الأنباء
الاحد 17 مارس 2013

أكدت مديرة إدارة المشاريع في شركة تساهيل الالكترونية المعلوماتية الشيخة مريم صباح الناصر الصباح أن «تساهيل المعلوماتية» قادرة على مواجهة كل التحديات مهما عظمت، فهي تواصل تطوير أدواتها وذاتها وتنافس كبرى الشركات الأوروبية والأميركية، وتقدم خدماتها السرية لكبرى الشركات والمنظمات والمؤسسات الحكومية والوزارات المختلفة، مشيرة إلى أنها قامت بحماية العديد منها من هجمات للهاكرز كادت تودي بملفات في غاية الأهمية. وذكرت في حوار خاص لـ «الأنباء» أن الكويت دولة مستهدفة من قبل مجموعات من الهاكرز، وهي حتى الآن لا تشعر بالخطر المحدق بها على الرغم مما يحدث في العالم من جرائم الكترونية، وانهيارات في الاقتصادات نتيجة القرصنة، وإفلاس في البنوك الكبرى واختراقات وتسريب معلومات في أضخم مراكز صنع القرار في العالم. وأبدت الشيخة مريم استعداد «تساهيل» لاختبار أي نظام معلوماتي مجانا للوقوف على مدى قدرته على الصمود أمام الاختراق، واختراقه من قبل مهندسي الشركة لتأكيد قدرتنا على اختراق أي منظومة مهما كانت قوتها وحصانتها، إضافة إلى تأكيد الشركتين على توقيع اتفاقية لسرية المعلومات. وفيما يلي تفاصيل الحوار:

حوار: منى الدغيمي

مدير إدارة المشاريع في شركة تساهيل الإلكترونية المعلوماتية مريم صباح الناصر في حوار خاص لـ "الأنباء":

الكويت لا تعترف بالجرائم الإلكترونية كتهديد.. ولا ترصد أي مبالغ لمواجهتها

انتشرت في الآونة الأخيرة وبشكل ملحوظ ظاهرة اختراق مواقع المؤسسات الحكومية والشركات الكبرى فيما بات يعرف بالجرائم الالكترونية، برأيك ما الأسباب التي تدفع الهاكرز أو أي جهة إلى هذه العمليات غير الشرعية والقانونية؟

● **بات لدينا اليوم ما يعرف بالثورة التقنية التي لم يشهد لها العالم مثيلا، وهناك تسارع كبير في المنافسة بين كبرى الشركات العاملة في مجال البرمجيات والبرامج المتنوعة، والتي أصبحت البرامج المرتبطة بالانترنت الشاغل الأساسي لكل العالم في هذه الأيام.**

لقد استطاع الهاكرز أو مجرمو الانترنت أن يطوروا كثيرا من إمكاناتهم وقدراتهم الاختراقية بسبب الكم الهائل والطفرة الحاصلة في مجال التقنية والانترنت، وهذا الأمر يشكل خطرا كبيرا على الشركات الكبرى والمؤسسات الحكومية التي لم تقم بتعزيز دفاعاتها ومواكبة التطورات الهائلة الحاصلة خلال الفترة القليلة الماضية.

ومما يعزز الخطر أكثر من السابق عدم قدرة تتبع الفاعلين في العديد من الدول، وانفتاح العالم بشكل كبير وعدم وجود قوانين ناظمة للتعامل مع شبكة الانترنت والتفاعل مع الجهات العاملة على الشبكة العالمية.

هل ترين أن عدم تمكين الدفاعات ضد الاختراقات هو السبب الرئيسي في كثرة الجرائم الإلكترونية في الفترة الأخيرة؟

● **عدم تمكين الدفاعات هو أحد الأسباب وليس السبب المباشر، فهناك أسباب مثل عدم قيام الكثير من المؤسسات باستخدام وسائل حماية مناسبة أو عدم استخدامها بالشكل الصحيح.**

ولكن المشكلة الكبرى التي تعاني منها الكويت بالتحديد هي عدم الاعتراف بأن الجرائم الالكترونية تهديد حقيقي، وبالتالي لا يتم رصد أي مبالغ أو تخصيص أي تمويل لمواجهتها، ونحن هنا لا نعني فقط خطر تسرب المعلومات من المؤسسات الحكومية، بل التهديد بالفقدان الكلي للمعلومات أو التوقف الكامل لجميع المعاملات التجارية مما يفقد الشركات ثقة التعامل معها وحرفيتها وهذا يتسبب في خسارة الملايين وبالتالي يحدث انهيار اقتصادي يشل مرافق الدولة ويعرضها لاهتزاز مركزها عالميا.

هل ترين الإشارة إلى الهجمات التي وقعت في أميركا والعديد من الدول؟

● **بالطبع، فلدينا هجمات أغسطس على (Aramco & RasGas) والتي أغلقت مواقعها الالكترونية وعلق العمل ببريدهم الالكتروني، وهذا تسبب لهم في خسائر كبيرة انعكست على اقتصاد الدولة ككل، وهزت من ثقة المتعاملين معهم.**

وهناك أيضا مخاوف من الهجوم على إحدى الوزارات السيادية في الدولة وسرقة الأسماء والمعلومات الشخصية ونشر الانتهاكات على موقع «twitter» الشهير.

الشيخة مريم صباح الناصر الصباح (محمد خلوصي)

هنالك مخاوف من الهجوم على إحدى الوزارات السيادية في الدولة وسرقة الأسماء والمعلومات الشخصية ونشر الانتهاكات على موقع "تويتر"

ومن المخاوف أيضا الهجوم على موقع لإحدى المؤسسات التعليمية والتلاعب بالنتائج والدرجات وتغيير قائمة القبول، فهذا الأمر سيتسبب في دمار هائل وانهيارات اقتصادية لا يمكن حصر نتائجها أو التعرف على أبعادها وخسائرها وخصوصا إذا كانت في قطاعات مالية كبرى كالمؤسسات الكبرى والبنوك والوزارات.

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

● **نحن نلاحظ أن الوعي يمر بمراحل متعددة وبطيئة، وللأسف لا يتم التحرك من قبل المنظمات إلا بعد التعرض للهجوم أو أن يتعرض أقرانها للاختراق.**

ولدينا منظمات واعية لهذا الأمر فأنشأت شكلا من أشكال الأمان ولكنها لم تستغله الاستغلال الصحيح أو قامت باستغلاله ولكن بعد فوات الأوان.

على الحكومة مسؤولية تنسيق الجهود وفرض القواعد واللوائح لمكافحة المشكلة، وعدم الاكتفاء فقط بتأمين الحماية الالكترونية، فنحن بحاجة ماسة إلى طرف ثالث للمراقبة بشكل نصف سنوي على أقل تقدير، فهذا يضمن المصداقية ويعطينا نتائج مضمونة.

وخير مثال على هذا ما قام به بنك البحرين المركزي من فرض خطوط ومبادئ تلتزم بها كل البنوك العاملة في المملكة في مجال أمن المعلومات، وقد استدعى ذلك مراقبة واختبارا نصف سنوي من قبل طرف ثالث أو أي شركة متخصصة في هذا المجال.

وهنا لابد من أن نذكر أن كبرى المنظمات التي تمتلك معلومات ضخمة وذات حساسية عالية تنفذ نوعا من تلك الأنظمة، ولكن بشكل ذاتي من دون إشراف من أي طرف خارجي.

هل أدى عدم وجود قوانين وتشريعات خاصة بمكافحة الجريمة الالكترونية إلى انتشارها أكثر، لاسيما على مستوى الكويت؟

● **للأسف نعم، ونحن نأمل أن تتعامل الحكومة مع هذه المشكلة على انها من أهم مشكلات العصر، وهناك في الحقيقة ما يدعو للتعجب من عدم الاهتمام بهذه المشكلة على الرغم من تعرض قطاعات تكنولوجيا المعلومات يوميا للكثير من المخاطر والاختراقات والضربات الموجعة.**

إن مستخدمي الانترنت في منطقتنا على قدر جيد من المهارة والمعرفة في مجال تكنولوجيا المعلومات، لذا يجب أن تكون هناك حدود لا يمكن تجاوزها، وهذا الأمر لا يمكن لأي جهة تحقيقه إلا إذا كانت جهة حكومية.

كيف تقيمين الوسائل الحديثة لمكافحة الجرائم الالكترونية؟

● **في ظل التطور المتسارع فإن الاستراتيجيات والحلول لا تنتهي في مواجهة هذه الجرائم، والمفتاح يكون في أن نضع أنفسنا مكان مجرم الانترنت وأن نفكر في الطريقة ذاتها التي يفكر فيها، بالإضافة إلى محاولة فهم ماذا يريد؟ وما الطريقة التي سيسلكها للاختراق والحصول على ما يريد، وكيفية حماية أنفسنا قبل حدوث الجريمة، فهذا الأمر يتطلب جهدا كبيرا في متابعة وتوثيق الجرائم الالكترونية، ومنحها القدر الكافي والنصيب العادل من الأهمية، من خلال إنشاء مؤسسة حكومية متخصصة في هذا المجال.**

قدر حجم خسائر الجرائم الالكترونية في السعودية بـ 427 مليار ريال في 2012، في ظل عدم وجود تقديرات صادرة من الكويت، ما الأسباب وراء ذلك؟

● **هذا الأمر صحيح، والمشكلة تكمن في أنه لا يتم الإبلاغ عن الجرائم الالكترونية بآلية صحيحة أو من خلال تقارير مناسبة أو وعي يقظ، لذلك من الصعب تقدير حجم الخسائر في الكويت على الرغم من توقعي بأنها كبيرة جدا، وخصوصا إذا ما قرأنا جيدا ما أشارت إليه أبرز المؤسسات المالية والاستشارية من أن جرائم الانترنت قد زادت بنسبة 17٪، بالإضافة إلى غياب المنظمات المتخصصة في كشف ومكافحة هذه الجرائم.**

يتخوف المتخصصون في الوقت الحالي مما يسمى بـ «البوت نت» أو «شبكة الروبوت» لاختراق أجهزة الكمبيوتر، هل من وسائل حديثة للتصدي لهذه الشبكات؟

● **بالطبع، فمحترفو اختراق الأجهزة أو الهاكرز كما يدعون، يستخدمون تقنيات ذكية للتعامل مثل(Bot_net) او(cyber robot) او(zero day attack) للتحكم بالأجهزة ثم يستخدمون هذه التقنيات في وقت لاحق لشن هجمات متطورة، ولكن يمكن للشركات إجراء عمليات تقييم قابلية التأثر، وتقنيات اختبار الاختراق لتحديد المخاطر على البنية التحتية لتكنولوجيا المعلومات والتعرف على الخطر الحقيقي المنتظر قبل وقوعه.**

ووفقا لخبرائنا فإن مستخدمي الانترنت يصابون بمرض يسمى بـ (click mania) وهو النقر فوق كل شيء من دون قراءته أو فهم ماهيته مما يهدد امن شبكاتهم وأنظمة معلوماتهم، ولذا يمكن تسليط الضوء على ذلك من خلال إطلاق حملات توعوية عامة لتحسين المعرفة لدى مستخدمي شبكة الانترنت.

«تساهيل» تقدم الاستشارات المعلوماتية وخدمات الكترونية ومعلوماتية، هل وجدتم إقبالا محليا وخليجيا على خدماتكم، وما أبرز القطاعات التي تتعاملون معها؟

● **لابد من أن نشير هنا إلى أنه منذ عام أصدرت الولايات المتحدة الأميركية تحذيرا للشركات العاملة في الشرق الأوسط بأنها ستكون هدفا للمخترقين ومجرمي الانترنت والهاكرز، ثم توارادت الأنباء عن اختراقات لبعض كبرى شركات النفط في المنطقة.**

وبعد ذلك أصدرت مجموعة (Hack visit) المشهورة قائمة بالشركات المستهدفة ومنها بعض الشركات الكبرى الكويتية، ولذلك فقد بدأ الوعي ينتشر بضرورة وجود طرف قادر على المتابعة وضمان أمن المعلومات المخزنة.

وأما بخصوص أبرز عملائنا فنحن نتعامل مع كبرى الشركات والوزارات والهيئات والبنوك.

هل من أسماء معينة؟

● **نحن نعمل مع أبرز واهم قطاعات الدولة والوزارات السيادية الحكومية وكبرى الشركات في الكويت التي تعتبر الأكثر استهدافا، وفي الوقت نفسه هي مخزن مهول للمعلومات فائقة الأهمية.**

أما بخصوص الأسماء فهناك سرية تامة حول هذا الأمر وتحفظ شديد على كشف أسماء عملائنا لأننا نضمن لهم الحماية والسرية التامة، وهذا هو صميم عملنا.

هل تصديتم لأي اختراق حصل خلال أداء أعمالكم؟

● **هذا الأمر طبيعي جدا، فقد وقعنا أمام الكثير من المشاكل والاختراقات وتمكنا من حماية أكثر الجهات الحكومية حساسية من الاختراق، وهناك حالات كادت أن تخترق وتؤذي كما هائلا من المعلومات وتجعلها في مهب الريح استطعنا التصدي لها ومنعها من الوصول إلى أهدافها وتحقيق مراميها السيئة.**

ما الطموحات التي تحاولون الوصول إليها، ومن أبرز منافسيكم؟

● **نحن ننافس كبرى الشركات العالمية في أوروبا وأميركا، ولدينا الكفاءات القادرة على المتابعة ومهندسون متخصصون في مجالات الحماية والتقنية على أعلى المستويات، ونحن نتطلع إلى الانتشار أوسع من دائرة دول الخليج العربي لأننا نمتلك كل مقومات القوة والجاهزية العالية للتصدي لأي اختراق وحماية عملائنا من أي هاكرز يحاول الدخول وسرقة المعلومات.**

وقد حصلنا على شهادة امن المعلومات ونتعامل مع عباقرة الانترنت في العالم الذين يعملون تحت لواء «تساهيل» ويقدمون لنا الخبرات الكبرى.

هناك توقعات بأن عام 2013 سيكون حافلا بتطوير مشغلي الشبكات الإجرامية لوسائلهم من اجل القيام بهجمات مقنعة وأكثر تطورا وتعقيدا، ما الإجراءات التي ستقومون بها للتصدي لهذا الهجوم وحماية الشبكة من هذه الاختراقات؟

● **نحن فخورون جدا بمستوى المخترقين المهرة لدينا في الكويت، ولكن ما نود القيام به هو توجيه هذه المهارة والطاقة إلى شيء منتج وبناء، ونحن في تساهيل المعلوماتية ندرك جيدا ما نحن بصدد مواجهته، فمهندسونا هم الأفضل عالميا، وهم الأكثر رواجا في تقديم المحاضرات، وإطلاق الندوات محليا وعالميا.**

إن ما نقوم به لا يشجع فقط على تحصيل المعرفة في قطاع تكنولوجيا المعلومات ولكننا نسعى للإرشاد والتعريف بكيفية القيام بذلك بطريقة أكثر مهنية واحترافية من شأنها إفادة مجتمعنا والمحافظة عليه.

لا أبالغ إن قلت إن مهندسينا المهرة مطلعون ومدربون جيدا، فقد عملوا مع مؤسسات متخصصة في جميع أنحاء العالم وتقييمات الشركات لهم مبهرة.

ما رسالتك للشركات الكبرى والمؤسسات في الكويت الحكومية؟

● **تظن العديد من الشركات الكبرى في الكويت انها ليست بحاجة إلى ما تقدمه تساهيل المعلوماتية، ويعتقدون ان لديهم حائط امان الكترونيا صلبا قادرا على مواجهة أي اختراق أو هجوم، لذا يسعدنا أن نقوم أمامهم باختبار أنظمة الاختراق على أجهزتهم وفي مكاتبهم وأمام أعينهم، وفي الوقت الذي يحددونه لنبين لهم سهولة التسلل إلى جهاز كل موظف في شركتهم، وهذا الأمر أعتقد أنه ليس صعبا على مهندسينا، ولكنه صعب جدا على من يعملون في هذه الشركة عندما يعلمون أنه من السهولة بمكان خرق أنظمة الدفاع لديهم والتسلل إلى أجهزتهم وسحب جميع المعلومات منها، إضافة إلى توقيعنا على اتفاقية سرية المعلومات، وهذا الأمر سيعزز من ضمان السرية والمعلومة لدى جميع عملائنا.**

«تساهيل» صمام أمان ضد أي اختراق للهاكرز وحماية أمن المعلومات لكبرى الشركات والمؤسسات الحكومية

حصلنا على شهادة أمن المعلومات ونتحفظ على أسماء عملائنا من كبرى الشركات والوزارات تنفيذاً للسرية وأعلى درجات الحماية

تمكنا من حماية أقوى الجهات الحكومية من عمليات اختراق محققة وضياع المعلومات وجعلها في مهب الريح

مستعدون لاختبار أي نظام معلوماتي مجاناً للنظر في مدى قدرته على الصمود في وجه الاختراق وتوقيع اتفاقية سرية المعلومات

«تساهيل» تضم نخبة من المهندسين وعباقرة المعلوماتية في العالم وتخوض منافسة مع كبرى الشركات في أوروبا وأميركا

من الصعب تقدير حجم الخسائر التي تسببها الجرائم الالكترونية في الكويت لغياب المنظمات المتخصصة في كشف ومكافحة هذه الجرائم

«تساهيل» تتحدي أي نظام اختراق متطور

شددت مريم الصباح على أن «تساهيل الالكترونية المعلوماتية» تقدم أرقى أنواع الخدمات في مجال التقنيات ومحاربة الهاكرز والمحافظة على سلامة منظومة المعلومات.

وأشارت إلى أن «تساهيل» ترفع إشارات التحدي في وجه أي نظام اختراق يتم تطويره وتقف في وجه التحديات وتقدم نفسها على أنها صمام الأمان لحماية المؤسسات الحكومية والشركات الكبرى.

وأضافت: «ليس مستغربا أن تقدم «تساهيل» نفسها على أنها قادرة على حماية أمن المعلومات في ظل جمعها لنخبة من المهندسين وعباقرة المعلوماتية في العالم وأقوى الهاكرز الذين تم تحديد وجهاتهم لتكون في مجالات الحماية لا القرصنة».

مريم الصباح متحدثة للزميلة منى الدغيمي