إتقان الامتثال من أجل مستقبل آمن

تحرير: السيد/ أندرو موليجان- مدير شريك لدى شركة فورتانكس" بمنطقة أوروبا والشرق الأوسط وأفريقيا، والسيد/ سفيان العبدي- رئيس قسم الخدمات السيبرانية لدى شركة كي بي إم جي" قطر

(تاريخ النشر: 18 يونيو) يُحدد لاحقًا

يواصل العملاء والموظفون عبر مختلف الأسواق والمناطق الجغرافية سعيهم للحصول على تجارب جديدة ومُحسنة، حيث يُطالبون بتجارب تتسم بإمكانية الوصول عند الطلب، وسهولة استخدام عالية، ومحتوى وتجربة تصفح أكثر تخصيصًا. وبالتالي، تواجه الشركات تغييرات تكنولوجية لمعالجة التجارب الرقمية المتسارعة وتبني مفهوم السحابة، والذكاء الاصطناعي وتقنيات تعلم الآلة لتلبية المتطلبات المتزايدة.

جدير بالذكر أن هذا التسارع في الثورة الرقمية أدى إلى تطور التهديدات الرقمية وزيادة معدل الجرائم الإلكترونية. كما يُتوقع أن ترتفع التكاليف والخسائر الناتجة عن الجرائم الإلكترونية من 8 تريليونات دولار إلى 10.5 تريليون دولار في الفترة بين عامي2023 و2025.

من هذا المنطلق، تبرز أهمية تنظيم هذا الأمر وضرورة إعداد متطلبات إلزامية لحماية البيانات. فرغم اتسام المشهد التنظيمي العالمي بالتفكك على مدار سنوات عدة إلا أن بعض الأسواق -مثل أوروبا والصين والولايات المتحدة- بدأت الآن في تولي قيادة هذا المسار وإرساء المعايير والمبادئ ذات الصلة، في حين تسير على نهجها العديد من الأسواق الأخرى. وقد تجلت هذه المعايير والمبادئ في مجالات الأمن والخصوصية والذكاء الاصطناعي مما يتيح للمؤسسات الرائدة فرصة اتباع نهج قائم على المبادئ لحماية المعلومات السرية وإدارتها بشكل استباقي وفعال، وذلك على الصعيدين المحلي والدولي.

بالتعاون مع مجلس معايير أمان صناعة بطاقات الدفع، عُقدت مؤخرًا ندوة للعاملين في قطاع الخدمات المالية، حيث قادت شركتي "فورتانيكس" و "كي بي إم جي" مناقشة تفاعلية مع أكثر من 20 قائدًا من كبار المؤسسات المالية حول فرص التكيف مع معايير الامتثال لمواجهة تحديات الأمن السيبراني المستجدة.

يدعم قانون المرونة التشغيلية الرقمية ومعيار أمان بيانات صناعة بطاقات الدفع 4.0 وتوجيهات شبكات وأنظمة المعلومات 2 - على سبيل المثال لا الحصر- الحوكمة المحسنة وإجراء عمليات التدقيق والتخفيف من المخاطر الإلكترونية، مما يساهم في الحد من الاضطرابات المتعلقة بتكنولوجيا المعلومات والاتصالات، وتحسين المرونة، والإدارة المتوائمة على مستوى الشركات الفردية والجهات الخارجية الموسعة والمؤسسات في سلاسل التوريد.

أما على الصعيد الداخلي، فيجب على رؤساء أمن المعلومات التواصل والتنسيق مع مجالس الإدارة بالمؤسسات لتوفير قيادة تعطي الأولوية للأمن السيبراني. - تزايدت أهمية هذا التواصل بسبب المخاطر المحتملة للمسؤولية الشخصية.

قد يؤدي عدم الامتثال للوائح إلى فرض عقوبات متعددة -مثل: الغرامات المالية التي قد تصل إلى 4٪ من الإيرادات السنوية في حال مخالفة اللائحة العامة لحماية البيانات أو 20مليون يورو- أو تعرض السمعة والعلامة التجارية للمخاطر، حيث قد يتخذ العملاء قرارهم بعدم التعامل مع الشركة أو اختيار الموظفون الاستقالة أو انخفاض الفوائد المالية وارتفاع تكاليف التدقيق والتأمين وانخفاض قيمة الأسهم في السوق.

يُثير هذا الصدد عدة تساؤلات أهمها: كيف يُمكن للشركات أن تتعامل على نحو فعال؟ وما المقصود بكل ذلك؟

يتمثل الهدف النهائي في إدارة حماية البيانات، وفهم المخاطر والحد منها، والتأكد من وجود خطط مناسبة للتعامل مع التهديدات

عند وقوعها على الرغم من تعقيدات مشهد تكنولوجيا المعلومات والاتصالات في كل من الشركات الفردية وبيئات الأطراف الخارجية. في الحقيقة، يُمكن تحقيق هذه المتطلبات من خلال اتخاذ الإجراءات التالية:

- وضع أطر أكثر فعالية لإدارة المخاطر المتعلقة بتكنولوجيا المعلومات والاتصالات والرقمية المعقدة، سواء المملوكة أو التابعة لأطراف خارجية ·
- وضع الخطط)مثل خطط التعافي من الكوارث واستعادة القدرة على مواصلة العمل بعد وقوع الكوارث،والاستجابة للحوادث، وغير ذلك(لتحمل حالات التعطل والاستجابة لها والتعافي منها ·
- تأمين البيانات دون أن يحول ذلك من مشاركة المعلومات)مثل: الخدمات المصرفية المفتوحة، واستكمال المعاملا توإج راء المقاصة عبر الحدود وبين المؤسسا ت(.
- تبني سياسة الإبلاغ ورفع التقارير والحوكمة وإعمال مبدأ التدقيق وتحسينا تالعمليا ت.
- إدارة الوصول إلى البيانات لدعم الخصوصية والأمن خلال الوقت المحدد بُغية تقليل الوصول غير المصرح به وتسرب البيانا ت.
- تنظيم التدريبات المستمرة وبرامج محاكاة المرونة التشغيلية للخطط وجاهزية الأفراد.

يتضمن مفهوم أمن البيانات حماية سرية البيانات وسلامتها ونزاهتها وتوافرها وأصالة المرسل إليهم ومساءلة المطلعين عليها وعدم التنصل من استلامها وحمايتها من مختلف أنواع التهديدات. ومن ثم، يضمن تعزيز حماية البيانات بهذا المستوى العالي استمرار نشاط المؤسسة أو الفرد دون أي عوائق.

تتبنى شركة "فورتانيكس" استراتيجية قائمة على نهج "البيانات أولًا" لتأمين البيانات في جميع أنحاء العالم. تتميز منهجية حماية البيانات بدلًا من البيئة في فقدان البيانات لسريتها وأهميتها للأشخاص غير المصرح لهم، سواء أثناء الاستخدام أو النقل أو التخزين. نشهد حالات متكررة لخرق البيانات وهجمات برامج الفدية الضارة، حيث غالبًا ما تفشل أنظمة الأمن المحيطي أو يقع خطأ بشري، مما يعرض البيانات لخطر كبير.

ُمكن للمؤسسات تشغيل بيئة تنفيذ موثوقة للاستفادة من نهج "الدفاع في العمق"، المبني على أساس الحوسبة السرية. تتكون هذه البيئة من مجموعة متنوعة من نظم التخزين المشفرة، وتمكين التعاون والحساب متعدد الأطراف، والتحكم في الوصول القائم على الصلاحيات والقواعد والأدوار، مما يسهل عمليات التدقيق والتتبع. كما تسمح بيئة البرمجيات المُقدمة كخدمة عبر الإنترنت والتي تتبنى نهج "انعدام الثقة" بالمصادقة وتوثيق المستخدمين والأجهزة والتحقق منهم عبر جميع مستويات الحوسبة، وبالتالي، تتيح للمؤسسات وأطرافها الخارجية العمل في بيئة آمنة للحصول على أعلى مستويات الأمان للبيانات.

تزداد المرونة التشغيلية باعتماد استراتيجية أمان تعتمد على نهج "البيانات أولاً"، مما يسمح للشركات بالتركيز على تقديم أفضل الخدمات للعملاء وتلبية توقعاتهم. فضلًا عن ذلك، توفر هذه الاستراتيجية فرصًا جديدة لتحقيق الإيرادات والتوسع في السوق والقدرة على تعزيز الميزة التنافسية من خلال المشروعات والشراكات الجديدة المحتملة، حيث يُمكن اتخاذ قرارات العمل والرؤى ذات الصلة باستخدام نماذج آمنة للذكاء الاصطناعي والتعاون في مجال البيانات مع الأطراف الخارجية.

يتمثل الاعتبار التالي الواجب مراعاته بمجرد استيفاء معايير الامتثال في "مراقبة التقنيات الجديدة". فعلى الرغم من أن الأطر الزمنية لا تزال غير محددة بدقة، إلا أن أهمية مفهوم "تشفير ما بعد الكم" تتزايد بشكل ملحوظ. أكدت 27 ٪ من المؤسسات -وفقًا للأبحاث المُجراة بواسطة شركة "كي بي إم جي"- أنها ستستثمر في مجال الحوسبة الكمية في السنوات الثلاث إلى الخمس القادمة – ومن المتوقع أن يكون هذا الوقت متأخرًا جدًا!

على الرغم من تخصيص الميزانيات، إلا أن المؤسسات مازالت في مرحلة التعلم، حيث تُطرح التساؤلات حول الخوارزميات التي ستسمح باتباع نهج مستدام. وبالتالي، ينبغي على الشركات اتخاذ إجراءات فورية وتسريع استراتيجياتها للحد من المخاطر، سواء لمواجهة التهديدات المستقبلية أو لحماية البيانات والمفاتيح المسروقة حاليًا. تجدر الإشارة إلى أن نهج "السرقة الآن وفك التشفير لاحقًا" يعتمد على ندرة تغيير الأفراد لحساباتهم المصرفية أو مقدمي خدمات الرهن العقاري أو مقدمي خدمات المعاشات التقاعدية، مما يُمثل تحديًا كبيرًا.

تجدر الإشارة أيضًا إلى ضرورة بناء خوارزميات تشفير مقاومة للاختراق للتصدي لهذه التهديدات، حيث أنه من المتوقع أن تتمكن أجهزة الكمبيوتر الكمية من فك أنظمة تشفير المفتاح العام بسهولة أكبر بسبب معدلات المعالجة الأعلى.

تدعم شركة "فورتانكس" العملاء عبر مراحل الانتقال الأربعة إلى تقنيات تشفير ما بعد الكم المتمثلة في الاكتشاف والتقييم والتخطيط والتنفيذ، لضمان أعلى مستوى من الأمان. فبمجرد التعرف على الوضع داخل الشركة، يجب اتخاذ قرارات وإجراءات واضحة، لا يُمكن تجاهل الأمر!

لمزيد من المعلومات فيما يتعلق بهذا الصدد، والبدء في تطبيق تقنيات تشفير ما بعد الكم وضمان الامتثال لأمن البيانات، يُرجى التواصل معنا.