حماية البيانات في المنطقة وتحدي

الامتثال للأمن الإلكتروني

واقع الأمن السيبراني في العالم

كشف "مؤشر مستوى الاختراقات" الصادر مؤخراً عن "جيمالتو" الشركة العالمية العاملة في مجال حلول الأمن الرقمي تعرّض ما يقارب 10 مليارات من سجلات البيانات عالمياً خلال السنوات الخمس الماضية لحالات سرقة أو فقدان أو إفشاء علني، بمعدل تعرض 5 ملايين من سجلات البيانات للاختراق يومياً ويمثل المؤشر قاعدة بيانات عالمية تعمل على تتبع وتحليل خروقات البيانات ونوع البيانات المتأثرة وكيفية الوصول إليها أو فقدانها أو سرقتها.

دبي - وائل اللبابيدي

أكّد مسؤولون حكوميون أن دبي وضعت الأمن الإلكتروني على رأس أولوياتها منذ شرعت في تأسيس البنية التحتية الرقمية والخدمات والتجارب المبنية على التقنيات منذ أكثر من 17 سنة، عندما أطلق صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي، رعاه الله، الحكومة الإلكترونية، وصولاً إلى الحكومة الذكية والمدينة الذكية، لافتين إلى حرص الحكومة على الاطلاع على مختلف الممارسات العالمية في المجال، وضمنها تشريع حماية البيانات الأوروبي أو General Data Protection Regulation» GDPR»، ووضع ما يلائم دبي من جهة أخرى، بما يخدم مسيرة الدولة لتكون المدينة الأسعد على وجه الأرض.

وقال خبراء في الأمن الإلكتروني إن الغرامات التي تواجه الجهات غير الملتزمة باتخاذ التدابير المطلوبة للامتثال للائحة العامة لحماية البيانات (GDPR)، والتي تدخل حيز التنفيذ بعد بضعة أسابيع، تصل إلى 20 مليون يورو (91 مليون درهم)، أو 4٪ من إجمالي المبيعات السنوي -أيهما أكثر. وشدد الخبراء على ضرورة التزام الشركات الإماراتية التي لها وجود في الاتحاد الأوروبي الكامل بهذه اللائحة التي ستسري على كل الشركات والمؤسسات التي تعالج البيانات الشخصية للمواطنين الأوروبيين في الإمارات - بما فيها المستثمرون في القطاع العقاري على سبيل المثال - خصوصاً أن الاتحاد الأوروبي يعتبر أحد أكبر الشركاء التجاريين للإمارات.

تحوّل

وقال عامر شرف، مدير إدارة التعاون ودعم الامتثال بمركز دبي للأمن الإلكتروني: حققت دبي الريادة والسبق في التحوّل الرقمي على مدى السنوات الماضية، وفي رحلتها المستمرة لبناء المستقبل وضعت الأمن الإلكتروني على رأس الأولويات، لأن البنية التحتية الرقمية والخدمات والتجارب المبنية على التقنيات هي العمود الفقري لحياة المستقبل الذي بدأت دبي ببنائه، ليس اليوم، ولكن منذ أكثر من 17 سنة، عندما أطلق سيدي صاحب السمو الشيخ محمد بن راشد آل مكتوم الحكومة الإلكترونية وصولاً إلى الحكومة الذكية والمدينة الذكية. وكان لا بُد من حماية هذه الإنجازات خاصة بعد تنامي أهمية الأمن الإلكتروني، لأن المخاطر أصبحت تتطور بنفس سرعة تطور التقنيات وأحياناً أسرع منها. ولهذا تم إطلاق مركز دبي للأمن الإلكتروني عام 2014 بموجب القانون رقم (11)، بهدف تطوير وتنفيذ تشريعات وسياسات خاصة بأمن المعلومات، ووضع معايير الممارسات الجيدة الخاصة بالأمن الإلكتروني في مختلف قطاعات إمارة دبي، وتبعه إطلاق استراتيجية دبي للأمن الإلكتروني عام 2017.

توافق

ورداً على سؤال عن مدى توافق منظومة الأمن الإلكتروني في دبي مع تشريع حماية البيانات الأوروبي GDPR قال: إن لكل منطقة في العالم احتياجاتها، وتضع الأطر التي تلبي هذه الاحتياجات، ولكن في الوقت ذاته نحن في دبي مدينة ذات معايير مستقبلية، فنصمم أطرنا لتكون متوافقة مع احتياجات المستقبل، لذلك جاء نظام أمن المعلومات لحكومة دبي المعروف بـISR في عام 2012 ، وبعده استراتيجية دبي للأمن الإلكتروني، لتحمي البيانات والبنية الرقمية لدبي، وفق أفضل المعايير العالمية، ولكن في الوقت ذاته وفق ما يلبي النموذج المستقبلي لدبي، ولذلك تجد منظومتنا في دبي تلتقي مع العديد من المعايير والأنظمة الدولية، ومنها المواصفة الأوروبية في المعايير الرئيسة لـGDPR، وخاصة في مجالات حوكمة أمن المعلومات، والوصول إليها وإدارة تبادل المعلومات وأمن وإدارة الخدمات التي يقدمها مزودون ومبادئ أمن الحوسبة السحابية. وأردف: دبي تتطلع لتكون المدينة الأذكى والأسعد، ولتحقيق ذلك جاء مركز دبي للأمن الإلكتروني مع مهمة لجعل دبي المدينة الأكثر أماناً إلكترونياً في العالم. واستراتيجية دبي لأمن المعلومات جاءت شاملة تغطي في مبادئها الامتثال للتشريعات، والتبادل الآمن للمعلومات، وكذلك مبدأ التعاون، لأن مخاطر الأمن الإلكتروني تتخطى حدود الدول، فنص هذا المبدأ على بناء الشركات مع المدن المحلية والعالمية والدول الأخرى، إضافة إلى تبادل المعلومات حول المبادرات المختلفة لمواجهة المخاطر، ومبدأ تقييم المخاطر الذي ركّز على أهمية وعي وإدراك ودراية الجمهور على اختلافه بدوره في تلافي مخاطر الأمن الإلكتروني.

سياسات البيانات في دبي تراعي تطورات المستقبل والممارسات العالمية

«تنظيم الاتصالات» تعزّز الأمن السيبراني في الجهات الحكومية والاتحادية


■ معتز بن علي


■ وليد كمال


■ يونس آل ناصر

سريان

تسري اللائحة العامة لحماية البيانات على معالجة البيانات الشخصية للأفراد في الاتحاد الأوروبي / المنطقة الاقتصادية الأوروبية من قبل جهات مراقبة أو معالجة لا يقع مقرها في المنطقة. وبعبارة أخرى، سيسري الأمر على كلّ الشركات والمؤسسات التي تعالج البيانات الشخصية للمواطنين الأوروبيين، بغض النظر عن موقع هذه الشركات أو المؤسسات في أي مكان من العالم.

وقال المهندس عادل المهيري، مدير مركز الاستجابة لطوارئ الحاسب الآلي التابع للهيئة العامة لتنظيم قطاع الاتصالات في الدولة: إن من أهم التدابير التي اتخذتها الهيئة بخصوص تعزيز الأمن السيبراني زيادة الوعي الأمني السيبراني في الجهات الحكومية والاتحادية بإطلاق حملة «لا يخدعونك»، ويأتي ذلك بسبب قلة الوعي الأمني وازدياد نسبة الهجمات الإلكترونية التي تتضمن الهندسة الاجتماعية، وهي من أهم وأسهل الهجمات الإلكترونية التي تترتب عليها الرسائل والمكالمات الاحتيالية.

وأردف: توجهات عمليات الاختراق في هذا العام هي الهندسة الاجتماعية، ويأتي ذلك بسبب زيادة الاختراقات الاحتيالية التي تسببت في اختراق البرنامج الإلكتروني للتواصل الاجتماعي «واتس آب» بنسبة كبيره في بداية هذا العام.

سياسات

من جانبه، اعتبر يونس آل ناصر، مساعد المدير العام لدبي الذكية والمدير التنفيذي لمؤسسة بيانات دبي، أن سياسة حماية البيانات واحدة من أهم سياسات البيانات الخمس التي أطلقتها دبي الذكية خلال العام الحالي، وحددها قانون البيانات كمنظومة تحكم نشر وتبادل البيانات، لافتاً إلى أن لائحة سياسات البيانات تركز في الوقت ذاته على البيانات ذات الأولوية للنشر والتبادل في الجهات الحكومية، وهي أربعة: السجلات المرجعية الرئيسة، وبيانات يتم نشرها وتبادلها لأغراض الخدمات الإلكترونية أو الذكية، والبيانات ذات الأولوية العالية لتنفيذ مبادرات حكومية استراتيجية أو تمكين التحول الذكي، إضافة إلى البيانات التي يتم طلبها من أكثر من جهة في دبي. وتغطي لائحة بيانات دبي ثلاثة مجالات، هي حماية البيانات واستخدام وإعادة استخدام البيانات والحوكمة.

وأضاف: شملت سياسة حماية البيانات في دبي ثلاثة مجالات رئيسية، هي معايير تصنيف البيانات، وحماية الخصوصية وحماية الملكية الفكرية وأمن المعلومات. أما بالنسبة لاستخدام وإعادة استخدام البيانات فشمل ذلك مجالات نشر البيانات المفتوحة، وتبادل البيانات المشتركة، بالإضافة إلى تسييل البيانات، وفي مجال الحوكمة حرصنا على تشكيل فرق للبيانات ووضع المعايير الفنية وآلية تلقي الشكاوى والتظلمات بحيث نحقق عبر ذلك كله سعادة ورضا الناس، ونحقق فهماً مشتركاً لكل ما يتعلق بالبيانات.

تطور

وقال آل ناصر: هناك أمران يميزان سياسات البيانات في دبي، يتمثل أولهما في أنه تم تصميمها لتناسب مستوى التطور والتقدم الهائل وشكل المستقبل

إنفاق


محمد عارف

قال محمد عارف المدير الإقليمي لأماكن العمل الحديثة لدى شركة مايكروسوفت الخليج إنه من المتوقع أن يزيد حجم الإنفاق على سوق الأمن والحماية في دول مجلس التعاون الخليجي ليصل إلى 10,41 مليارات دولار بحلول نهاية عام 2022 حسب دراسة خاصة لشركة «ريسيرش أند ماركت دوت كوم»، لذلك تعي دول المنطقة التحدي الكبير الذي يقع على عاتقها من أجل ضمان توفير الحماية اللازمة لتحقيق جميع أهدافها، وضرورة الاستثمار في هذا المجال الذي يعد العنصر الأساسي لنجاح أي مشروع. ولفت إلى أن مايكروسوفت تساعد من خلال التزامها تجاه دول المنطقة بتعزيز المجال الأمني من خلال قيامها بتحديث ما يقرب مليار جهاز ويندوز في جميع أنحاء العالم كل شهر، وتدير أكبر خدمة لمكافحة الفيروسات والبرامج الضارة في العالم. وأضاف: تقوم مايكروسوفت ببناء معلومات استخباراتية واسعة النطاق لـ300 مليار طلب مصادقة ومعالجتها كل شهر، كما تضيف مايكروسوفت عدة غيغابايت من بيانات القياس عن بعد إلى نظامها الأمني الذكي وتشمل 1,3 مليار مصادقة على Azure Active Directory يومياً ومسح أكثر من 200 مليار بريد إلكتروني للكشف عن البرامج الضارة كل الشهر، وتابع: يعد هذا الامتثال مهماً للمنظمات في الإمارات وذلك لأن الاتحاد الأوروبي يعتبر أحد أكبر الشركاء التجاريين، كما أن سوق الاتحاد الأوروبي يوفر عروضاً وفرصاً كبيرة لكثير من الشركات في جميع أنحاء المنطقة.

تحسن


حسام صيداني

لفت حسام صيداني، المدير الإقليمي لشركة «سيمانتك» في منطقة الخليج إلى أن البيانات الخاصة بالإمارات ضمن تقرير التهديدات الأمنية عبر الإنترنت 2017 لسيمانتك تشير إلى تحسن مستويات أمن البيانات مقارنة بالمستويات العالمية، حيث تراجعت مرتبة الدولة من المركز 51 في عام 2016 إلى 52 خلال 2017 من حيث تهديدات أمن البيانات. لكنّ الإمارات في المقابل قفزت هذا العام من المرتبة الـ10 بمنطقة الشرق الأوسط وأفريقيا لتصل إلى المركز التاسع بحسب التقرير. وخلال العام الماضي، واجهت شبكات المعلومات في دولة الإمارات تهديدات، تمثلت بشكل أساسي في الجهات والأفراد بمجال صّك العملات المشفرة وبرمجيات الفدية والبرمجيات الخبيثة. وسجّلت دولة الإمارات نسبة أقل من حيث برمجيات الفدية على مستوى العالم (المركز 41)، حيث حلت في المرتبة السادسة ضمن الدول الأكثر استهدافاً لبرمجيات الفدية في منطقة الشرق الأوسط وأفريقيا العام الماضي، متراجعةً بمقدار 4 مراكز عن العام 2016.

نصائح مهمة للشركات

- من أجل التحصّن من التهديدات الأمنية المتنامية في يومنا هذا والوقاية من المخاطر المستقبلية، يجب على الشركات اعتماد حلول أمنية تتيح سوية أعلى من الشفافية في كافة الشبكات، مع تمتعها بإمكانيات كشف الخروقات بشكل فوري، وتوفير الحماية من الهجمات وتعزيز نقاط الضعف.
- المسح في الوقت الحقيقي: يسمح المسح الفعال والأتوماتيكي باكتشاف البرمجيات الخبيثة بكفاءة عالية، مع تحسين أداء الآلات.
- التحليل السلوكي: تسمح هذه القدرات برصد وحجب البرمجيات الخبيثة المتقدمة القادرة على تجاوز الدفاعات التقليدية.
- التعلّم الآلي عالي الموثوقية: يسمح توظيف المدخلات البشرية وبيانات التهديدات برصد المخاطر بسرعة والحماية من التهديدات المعروفة وغير المعروفة.
- أمن النقاط النهائية: تقنية أمنية تقوم على تحديد الوصول (sandboxing)، وكشف الخروقات، وتعزيز مستشعرات النقاط النهائية بهدف اكتشاف أي أنشطة مشبوهة، والحيلولة دون وقوع أي هجمات.

9 مليارات دولار خسائر متوقعة لهجمات البريد الإلكتر

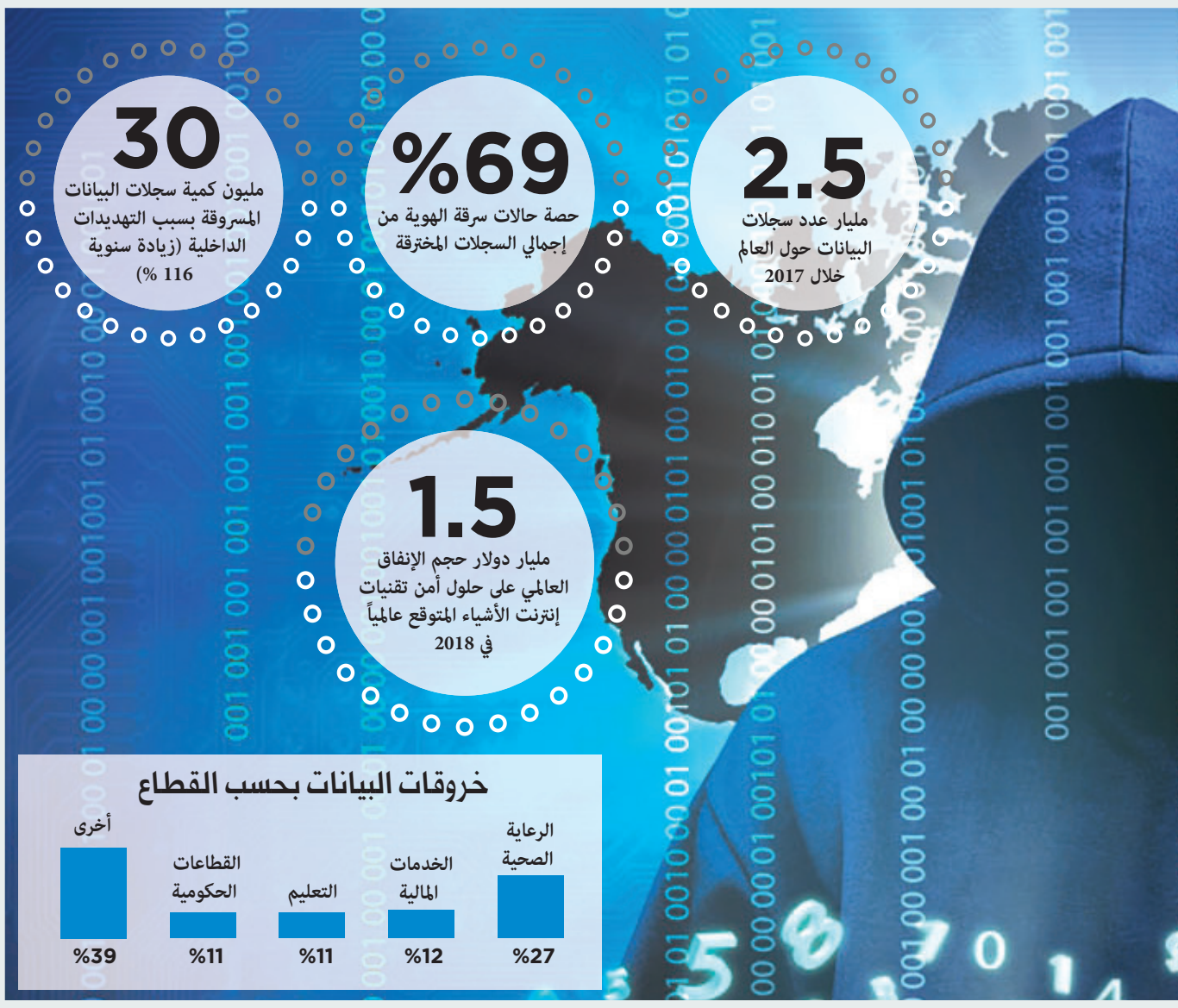
توقع تقرير حديث عن «ترند مايكرو» تضاعف معدل هجمات اختراق البريد الإلكتروني خلال 2018، لتفضي إلى خسائر تفوق قيمتها 9 مليارات دولار حول العالم. ولكن بالمقابل بالإمكان الحد من هذه الخسائر بشكل جزئي عبر تعزيز الوعي بطبيعة وأساليب هذا النوع من الهجمات والتكتيكات المتبعة فيها، ما سيؤدي إلى تعزيز القدرة على رصد التهديدات والإبلاغ عن الرسائل الاحتيالية. البريد الإلكتروني.

وقال معتز بن علي نائب رئيس شركة «ترند مايكرو» لمنطقة الشرق الأوسط وشمال أفريقيا إن التصدي لتلك الهجمات سيعتمد ذلك بشكل كبير على مدى معرفة الأساليب التي ينتهجها القراصنة في محاولاتهم لاختراق وهو أمر فائق الأهمية في التصدي لهذه الهجمات كما ثبت للشركة. وأضاف: سنواصل رؤية حالات اختراق لحسابات البريد الإلكتروني العائدة لمسؤولي الشركات، والتي تهدف إلى الحصول على مبالغ من المال، وقد لاحظنا زيادة ملموسة في الهجمات التي تستخدم عناوين بريد إلكتروني تابعة للرؤساء التنفيذيين.

وتجدر الإشارة أيضاً إلى أن القراصنة يعمدون إلى استخدام ملفات البي دي إف PDF ومواقع التصيّد الإلكترونية (Phishing)، وذلك بدلاً من تطبيقات التجسس على لوحة المفاتيح (keyloggers) المترافقة بخدمات تشفير، والتي تعتبر أعلى كلفة، إذ يسمح لهم التصيّد باختراق الحسابات بتكلفة أقل. وشهد العام الماضي موجة واسعة من هجمات برمجيات الفدية حول العالم، والتي كلفت الشركات المستهدفة مليارات الدولارات مثل فيروسي «نوت بيتيا» و«وانا كراي» الذي سجل 300 ألف إصابة لقراصنة الاختراق، وأدى إلى خسائر تخطت

ـــات القرصنـــة

ـي حماية للمستقبل



■ غرامات قاسية تنتظر الكيانات غير الملتزمة بلائحة الحماية الأوروبية

■ الشركات الإماراتية المتعاملة مع الاتحاد الأوروبي مطالَبة بالامتثال للائحة


■ عادل المهيري


■ عامر شرف

الـذي تتطلـع قيادتنا لبلوغه من جهـة، وفي الوقت ذاتـه حرصنا على الاطلاع على مختلف الممارسـات العالمية في المجال وضمنها تشـريع حماية البيانات الأوروبـي GDPR ووضعنـا ما يلائم دبـي من جهة أخرى بما يخدم مسـيرتنا لنكون المدينة الأسعد على وجه الأرض.

وتابع: سـبقنا العديد من أكثر مـدن العالم تطوراً فـي التحـوّل الرقمـي، وأنا أؤمـن أننا نشـهد حالياً نقطـة تحوّل فـي نظرة قـادة العالـم وخبرائه نحو البيانـات بالنظـر إليها كنفط المسـتقبل وأن مقدرة الـدول والمدن والإنسـان بشـكل عام علـى تحليل البيانـات ومعالجتها هـي التي سـتحدد قدرته على الجاهزية للمسـتقبل. ونحن بإطلاق سياسات بيانات دبي كتشـريع الذكي سيمكننا تحقيق التحوّل الرقمي والاستفادة القصوى من البيانات بمستقبل دبي.

غرامات

وأكّد وليد كمال نائب أول للرئيس للأمن التكنولوجي وإدارة المخاطـر فـي شـركة الإمـارات للاتصـالات المتكاملـة «دو» أهميـة الالتـزام باللائحـة العامة لحمايـة البيانـات والعمل بموجبها، مشـيراً إلى أنه في حال وجود شـركات تعمل فـي الاتحاد الأوروبي أو لديهـا مكاتب في الاتحـاد الأوروبي أو تتعامل مع بيانات وتعامـلات لمواطنين من الاتحـاد الأوروبي، فيجب عليها معرفة هذه اللائحة وأن تكون مستعدة لتطبيقهـا، لافتاً إلى أن التأثيـرات المتوقعة في حال عدم الالتـزام بتلك المتطلبات سـتؤدي إلى غرامات باهظـة تقـدر بملايـين الـدولارات بحسـب أرباح الشـركات السـنوية. وأضاف: يجب على الشـركات الإماراتيـة التي لها وجود بالاتحـاد الأوروبي الالتزام الكامل بهـذه اللائحة. وتفرض المادة 33 من اللائحة الإبلاغ عن الخروقـات المتعلقة بأمن بيانات الأفراد، وهذا يعني أن على جميع الشركات الإماراتية الالتزام بالإبلاغ بحسـب المادة 33. وفي حال وجوب الإبلاغ يجب الإبلاغ دون تأخير وألا تتجاوز المدة 72 سـاعة من تاريـخ الإفصاح. ويجب إبـلاغ الجهات المختصة فـي الوقـت المحدد ويجب ألا يتم تبريـر أي تأخير. وحول التدابير التي تتخذها «دو» حالياً لحماية بيانات عملائهـا، قال كمال: نسـتثمر حالياً فـي حلول أمنية لصـد التهديدات المتعلقة بهجمـات حجب الخدمة الموزعة DDOS التي بدأت تزيد عن السـابق والتي تسـتهدف غالباً الأجهـزة المتعلقة بأنترنت الأشـياء وكذلـك لحمايـة عملائنا من خلال توفيـر الخدمات بشـكل دائم من غير انقطاعات نتيجة تلك الهجمات. ونعمـل أيضـاً على وضـع أنظمة الحمايـة لعملائنا لتمكينهـم من تصفح الإنترنت بأمان ويسـر وضمان عدم دخول المواقـع التي تحتوي على برامج خبيثة، إضافـة إلى أننا نقدم برامج توعيـة مختلفة لعملائنا على مدار العام.

وأوضـح الدكتـور معتز بـن علي نائب رئيس شـركة «تريـند مايكرو» لمنطقة الشـرق الأوسـط وشـمال إفريقيا المتخصصة في الأمـن الإلكتروني إن اللائحة العامة لحماية البيانات هي عبارة عن قانون تنظيمي جديد سـنّه الاتحاد الأوروبي بعد أن عمل عليه لمدة 4 سـنوات قبل المصادقة عليه فـي 14 أبريل 2016. وسـتحل اللائحة الجديدة محل سابقها توجيه حماية البيانـات رقـم EC/46/95 الذي كان قـد اعتُمد في عـام 1995، ويتلخص الهـدف منها في ضبط وتنظيم معالجة البيانات الشخصية للأفراد الذي سيشار إليهم في هذا المستند باسـم المواطنين الأوروبيين، وهم المقيمون في المنطقة الاقتصادية الأوروبية (EEA)، أي الـدول الأعضاء في الاتحاد الأوروبي بالإضافة إلى آيسـلندا، وليختنشـتاين، والنرويج. وقـد تم تصميم اللائحة العامة لحماية البيانات العامة على نحو أوسع نطاقاً بحيث تواكب أهم التغيرات، مع إيلاء الاهتمام المطلوب لمشهد الأمن السيبراني في الوقت الراهن.

وحـول ضرورة امتثال الشـركات الواقع مقرها في الإمـارات والتي تملـك فروعاً في الاتحـاد الأوروبي للائحـة، قـال بن علـي: تسـري اللائحة علـى كافة الشـركات التي تقـوم بمعالجة البيانات الشـخصية للمقيمين المنطقـة الاقتصادية الأوروبية في الاتحاد الأوروبـي، بغـض النظر عـن موقع الشـركة، أي أن اللائحـة العامة لحماية البيانات تسـري على معالجة البيانـات الشـخصية مـن قبـل الجهـات المراقِبـة (الشركات)، والمعالجين (الجهات التي تعالج البيانات لصالح الشـركات) في المنطقة الاقتصادية الأوروبية، بغـض النظر عمّـا إذا كانت عمليـات المعالجة تتم داخل هذه المنطقة أم لا. ويجب على الشركات التي لا تنتمي لـدول المنطقة الاقتصادية الأوروبية، والتي تقـوم بمعالجة بيانات مواطني هذه الدول، أن تعيّن ممثلين لها ضمن تلك المنطقة.

3 خطوات لامتثال الشركات في الإمارات


■ أندرو كالثورب

قـال أنـدرو كالثـورب، الرئيـس التنفيذي لشـركة استشـارات البنية التحتيـة لتقنية المعلومـات كونـدو بروتيغـو ومقرهـا الإمارات، إن أمام المؤسسـات والشركات العاملـة في الدولة بضعة أسـابيع لتعمل علـى ضمان توافـق أعمالها مـع القانون الأوروبـي لحمايـة البيانـات، وأنها تحتاج للقيـام بثـلاث خطوات مطلوبـة لتحقيق الامتثال للقانون الأوروبي لحماية البيانات.

1. استكشاف البيانات

أكّد كالثورب أن الخطوة الأولى تتمثل في فهم الشـركات لطبيعـة بياناتها وأهميتها. ويحتاج كبار مسؤولي تقنية المعلومات في دولة الإمارات إلى المسـارعة إلى تحديث البنيـة التحتية الخاصة بـإدارة المعلومات وتقنية المعلومات، مـن أجل التمكّن من البحث في بيانات شـركاتهم واستكشـافها ومراجعتها.

2. فرز البيانات

وأشار الرئيس التنفيذي إلى ضرورة تحديد أي البيانـات يجـب حفظها، وهـو ما يُعدّ مشـكلة بالنظر إلى أن القانـون الأوروبي الجديد يتطلـب من الشـركات الاحتفاظ بالبيانات مع استمرار اسـتخدامها لغرضها الأصلـي، علـى أن يتم حذفهـا بعد ذلك. وتتماشـى مسـألة حماية البيانات وأمنها بالتوازي مع مسألة تصنيفها.

3. اتخاذ الإجراءات

تحتاج الشـركات فـي الدولة للمسـارعة إلى اتباع نهج اسـتباقي في سبيل الامتثال للقانـون الأوروبـي لحمايـة البيانات، في وقت يتزايد الإقبال على تبني الحلّ الشامل لإدارة البيانات Data Management 360 for GDPR، من ڤيريتـاس والذي يخولها الامتثال للقانون الجديد.

ضرورة الاستجابة السريعة للمتطلبات


هادي جعفراوي

شـدد هادي جعفراوي، المديـر الإداري لشـركة «كوالـس» الشـرق الأوسـط على أنـه بمجرد دخـول اللائحة العامة لحمايـة البيانات حيز التنفيذ في يوم 25 مايـو المقبـل، يتعين على المؤسسـات والشـركات في الشرق الأوسط أن تكون جاهزة في أي لحظة للاستجابة السريعة للمتطلبات المتعلقة بقواعد المعلومات الخاصـة لعملائهـا فـي دول الاتحـاد الأوروبي.

حقوق

وأضـاف: علـى سـبيل المثـال، يمكـن للمواطـن العـادي المطالبـة بحقه في حـذف أي بيانـات خاصة بـه من على نظام الشركة. هذه الذراع الطويلة للائحة العامـة لحمايـة البيانـات، قـد تفاجئ الشـركات في بعض الأحيـان، وبالإضافة إلـى ذلك يتعيـن على فـرق تكنولوجيا المعلومـات ضمان امتثالها، وأيضاً امتثال جميع أقسـام المؤسسـة أو الشركة، بل وكل شـركات الطرف الثالـث أيضاً. على سـبيل المثال، هل قامت وحدة التسويق بتطويـر موقع علـى الويـب تجمع من خلاله معلومات العملاء؟

معالجة

وتابع: إذا كان الأمر كذلك، يتعين معرفة كيـف يتم معالجـة البيانـات وتخزينها؟ فمثل هذه الإجراءات غير الواضحة يمكن أن تؤدي إلى تداعيات خطيرة إذا لم تتم معالجتها. نشر مكتب مفوض المعلومات لـدى حكومـة المملكة المتحـدة دليلاً مفصـلاً يتضمن الخطوات التي يمكن أن تتبعها المؤسسات، والتي تشمل تحديث الإجراءات والتخطيط للتعامل مع طلبات وصول الأشخاص إلى البيانات، ومراجعة طـرق البحث والحصول على، وتسـجيل الموافقـة على معالجة البيانات والمزيد. وستمثل هذه الممارسات الآمنة، مقترنة بحلـول قويـة لإدارة أصـول وحـدات المعلومـات، أداة قويـة لأولئـك الذين يتطلعـون إلى المضي قدمـاً في التطور والاستعداد للمستقبل.

شراكات

ولفت إلـى أن الاتحـاد الأوروبي يتمتع بعدد من الشـراكات الاستراتيجية القوية مـع العديـد مـن دول منطقة الشـرق الأوسط، ولن يتأثر حجم التجارة المتبادلة بينهما باختـلاف معدل الناتـج المحلي الإجمالي.

وقال: إذا اختارت الشركات عدم الامتثال للوائح، فقد يؤثر هذا سلباً على أعمالها. حيث قد تقرر جهات الأعمال في الاتحاد الأوروبـي عـدم الدخـول في شـراكات تجاريـة مع أطراف خارجيـة، ما لم تكن تعمل وفقاً للوائح والقوانين. ومن حيث التكلفة، فـإن التدابير المطلوبة للامتثال لقوانين اللائحـة العامة لحماية البيانات تسـتحق الاسـتثمار لموافاتهـا، حيـث سـتواجه الجهات غيـر الملتزمة غرامات تصـل إلى 20 مليـون يـورو، أو 4٪ من إجمالي المبيعات السنوي أيهما أكثر.

الابتزاز الرقمي

سـيكون الابتزاز الرقمي في عام 2018 من أهم ركائـز عمل المجرمين السـيبرانيين، وسـوف يدفعهم إلـى تطويـر منهجيات جديدة تسـمح لهم بالحصـول على مبالغ ضخمـة. وتتمثل أهم مكامن الخطورة في حقيقة أن أي هجمات سـتؤدي إلى أضرار أكبـر وأكبر بحكم اتسـاع نطـاق إنترنت الأشـياء ليغطـي مجالات أكثـر وأكثر من الحيـاة الرقميـة الذكيـة فـي كل مكان، وستدفع هجمات اختراق البريد الإلكتروني المزيـد من الشـركات والمؤسسـات إلى اتخـاذ احتياطـات أقوى لحمايـة أموالها. وكل ذلـك بالتوازي مع اسـتمرار انتشـار الأخبـار الكاذبـة والبروباغنـدا باعتمـاد الأساليب التقليدية ذاتها، مع الإشارة أيضاً إلـى أن التعلّـم الآلي وتطبيقـات «بلوك تشـين» ينطويان على فرص وتحديات في آنٍ معاً. ولا شـك أن الشـركات سـتواجه صعوبات في تطبيق اللائحة العامة لحماية البيانات GDPR، ولن يقتصر التحدي على مكامن الضعف والنقاط الحساسـة، وإنما سيشمل الثغرات في الإجراءات الداخلية، والتـي يمكن النفاذ منها لإلحاق أضرار في الإنتاجية.

ـوني العام الجاري

قيمتهـا 4 مليـارات دولار. وذكر تقرير صادر عن«تريند مايكرو»أن التهديدات التقليدية مثل اختراق حسابات البريد الإلكتروني المؤسسية (BEC) ما زالت تمثل خطراً على الشركات. وفي الوقت ذاته دخلت العملات الرقمية المتقلبة على مشهد المخاطر بقوة عبر تسجيلها ارتفاعاً سريعاً وقوياً في القيمة، لذا لجأ المجرمون السيبرانيون في هذه البيئة إلى منهجيات قديمة بهدف الاستفادة من توجهات العمـلات الرقمية، فضلاً عـن محاولتهـم الاسـتفادة من نقاط الضعف بأساليب جديدة.

الهندسة الاجتماعية طريق الاختراق

تتمثـل الهندسـة الاجتماعيـة في مجموعة من التقنيات المسـتخدمة يسـتخدمها المخترقـون لجعـل النـاس يقومون بعمل ما أو يفضون بمعلومـات سـرية. وتُسـتخدم الهندسـة الاجتماعيـة أحياناً ضمن احتيـال الإنترنت لتحقيـق الغرض المنشـود مـن الضحيـة، حيـث إن الهـدف الأساسـي للهندسـة الاجتماعية هو طرح أسـئلة بسيطة أو تافهة عن طريق الهاتف أو البريد الإلكتروني مع انتحال شـخصية ذي سلطة أو ذات عمل يسمح له بطرح هكذا أسئلة دون إثارة الشبهات.

ويقوم المخترقون عادة باستخدام بعض المحفزات الأساسـية للسلوك البشـري مثل زرع الخوف والفضول والإلهـاء والحماسـة وغيرها. حيث يمكن لصورة عبر البريد الإلكتروني أن تثيـر عواطـف الضحيـة للتبرع لجهة خيرية معينة بشـكل مخادع، أو مـن خـلال إثارة الخـوف داخل المسـتخدم عبـر إعلامـه باختراق إحدى حسـاباتك وأنه يجب إعادة تعيين كلمـة المـرور، أو يُمكن أن يدفـع الفضول الضحية لمشـاهدة إحـدى الصورة المضحكـة أو قراءة خبر مثير للاهتمام.

إغلاق الفجوات الأمنية

- أصبـح الولـوج إلـى المعلومـات من أجهزة وتطبيقات متعددة أمراً طبيعياً للغايـة في عالمنا الحالـي الآخذ في الترابط مع بعضه أكثر فأكثر، وبإمكان المستخدمين إغلاق الفجوات الأمنية باسـتخدام الإعدادات المناسبة، بغض النظر عن الجهاز أو التطبيق أو الشبكة.
- تغيير كلمـات المرور الافتراضية. يجب استخدام كلمات مرور فريدة ومعقدة للأجهـزة الذكيـة، ولاسـيما أجهـزة التوجيه (الراوترات)، بهدف الحد من احتمال تعرضها للاختراق.
- يجـب تعديـل الإعـدادات الافتراضية للأجهـزة بهدف ضمـان الحفاظ على الخصوصية بشـكل دائم واسـتخدام منهجيات تشفير صارمة للحيلولة دون مراقبـة البيانات أو اسـتخدامها على نحو غير مسموح به.
- يجـب تحديث البرمجيـات الثابتة أولاً بـأول، أو تفعيـل خاصيـة التحديث التلقائـي في حـال توافرهـا، وذلك بهـدف إغلاق الفجوات التي قد تمثل نقاط ضعف.
- يجـب التنبّـه دومـاً إلـى الرسـائل الإلكترونية الواردة والمواقع التي تتم زيارتهـا، فهذه قد تحـوي على عناصر غير مرغوب بهـا، أو برمجيات خبيثة للتصيّد أو هجمات مدروسة.