ملف البيان

ارتباط وثيق بين التوترات الجيوسياسية والهجمات الإلكترونية

سباق التسلح السيبراني.. جيل جديد من الحروب

«بيرل هاربور رقمي» لم يعد ضرباً من الخيال

- الهجمات السيبرانية تفتقر إلى «قواعد الاشتباك»
- المخاطر تهدّد 5,2 تريليونات دولار من الأصول عالمياً
- «المرونة السيبرانية» محورية لتعزيز الدفاعات
- 500 مجموعة هجوم سيبراني في العالم
- الأمن الرقمي عامل رئيس في تطوير «الجيل الخامس»
- «إنترنت الأشياء» نافذة للمخترقين لسرقة البيانات


مايكل بيرج


نيك آلن


ماهر ياموت


وليد كمال


علي جيما


محمد عارف

دبي - وائل اللبابيدي

تغلغل العالم الرقمي في كافة جوانب حياتنا الشخصية والاقتصادية والمجتمعية، وأصبحت الرقمنة في قلب الخدمات العامة والشركات التجارية والأنظمة الصناعية والبنى التحتية التي نعتمد عليها، من البنوك إلى المطارات والقطارات والمستشفيات إلى محطات الطاقة والمصانع والقطاعات الأمنية والجيوش وغيرها، وبالرغم من الفوائد الاقتصادية الكثيرة للتحول الرقمي وتحول تقنيات الحوسبة إلى محرك رئيسي لنمو كافة القطاعات الاقتصادية الأساسية، إلا أن هذا التطور التقني الهائل والسريع وعدم وجود قوانين دولية ضابطة للأسلحة السيبرانية فتح في المقابل باب الفرص أمام جماعات الاختراق لتعطيل أو شل شبكات البيانات والخدمات الحيوية في الدول المستهدفة بشكل استراتيجي وبعيداً عن استخدام الصواريخ والطائرات والبوارج الحربية ،ولا شك، فإن الانتشار المتزايد لأجهزة إنترنت الأشياء المرتبطة بالشبكة العنكبوتية والتي سيصل عددها إلى نحو 300 مليار جهاز بحلول 2022، تمثل نافذة رئيسية للمخترقين لسرقة البيانات وإحداث أضرار مختلفة للمؤسسات والشركات.

وأكد خبراء لـ «البيان الاقتصادي» على هامش مشاركتهم في المنتدى الاستراتيجي العربي الذي عقد أخيراً في دبي أن الحروب السيبرانية أصبحت مكوناً أساسياً في معادلة الحروب الحديثة تمكن الدول من شن هجمات سيبرانية بأسلحة رقمية تشوبها السريّة وقدرة على تحقيق الأهداف دون المواجهة العسكرية أو خطر إصابة أو فقدان حياة الجنود، مرجحين ازدياد قدرة تلك الحروب على إحداث شلل اقتصادي في الدول المستهدفة. وفي عام 2011، أعلنت وزارة الدفاع الأمريكي أن الهجمات السيبرانية تعتبر «عملاً من أعمال الحرب» وتوجب «الرد العسكري».

وقال الخبراء إنه من الصعب التكهن بتوقيت حدوث هجمة سيبرانية ضخمة، ولكن هنالك ارتباطاً واضحاً بين التوترات الجيوسياسية والهجمات الإلكترونية. ويمكن القول بأن الدول الكبرى مثل الولايات المتحدة ستقوم في العام المقبل 2020 باستخدام أسلحتها ومقدراتها السيبرانية بشكل أكثر لتحييد الهجمات والحيلولة دون التصعيد إلى حرب سيبرانية شاملة من خلال اتباع وسائل حمائية ودعائية أكثر كفاءة.

دعم من حكومات

وتؤكد تقارير عدة ازدياد وتيرة هجمات الحروب السيبرانية بين بعض الدول بشكل ملحوظ والتي تقوم بها جماعات مدعومة من حكومات عدة، وباتت تلك الحروب تستهدف قطاعات حيوية مثل المنشآت النووية والبنى التحتية الكهربائية وشركات النفط والغاز وكذلك البنوك ولأهداف تتراوح من سرقة البيانات الحساسة والتسبب في إرعاب الضحايا مالياً وحتى التخريب.

وفيما تحاول الولايات المتحدة الأمريكية وإيران إبقاء الحرب السيبرانية الجارية بينهما بعيداً عن الإعلام، ولأسباب واضحة بالطبع، يحذّر خبراء من تبعات تلك الحرب على بعض الدول في الشرق الأوسط، مشيرين إلى أن كتائب الهجوم الإلكتروني الإيرانية مثل مجموعة APT33 وغيرها بدأت بالفعل سلسة من الهجمات السيبرانية تستهدف بنى تحتية حساسة مثل مصافي النفط وشبكات الكهرباء والمصانع في الشرق الأوسط بهدف تعطيلها، متوقعين أن تزيد تلك الكتائب هجماتها خلال العام المقبل.

وتؤكد تحليلات حديثة أجرتها «بلومبرغ إنتلجنس» أن الهجمات الإلكترونية تشكل بالإضافة إلى التغيرات المناخية التي تتيح المجال لهجمات أمنية فورية باختراق سيبرانية طورتها وكالة الاستخبارات الأمريكية وتضم أكثر من 7000 صفحة، واهمها «فولت 7» مخزون الأسلحة السيبرانية او سرداب التخزين الاساسي، ما أكد قيام الولايات المتحدة بتطوير أسلحة سيبرانية بإمكانيات كبيرة وواسعة لاختراق أنظمة خدمية خارجية من خلال مجموعة من أحصنة طروادة التي تعتمد على الأبواب الخلفية، تهديداً كبيراً لشركات النفط والغاز في المنطقة، فيما يتوقع تقرير لشركة «أكسنتشر» أن المخاطر السيبرانية تهدّد ما قيمته 5,2 تريليونات دولار من الأصول حول العالم وذلك من 2019 وحتى 2023.

وعي إماراتي

وأدت الهجمات التي وقعت خلال السنوات القليلة الماضية إلى قيام نشاط ملحوظ مؤخراً بين دول مجلس التعاون الخليجي لبناء قدرات الأمن السيبراني وإنشاء المؤسسات ووضع الاستراتيجيات. حيث أنشأت الإمارات الهيئة الوطنية للأمن الإلكتروني ومقرها أبو ظبي في أغسطس 2012، واعتمدت في عام 2017 «استراتيجية دبي للأمن السيبراني»، كما أطلقت الهيئة العامة لتنظيم قطاع الاتصالات في يونيو الماضي «الاستراتيجية الوطنية للأمن السيبراني». ومن المتوقع نمو الإنفاق على تكنولوجيا المعلومات في الإمارات بمعدل نمو سنوي مركب قدره 8٪ ليصل إلى 23,1 مليار درهم بنهاية عام 2019، وفقاً لغرفة تجارة دبي.

وبالمثل، تملك المملكة العربية السعودية ودول مجلس التعاون الخليجي الأخرى الموارد اللازمة للاستعانة بمصادر خارجية من الطراز العالمي للمساعدة في تطوير عملياتها الإلكترونية. ففي عام 2013، وهو العام الذي أعقب هجوم «شمعون» على أرامكو، اعتمدت المملكة العربية السعودية أول استراتيجية وطنية في الدول. وتتمتع نسبة كبيرة من الشركات الإماراتية بوجود بروتوكول للتعامل مع الهجمات لكن من الضروري اختبار وقت عمل بروتوكول التعامل مع المخاطر بشكل مؤتمت وهو ما توفره تقنية الذكاء الاصطناعي، علاوة على رسم هيكلة الأمن السيبراني بالاعتماد على نموذج «المرونة السيبرانية».

الجيل الخامس

ويعتبر خبراء أن التعاون على تحقيق الأمن السيبراني عاملاً بالغ الأهمية في تطوير تقنية الجيل الخامس، التي من شأنها تعزيز المكانة الاقتصادية لدولة الإمارات - وللمنطقة عموماً - من خلال توفير الاتصال الكامل للمزيد من الأشخاص والأشياء والأجهزة، وتعزيز مشاركة وتحليل البيانات، بالإضافة إلى زيادة الإنتاجية على صعيد العمل الحكومي والمجتمع والشركات وعلى المستوى الفردي أيضاً. وتقوم بنية أمن الشبكة في الجيل الخامس على أساس نظيرتها في الجيل الرابع مع المزيد من ميزات الأمن المعززة.

إدارة المخاطر

وقال وليد كمال نائب الرئيس الأول لأمن التكنولوجيا وإدارة المخاطر في مؤسسة الإمارات للاتصالات المحدودة «دو» إن البنية التحتية للاتصالات في الإمارات تتمتع بمستوى أمن فائق وتدعم تحقيق أهداف عمليات التحول الرقمي في القطاعات المختلفة. وأضاف: «يبشر طرح تقنية الجيل الخامس التي تتمتع بالنسبة للقطاعات وهذا بالطبع يتطلب تأمين هذه الشبكة ضد الخروقات، مشيراً إلى أن تأمين الشبكة يعتمد على ركائز تتكامل مع بعضها وهي توظيف الذكاء الاصطناعي وقدرات الحوسبة الفائقة». ولفت كمال ضرورة تعزيز واجهات تطبيق البرامج (API) في المؤسسات والشركات بتقنيات مصادقة عالية لسد الثغرات وأنظمة حوسبة قادرة معزّزة بالحماية من هجمات حجب الخدمة علاوة على تعزيز أمن الدخول إلى الأنظمة والوصول إلى البيانات.

سَد الثغرات

وقال علي جيما رئيس العلاقات الحكومية والصناعية في شركة «إريكسون» إن أهداف الهجمات السيبرانية أصبحت أكثر تنوعاً وتتراوح من سياسية إلى اقتصادية. وأشار إلى أن تقنية الجيل الخامس ستكون عاملاً رئيسياً في إضافة القيمة وتطور العديد من القطاعات ولكنها لا علاقة لهذه التقنية في ازدياد أو انخفاض الهجمات السيبرانية بل قد تساعد في تعزيز الدفاعات السيبرانية وسَد الثغرات التي كانت موجودة في الجيل الرابع. وأضاف: «من الضروري إيجاد الشريك المناسب وتعزيز الثقة بين جميع الأطراف ضرورة جداً كذلك في أي استراتيجية أمن سيبراني فعالة. وتشير الدراسات إلى أن عامل المخاطرة حتى 2023 يصل إلى 5,2 تريليونات دولار، ونتوقع أن تزيد وتيرة وتعقيد الهجمات في المستقبل».

استراتيجية وطنية

من جانبه أكد محمد عارف، الرئيس التنفيذي للأمن في مايكروسوفت الإمارات أهمية «الاستراتيجية الوطنية للأمن السيبراني» التي أطلقتها الإمارات هذا العام في خلق بيئة سيبرانية آمنة وصلبة في الدولة تساعد على تمكين الأفراد والمؤسسات من تحقيق طموحاتهم في بيئة آمنة ومزدهرة. وأضاف: «على الشركات أن تضع في صميم رحلتها نحو تحقيق هذه الاستراتيجية تبني الحوسبة السحابية المناسبة وتقنياتها المتصلة، حيث أن هناك مجموعة من المعايير يستوجب توافرها من أجل بلوغ هذا الهدف.

وعلى صعيد دول المنطقة، تقوم الدول والشركات في جميع أنحاء المنطقة بتحويل اهتمامها بشكل تدريجي إلى السياسات التي تتناول خصوصية البيانات على المستوى الوطني، ومع ذلك فإن أبحاث مايكروسوفت تظهر أن ما يزيد على ثلث كبار مسؤولي أمن المعلومات في الشرق الأوسط لم يقوموا بعملية تصنيف البيانات الخاصة بهم، فيما أظهرت نفس الأبحاث أن ما يقرب من النصف بصدد اقتناء حلول لتصنيف البيانات، في حين أظهرت الدراسة أن 20٪ فقط منهم استطاعوا الحصول على الحلول المناسبة لتصنيف البيانات. وأضاف: «يمكن لتكنولوجيا السحابية أن تساعد الشركات على تسريع جهود الامتثال من خلال تبسيط عمليات تصنيف البيانات المعقدة. وفي واقع الأمر إن علامة التوبيخ الجديدة لتصنيف البيانات تسمح للشركات بعرض كافة بياناتهم الحساسة عبر مايكروسوفت 365، بحيث إنها تكون مصنفة ضمن أنواع المعلومات الحساسة أو المرتبطة باللوائح، كما ستمتلك القدرة على اكتساب رؤى خاصة بالسياسات الموصى بها لحماية البيانات وتسهيل تبويب البيانات وفقاً لمدى حساسيتها».

الهجمات السيبرانية تفتقر إلى «قواعد الاشتباك»

وحول الإجراءات التي يجب على دول الشرق الأوسط اتخاذها للحد من مخاطر وتبعات الهجمات الإلكترونية، أفاد آلان: «أعتقد أنه على دول المنطقة تحديد وفهم ونقييم دفاعاتها الحالية والاستثمار في دفاعاتها التكتيكية ودمج «نموذج المرونة» في خلال تحديث أو بناء الشبكات والبنى التحتية». وتوقع آلان استمرار إيران في التصعيد وشن المزيد من الهجمات الإلكترونية تجاه دول المنطقة وذلك كأحد سبل مواجهة الضغوط الأمريكية التي تفرضها الولايات المتحدة على إيران.

تفاعلات دولية

ويقول ماهر ياموت، باحث أمني أول في «كاسبرسكي» إن الأوضاع الجيوسياسية في الشرق الأوسط يجعلها أكثر عرضة لمثل هذه الهجمات الموجهة، خصوصاً مع تحول الفضاء الإلكتروني إلى ساحة للتفاعلات الدولية. وأضاف: «تبرز في هذه الآونة العديد من الأنماط التوظيفية للهجمات السيبرانية، سواء على صعيد الاستخدامات ذات الطبيعة المدنية أو العسكرية، الأمر الذي جعل هذا الفضاء مجالاً للصراعات المختلفة، سواء للفاعلين من الدول أو غير الدول لحيازة أكبر قدر من النفوذ والتأثير السيبراني. ولذا نتوقع ازدياد عدد هذه الهجمات في السنوات المقبلة بسبب استمرار تشنج الأوضاع الجيوسياسية، والتغيرات الاقتصادية، وازدياد عدد الدول والفرق التي تملك قدرات في الفضاء السيبراني. وحول نقاط الضعف التي من المتوقع أن يقوم المهاجمون باستغلالها، يفيد ياموت: «لطالما ركز المهاجمون على استغلال نقاط الضعف المعتادة كاختراق الثغرات، إيميلات الاصطياد، وغيرها لاختراق الأنظمة. هذا التركيز يأتي نتيجة نجاح هذه الطرق في إيصال الملفات الخبيثة التي تخول المخترق من سرقة ملفات خاصة ومثلها من معلومات شخصية أو ذات أهمية للمؤسسات. نتوقع أن المهاجمين سيتمرون في استغلال نقاط الضعف هذه، ولكن مع التركيز على تقنية معتمدة مؤخراً في اختراق جهات ذات حماية عالية، وهي الاختراق عبر سلسلة التوريد».


نبل ماكليني


ديفيد غراوت


حيدر باشا

تنسيق متبادل للاستخبارات الرقمية

يؤكد الخبراء أن الدفاع السيبراني الفعال يجب أن يستند إلى مستوى عالٍ من التعاون والتنسيق المتبادل للاستخبارات الرقمية، لتمكين استجابة إقليمية أو عالمية فعالة ضد التهديدات السيبرانية الدولية، مشيرين إلى أن الحوار والتعاون، السبيل الأمثل أمام المجتمع الدولي لمواجهة المخاطر السيبرانية التي تحدق باقتصادات العالم. حيث يستغل المخترقون الثغرات الأمنية المعروفة بـ«نقاط الضعف الآنية» Zero day في تلك الأجهزة كناية عن عدم الضحية بوجودها أصلاً وبالتالي عدم قدرته على التصدي لها في الوقت اللازم.

بيرل هاربور رقمي

ويؤكد نيل ماكليني، رئيس نظم المعلومات الحربية، والأمن السيبراني لمنطقة الشرق الأوسط في شركة «تاليس» أن عواقب الهجمات السيبرانية يمكن أن تتجاوز العواقب المحتملة للهجمات أنظمة الكمبيوتر والأجهزة المتصلة لتستهدف البنية التحتية بأكملها، مثل الأنظمة الانتخابية أو شبكات الكهرباء أو محطات التصنيع. وكما هو مذكور في دليل «تاليس» للهجمات السيبرانية فإن القطاعات الأكثر استهدافاً من قبل هذه الهجمات الكبرى هي الدول وقدراتها الدفاعية، يليها القطاع المالي والطاقة والنقل. ما يعني أن السيناريو الافتراضي المعروف باسم «بيرل هاربور الرقمي»، الذي يضع تصوراً لهجمة رقمية كبرى لم يعد ضرباً من الخيال ويمكن أن يعصف بالمدن الذكية المستقبلية وبُناها التحتية الرئيسية. ويشير ماكليني أن التحدي الرئيسي يكمن في بقائنا متقدمين بخطوة واحدة عن المهاجمين السيبرانيين أثناء سيرنا في رحلة التقدم الرقمي. فضمان الأمن الرقمي هي معركة لا نهاية لها! وتتطلب دفاعات جديدة على الدوام، لذا تعمل منظمات مثل «تاليس» على تقديم حلول متقدمة منذ البداية حتى النهاية لمساعدة عملائها على التعرف على تحديات الأمن السيبراني، ومنعها واكتشافها والاستجابة لها.

انتباه المهاجمين

ويتوقع ديفيد غراوت، كبير المسؤولين التقنيين في أوروبا والشرق الأوسط وأفريقيا لدى «فاير آي» ازدياد وتيرة الهجمات السيبرانية على دول الشرق الأوسط خلال الفترة المقبلة مبرراً ذلك بأن «المشهد السياسي في الشرق الأوسط لا يزال متقلباً»، خصوصاً وأن التطور الاقتصادي والتحول الرقمي الحاصل يجذب انتباه المهاجمين للقيام بهجمات إلكترونية. ويضيف: «تعتبر المجموعات الإلكترونية المدعومة من حكومات دول أو دول قومية (مركزية) من أكثر المجموعات خطراً، وذلك بسبب الموارد الهائلة الموجودة تحت تصرفها. ونحن ندعو هذه الجماعات بمجموعات التهديد المستمر المتقدم (APT) لأن حملاتهم غالباً ما تكون مستمرة ولا تقتصر على هجوم واحد فقط. والعناصر النشطة بشكل خاص هي APT41 وAPT10 من الصين و APT39 من إيران. ويجب أن نذكر أيضاً المجموعات ذات الدوافع المالية مثل FIN7 التي نعتقد أنها من أوروبا الشرقية. ويمكن أن تلحق هذه المجموعات أضراراً شديدة بالمنشآت التي تهاجمها. حيث يمكنهم سرقة الملكية الفكرية، والقيام بهجمات من أجل الفدية أو مهاجمة شركة أو حتى مدينة (كما رأينا في نيو أورلينز) وجعلها مقطوعة عن العالم الخارجي وإلحاقها خسائر فادحة».

دوافع الهجمات

وقال حيدر باشا مدير أول ورئيس أمن المعلومات لدى «بالو ألتو نتوركس» في الشرق الأوسط وأفريقيا إن دوافع الهجمات السيبرانية ومتنوعة وتتراوح من سياسية إلى اقتصادية، مشيرة إلى أن مجموعات الهجوم السيبراني في العالم يصل عددها اليوم إلى أكثر من 500 مجموعة، مشيراً إلى أن الهدف الأساسي من الهجمات يبقى إلحاق الضرر بالضحية إما سياسياً أو اقتصادياً. وأضاف: «هنالك وعي متزايد حول مخاطر الأمن السيبراني وضرورة مجابهتها، خصوصاً مع زيادة تعقيد الهجمات وتزايد قدرتها على تعطيل مكونات اقتصادية مهمة في الدول. وتتمتع نسبة كبيرة من الشركات الإماراتية بوجود بروتوكول للتعامل مع الهجمات لكن من الضروري اختبار وقت عمل بروتوكول التعامل مع المخاطر بشكل مؤتمت وهو ما توفره تقنية الذكاء الاصطناعي، علاوة على رسم هيكلة الأمن السيبراني بالاعتماد على نموذج «المرونة السيبرانية».

الجيل الخامس

ويعتبر خبراء أن التعاون على تحقيق الأمن السيبراني عاملاً بالغ الأهمية في تطوير تقنية الجيل الخامس، التي من شأنها تعزيز المكانة الاقتصادية لدولة الإمارات - وللمنطقة عموماً - من خلال توفير الاتصال الكامل للمزيد من الأشخاص والأشياء والأجهزة، وتعزيز مشاركة وتحليل البيانات، بالإضافة إلى زيادة الإنتاجية على صعيد العمل الحكومي والمجتمع والشركات وعلى المستوى الفردي أيضاً. وتقوم بنية أمن الشبكة في الجيل الخامس على أساس نظيرتها في الجيل الرابع مع المزيد من ميزات الأمن المعززة.

إدارة المخاطر

وقال وليد كمال نائب الرئيس الأول لأمن التكنولوجيا وإدارة المخاطر في مؤسسة الإمارات للاتصالات المحدودة «دو» إن البنية التحتية للاتصالات في الإمارات تتمتع بمستوى أمن فائق وتدعم تحقيق أهداف عمليات التحول الرقمي في القطاعات المختلفة. وأضاف: «يبشر طرح تقنية الجيل الخامس التي تتمتع بمستوى سرعات عالية للغاية بآفاق واسعة بالنسبة للقطاعات وهذا بالطبع يتطلب تأمين هذه الشبكة ضد الخروقات، مشيراً إلى أن تأمين الشبكة يعتمد على ركائز تتكامل مع بعضها وهي توظيف الذكاء الاصطناعي وقدرات الحوسبة الفائقة». ولفت كمال ضرورة تعزيز واجهات تطبيق البرامج (API) في المؤسسات والشركات بتقنيات مصادقة عالية لسد الثغرات وأنظمة حوسبة قادرة معزّزة بالحماية من هجمات حجب الخدمة علاوة على تعزيز أمن الدخول إلى الأنظمة والوصول إلى البيانات.

سَد الثغرات

وقال علي جيما رئيس العلاقات الحكومية والصناعية في شركة «إريكسون» إن أهداف الهجمات السيبرانية أصبحت أكثر تنوعاً وتتراوح من سياسية إلى اقتصادية. وأشار إلى أن تقنية الجيل الخامس ستكون عاملاً رئيسياً في إضافة القيمة وتطور العديد من القطاعات ولكنها لا علاقة لهذه التقنية في ازدياد أو انخفاض الهجمات السيبرانية بل قد تساعد في تعزيز الدفاعات السيبرانية وسَد الثغرات التي كانت موجودة في الجيل الرابع. وأضاف: «من الضروري إيجاد الشريك المناسب وتعزيز الثقة بين جميع الأطراف ضرورة جداً كذلك في أي استراتيجية أمن سيبراني فعالة. وتشير الدراسات إلى أن عامل المخاطرة حتى 2023 يصل إلى 5,2 تريليونات دولار، ونتوقع أن تزيد وتيرة وتعقيد الهجمات في المستقبل».

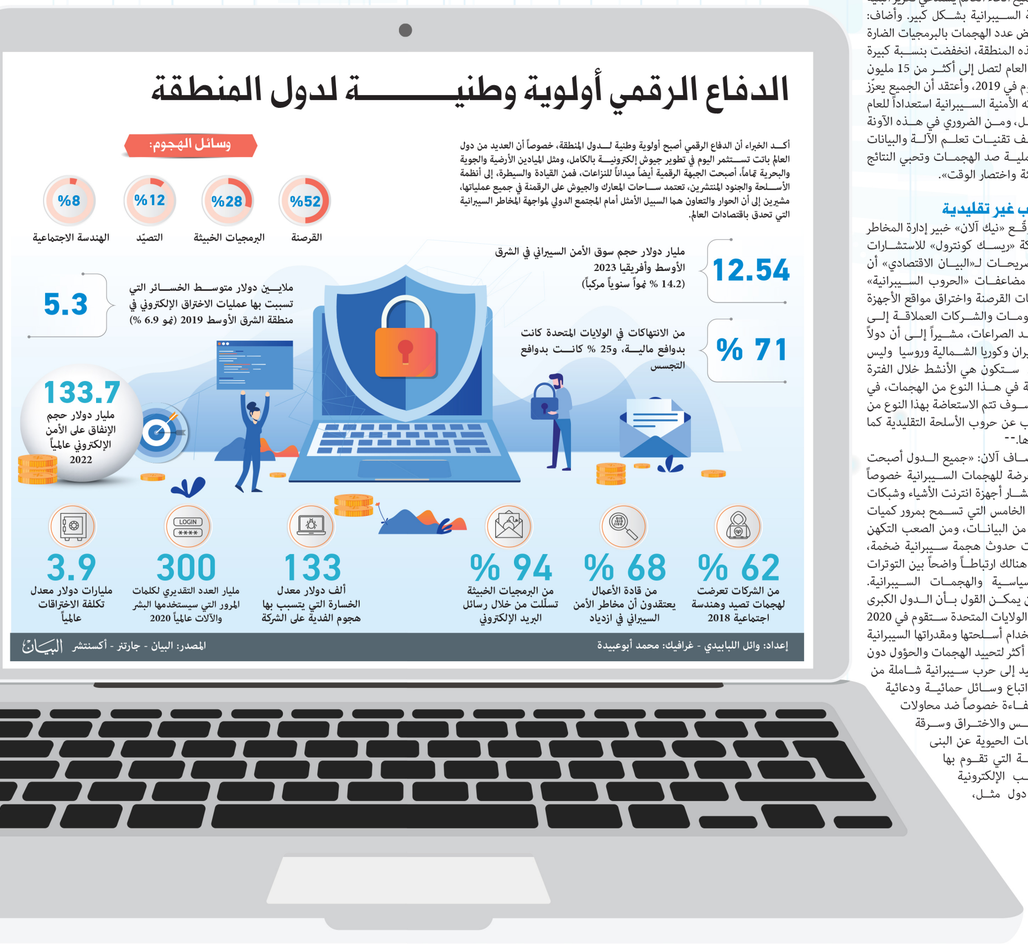
استراتيجية وطنية

من جانبه أكد محمد عارف، الرئيس التنفيذي للأمن في مايكروسوفت الإمارات أهمية «الاستراتيجية الوطنية للأمن السيبراني» التي أطلقتها الإمارات هذا العام في خلق بيئة سيبرانية آمنة وصلبة في الدولة تساعد على تمكين الأفراد والمؤسسات من تحقيق طموحاتهم في بيئة آمنة ومزدهرة. وأضاف: «على الشركات أن تضع في صميم رحلتها نحو تحقيق هذه الاستراتيجية تبني الحوسبة السحابية المناسبة وتقنياتها المتصلة، حيث أن هناك مجموعة من المعايير يستوجب توافرها من أجل بلوغ هذا الهدف.

وعلى صعيد دول المنطقة، تقوم الدول والشركات في جميع أنحاء المنطقة بتحويل اهتمامها بشكل تدريجي إلى السياسات التي تتناول خصوصية البيانات على المستوى الوطني، ومع ذلك فإن أبحاث مايكروسوفت تظهر أن ما يزيد على ثلث كبار مسؤولي أمن المعلومات في الشرق الأوسط لم يقوموا بعملية تصنيف البيانات الخاصة بهم، فيما أظهرت نفس الأبحاث أن ما يقرب من النصف بصدد اقتناء حلول لتصنيف البيانات، في حين أظهرت الدراسة أن 20٪ فقط منهم استطاعوا الحصول على الحلول المناسبة لتصنيف البيانات. وأضاف: «يمكن لتكنولوجيا السحابية أن تساعد الشركات على تسريع جهود الامتثال من خلال تبسيط عمليات تصنيف البيانات المعقدة. وفي واقع الأمر إن علامة التوبيخ الجديدة لتصنيف البيانات تسمح للشركات بعرض كافة بياناتهم الحساسة عبر مايكروسوفت 365، بحيث إنها تكون مصنفة ضمن أنواع المعلومات الحساسة أو المرتبطة باللوائح، كما ستمتلك القدرة على اكتساب رؤى خاصة بالسياسات الموصى بها لحماية البيانات وتسهيل تبويب البيانات وفقاً لمدى حساسيتها».

الدفاع الرقمي أولوية وطنية لدول المنطقة

أكد الخبراء أن الدفاع الرقمي أصبح أولوية وطنية لدول المنطقة، خصوصاً أن العديد من دول العالم باتت تستثمر اليوم في تطوير جيوش إلكترونية بالكامل، ومثل المبادين الأرضية والجوية والبحرية تماماً، أصبحت الجبهة الرقمية أيضاً ميداناً للنزاعات، فمن القيادة والسيطرة، إلى أنظمة الأسلحة والجنود المنتشرين، تعتمد ساحات المعارك والجيوش على الرقمنة في جميع عملياتها، مشيرين إلى أن الحوار والتعاون هما السبيل الأمثل أمام المجتمع الدولي لمواجهة المخاطر السيبرانية التي تحدق باقتصادات العالم.



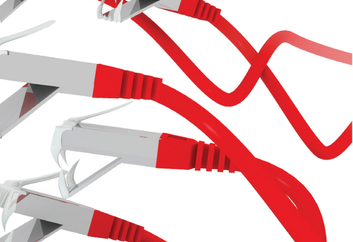
«هواوي»: الأمن السيبراني تحدٍ عالمي يتطلب تعاون القطاعات كافة

قال نان جيان فينغ، مدير شؤون الأمن السيبراني في شركة «هواوي» إن الأمن السيبراني تحد عالمي يواجهنا جميعاً مما يتطلبّ تعاون كافة القطاعات والهيئات التنظيمية على توحيد معايير وآليات الكشف عن التهديدات التي تواجه الأمن السيبراني، مع التزام شركات تزويد المعدات وشركات الاتصالات وغيرها من الجهات المعنية بالنظام الإيكولوجي لتقنية المعلومات والاتصالات بتطبيق هذه المعايير والآليات.

وأضاف: «وباعتبارنا من مزودي المنتجات والحلول، فإننا في هواوي ندرك أهمية دورنا في الحفاظ على الأمن من خلال ريادتنا في مجال الابتكارات التكنولوجية، وعملنا الجاد على نشر النظام الإيكولوجي لتقنية المعلومات والاتصالات على نطاق واسع، إذ يمثل أمن الشبكة أولوية قصوى بالنسبة لنا. وتحقيقاً لهذه الغاية ينبغي علينا الالتزام بالمعايير العالمية لأمن الشبكات بحيث نضمن تحقيق المصلحة العامة».

وتُبدي هواوي استعدادها للعمل مع جميع الحكومات والعملاء والشركاء على تنفيذ إجراءات فعالة للتخفيف من الجيوسياسية والهجمات الإلكترونية الرقمي. كما شاركت هواوي في النشاطات المعنية بوضع معايير الأمن السيبراني للاتصالات التي ينظمها كل من قطاع تقييس الاتصالات في الاتحاد الدولي للاتصالات (ITU-T) ومشروع شراكة الجيل الثالث (3GPP) ومجموعة مهندسي شبكة الإنترنت (IETF) وغيرها من النشاطات. كما انضمت الشركة إلى عدة منظمات أمنية، وعقدت شراكات مع شركات الأمن الرئيسية لضمان أمن مستخدميها على الشبكة.

«فولت 7» سرداب التخزين



في مارس 2017، سرّب موقع «ويكيليكس» لائحة طويلة بأسماء برمجيات وأدوات تجسس وبروتوكولات التشغيلية ووسائل اختراق سيبرانية طورتها وكالة الاستخبارات الأمريكية وتضم أكثر من 7000 صفحة، واهمها «فولت 7» مخزون الأسلحة السيبرانية او سرداب التخزين الاساسي، ما أكد قيام الولايات المتحدة بتطوير أسلحة سيبرانية بإمكانيات كبيرة وواسعة لاختراق أنظمة خدمية خارجية من شي، ما من الداخل سيوفر بديلاً لتدمير منشآة نووية من الجو، على سبيل المثال. ويشير خبراء إلى أنه نموذج فعال ومخيف من نمو الإنفاق على تكنولوجيا المعلومات في الإمارات بمعدل نمو سنوي مركب قدره 8٪ ليصل إلى 23,1 مليار درهم بنهاية عام 2019، وفقاً لغرفة تجارة دبي.

«ستكسنت» أول سلاح رقمي

يعتبر «ستكسنت» Stuxnet أول سلاح رقمي في العالم قامت بتطويره الولايات المتحدة في 2010. وقبل ستوكسنت، ركزت معظم عمليات أمريكا السيبرانية العسكرية والاستخباراتية على سرقة البيانات أو تحريفها، أو استخدمت أدوات سيبرانية للمساعدة على توجيه أسلحة أمريكية وأما هذا الفيروس فتصوره المسؤولون الأمريكيون كبديل للأسلحة التقليدية، على أساس أن استخدام فيروس كمبيوتر لتخريب آلية عمل

«سوني» تنتج «فيلم المقابلة»

وجّه مكتب التحقيقات الفيدرالية الأمريكي في نوفمبر 2014، أصابع الاتهام إلى كوريا الشمالية بشن هجمات إلكترونية على شركة «سوني» بسبب إنتاج الشركة الأمريكية للفيلم الساخر «المقابلة» والمتعلق بزعيم البلاد كيم جونغ أون. حيث تمكن المخترقون من الدخول إلى أنظمة الشركة وسرقة محتوى الفيلم ومعلومات شخصية سرية عن الممثلين ومعلومات عن رواتب التنفيذيين في الشركة وخطط «سوني» المستقبلية وحتى رسائل البريد الإلكتروني للمسؤولين في «سوني». وقررت «سوني» وسط تلك الزوبعة الإعلامية والسياسية آنذاك إلغاء عرض الفيلم في دور السينما. وانتقد حينها رئيس مجلس النواب الجمهوري الأسبق نيوت جينجريتش في تغريدة على «تويتر» قرار «سوني» إلغاء عرض الفيلم قائلاً: «مع انهيار سوني خسرت أمريكا أول حرب إلكترونية، هذه سابقة خطيرة جداً».

بيانات بطاقات بنكية لـ 15 مليون عميل إيراني

انتشرت على مواقع التواصل الاجتماعي في الثالث عشر من ديسمبر الجاري، بيانات بطاقات بنكية لـ 15 مليوناً من عملاء ثلاثة بنوك في إيران في أكبر عملية تسريب لبيانات بنكية في تاريخ البلاد. وفيما تحاول السلطات الإيرانية حتى الآن إلقاء اللوم على مخترقين أفراد، يرجح خبراء الأمن السيبراني أن العملية كانت من تخطيط وتنفيذ عمل وكالات الاستخبارات الأمريكية، خصوصاً مع وجود عقوبات على البنوك المستهدفة فرضتها عليها الولايات المتحدة الأمريكية بسبب تورطها في تحويل أموال للحرس الثوري الإيراني الذي تصنفه واشنطن منظمة إرهابية. وتمثّل هذه الضربة الاقتصادية نموذجاً لتحول الحروب التقليدية تدريجياً نحو الفضاء السيبراني. ومن جانبها تتهم الولايات المتحدة إيران بشن هجمات إلكترونية كبيرة ضد أهداف أمريكية، بما في ذلك «بنك أوف أمريكا» و«جيه بي مورغان تشيس» و«ويلز فارغو». ويشير خبراء إلى أن تلك الجماعات «تتمتع بقدرات تكنولوجية فائقة وعادة ما تكون في يد أجهزة المخابرات الحكومية».

60 عصابة قرصنة سيبرانية

يصف «دليل الهجمات الرقمية» من «تاليس» (The Cyberthreat Handbook) أنشطة ما يقرب من 60 عصابة قرصنة سيبرانية ذائعة الصيت ناشطة حالياً حول العالم، بما في ذلك أساليبهم وتقنياتهم ودوافعهم والقطاعات التي يستهدفونها. وقد حدد خبراء تاليس في هذا التقرير غير المسبوق وعبر تحليل مصادر متعددة مثل المعلومات الاستخباراتية أربع فئات رئيسية من المهاجمين استناداً إلى دوافعهم وأهدافهم النهائية، وتوصلوا للتالي:

- الفئة الأكبر (49٪) تتشكل من الجماعات التي ترعاها الدول لسرقة بيانات حساسة لأغراض سياسية. ويعود السبب في النسبة العالية لهذه الفئة إلى الموارد المالية والبشرية الكبيرة المتاحة لها لضمان فاعلية أنشطتها.
- تليها فئة المناصرين لقضايا معينة (26٪) والتي تبرر هجماتها بدوافع أيديولوجية وينصب تركيزها عموماً على التنديد بأنشطة المنظمات التي يرونها غير مقبولة، والإضرار المتعمد بعلاماتهم التجارية أو صورتهم أمام العامة.
- يتبعهم عن كثب فئة مجرمو الإنترنت (20٪) المتعطشين للمكاسب المالية، ويستهدفون بشكل رئيسي الشركات والقطاع المالي.
- أما جماعات الإرهاب الإلكتروني (5٪) فيقومون عادة بحملات دعائية لتجنيد متعاطفين جدد أو محاولة تدمير بيانات ضحاياهم.

وبين أكثر الجماعات خطورة ونشاطاً في الوقت الحالي منظمة تطلق على نفسها اسم TA505/ATK103، والناشطة منذ عام 2014 على الأقل، وهي المسؤولة عن بعض أكبر حملات البريد العشوائي التي تم رصدها على الإطلاق، وتستخدم برمجيات الفدية الخبيثة بأعداد ضخمة وعلى نطاق واسع، بهدف تحقيق المكاسب المالية، وتمت ملاحظة أن أنشطتهم متكيفة للغاية، وكثيراً ما تبدل تكتيكاتها الهجومية، وتستخدم «البرمجيات الضارة الجاهزة».