداد بسرعة هائلة. وفي ظل استخدام عشرات الآلاف من الأشخاص لهذه التكنولوجيا، لن يكون من المستغرب وجود بضع أناس أشرار. وهناك احتمال آخر هو الهجوم على فرد بعينه. إذا استطعت التوصل إلى علاج لمرض السرطان يختلف باختلاف المرضى، فيمكنك التوصل إلى سلاح بيولوجي مصمم للهجوم على الشفرة الوراثية الخاصة بشخص ما. ونحن غير مستعدين إطلاقا لمواجهة تلك الأحداث السيئة.

وفي المقابل وعلى صعيد الذكاء الصناعي، ينبغي أن نستغل ما لدينا من كم بيانات هائل في حل الجرائم. كذلك سوف نرى تطورا كبيرا في التكنولوجيا العسكرية، حيث سنجد روبوتات مسلحة، وطائرات تعمل من دون طيار تستخدم ضمن قوات حماية القانون المدنية.

*** «مشروع مانهاتن» جديد**

ويرى غودمان ضرورة وضع مشروع جبار لمكافحة اختراق الإنترنت. فالمستقبل التكنولوجي المذهل، الذي وعدنا به «سيليكون فالي»، لن يكون مجانيا وبلا مقابل، بل سيحتاج إلى وقت، ومال، وجهد ودمان.

وللمقارنة فكروا في الخطر الوجودي، الذي واجهته قوات الحلفاء خلال الحرب العالمية الثانية، وهو احتمال أن يسبق النازيون غيرهم في تصنيع قنبلة نووية. ودفع هذا الخطر الحلفاء إلى التحرك، وبذل الجهد. في مشروع مانهاتن، زاد عدد الحلفاء عن 110 آلاف شخص حول العالم يعملون على مدار الساعة، وطوال أيام الأسبوع.

واختيار هذا التشبيه يأتي من أجل وضع مشروع مانهاتن جديد لمقاومة خطر الجرائم الإلكترونية لأن ما نواجهه من خطر لا يقل عن ذلك الخطر. والكومبيوتر يشغل مركز العالم الذي نبنيه، وهو عنصر أساسي في شبكات الكهرباء، والدفاع الوطني، والرعاية الصحية، والنقل. وقد يؤدي احتراق تلك الأنظمة إلى انقطاع الكهرباء، أو المياه النظيفة، أو تسرب الصرف الصحي إلى الشوارع.

لندن: «الشرق الأوسط»