الأنباء
الاثنين 15 يوليو 2013

ملف الأسبوع

مدير تطوير الأعمال بشركة تساهيل الإلكترونية في حوار خاص مع «الأنباء»

أحمد بشير: المؤسسات الكويتية الحساسة لاتزال غير واعية بحجم خطورة القرصنة الإلكترونية

أحمد بشير

أحمد بشير متحدثا للزميلة منى الدغيمي (سعود سالم)

قال مدير تطوير الأعمال في شركة تساهيل الإلكترونية أحمد بشير ان المؤسسات الكويتية الحساسة لاتزال غير واعية بحجم خطورة القرصنة الإلكترونية وإلى الآن تقتصر فقط على قسم خاص لإدارة النظم الإلكترونية داخلي دون تخصيص خلية معنية بحماية النظم الداخلية من الاختراقات.

وأضاف في حوار خاص لـ «الأنباء» ان الكويت بحاجة الى قوانين إجبارية تلزم المؤسسات بضرورة التزود ببرمجيات حماية متطورة، لاسيما داخل المؤسسات الحساسة للدولة ومؤسسات القطاع الخاص المستهدفة دون غيرها لاسيما البنوك.

وأشار بشير الى أن التطور التكنولوجي خلق ما يطلق عليه «الحرب التكنولوجية»، معتبرا أنها أخطر من الحروب التقليدية، مشيرا الى أنها أصبحت تهدد الأمن الاقتصادي والأمن الدولي، وفيما يلي تفاصيل الحوار:

ما الجهود الكفيلة بالتصدي للخسائر المالية للاختراقات الإلكترونية؟

● **للأسف «نحن رد فعل لفعل» لا نستبق الفعل بتجهيز الجدار الناري لصد الاختراق المتوقع وليست لدينا قرارات دائمة ومتابعة دورية لدرء الخسائر التي قد تنتج عن أي اختراق غير متوقع وغير مستعد له الاستعداد الكافي.**

وأرى انه على المؤسسات ان تكون مطلعة على البرامج المقاومة أو المدافعة عن أي اختراقات، وأن تكون على تواصل بشركات ذات اختصاص لا ان تنجر وراء الإعلانات المموهة لبرامج قد تكلفها أموالا دون نتائج إيجابية.

وأحب ان أوجه الدعوة الى كل الشركات بأن تعي أهمية التزود ببرمجيات متطورة لحماية مخزون معلوماتهم من القرصنة المتعددة والمتطورة لأن هذا لن يكلفها شيئا مقارنة بالخسائر التي قد تسفر عن خرق مركز المعلومات أو أسرار مهمة لمؤسسة حساسة.

التطور التكنولوجي خلق ما يطلق عليه «الحرب التكنولوجية» وهي أخطر من الحروب التقليدية

فأي تعطيل أو عطب يطرأ على الموزع الرئيسي للإنترنت لأي شركة اتصالات يمكن أن يكلفها خسائر كبيرة لا تقارن ببعض الآلاف التي قد تستثمرها في برمجيات للحماية، وأتوقع ان قطاع الاتصال مجهز ببرمجيات حماية متطورة لأن دقيقة تعطيل تكلفهم ملايين، لذلك يجب على القطاعات الأخرى التي تعتبر مستهدفة أكثر من غيرها كالبنوك والقطاع النفطي ان تحصن شبكة اتصالها الداخلية والخارجية ببرمجيات حماية كافية لتتصدى لأي هاكرز لاأخلاقي.

هل الكويت بحاجة الى فنيين قادرين على التعامل مع الجرائم الالكترونية أم الى قوانين رادعة؟

● **المشكلة في الكويت تثقيفية بالأساس لأن المؤسسات الكويتية، لاسيما الحساسة منها كمؤسسة النفط والبنوك، لاتزال غير واعية بحجم خطورة القرصنة الإلكترونية والى الآن يقتصرون فقط على قسم خاص بالإدارة الإلكترونية داخلي دون تخصيص خلية معنية بحماية النظم الداخلية من الاختراقات التي قد تسببها مجرد نقرة بالخطأ على رسالة مجهولة عن طريق البريد لإلكتروني.**

وأرى أن التطور الحديث للتكنولوجيا جعلت الشبكة مفتوحة بين المؤسسة والعالم الافتراضي، هذا ما جعل الأسرار الداخلية عرضة للقنص من طرف جهات مختلفة، سواء كانت منظمة أو عشوائية، لذلك الكويت بحاجة الى قوانين إجبارية تلزم المؤسسات بضرورة التزود ببرمجيات حماية متطورة، لاسيما داخل المؤسسات الحساسة للدولة ومؤسسات القطاع الخاص المستهدفة دون غيرها، خاصة البنوك.

وأرى ان الكويت الى الآن لم تمنح قطاع الأمن الإلكتروني الأولوية المستوجبة رغم وقوع خسائر كبرى في بعض المؤسسات الحساسة، لاسيما الهجوم الإلكتروني الأخير على مؤسسة النفط التي تعرضت الى هجوم من قبل مجموعة «أنونموس» التي تستهدف المواقع الإلكترونية للمؤسسات النفطية في كل دول العالم، وأعتقد ان الكويت بحاجة ملحة إلى سن قوانين إجبارية من الدولة ولا تفتقر إلى الفنيين لأن الخطر يهدد أسرار دولة بكاملها وليست مؤسسة بعينها، وأخلاقيات الهاكرز تختلف.

ما مدى تكلفة برمجيات الحماية بالنسبة للبنوك أو الشركات؟

● **مقارنة بالخسائر التي قد تسفر عنها الهجمات الإلكترونية التي تقدر بالملايين فان تكلفة برمجيات الحماية لا تتجاوز بعض الآلاف، وأرى ان برمجيات الحماية إذا قورنت بالخسائر لا تقدر بشيء فمثلا «tripe wire» وهو أحد البرمجيات المتطورة للحماية من القرصنة الإلكترونية بالنسبة لسعره لا يمثل شيئا بما يوفره من طرق حماية متطورة.**

أرى ان الشركات الحساسة خاصة إذا استثمرت بعض الآلاف في حماية امن معلوماتها سيقيها من خسائر ليست مادية فقط.

ما أهم برامج الحماية وآليات مواجهة القرصنة؟

● **هناك أكثر من برنامج للحماية متطور وهناك كذلك أنواع من الجدار الناري و«tripe wire» من البرمجيات الحماية المتطور وتجدر الإشارة هنا الى ان الخطر الذي يهدد مختلف المؤسسات من الداخل وليس من الخارج فقط لأن سوء الاستخدام أو قلة المعرفة باستخدامات الكمبيوتر المتعددة قد تفتح ثغرات للهاكرز للاختراق السريع لمركز المعلومات للمؤسسة وتدميره أو قنصه، لذلك أدعو المؤسسات إلى استخدام برامج متطورة ضد الڤيروسات المختلفة لحماية المنظومة الإلكترونية الداخلية.**

ما الحلول الكفيلة للتصدي للتطور السريع لبرامج الاختراق؟

● **يجب ان تكون هناك دراسة مستفيضة للبرمجيات ومتابعة دورية ومواكبة تطوير برمجيات الحماية لأن في المقابل الهاكرز سريع التطور ويجب ان نضع أكثر من برنامج وأكثر من جدار للحماية، لكن هناك نقطة مهمة يجب ان أشير إليها وهي انه لا يكفي ان نتزود ببرنامج حماية متطور، لكن الجزء الأهم كيفية ربط الشبكة الإلكترونية بطريقة محكمة لحمايتها من الثغرات.**

ويجب ان تكون هناك عمليات تدقيق دورية على منظومة البرمجيات التي تحمي بيانات المعلومات وعملية التدقيق تشمل المنظومة الإلكترونية الداخلية والخارجية أو بمعنى أدق التدقيق على سلامة البنية التحتية للشبكة الإلكترونية كل 6 أشهر على الأقل من طرف خبراء فنيين. وقد بدأ حديثا في الكويت التوجه من بعض الشركات للاستعانة بشركات تدقيق فني للشبكات الإلكترونية على العالم الخارجي والافتراضي. والحل ليس بشراء أي تكنولوجيا حديثة، بل في كيفية اختيار التكنولوجيا التي تتماشى مع طبيعة المنظومة الإلكترونية لكل مؤسسة.

ما أشهر برامج القرصنة؟

● **هناك أكثر من برنامج للقرصنة وهي متعددة، ويمكن بكل سهولة للأسف الدخول على شبكة الإنترنت وتحميل نماذج منها مجانا وهي متاحة لا تكلف مشتريها إلا بعض الدولارات، ويمكن ان تسفر عن خسائر كبيرة، وهذا يرجع الى قلة الوعي بخطورة هذه البرامج التي تحمل تسميات مختلفة ومتغيرة.**

ما أسباب انتشار الجريمة الإلكترونية بشكل لافت للانتباه؟

● **في الحقيقة الأسباب تختلف باختلاف هدف كل هاكرز، فهناك من يريدون جذب الانتباه إليهم، وهناك من لهم هواية الاختراق، وهناك مجموعات منظمة لهم رسالة محددة، وتوجد مجموعات مجندة، كذلك التطور التكنولوجي السريع من أسباب انتشار الجريمة الإلكترونية لأنه فتح المجال للأسف لانتشار القرصنة الإلكترونية، وذلك لغياب قوانين رادعة ولصعوبة توصيف الجريمة في بعض الأحيان.**

فالتطور التكنولوجي خلق ما يطلق عليها «الحرب التكنولوجية» وهي أخطر من الحروب التقليدية، حيث أصبحت تهدد الأمن الاقتصادي والأمن الدولي.

لماذا البنوك الأكثر استهدافا من طرف الهاكرز؟

● **البنوك الأكثر استهدافا من طرف «الهاكرز» لأنها باختصار موضع الأموال، وهي تستقطب الهاكرز الباحث عن الاستيلاء عن الأموال بطريقة «سهلة» وتحويلها الى أرصدة مختلفة ثم سحبها فيما بعد، لذلك يجب ان تكون البنوك من المؤسسات الأكثر حرصا على التزود ببرمجيات الحماية والتدقيق عليها بصفة دورية.**

هل المؤسسات الكويتية واعية إلى ضرورة إنشاء إدارة خاصة لمكافحة الجريمة ذات الطابع الإلكتروني؟

● **أتوقع ان هذا موجود في الوزارات الحساسة كوزارة الداخلية ووزارة الدفاع، لكن المؤسسات الأخرى مازالت ينقصها الوعي، ويجب أن تكون هناك دورات وحملات توعية لحث مختلف المؤسسات الحساسة على إحداث إدارة خاصة لحماية أمن معلوماتها لأن أي خطورة لا يمكن توقع حجم خسارتها ومدى تهديدها لأمن الدولة في حد ذاتها.**

وأرى ان السوق الكويتي الإلكتروني لايزال يعيش هدوءا نسبيا وأتوقع ان تحدث قفزة في آخر السنة الجارية، وكذلك السوق التكنولوجي الكويتي يشكو دورة مستندية بطيئة جدا والقطاع التكنولوجي لا يتوافق مع البطء لان البرمجيات سريعة التطور، لذلك يجب محاربة هذه الدورة المعقدة وتسريع الإجراءات وأخذ القرار لحماية أمن البلد.

● **منى الدغيمي**

«الأنباء» تفتح ملف الاختراقات الإلكترونية للتعرف على طبيعتها والجهود المبذولة لمواجهتها

مصرفيون لـ «الأنباء»: مواجهة الجريمة الإلكترونية منوطة بتحديث أنظمة الحماية ورصد ميزانيات خاصة من قبل البنوك المحلية

عبدالله الحميضي

نجاة السويدي

علي المديهيم

عباس المجرن

اتسع نطاق استهداف القرصنة الإلكترونية ليطول المؤسسات والأفراد على السواء، وقد ساعد على تزايد عمليات الاختراق الأمني للمعلومات التقدم التكنولوجي الكبير لوسائل الاتصال وتنوع برامج تداول المعلومات وحرية وصولها لمستخدميها إلى جانب التطور التقني في نقل وتخزين البيانات عبر شبكة الإنترنت والانتشار الواسع للهواتف والأجهزة الذكية واستخدام قنوات عديدة للتجارة الإلكترونية.

وبات قراصنة الشبكة العنكبوتية أو ما يطلق عليهم اسم «الهاكرز» هاجسا يرهق تفكير وميزانيات الكثير من الشركات والبنوك وحتى المشاهير مما دعا إلى استغاثة الشركات بأصحاب الخبرات التقنية لتطوير برامج حماية تكفل أمن معلوماتهم وتقيهم من الخسائر الكبيرة.

«الأنباء» رصدت آراء بعض المصرفيين والاقتصاديين حول آليات التصدي لمخاطر الاختراق في القطاعات الاقتصادية عموما والقطاع المصرفي خاصة وطرق حماية المعاملات المصرفية من أيدي القراصنة وتوخي أقصى درجات الحيطة والحذر واتخاذ التدابير التقنية الحديثة للسيطرة عليها، كما نصحوا بضرورة اتباع تعليمات وقواعد الأمان عند إجراء المعاملات المصرفية على الإنترنت بواسطة الحاسوب أو عن طريق الهواتف الذكية أو الحواسب اللوحية أثناء التنقل والتجول، وفيما يلي التفاصيل:

الحميضي: أهمية وإلزامية تحديث برامج الحماية في البنوك لضمان أمان إجراءات المعاملات المصرفية

بداية شدد رئيس مجلس إدارة شركة التسهيلات التجارية عبدالله الحميضي على ضرورة تثبيت برامج مكافحة الڤيروسات مع تحديثها بصورة منتظمة، بغرض الحماية من أي اختراقات، التي قد تتمكن من الاطلاع على جميع البيانات الحساسة أثناء إجراء المعاملات المصرفية على الإنترنت أو التلاعب فيها.

ورأى الحميضي أن هناك ضرورة لاستخدام نظم تشغيل وبرامج متطورة لضمان الحماية والأمان من أي عمليات اختراق مهما كانت تكلفتها، مبينا أنه إلى جانب ذلك يجب القيام بإجراءات وتدابير الأمان التقني خاصة أثناء الاتصال بشبكة الإنترنت.

رصد ميزانيات

بينما رأت الخبيرة الاقتصادية نجاة السويدي ضرورة رصد ميزانيات خاصة لتطوير أجهزة الحماية المصرفية في البنوك خاصة بعد أن تعرضت عدة بنوك لعمليات اختراق على شبكاتها المصرفية من قبل بعض الهواة من اجل إثبات الذات أو من أجل تحصيل أموال غير مشروعة.

السويدي: ضرورة رصد ميزانيات خاصة لتطوير أجهزة الحماية المصرفية في البنوك

وقالت السويدي إن النظم الموجودة حاليا في أغلب البنوك لا تتماشى مع المعايير العالمية الموضوعة من قبل المؤسسات المصرفية لوقاية الشبكات المصرفية من الاختراق، حيث تنظر بعض البنوك إلى أنها مرتفعة التكلفة وتحتاج إلى فريق عمل مما يزيد من المصاريف الإدارية لديها والبعض الآخر يرى أن عمليات الاختراق في الكويت مازالت عند مستويات طبيعية ولا داعي للتكلفة وشراء نظم حماية جديدة، وهو الأمر الذي انعكس بالسلب على عدة بنوك محلية مؤخرا خاصة التي تعمل وفق الشريعة الإسلامية التي تستخدم نظما قديمة بعيدة عن التطور التكنولوجي الذي تستخدمه البنوك الأجنبية.

وأضافت ان مستويات الاختراق في البنوك الأجنبية قد وصلت لمستويات متدنية بنهاية العام الماضي نظرا لاستخدامها نظم حماية مرتفعة التكلفة الأمر الذي اصبح يمثل عقدة كبيرة لدى العديد من المخترقين مما دفعهم إلى التوجه نحو الوطن العربي نظرا لانخفاض آليات ونظم الحماية فيها كالمؤسسات الاقتصادية في شتى القطاعات وهو ما ظهر خلال الآونة الأخيرة حينما حدث اختراق لشركة سعودية كبرى ومن ثم انتقل الأمر إلى عدة دول خليجية منها الكويت، لذا هناك حاجة ماسة إلى تغيير وتطوير أنظمة الحماية سواء في القطاع المصرفي بشكل خاص او في القطاعات الاقتصادية بشكل عام.

تعاون مصرفي

من جانبه، أكد مدير عام الخدمات المصرفية في البنك التجاري سابقا علي المديهيم ضرورة تعاون البنوك مع عملائها من اجل كبح عمليات الاختراق على المصارف بشكل عام وذلك عبر التزام الطرفين بالتعليمات والمعايير الموضوعة لمواجهة تلك المخاطر التي اصبحت ظاهرة في مجتمعنا وتحتاج إلى وقفة للسيطرة عليها، مبينا ان مستويات الاختراق في الكويت مازالت عند مستوياتها الطبيعية ولا داعي للقلق حيالها شريطة ان تقوم البنوك بتحديث أدواتها المصرفية المتعلقة بتكنولوجيا حماية الشبكات المصرفية والاستعانة بجميع الخبرات العالمية لتطبيق احدث نظم الحماية الموجودة بالعالم.

المديهيم: «الكريدت كارد» أكثر الأدوات المصرفية عرضة للاختراق ويجب تحديثها

وقال المديهيم ان عملاء البنوك يقع على عاتقهم نسبة كبيرة من عمليات الاختراق التي تحدث حيث يضع العديد منهم بياناتهم المصرفية متضمنة اسم المستخدم وكلمة السر على الهواتف الذكية التي اصبحت عرضة للاختراق في أي وقت الأمر الذي يعرض العميل إلى تكبد خسائر قد تصل إلى تصفية حسابه بالكامل لذا هناك ضرورة لاتباع إجراءات البنوك التي يرسلونها لعملائهم حتى يتلافى العملاء أي خسائر.

وأضاف: من اكثر الأدوات المصرفية عرضة للاختراق هي «الكردت كارد» نظرا لما يحمله من جميع البيانات المتعلقة بحساب العميل مما يسهل على الهاكرز الحصول عليها اثناء تواجده في أي من الأماكن العامة والقيام بعمليات سحوبات مالية من شبكة الانترنت، لذا هناك ضرورة من الاحتفاظ بها في أماكن مخصصة لها وعدم إخراجها إلا في أوقات استخدامها فقط وعدم اضطلاع أي أحد عليها.

المجرن: البنوك المحلية بحاجة إلى تعزيز شبكة حمايتها المصرفية

قواعد البيانات

من جانب آخر، قال الخبير المصرفي عباس المجرن ان البنوك المحلية بحاجة إلى تعزيز شبكة الحماية لديها وتطويرها عبر تحديث قواعد بياناتها المستخدمة التي تتمثل في برامج الاوراكل وسيسكو وهما من ابرز البرامج التي تستخدمها البنوك المحلية حاليا إلا انها في حاجة إلى تحديث حتى يتم سد جميع الثغرات التي حدثت بها نظرا للتطور التكنولوجي الذي يحدث يوميا على تلك البرامج.

وأضاف المجرن أن هناك ضرورة لإجبار البنوك المحلية على استخدام برامج حماية متطورة وفق معايير عالمية حتى وان كانت مكلفة وذلك عبر الاستعانة بكبرى المؤسسات العالمية العاملة في مجال نظم الحماية من الاختراقات.

وأوضح ان حرب تكنولوجيا الاختراقات مستمرة ويجب على البنوك متابعتها لحظة بلحظة حتى تتمكن من سد أي ثغرات قد تواجهها في المستقبل جراء أي عملية اختراق.

● **محمود فاروق**