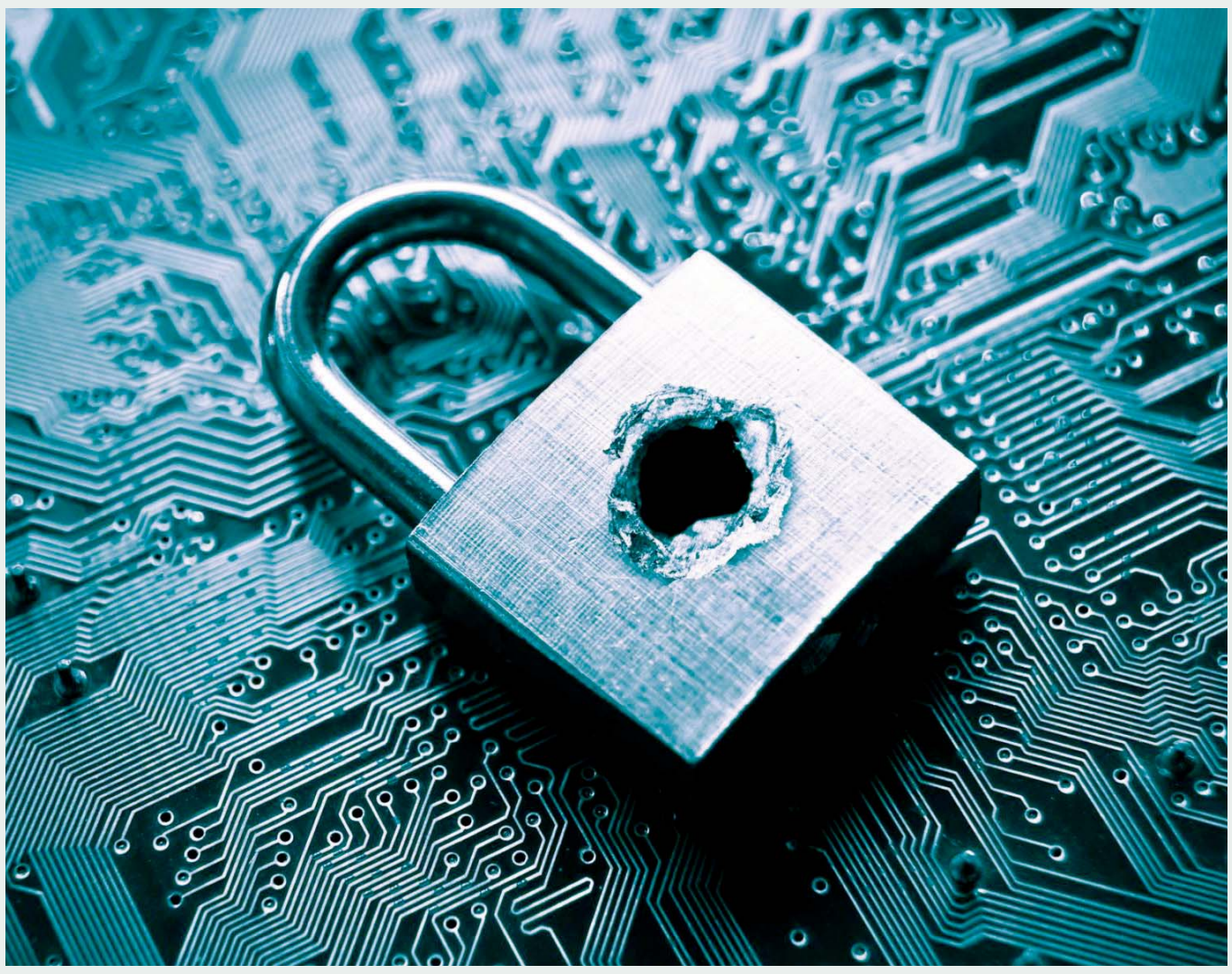
حمايـة البيانـات فـي المنـطـقـ

الدفاع السيبراني الإقليمي..

تحول في أساليب التعامل مع الهجمات في الإمارات

ضرورة لإنشاء دفاع تقني يوازن بين التحوّل والحماية



■ دبي - وائل اللبابيدي

حـذّر خبـراء في الأمـن الإلكتروني، من أن دول المنطقـة اليوم، تقف أمام تحدٍ حقيقي، وهو إنشـاء نظـام دفاع تقني، يقـارب بين ضرورات التحوّل الرقمي من جهة، وتوظيف أنظمـة لمراقبة وحماية والبيانـات من جهـة أخـرى، باعتبار أن البيانات باتت هي نفط المنطقة الجديد، وتحتاج إلى أسـاليب جديـدة ومبتكرة وحديديـة لحمايتها. ولفـت الخبراء إلى أن القرصنـة فـي عالمنا اليـوم، تحولّت من اسـتخدام أسـلحة مادية إلى أسـطر برمجية، وأن عدم وجـود أنظمة حماية مدمجة في تقنيات الـذكاء الاصطناعي، الآخـذة فـي الانتشـار، قد يـؤدي إلى مشـاكل كبيرة فـي المسـتقبل، بما في ذلـك تسـريب أسـرار الـدول والبيانات المؤسسـية والشـخصية. وربما كان هذا الواقـع، هو ما دعـا الملياردير الأميركي وارن بافيت، ليقول عبارته الشـهيرة: «إن خطر الهجمات السـيبرانية على البشرية، هو أكبر من خطر الأسلحة النووية».

تعاون

وتحضيـراً لبدء تطبيـق «اللائحة العامة لحمايـة البيانـات» فـي دول الاتحـاد الأوروبي، والتـي أعلن عنها خلال مؤتمر دافوس الأخير، وسـيتم تطبيقها في مايو القادم، دعـا الخبراء إلـى أهمية تعاون حكومـات دول مجلـس التعـاون، فـي إصدار نسخة من «اللائحة العامة لحماية البيانـات»، خاصـة بالمنطقة، مشـيرين إلى أنه من خلال تقديم نسـخة إقليمية مـن تلك التشـريعات، فـإن الحكومات فـي دول مجلس التعاون، سـتتمكن من مراقبة البيانات وحمايتها بشكل استباقي أشـمل، دون الاكتفـاء بمجـرد الاعتماد على القوانين التشـريعية في مكان آخر. وأكّد الخبراء، أن أهمية اللائحة لا تقتصر على حمايـة البيانات فحسـب، بل هي ضروريـة جداً لتطوير أفضل الممارسـات عنـد الاسـتجابة للحـوادث. وهنـا يثور تسـاؤل مهم، مفاده: «هل يصبح 2018 عـام، الذي يحظى فيه الأمن المعلوماتي أخيراً بالاهتمام الذي يستحقه؟».

خطة دبي

وفـي هـذا الإطـار، أكّـد الخبـراء أن إطـلاق «خطة دبي الاسـتراتيجية للأمن الإلكترونـي» في مايـو 2017، أكّد ريادة وجديّـة الإمـارات فـي انتهاج أسـاليب إيجابيـة للتعامـل مـع هذه المسـألة، نظـراً لأنها أصبحت علـى بيّنة من الآثار المدمرة التي أحدثتها موجات الهجمات التي وقعـت حديثاً، في خطوة تجسـد حـرص دبـي علـى الوصول إلـى أعلى مراتـب الابتـكار والحمايـة الإلكترونية عالميـاً. ونّوه الخبراء بمبـادرات «قانون حماية الخصوصيـة»، الخاص بمركز دبي المالـي العالمـي، على جميـع وحدات التحكـم في البيانـات، التي تعمل خارج المركز، ووضـع المصرف المركزي لدولة الإمارات، الخصوصية في أولوياته، حيث يفـرض إطاره التنظيمـي، حماية بيانات المسـتخدم، كمـا يحظر تخزيـن بيانات المستخدم خارج الدولة.

إنفاق

ووفقاً لشركة «غارتنر»، يسير حجم إنفاق منطقة الشـرق الأوسـط وشـمال أفريقيا علـى خدمات وتقنيات أمـن المعلومات بخطـى ثابتة، ليصل إلى حوالي 2,2 مليار دولار فـي 2018، وهـو ما يشـكل 2,2 ٪ فقـط من حجـم 96,3 مليـار دولار، هي الإنفـاق العالمـي على أمـن المعلومات المتوقـع خلال 2018. وقالت كريسـتينا تانتسـيورا مديرة تطوير الأعمال لمنطقة الشرق الأوسـط وشـمال أفريقيا، مديرة لـدى «إنفواتش جلـف»، المتخصصة في مجال حلول الأمـن الإلكتروني المتكاملة للشـركات، إن الهجمـات السـرية التـي تهـدد البيانـات الضخمة، سـتصبح أكثر كثافة وتعقيـداً، خصوصاً مع زيادة تنظيم البيانـات الضخمة فـي المنطقة، مرجحة استهداف مراكز البيانات الكبيرة، وخدمات الإنترنـت التـي تدير بيانـات ملايين من المسـتخدمين، مؤكدة أهمية أن تركّز أي دولة تعتزم الانتقـال إلى الفضاء الرقمي، التركيز على السـيادة والحقـوق الرقمية لجميع المشـاركين خلال رحلتها الرقمية، وأن الهجمـات السـيبرانية، باتت ضريبة باهظة للتحول الرقمي والرقمنة.

ممارسات

ووفقاً للممارسـات الدولية، فإن التكاليف الحقيقيـة للأضرار الناجمـة عن مثل هذا النـوع مـن الجرائـم، أعلى بكثيـر، نظراً لعدم اسـتعداد العديد مـن الضحايا، ولا سـيما الشـركات الكبيـرة أو المصـارف، للكشف عن تعرضها لمثل هذه الحوادث. وبالتالـي، قـد يتضاعف حجم الخسـائر مرتيـن، أو حتى ثلاث مرات، خلال الفترة المقبلـة. وأضافـت أن هنـاك مبـدأ في الإمارات يقوم على «الابتعاد عن النسـخ، وإنشاء الجديد»، كحال دول مثل روسيا أو الصين، خصوصاً أن نسخ تجارب الآخرين، لا يـؤدي إلـى أي شـيء جيـد، وخاصة فـي مجال الأعمـال والشـركات. وينبغي أخذ خصوصيات الدولة وشـعبها وثقافتها وأعرافها بعين الاعتبار، كل على حدة، بما في ذلك عند تطبيق التقنيات الجديدة.

فرص أم تحديات

مـن جانبه، لفت سرينيفاسـان سـي آر رئيـس الشـؤون الرقميـة، فـي «تاتـا» للاتصالات، إلـى أن القرصنة الإلكترونية كانت أحد أهم المواضيع التي تم طرحها خلال أعمال المنتدى الاقتصادي العالمي الأخير في دافوس السويسـرية، مشـيراً إلـى أن قوة التقنية، سـتكون أحد أهم القوى المؤثرة في 2018، والتي قد تأتي بالفرص الواعـدة للمجتمع، أو تلقي في طريقه المخاطر، متسـائلاً إن كان الأمن المعلوماتي سيحظى خلال 2018، أخيراً، بالاهتمام الذي يستحقه.

نشر الوعي

مـن جانبـه، دعـا عـلاء هـادي مديـر الأسـواق عالية النمو والشـرق الأوسط لـدى «آربـور»، إلى ضرورة نشـر الوعي حول «اللائحة العامـة لحماية البيانات» خـارج حـدود أوروبا، مشـيراً إلى وجود بعـض التصـورات الخاطئـة حـول تلك اللائحة. وأضاف: «من تلك التصورات، أن متطلبات اللائحة العامة لحماية البيانات، تقتصر فقط على المؤسسـات الموجودة فعليـاً في الاتحاد الأوروبـي، إلا أن هذا ليس صحيحـاً، فاللائحـة العامة لحماية البيانـات، تطبق بشـكل صريح على أي عمـل يجمـع أو يعالج بيانات شـخصية لمواطني الاتحاد الأوروبي، سـواء بشكل مباشر، أو غير مباشر، كطرف ثالث. وهذا يعنـي بنحو أساسـي، أن اللائحة العامة لحمايـة البيانات، هي لائحة عالمية تؤثر في العديد من القطاعات المختلفة، مثل التجزئة والرعاية الصحية والقطاع المالي، على سبيل الذكر لا الحصر.

وأضـاف هادي: «أما عن الآثـار المترتبة للائحـة العامـة لحمايـة البيانـات، فإن التصـور الخاطـئ الأخير، يظهـر في أن هناك قـدراً كبيراً مـن الاهتمام، ينصب علـى المسـتويات الجديـدة للغرامات، ويبين بوضوح، حق الأفراد في التعويض، نتيجة عدم الامتثال للائحة العامة لحماية البيانـات. إلا أنـه من المهـم، تذكر أن الممارسـات الأمنيـة التـي تطالـب بها

كريستينا تانتسيورا: مراكز البيانات الكبيرة الهدف الأكبر للقراصنة

سرينيفاسان سي آر: قوة التقنية أحد أهم القوى المؤثرة العام الجاري

علاء هادي: الممارسات الأمنية تحافظ على ثقة العملاء

إياد شهابي: على الدول تبادل أفضل الممارسات لحماية البيانات

هجمات حجب الخدمة

كشـفت المختبرات التقنية التابعة لشـركة F5 نتوركـس، الأسـبوع الماضي، عـن إحصـاءات جديدة، تشـير إلى مواصلة هجمات حجب الخدمة الموزعـة، نموها وتطورها على مستوى الشرق الأوسط وأوروبا وأفريقيا. حيث شـهد عـام 2017، ارتفاعاً بنسـبة 64 ٪ على مسـتوى الحوادث الأمنيـة الإلكترونية الأقل حدةً، كما أشـارت البيانـات أيضاً، إلـى أن أوروبا والشـرق الأوسـط وأفريقيـا، تقف في خـط الواجهة أمـام التهديـدات الإلكترونية، فقد تجـاوزت حصة المنطقة نسـبة 51 ٪ مـن إجمالي الهجمـات العالمية المسجلة خلال العام الماضي.

أمـا التغيـر الرئيـس علـى خارطة الهجمـات، فتمثـل بالانخفـاض النسـبي في قوة وانتشار الهجمات أحاديـة الجهـة، حيث رصـد مركز العمليـات الأمنيـة، تجـاوز سـعة الهجمـات متعددة الاتجاه في يناير الماضـي، الـ 100 غيغابايـت في الثانية، مع تجـاوز قوة البعض منها الـ 400 غيغابايت فـي الثانية، مع سـعات أكبـر، بالمقارنة مـع العام الماضـي، في مؤشـر لوجود توجه نحو تبني هجمـات حجب الخدمة الموزعـة الأكثر تطوراً ضمن الطبقة السـابعة، التي غالباً مـا تكون أكثر تأثيراً وفعاليـةً، رغم أنها لا تتطلب اسـتخدام عرض نطاق ترددي كبير. كمـا أن 66 ٪ مـن هجمات حجب الخدمـة الموزعة المسـجلة، كانت متعددة النواقـل، وتطلب التصدي لها، الاستعانة ببرامج وخبرات للحد من حدتها.

تداعيات اللائحة

■ ديباك ناراين

قال ديبـاك ناراين رئيس هندسـة الأنظمـة لـدى «فـي إم ويـر» VMware، لمنطقة الشرق الأوسط وتركيا وشمال أفريقيا: «يزداد تركيز الهجمـات الإلكترونية على منطقة الشـرق الأوسـط بصورة مستمرة، ما يجعل موضوع الأمن الإلكتروني هدفاً أساسـياً للمؤسسات، في ظل معرفتهـا بالأضـرار التي قد تحدث نتيجة عملية الاختراق الإلكتروني، سـواء الأضـرار الماديـة، أو تلـك التـي تطـال العمليـات، وتزعزع ثقـة العملاء في العلامـة التجارية للمؤسسة. وسـيكون قانون تنظيم حمايـة البيانات العامة (GDPR)، حافـزاً للحكومـات المحليـة والمؤسسـات الخاصـة، لفـرض سياسـات أمنية أقـوى، والإفصاح عـن الخروقـات الأمنيـة التي قد تحدث. كما سـيفرض هذا القانون على المؤسسات، إعادة النظر على البيانات التـي تحتفظ بها، وكيفية إدارتهـا بصـورة شـاملة. ويمكـن للمؤسسـات، حمايـة معلومـات عملائها، وكذلك معلوماتها الخاصة، مـن خـلال تحسـين العمليـات التجارية لحماية البيانات الشخصية.

الشركات الأوروبية في المنطقة مطالبة بتنفيذ اللائحة

أكّـد خبـراء، أنه بدءاً مـن تاريخ 25 مايو المقبل، سيتحتم على أي شركة في منطقة الشرق الأوسط، تمتلك فروعاً لها في دول الاتحاد الأوروبـي، تنفيذ قوانين «اللائحة العامة لحماية البيانـات»، التي قالوا إنها ستحدث تغييرات غير مسبوقة في طريقة جمـع المؤسسـات للبيانات الشـخصية لمواطنـي الاتحـاد الأوروبـي، وسـبل معالجتهـا وحمايتهـا، وسـيجب الإعلام عـن الخروقـات الأمنية خلال 72 سـاعة مـن حدوثها، بالنسـبة لجميع الشـركات والهيئات والمؤسسات التي تمتلك عملاء لها في دول الاتحاد الأوروبي.

وعلـى الرغـم مـن اهتـمام المنطقة باللوائح والتشـريعات، إلا أنـه إلى حين تنفيـذ واخـتبار هذه الـقوانين في ما يخص الهيئات غيـر الأوروبية، فإن الوضع فـي دول الخـليج العربـي يبقـى غير مؤكد، مشـيرين إلى أن تلك التشريعات، تهدف إلى توحيد أنظـمة حماية وتبادل البيانـات لجمـيع الشـركات والقاطنين فـي دول الاتحـاد الأوروبـي، وأن استعداد الحكومات في الخـليج العربي لاتخاذ نهج مماثل، سيمـكنها من مراقبة البيانات وحمايتها بشكل استباقي أشمل، أكثر من مجرد الاعتـماد عـلى الـقوانين التشـريعية فـي مـكان آخـر، ويحسـن فرصهـا في تأمين بنيتهـا المعلوماتية في المستقبل.

ولفـت الخبراء إلـى أن مخـازن البيانات الضخمة، ستكون الهدف الرئيس للقراصنة فـي 2018، وذلـك بالتزامن مـع ارتفاع وتيـرة هجمات الفديـة الخبيثة، وحجب الخدمـة، وتصّيـد البريـد الإلكترونـي للشـركات، مشـيرين إلى «تأخر» معظم دول المنطقة بمشـاكل الأمن الإلكتروني والمعلومات، في الوقت الذي يتسابق فيه سكان المنطـقة لتبني التقنيات الحديثة والناشئة.

وأضـاف الخبراء: «سـيكون قانون تنظيم حمايـة البيانات العامـة (GDPR)، قادراً علـى التأثير فـي المؤسسـات والهيئات العامـة داخل وخارج أوروبا، إذ إنه يفرض على الشـركات تعزيـز سياسـات حماية البيانات الخاصة بها، والإجراءات المتبعة، وتحديد الامتثال، والثغرات التقنية، فضلاً عـن التخطيـط للتعامـل مع تشـريعات خصوصيـة البيانات على أسـاس عالمي، مـع تأثـر المؤسسـات غيـر الخاضعة له بصورة مباشـرة في المنطقة، إذ سيترتب عليها، زيـادة إجراءات حـماية البيانات الخاصة بها».

ـــة وتحديات القرصنة 1-2

ثغرات تنتظر الإغلاق

■ 2.2 مليار دولار إنفاق المنطقة على أمن المعلومات

■ الهجمات السيبرانية أخطر من الأسلحة النووية

سوق أمن الفضاء الإلكتروني في دول الخليج

توقع تقرير حديث لشركة "ريسرتش آند ماركتس" المتخصصة في مجال الأبحاث التقنية، نمو سوق أمن الفضاء الإلكتروني في دول مجلس التعاون الخليجي إلى أكثر من 10.40 مليار دولار (38.17 مليار درهم) بحلول نهاية 2022، في حين وصل حجم إنفاق المنطقة على خدمات وتقنيات أمن المعلومات إلى 1.9 مليار دولار (7 مليارات درهم) نهاية العام الماضي.

22.14 مليار دولار
حجم سوق الأمن الإلكتروني في المنطقة بحلول 2022 (14.2 % نمو سنوي مركب)

% 5.6
حصة أمن المعلومات من إجمالي ميزانية تقنية المعلومات في شركات المنطقة

4.94 ملايين دولار
متوسط الخسائر التي تسببت بها عمليات الاختراق الإلكتروني في المنطقة 2017 (نمو 6.9 %)

7.5 ملايين
عدد هجمات حجب الخدمة الموزعة عالمياً 2017 (نمو 10 %)

154.7 دولارا
متوسط الخسارة التي تتعرض لها المؤسسة نتيجة الاختراق الإلكتروني لكل سجل يتعرض للضياع أو السرقة

11.7 مليون دولار
متوسط تكلفة أمن المعلومات سنوياً في الشركات عالمياً

إعداد: وائل اللبابيدي - غرافيك: حسام الحوراني البيان
المصدر: البيان - "تنسكاوت آربور" - معهد "بونيمون" - "آي بي إم"

أشهر الهجمات 2017

- إصابة فيروس الفدية "وانا كراي" أكثر من 300 ألف حاسوب في 150 دولة
- تسريب 143 مليون رقم ضمان اجتماعي في الولايات المتحدة من شركة "إيكويفاكس" للائتمان
- 36 % زيادة عدد هجمات الفدية
- 230 ألف عدد البرمجيات الخبيثة Malware التي يتم انتاجها يومياً
- 4000 عدد هجمات الفدية المسجلة يومياً في العالم خلال النصف الأول 2017

راي كافيتي:
تفاوت أداء الحكومات في التعامل مع الهجمات

اللائحة العامة لحماية البيانات، ستساعد المؤسسات في الحفاظ على ثقة عملائها وشركائها للمضي قدماً. كما يتطلب النجاح المستقبلي للأعمال، حماية البيانات الشخصية وشبكة الاتصال وتوفر الخدمة، سواء مع اللائحة العامة لحماية البيانات أو من دونها».

دفاعات إلكترونية

من جانبه، قال إياد شهابي نائب رئيس منطقة الشرق الأوسط وشمال أفريقيا وتركيا، في شركة «بي تي» للاتصالات البريطانية، إنه فيما تساعد التطورات التقنية في تبسيط العمليات وزيادة كفاءة الأعمال، فإنها تتيح في المقابل بوابات جديدة تسهّل ولوج مجرمي الإنترنت إلى الأنظمة، مؤكداً أن مجرمي الإنترنت، أصبحوا أكثر استعداداً وتمكّناً من التسلل إلى أكثر الشبكات المؤسسية تطوراً، لذلك، بات من المحتّم أن تعمل

أمير كنعان:
الجهات المحلية مطالبة بمراجعة التشريعات

الحكومات الآن على وضع دفاعات إلكترونية لحماية مؤسساتها من أكثر التهديدات المتقدمة خطورة.

وأضاف شهابي: «وفي هذا السياق، نرى أن الحكومات في المنطقة، بدأت في انتهاج أساليب إيجابية للتعامل مع هذه المسألة، نظراً لأنها أصبحت على بيّنة من الآثار المدمرة التي أحدثتها موجات الهجمات التي وقعت حديثاً. وفي عام 2017، أطلق صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، وسمو الشيخ حمدان بن محمد بن راشد آل مكتوم ولي عهد دبي، رئيس المجلس التنفيذي، «خطة دبي الاستراتيجية للأمن الإلكتروني»، في خطوة تجسد حرص الإمارة على الوصول إلى أعلى مراتب الابتكار والحماية الإلكترونية عالمياً. وإضافة إلى ذلك، أنشأت السعودية «الهيئة الوطنية للأمن

طارق عباس:
يجب إدماج حماية البيانات في ثقافة الشركة

السيبراني»، لتعزيز الأمن الإلكتروني للدولة، وحماية مصالحها الحيوية، وأمنها القومي، وبنيتها التحتية الحرجة».

تضافر الجهود

وأشار الشهابي إلى أن نجاح الدول في فرض الأمن الإلكتروني في عالم اليوم، الذي تحدِق به التهديدات وتضربه من كل جانب، يقوم على ركائز مهمة، تشمل التعاون، ولا تقتصر على التقنية. ولذلك، ينبغي على كل شركة ومؤسسة في القطاعات التجارية والمالية وقطاعات الاتصالات والطاقة والحكومة، أن تعتبر نفسها مهدَّدة من نوايا المجرمين الإلكترونيين التخريبية، الهادفة إلى تحقيق المكاسب، وهذه الشبكة المتنامية من المجرمين الإلكترونيين، عازمة على تطوير طرق هجوم أكثر تقدماً لاختراق أنظمة الشركات والمؤسسات. وعليه، فإن من المهم أن تضافر الدول والحكومات جهودها، وتتبادل أفضل الممارسات، ويتعلم بعضها من البعض الآخر، لا سيما أن المجرمين الإلكترونيين لا تحدّهم في نشاطاتهم الخبيثة أية حدود جغرافية، وبالتالي، فإن مواجهتهم يجب أن تعتمد على التعاون والابتكار، بطرق متوافقة مع أساليبهم، وهذا الأمر يتطلب الإمساك بزمام المبادرة، وتعاون الحكومات في العمل معاً.

تعامل نسبي

ويقول راي كافيتي نائب الرئيس، الشرق الأوسط وتركيا وأفريقيا في «أتيفو نيتوركس»، إن تعامل حكومات المنطقة مع تهديدات الأمن الإلكتروني، لا يزال نسبياً، وأن بعض الحكومات تقوم بجهود أكثر من غيرها في هذا المجال. وأضاف: «تقوم معظم الحكومات في كل دولة، بتطوير إطارها الخاص للدفاع السيبراني على أجزاء مختلفة من الأمن السيبراني، وكشفه وحلول الاستجابة له. ونعتقد بأن التعاون بين البلدان في هذه المنطقة، مهم لمكافحة الهجمات السيبرانية، وإلحاق الضرر بها، إلى البنية التحتية المختلفة للشبكات والشبكات الحكومية».

أولوية ملحة

من جهته، قال أمير كنعان، المدير التنفيذي لمنطقة الشرق الأوسط وتركيا وأفريقيا في شركة «كاسبرسكي لاب»، إنه مع تحول الشرق الأوسط بشكل متزايد إلى هدف للهجمات الإلكترونية، تزداد أهمية النظر إلى أمن البيانات، كأولوية ملّحة. وأضاف: «لا يزال قطاع الأمن الإلكتروني في الشرق الأوسط، ينمو لتلبية المتطلبات الضرورية التي من شأنها ضمان الإتاحة والموثوقية والسلامة، وهي العناصر الثلاثة الأساسية لضمان بناء أساس قوي لكفاءة العمليات». وبالتوازي مع ذلك، نجد أن هذا الأمر مدفوع أيضاً بالقوانين والتشريعات المحلية، والتبني التدريجي لمعايير الأمن الإلكتروني في المنطقة، ونحن في كاسبرسكي لاب، نرى أن من المفيد للبلدان في المنطقة، أن يكون لديها وسائل حماية البيانات الخاصة بها. وعندما تدخل اللائحة التشريعية العامة لحماية البيانات، حيز التنفيذ في أوروبا، فستعطي الممارسات المتعلقة بسلامة البيانات في المؤسسات، دفعة قوية، وهو ما يمكن أن يكون بمثابة حافز للجهات التنظيمية المحلية، لمراجعة القوانين والتشريعات القائمة وتحديثها، كما أنها قد تكون فرصة لتطبيق قوانين جديدة.

فهم التشريعات

وقال طارق عباس رئيس هندسة الأنظمة لدى «بالو ألتو نتوركس» في الأسواق الناشئة، إنه في ظل قانون تنظيم حماية البيانات العامة (GDPR)، ينبغي على الشركات فهم التشريعات الخاصة بحماية البيانات والتوافق معها. وتتعرض المؤسسات في منطقة الشرق الأوسط، لضغوط كبيرة، لتقييم الأنظمة التي تستخدمها، واختبارها وتغييرها عند الضرورة، وذلك للتأكد من أن مؤسساتهم لديها الرؤية التي تحتاجها، وأن الضوابط والعمليات لديها قوية بما فيه الكفاية. وبمرور الوقت، سيؤدي ذلك بلا شك إلى تعزيز ممارسات أمن البيانات، ويكون حافزاً للتغيير الإيجابي، في ما يتعلق بالأمن الإلكتروني في المنطقة، في القطاعين العام والخاص. وبما أن خروقات البيانات مكلفة للغاية، سواء لدى تطبيق قانون (GDPR)، أو عدم تطبيقه، فإن على المؤسسات أن تكون حازمة في عملية إدماج حماية البيانات في ثقافة الشركة.

استراتيجية دبي للأمن الإلكتروني

أطلق صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، في مايو من العام الماضي، بحضور سمو الشيخ حمدان بن محمد بن راشد آل مكتوم ولي عهد دبي، رئيس المجلس التنفيذي، وسمو الشيخ مكتوم بن محمد بن راشد آل مكتوم نائب حاكم دبي «خطة دبي الاستراتيجية للأمن الإلكتروني»، والتي تهدف لتعزيز مكانة دبي كمدينة عالمية رائدة في الابتكار والسلامة والأمن.

ودعا سمو الشيخ محمد بن راشد آل مكتوم، جميع المؤسسات الحكومية والخاصة والأفراد في الإمارة، إلى توحيد الجهود، من أجل توفير فضاء إلكتروني آمن، ولجعل دبي أأمن مدن العالم إلكترونياً. وتركز الخطة على خمسة محاور رئيسة، حيث يهدف المحور الأول إلى زيادة وعي المجتمع بمخاطر الأمن الإلكتروني، للتأكد من بناء مجتمع يعي ويدرك مخاطر الأمن الإلكتروني، وبناء الوعي والمهارات والقدرات اللازمة لإدارة مخاطر الأمن الإلكتروني في المؤسسات الحكومية والخاصة والأفراد في إمارة دبي.

أما المحور الثاني، فيُعنى بالابتكار والبحث العلمي في مجال الأمن الإلكتروني، وإنشاء فضاء إلكتروني يتسم بالحرية والعدل والأمن، ويشجع الابتكار في إمارة دبي. ويهدف المحور الثالث، إلى بناء فضاء إلكتروني آمن، بوضع ضوابط لحماية سرية البيانات ومصداقيّتها وتوافرها وخصوصيتها. وسيتم العمل ضمن المحور الرابع، على الحفاظ على مرونة الفضاء الإلكتروني، وضمان استمرارية أنظمة تكنولوجيا المعلومات وتوفرها في الفضاء الإلكتروني. ولن تنجح تلك الأهداف إلا بالتعاون المحلي والدولي بين القطاعات المختلفة، ولذلك، فإن المحور الخامس، يعنى بهذا الجانب. وستشهد المرحلة المقبلة، العديد من المبادرات الفعالة، التي من شأنها أن تسهم في تحقيق أهداف الاستراتيجية، وتوفير فضاء إلكتروني آمن للمستخدمين، ما سيجعل تجربة دبي في مجال الأمن الإلكتروني، نموذجاً عالمياً يحتذى به.

عصر رقمي مظلم

أكّد ألويس زوينجي، المدير الإداري في المنتدى الاقتصادي العالمي، رئيس المركز العالمي للأمن المعلوماتي، الذي أطلق في يناير الماضي، أن التراخي في اتخاذ أي خطوات اليوم، سيؤدي إلى «عصر رقمي مظلم»، حسب تعبيره، لافتاً إلى أن زيادة الضغط في عام 2018، من ناحية اللوائح التنظيمية والمستهلكين، تعني أنه لم يعد مقبولاً أي عذر أو اعتذار، وأنه «إن لم تجعل الأمن أولوية في هذا العام، فإن مؤسستك تواجه خطر مواجهة خسارة ضخمة نتيجة الإهمال المتعمد».

■ ألويس زوينجي

ولا يمثل الأمن المعلوماتي، مجرد مشكلة للحكومات فحسب، إذ أشارت التقارير، إلى أن الأهداف الرئيسة التي يهاجمها قراصنة المعلومات، لا تقتصر على الهيئات الحكومية المالية، بل كذلك الشركات الكبيرة، التي تملك من المال ما يكفي لدفع فدية للقراصنة بالعملة المشفّرة، ما يساعدهم في تمويل عمليات قرصنة أخرى. وتسبب الهجمات الإلكترونية لفترات طويلة على الشركات، تكبدها تكاليف مالية كبيرة، وتراجع سمعتها.

ووفقاً لدراسة حديثة، أجرتها شركة أكسنتشر، يبلغ متوسط التكلفة السنوية للأمن المعلوماتي للشركات اليوم، نحو 11,7 مليون دولار. ولا ريب، المحافظة على الأمن المعلوماتي مسألة تحتاجها الشركات حتماً. ويدعم تقرير أكسنتشر ذلك، بالإشارة إلى أن متوسط العدد السنوي للخروقات الأمنية، ارتفع بنسبة 27,4 ٪. ما يجعلها مسألة جوهرية للرئيس التنفيذي للشركة، خاصة أن مستويات الابتكار والأتمتة، ترتفع اليوم بصورة متسارعة، ويزداد ارتباطها بالتقنية.

الدولة تظهر أعلى درجات النضج في حماية بياناتها

قال محمد أبو خاطر نائب رئيس المبيعات في منطقة الشرق الأوسط وأفريقيا لدى «فاير آي»، المتخصصة في الأمن السيبراني، حول إذا ما كانت الحكومات الخليجية تتصدى للتهديدات الإلكترونية كما يجب: «في المجمل نعم. إلا أن هذا الأمر يختلف من دولة خليجية لأخرى، فعلى سبيل المثال، تظهر الإمارات والسعودية أعلى درجات من النضج، بكونها من أوائل الدول التي تعين هيئات تنظيمية متخصصة في مراقبة المشهد الإلكتروني. إذ تمتلك الإمارات عدداً من الهيئات، مثل الهيئة الوطنية للأمن الإلكتروني، والهيئة العامة لتنظيم قطاع الاتصالات، ومركز دبي للأمن الإلكتروني، في حين تمتلك السعودية كلاً من الاتحاد السعودي للأمن السيبراني والبرمجة، والهيئة الوطنية للأمن السيبراني، وغيرها من الهيئات الأخرى المتخصصة، التي تعمل على سن الأنظمة والقوانين، ومراعاة أعلى المعايير الأمنية، ضمن كافة المؤسسات الحساسة تجاه الأمن الوطني في المملكة. وتستثمر الدولتان كثيراً في تدريب وتعليم المواهب الوطنية، بهدف الارتقاء بمهاراتهم، وتمكينهم من التصرف كفرق استجابة فاعلة عند الطوارئ».

وأضاف أبو خاطر، أنه على الرغم من تلك التدابير، إلا أن الحكومات تحتاج إلى المزيد من التعاون مع القطاع الخاص، بهدف إجراء تحقيقات فعالة، وتحديد المهاجمين والتصدي لهم. وتعمل المجموعات الإجرامية الأكثر تعقيداً في المنطقة، مثل مجموعة APT34، على استهداف الهيئات الحكومية، إلا أن عدداً أكبر من الهجمات الإلكترونية بات يؤثر كثيراً في مؤسسات القطاع الخاص أيضاً. وإلى حين اتخاذ المزيد من الإجراءات، للحد من قدرات مجرمي الإنترنت وتحييدهم، فإن حجم ووتيرة الهجمات، ستواصل ارتفاعها. وتوفر الهجمات المتواصلة التي تستهدف الضحايا من القطاع الخاص، فرصاً حقيقية للحكومات والهيئات الناظمة للقوانين، لتعقب المهاجمين والتصدي لأنشطتهم الإجرامية وإيقافها، وفق نهج استباقي شامل. وأوضح: «باتت معظم الدول تمتلك الكثير من الأطر والهيئات المنظمة والمتحكمة بالبيانات لديها. وتعرف دول الشرق الأوسط وأفريقيا، ودول الخليج العربي، باتباعها قواعد صارمة للحفاظ على سرية البيانات وبروتوكولات مشاركة البيانات الخاصة بالتقنيات السحابية، وخدمات استضافة البيانات داخل الدولة وغيرها. وعلى مدار السنوات القليلة الماضية، لاحظنا بذل الهيئات الحكومية، مثل جهاز استخبارات الإشارة، للمزيد من الجهود، لضمان الالتزام مع التشريعات والقوانين المحلية».

■ محمد أبو خاطر