

خلال ورشة عمل بالجلسة الثالثة لمنتدى الحكومة الإلكترونية

# الاستجابة للأحداث الأمنية والمعلوماتية والتحقيقات الجنائية والحل الآمن للتشارك في تبادل وتخزين الوثائق مطلب مهم

لشركة هواوي متشدد، موضحاً ان التطفل هو سلوك غريب لرؤية أي شيء بشكل غير قانوني.

## صناعة مخيفة

أما العضو المنتدب لكاسبرسكي خالد أبو بكر فقد استعرض الحلول الأمنية من الشركة، متسائلاً: عن مدى استجابة الجهات قبل أو بعد وقوع الحدث وهل المهاجمون متقدمون عنا؟ وهل الشركات تعمل لإيجاد فيروسات لزيادة مبيعاتها؟

وأضاف ان الشركة اكتشفت كثيراً من الهجمات خلال الفترة الماضية، حيث تم العمل لإيجاد برنامج ضار لمهاجمة النظام التشغيلي، وقد تم تمويله من قبل حكومات لمهاجمة حكومات أخرى في بعض الدول.

وأشار إلى ان شركات التكنولوجيا ليست أمنية بالشكل الكافي وأن هذه الشركات تحاول فقط ان يكون لديها تكنولوجيا.

وقال: شركتنا تنفق أموالاً على البحوث والتطوير ولكن ليست لدينا أموال كالحكومات لعمل برامج ضارة، نحاول نصل إلى نقطة لتحقيق الأمن للأفراد. وأشار إلى ان هذه الصناعة مخيفة وعالية الثمن والمهاجمون يحذون مهاجمة الهواتف النقالة كونها تحوي معلومات وبيانات سرية والأفراد يشعرون انهم آمنون عبر استخدام هواتفهم النقالة.

وأشار إلى ان الشركة اكتشفت 300 ألف حادث لبرامج ضارة في تلك الهواتف خلال النصف الأول من 2013 وحالياً هذا الرقم في تزايد ولا يوجد منسج للأمن في الهواتف النقالة.

وأوضح ان الهجمات المستهدفة تنمو يوماً بعد يوم بشكل متسارع في الكويت وصناعة النفط والغاز، كما ان هناك بنكين تعرضا لهجوم هذا العام.



خالد أبو بكر وجو سو واريك نيكلاوس وأوجوزان فيليزيباي خلال الجلسة الثالثة من المنتدى (قاسم باشا)



خالد عبدالكريم العنزي مترسدا الجلسة

## عاطف رمضان

استعرضت ورشة العمل للجلسة الثالثة من منتدى الحكومة الإلكترونية التي عقدت خلال اليوم الثالث من فعاليات المنتدى أمس برئاسة مدير إدارة تقنية المعلومات والبنية التحتية بالجهاز المركزي لتكنولوجيا المعلومات خالد العنزي، الاستجابة للأحداث الأمنية والمعلوماتية والتحقيقات الجنائية omnicrypt والأنظمة الحوسبة السحابية «الهواتف النقالة الأمنة» omnisafe لتخزين البيانات الآمن والحل الآمن للتشارك في تبادل وتخزين الوثائق وحلول شركة هواوي لمركز معلومات السحابية الخاصة بالحكومة الإلكترونية والحلول الأمنية من كاسبرسكي.

وقال مهندس اول امن النظم السحابية في مايكروسوفت الشرق الاوسط أوجوزان فيليزيباي ان مايكروسوفت لديها فريقان للأمن والخدمات ومهندسون متخصصون في مجال الحوادث الأمنية كفقدان البيانات أو سرقتها أو وجود فيروسات التي تتعرض لها البرامج.

وأضاف ان فريق الشركة يقوم بحل مثل هذه المشكلات من خلال دورات تدريبية تهدف إلى نقل الخبرات. مشيراً إلى ان فريق المستشارين لدى الشركة يقوم بتصميم البرامج حول وضع النقاط الأمنية وأن هناك مرحلة للاستجابة حيث يتم إرسال المتخصصين للتعامل مع هذه الحالات ولدى الفريق إمكانيات للوصول إلى النواقد.

وأفاد فيليزيباي ان المهاجمون أصبحوا أكثر ابتكاراً للسرقة، مبيناً ان فريق الشركة يتعامل مع هؤلاء وفق القانون ويتبادل المعلومات مع الجهات الحكومية خاصة المؤسسات العسكرية.

## فيليزيباي:

المهاجمون أصبحوا

أكثر ابتكاراً للسرقة

ومايكروسوفت

تتعامل معهم وفق

القانون

الجريمة المنظمة

الأسوأ عالمياً

لاستخدام أفرادها

أدوات خاصة

للمهاجمة

للحصول

على الأموال

## نيكلاوس: مخاطر

عالية تنتج

من مهاجمين

للخدمات المصرفية

الإلكترونية عبر

استخدام اسم

المستخدم وكلمة

السر

جو سو: 90٪ من

سرقة المعلومات

تتم من خلال

الموظفين

الداخليين للجهة

الحكومية أو

الشركة

الرئيس للمبيعات وأعمال

المشاريع في الشرق الأوسط

في هواوي جو سو ان الشركة

تقدم خدمات لأكثر من 45٪

من شركات النفط في العالم

بينها المملكة العربية

السعودية، مشيراً إلى أهمية

أمن الحكومات وأن النظم

السحابية اليوم بات وضعها

سهلاً ويجب بناء منصة ذات

طبقات للتطبيقات.

وأضاف ان طبقة جمع

المعلومات لا تسمح للأفراد

بتخزين المعلومات من خلال

قنوات متعددة للأبياد

والأيفون والحاسب الآلي.

وعن موضوع أمن

البيانات قال جو سو ان من

الأهمية بمكان أمن البنية

الأساسية، مشيراً إلى ان

مهاجمين يقومون بهجمات

تطفلية وأنه يمكن الكشف

عن ذلك والرء عليه وهناك

البرامج المضادة للتطفل

كفلتر لهذه المحاولات.

وقال: 90٪ من سرقة

المعلومات تتم من خلال

الموظفين الداخليين، واصفاً

ذلك بأنه مشكلة أمنية

أساسية، حيث يتم الهجوم

إما من الداخل أو الخارج فمن

الضروري معرفة من أين

تبدا المعالجة.

ولفت إلى ان النظام الأمني

وقال ان أمن المعلومات مهم

في هذا الموضوع، متسائلاً: ما

القدر الأمني الذي يمكن توافره

لنقل المعلومات أو الخدمات

من الحكومة إلى المواطن عبر

الهاتف أو الحاسب الآلي؟

ولفت إلى ان هناك مخاطر

عالية تنتج من مهاجمين فيما

يخص الخدمات المصرفية

الإلكترونية من خلال استخدام

اسم المستخدم وكلمة السر.

وذكر ان كلفة الوقاية من

عمليات التجسس في العالم

بلغت 300 مليون دولار وأن

نفس الأشخاص يهاجمون

الحكومات والمنظمات.

وبين ان هناك معياراً لإصدار

أرقام عشوائية وأن هذه الأرقام

إذا لم يتم تشفيرها فمن

السهولة السطو على المعلومات

وأن التشفير القياسي ليس

أمنياً في الهواتف النقالة وهناك

مؤسسات متخصصة في السطو

على الأيفون والبلاكبيري على

سبيل المثال وأن برامج التشفير

المتواجدة في الأسواق ليست

آمنة وهناك حلول خاصة ذات

ملكية قوية لكن ذلك يعتمد

على التطبيق الذي في حال

كان ضعيفاً سيكون النظام

كله ضعيفاً.

هجمات تطفلية

من جانب آخر، أفاد نائب

استعرض فيليزيباي

خلال الجلسة نظم التشغيل

في مايكروسوفت ومرآحل

تطورها وتكنولوجيا تخفيف

المخاطر، مشيراً إلى ان نظام

التشغيل أصبح أكثر قوة ضد

الهجمات والبرامج المهددة

والفيروسات ومنها منتج

«إمت» المخصص للحماية

ضد الهجمات والأخطاء التي

تحدث لتسريب البيانات

والتعرض لمخاطر الأمن.

وأشار إلى ان برنامج

الكهرباء من الدولة المعادية

من باب سلب قدراتها.

وبين أن من أسوأ الأمور

السائدة في العالم هي

الجريمة المنظمة لاستخدام

أفرادها لأدوات خاصة

للمهاجمة والحصول على

الأموال واستغلال الأنشطة

والبيانات المهمة التي يمكن

بيعها ونقلها من جهة

إلى جهة أخرى منافسة

للحصول على أموال. وقال:

هناك مهاجمون مجهولون

نشطاء في الفضاء الرقمي

وان وسائلهم لها دوافع

سياسية ويعملون لتدمير

قوة المستهدف وإتلافها

بأقصى قدر ممكن ومن

وسائلهم أيضاً التجسس

العسكري وغيرها من مثل

هذه الأمور.

حول أمنية

من جانبه، تحدث مدير

محفظة منتجات التشفير

العالية بشركة اومنيكس

بوسويسر اريك نيكلاوس

عن المنتجات الأمنية وتقديم

حلول أمنية عالية فيما يتعلق

بالتشفير، مشيراً إلى ان

الشركة تركز على التحديات

في الحكومة الإلكترونية.

وأضاف ان الحكومة

الإلكترونية في الكويت في

الترتيب العالمي 63 وفقاً للأمم

المتحدة وأن اتجاه المواطنين

أصبح ينصب على الهواتف

المحمولة للدخول من خلالها

على الخدمات الإلكترونية.

## الجلسة الختامية لمنتدى الحكومة الإلكترونية

# تطور القرصنة الإلكترونية يفرض تخصيص ميزانيات كافية وكفاءات متطورة لحماية أمن معلومات الحكومات والمؤسسات

المشركة عبدالله العجمي ان المؤشرات الأولية لحجم التجارة الإلكترونية في الكويت تقترب من مستوى الـ 300 مليون دينار خلال العام الحالي 2013، مشيراً إلى ان هذه التقديرات ترتكز على ما تم تحققة فعلياً خلال الأشهر المنقضية من العام الحالي.

ولفت في مداخلته حول مدى دعم كتي لت منظومة الحكومة الإلكترونية في الكويت التي ان نسبة النمو المتوقعة للتجارة الإلكترونية في الكويت خلال العام الحالي قد تزيد على 30٪ مقارنة بالقيمة المسجلة في العام الماضي والبالغة نحو 210.8 ملايين دينار.

ولفت العجمي إلى ان إحصائيات بوابة الدفع الإلكترونية التابعة لـ «كي» أكدت ان نمو التجارة الإلكترونية في الكويت يمضي في وتيرة مطردة وأفقياً في ظل تسارع الجهات والهيئات الحكومية والخاصة التي فضاء هذه التجارة التي تتحرك بخطى نحو الصدارة خلال الفترة المقبلة.

وأكد العجمي ان المستقبل سيكون للتجارة الإلكترونية، لافتاً إلى ان شركات عريقة بدأت تعرض بضاعتها عبر أجهزة الكمبيوتر بما يتيح للعميل التعرف على الشكل واللون والمواصفات عن بعد وهو الأمر الذي من شأنه ان يعزز قيم وحجم التجارة الإلكترونية في المستقبل القريب.

والخاصة توجيه روافد الاستثمار إلى استقطاب أحدث وسائل وتقنيات التكنولوجيا الحديثة، ودعم هذا القطاع المهم بجميع الوسائل الممكنة، مع إيجاد كوادر لديها القدرة على تقديم أفضل الخدمات، لافتاً إلى ان الولايات المتحدة الأمريكية توفر استثمارات طائلة لاستقطاب الكفاءات والكوادر المتخصصة في نظم حماية المعلومات.

وذكر ان الحاجة أصبحت ملحة للقيام بتحديث وتطوير أداء الشبكات في عصر التقنية السحابية والمحاكاة الافتراضية، وحث الشركات على ضرورة التعاون مع المزودين والمنتجين الذين يفهمون الشبكات والتكنولوجيا المتغيرة، من أجل الحصول على المساعدة اللازمة في هذا المجال، وأكد على أهمية وعي الحكومات الإلكترونية بالتحديات الكبيرة التي ستواجهها مستقبلاً إزاء أمن معلوماتها، لاسيما ان في 2020 التي ستشهد تطوراً في استخدامات النظم التكنولوجية حيث سيصبح هناك 15 مليار جهاز متصل بالانترنت ومعرض للاختراقات ان لم يكن مجهزاً بالحماية الكافية.

وقال ان شركة اس بي اي تسعى جاهداً إلى التطوير من الحلول التقنية والنظم المتطورة لحماية أمن معلومات الحكومات خاصة ولاسيما المعلومات ذات الحجم الضخم BIG DATA.

التجارة الإلكترونية

كشف المدير العام لشركة

الخدمات المصرفية الآلية



من اليمين: خالد العنزي وعبدالله العجمي وستيفن فيليب وأوغوسان فيليزيباي وكان الآن (قاسم باشا)

تكنولوجيا المعلومات بعدد من الحلول التقنية المضادة لجميع أنواع البرامج الضارة، وتحديد ما يمكن للموظفين القيام به على شبكة الشركة «وهذا من أولويات المحافظة على أمن التكنولوجيا اللازمة لدعم هذه المتطلبات المتنامية أصبح أمراً ضرورياً لبقاء جميع الشركات قادرة على المنافسة في العصر الحاضر.

وأشار في مداخلته إلى ان أغلب الحماية المتوفرة للبيانات غير محدثة بصفة دورية ومدققة ولا تتناسب مع وتيرة اعتماد الابتكار، وهنا يكمن دور شركات التقنية المتخصصة لتمكين الشركات من نشر التطبيقات المؤتقة وعلاج خروقات البيانات بسرعة وكفاءة، حيث يتم تزويد أقسام

استقطاب العملاء، من خلال عدد من القنوات المختلفة، بما في ذلك وسائل الاتصال الاجتماعية، تطبيقات الهواتف المحمولة وبيئات الإنترنت، «لذلك فإن الاستثمار في التكنولوجيا اللازمة لدعم هذه المتطلبات المتنامية أصبح أمراً ضرورياً لبقاء جميع الشركات قادرة على المنافسة في العصر الحاضر.

اوغوسان فيليزيباي ان استخدام التكنولوجيا في الوقت الراهن أصبح أمراً أساسياً لممارسة الأعمال، خاصة أن المنافسة كانت في السابق تقتصر على الشركات الكبيرة، ولكن مع ظهور تقنيات التكنولوجيا الحديثة، مثل الحوسبة السحابية، والعمل في المكاتب عن بعد إضافة إلى انتشار ظاهرة «أحمل جهازك معك»، BYOD، فتحت الساحة أمام الجميع للظهور والتطور، كما أتاحت الفرصة أمام شركات المشاريع الصغيرة والمتوسطة للاستفادة من التطبيقات والخدمات التي كانت مقتصرة على المؤسسات الضخمة، لافتاً إلى ان تطبيق أحدث التقنيات التكنولوجية في الشركات أصبح شرطاً مهماً في عملية

المعلومات للسنوات المقبلة، ولكن العيش في عالم يتزايد اتصاله أكثر فأكثر وفي صميم مجتمع رقمي يتطور بسرعة، نجد تزايد حاجة مليارات الأشخاص حول العالم للاتصال والتسوق والتعامل مع المصارف والعمل في كل وقت وكل مكان بطريقة آمنة وملائمة، لافتاً إلى ان نمو الطلب على الأمن الرقمي من الشركات والمؤسسات المصرفية، مشغلي الهواتف النقالة إضافة إلى الحكومات حول العالم، حيث يتم تزويدها بمجموعة كبيرة من حلول الأمن الدقيق بواسطة الهواتف النقالة.

نقاط ضعف الأجهزة

من جانبه، قال مدير أول

تطوير الأمن السيبراني في

مايكروسوفت الشرق الأوسط