تعيين أول امرأة في مجلس إدارة (فيس بوك)

واشنطن / متابعات:

أعلنت شبكة التواصل الاجتماعي (فيس بوك) أنها عينت السيدة شيريل ساندبرج مديرة للعمليات بالشركة، لتصبح أول امرأة تنضم إلى مجلس إدارة الشركة.

وفي معرض إعلانه عن تعيين ساندبرج قال مؤسس (فيس بوك) مارك زوكربرج: إن «شيريل كانت شريكتي في إدارة فيس بوك».

وأضاف وفقاً لمصادر إعلامية: «إن استيعابها لمهمتنا وفرصتنا على المدى الطويل وخبرتها في كل من (فيس بوك) ومجالس إدارات شركات عامة، يجعلها مناسبة لعضوية مجلس إدارتنا».

وقامت شبكة (فيس بوك) أيضاً بتغيير عناوين البريد الإلكتروني الافتراضية المستخدمة في الاتصال بين مستخدميها عبر الموقع.

وربما يثير تغيير عناوين البريد الإلكتروني إلى عناوين ضمن النطاق (آت فيس بوك دوت كوم) التي وفرها موقع التواصل الاجتماع لكل مستخدميه البالغ عددهم نحو 900 مليون مستخدم، رد فعل حاداً جديداً ضد الشركة لعدم إخطارها المستخدمين مسبقاً بشأن هذا التغيير.

وقال متحدث باسم (فيس بوك): «إنه تم عمل هذا التغيير لضمان سهولة الاتصالات لكل مستخدمي الموقع».

تعددت الجرائم المعلوماتية والقوانين غائبة

الاعتداء على البيئة المعلوماتية يتميز بسرعته الفائقة وتأثيره المدمر وقدرة مرتكبيه على الإفلات من العتاب

العالم يعيش ثورة هائلة في مجال المعلومات والاتصالات أتاحت للبشر قدراً هائلاً من المعرفة

القاهرة / أمير عكاشة :

الوجه القبيح للتقنية الحديثة

يشكل أمن المعلومات الرؤى والسياسات والإجراءات التي تصمم وتنفذ على مستويات مختلفة فردية ومؤسسية ومجتمعية، وتستهدف تحقيق عناصر الحماية والصيانة المختلفة التي تضمن أن تتحقق للمعلومات السرية أو الموثوقة، أي التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

إضافة إلى ذلك التكاملية وسلامة المحتوى أي التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات، أو عن طريق تدخل غير مشروع.

أما الاستمرارية فتعني توفر وإتاحة المعلومات أو الخدمات المبنية عليها لمستخدميها والمستفيدين منها والتأكد من استمرار توفرها والنظم التي تخدمها واستمرار القدرة على التفاعل معها والتأكيد كذلك على أن مستخدمها لن يتعرض إلى منع الاستخدام أو الحيلولة بينه وبين الدخول إليها، كما تعني أيضا ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها أنه هو الذي قام بهذا التصرف.

ويقول د.محمد زين (أستاذ التكنولوجيا بجامعة القاهرة) «يشكل الاعتداء على البيئة المعلوماتية الوجه القبيح للتقنية الحديثة، فالجرائم الناتجة عن هذا الاعتداء تتميز عن الجرائم العادية بسرعتها الفائقة وتأثيرها المدمر، وقدرة مرتكبيها على الإفلات من الملاحقة والعقاب في ظل افتقاد كثير من الدول أنظمة قانونية قادرة على التعامل مع هذا الاعتداء والجرائم الناجمة عنه».

وتشير إحصاءات دولية إلى أن هناك أكثر من ملياري شخص مستخدم لأجهزة الحاسب الآلي، فضلاً عن وجود أكثر من 13 مليار صفحة على شبكة المعلومات الدولية (الإنترنت) ونحو 300 مليون موقع عليها.

وهكذا اتسعت البيئة المعلوماتية لتصبح ميداناً فسيحاً للعدوان عليها، ولتشكل تحدياً رهيباً لمختلف الأجهزة في مواجهة هذا الاعتداء وما ينجم عنه من جرائم.

وتشير إحدى الدراسات إلى أن 24 إلى 42 ٪ من المنظمات في القطاعين الحكومي والخاص كانت ضحية لجرائم مرتبطة بالتقنية الحاسوبية، وأن 145 إلى 730 مليون دولار سنوياً خسارة 72 شركة بسبب جرائم الحاسب الآلي.

وبينت دراسة للأمم المتحدة عن مخاطر الحاسب الآلي أن 73 ٪ من الجرائم تتم في الداخل، وقدرت الخسائر الاقتصادية لهذه الجرائم عام 1993م بنحو ملياري دولار.

ويشهد قطاع تقنية المعلومات نموا متزايدا في العالم العربي وخصوصاً مع دخول شبكة المعلومات الدولية، مما عرض الكثير من النظم والشبكات التي كانت معزولة في الماضي لخطر الاختراقات الخارجية، ومكن كثيراً من المستخدمين من التعرف على البرامج التي تساعد على اختراق الأنظمة الحاسوبية والحصول عليها بسهولة، وذلك يضع عبئاً أكبر على مشغلي الأنظمة لمتابعة المعلومات الأمنية، وطرق الاختراقات المستحدثة لحماية أنظمة التشغيل الخاصة بهم.

وحيث إن الخبرات لازالت محدودة نسبياً فيما يتعلق بأمن المعلومات ولأنه لا يوجد نظام أمني رادع لهؤلاء المخترقين، فسوف تزداد المشكلة سوءاً مع ازدياد الاعتماد على الحاسب وشبكة المعلومات الدولية.

ومع قرب الانضمام لمنظمة التجارة العالمية تزداد الأهمية الاقتصادية لأنظمة المعلومات والحاسبات، وخصوصاً مع الانتشار الواسع للتجارة الإلكترونية مما يستلزم المزيد من العناية بقضايا أمن المعلومات.

ويقول د.نبيل حسن (أستاذ التكنولوجيا بجامعة القاهرة) «تنوعت وتعددت الجرائم المرتبطة والمرتكبة بواسطة المعلومات وتنوعت أساليب عرضها ومسمياتها من قبل الباحثين والكتاب والمعنيين بالمحافظة عليها وصيانتها من المتخصصين بعلم الحاسب الآلي والبرمجيات المختلفة».

تصنيفات الاعتداءات في الحقل التقني

أولاً: خرق الحماية المادية ويقصد بها قيام المهاجم بالبحث في مخلفات التقنية من القمامة والمواد المتروكة، بحثاً عن أي شيء يساعده على اختراق النظام، كالأدوات المدون عليها

كلمة السر أو مخرجات الحاسب أو الأقراص الصلبة المرمية بعد استبدالها أو غير ذلك من المواد أو أن يلجأ المهاجم إلى عملية الالتقاط السلكي، أي التوصل السلكي المادي مع الشبكة أو مع توصيلات النظام لاستراق السمع أو للسرقة والاستيلاء على المعلومات المتبادل عبر الأسلاك.

وقد يتم اختراق الحماية المادية عن طريق استراق الأمواج، وهو ما يحدث باستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم، باختلاف أنواعها، كالتقاط موجات شاشات الكمبيوتر الضوئية، أو التقاط الموجات الصوتية من أجهزة الاتصال.

وأخيراً قد يلجأ المهاجم في محاولة اختراق الحماية المادية إلى إنكار أو إلغاء الخدمة، أي الإضرار المادي بالنظام لمنع تقديم الخدمة.

ثانياً: خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين: تعد المخاطر المتصلة بالأشخاص والموظفين وتحديداً المخاطر الداخلية منها واحدة من مناطق الاهتمام العالمي لدى جهات أمن المعلومات، إذ ثمة فرصة لأن يحقق أشخاص من الداخل ما لا يمكن نظرياً أن يحققه أحد من الخارج، وتظل أيضاً مشكلة صعوبة كشف مثل هؤلاء قائمة، إن لم يكن ثمة نظام أداء وصلاحيات تتيح ذلك.

وثمة مسميات وطوائف عديدة لهذه المخاطر، أبرزها: التخفي بانتحال صلاحية شخص مفوض، واستغلال العلاقات الاجتماعية، أو القيام بأعمال الإزعاج والتحرّش، وربما التهديد والابتزاز، أو في أحيان كثيرة رسائل المزاح على نحو يحدث مضايقة وإزعاج بالغين، وكذلك القيام بقرصنة البرمجيات عن طريق نسخها دون تصريح، أو استغلالها على نحو يخل بحقوق المؤلف.

ثالثاً: خرق الحماية المتصلة بالاتصالات والمعلومات بأنواعها المختلفة : والمقصود بذلك الأنشطة التي تستهدف المعلومات والبرمجيات، وتشمل طائفتين:

1- هجمات المعلومات: وتشمل النسخ غير المصرح به للبيانات والمعلومات والأوامر والبرمجيات وغيرها، وتحليل الاتصالات والقيام بعمل قنوات مخفية تمهيداً لهجوم لاحق أو تخزين معلومات غير مشروعة.

2- هجمات البرمجيات: وتشمل المصائد أو الأبواب الخلفية (أي اختلاس الثغرات) والسرقة أو اختلاس المعلومة أو الاستخدام اللحظي (سرقة أو اختطاف الجلسات).

وتشمل أيضاً: الهجمات عبر التلاعب بنقل المعلومات عبر أنفاق النقل، والهجمات الوقتية (باستغلال وقت معين لتنفيذ الهجمة) وأخيراً استخدام البرمجيات الخبيثة كالفيروسات، وأحصنة طروادة، والدودة الإلكترونية، والرقائق، والأبواب الخلفية، والقنابل المنطقية، والماكينات والميكروبات فائقة الصغر، والاختناق المروري الإلكتروني، ومدافع (Here) وقنابل (Emp) ويجمع بين هذه الأنواع أنها برمجيات ضارة تستخدم للتدمير أو التعطيل، وإن كان بعضها يستخدم في الأغراض العسكرية.

رابعاً: الهجمات والمخاطر المتصلة بعملية الحماية وتشمل هذه الأساليب والاعتداءات: العبث بالبيانات مثل تغييرها أو إنشاء بيانات وهمية في مراحل الإدخال أو الاستخراج، وخداع بروتوكول الإنترنت، حيث الغش والخداع والإيهام والتقليد والمحاكاة والسخرية، وإن كان استخدامه الشائع الآن يتعلق بهجمات فيروسات الإنترنت، كما تشمل الأساليب والاعتداءات المتعلقة بعملية الحماية جمع كلمة السر والتقاطها باستخدام برمجيات يمكنها ذلك، والقيام بأساليب المسح والنسخ، والهجوم بأسلوب استخدام المزايا الإضافية.

بروز أمن المعلومات

ونستطيع القول إن العالم أصبح يعيش ثورة هائلة في مجال المعلومات والاتصالات أتاحت للبشر قدراً هائلاً من المعرفة لم يكن متاحاً من قبل، كما وفرت هذه التقنية الجديدة فرصاً للمؤسسات والشركات والمصارف والحكومات، لتقديم خدماتها بشكل غير مسبوق.

وإذا كان ذلك هو الوجه المضيء لهذه التقنية فإن الوجه الآخر تمثل في إمكانية الاعتداء والاختراق وممارسة الإتلاف والتخريب والتجسس، الأمر الذي فرض ضرورة توفير قدر من الحماية يتناسب مع مستوى أهمية المعلومات.

وفي ظل تنامي ظاهرة الاعتداء على هذه البيئة المعلوماتية وخطورته على الأمن الوطني، واتجاهات هذا الاعتداء ليطال الأجهزة والبرامج والمعلومات والاتصالات من خلال اختراق الحماية المادية وغيرها، برز أمن المعلومات ليشكل مجموعة الوسائل والطرق المعتمدة للسيطرة على كافة أنواع المعلومات وحمايتها من أوجه الاعتداء المختلفة، على أنه لا ينبغي المبالغة فيه إلى الحد الذي يؤثر على عنصر الأداء، كما لا ينبغي التراخي فيه بحيث لا تكفل إجراءاته الحماية الواجبة.

وفي هذا المجال برزت وسائل تقنية متعددة يتعين توافرها وفي الوقت نفسه ينبغي على العنصر البشري في هذه المنظومة أن يسلك السلوك الصحيح بعيداً عن الأخطاء والإهمال، وفي كل الأحوال يتعين عدم الاعتماد على التقنيات الأجنبية الخاصة بأمن المعلومات وخصوصاً على الشبكات الرسمية التابعة للدولة، فالتجسس الذي يعد أحد ظواهر العلاقات الدولية تعدى النطاق العسكري والسياسي ليشمل الجانب الاقتصادي، فالحل الأمثل لأمن المعلومات هو تطوير الحلول الوطنية أو على الأقل وضع الحلول الأجنبية تحت اختبارات مكثفة ودراسات معمقة.

(وكالة الصحافة العربية)عن

أخبار دوت كوم

استعمالك للبريد الإلكتروني يشجعك على الكذب

واشنطن / متابعات:

وجد باحثون في جامعة ماساشوستس الأميركية أن الأشخاص يميلون للكذب خلال التحادث أو التواصل مع الآخرين عبر البريد الالكتروني مقارنة بالمحادثات وجهاً لوجه. بعدما حللوا بيانات شملت عينة من (110) أزواج من الجنس نفسه من الطلاب الذين دخلوا في محادثات مدتها (15) دقيقة إما وجهاً لوجه أو عبر استخدام البريد الالكتروني أو الرسائل الفورية.

ولاحظ الباحثون وجود درجة من الخداع في طرق التواصل الثلاثة لكنها تزداد لدى استخدام البريد الإلكتروني والرسائل الفورية. وتبين أن الكذب هو أكثر رواجاً في رسائل البريد الالكتروني.

وقال الباحثون إنه بالإضافة إلى المسافة التي تفصل الشخص عن الآخر فإن التواصل عبر البريد الالكتروني لديه مكون آخر وهو (عدم التزامن) أي عدم التواصل في الوقت الحقيقي كما في الرسائل الفورية والمحادثات الفورية.

وقال العلماء «يبدو على الأرجح أن عدم التزامن في ما يخص البريد الالكتروني يجعل المستخدمين يشعرون بأنهم أقل ارتباطاً مع متلقي الرسالة الذي لن يرد فوراً عليها بل سيتأخر إلى نقطة معينة مستقبلاً».

(اخترت لك)

فلسفة مهندس كمبيوتر في الحياة

سئل مهندس كمبيوتر عن معنى الدنيا؟ فأجاب بعد ما أنتهى من تحميل برنامج الماسنجر وقال: ما الدنيا إلا ماسنجر كبير فيها ناس ((On line).

على طول جنبك ولو احتجتهم تلاقيهم دائماً جاهزين وناس (Off line)دائماً مش موجودين حتى لو كانوا قريبين وناس (Away) ابتعدوا من زمان وغابوا من سنين وناس (Busy) على طول مشغولين ويجروا ومش لاحقين,وناس (Out to lunch) عايشين علشان يأكلوا وعلى الدنيا ميتين, وناس(Blocked) جرحونا كثير وبوجودهم مش مرغوبين وناس (Delete) تعبونا معاهم وعلى فراقهم قادرين وفيها اللى عملوا (Sign in) دخلوا وباللي مستنيهم مش عارفين, وفيها اللي صاروا (Sign out) راحوا بس في قلوبنا محفورين.

(عالم الإنترنت)

قانون يجرم تحميل الملفات غير الشرعية في اليابان

طوكيو / متابعات:

مرر البرلمان الياباني مشروعاً جديداً يهدف إلى تعديل قانون حقوق النشر بحيث يجعل تحميل ملفات الموسيقى والأفلام بشكل غير شرعي جريمة يعاقب عليها بما يصل إلى عامين في السجن أو غرامة تصل إلى مليوني ين (حوالي 25 ألف دولار أمريكي) وسيتم تفعيل التعديل بدءاً من أكتوبر القادم.

وقد أشعل المشروع الجديد جدلاً كبيراً في وسائل الإعلام اليابانية، حيث يمكن أن يؤدي مجرد تحميل ملف واحد إلى العقوبة. وقد رحبت شركات الإنتاج الموسيقي في اليابان بمشروع القرار وقالت بأنها ستتخذ الإجراءات اللازمة لإعلام الناس بهذه العقوبات الجديدة. ورأى المدير التنفيذي لشركة (سوني ميوزيك) في اليابان أن هذا التعديل سيقلل من انتشار انتهاكات حقوق النشر على الانترنت.

إلا أن جهات قانونية أخرى، عارضت القرار وقالت أن التعامل مع النشاطات الشخصية بعقوبات جنائية يجب أن يتم بحرص شديد، كما أن الضرر الذي يمكن أن يتسبب به تحميل الملفات غير القانونية بشكل فردي هو ضرورة غير ذي أهمية على الإطلاق.

وأشارت دراسة أجرتها أحدى شركات التسجيلات في اليابان إلى أنه قد تم في العام (2010) تحميل حوالي 4.36 مليار ملف بشكل غير شرعي في اليابان، في مقابل (440) مليون ملف تم شراؤها بشكل قانوني.

عالم التجسس والهاكرز

مواقف للهاكرز

اعتاد أحد الهاكرز المحترفين أن يدخل على مواقع البنوك عبر الإنترنت ويتسلل بكل سلاسة إلى الأرصدة والحسابات فيأخذ دولاراً واحداً من كل غني ويضع مجموع الدولارات في رصيد أقل الناس حساباً..