إدارة تحديات أمن الفضاء الإلكتروني على مستوى الإدارة

د. كلوديا ناتانسون
وَسِّس – مُؤَسَّسَة "المتخصصون في المجال الأمنيُ"

إدارة تحديات أمن الفضاء الإلكتروني على مستوى الإدارة

يمكن تعريف أمن الفضاء الإلكتروني بأكثر من طريقة لكن ربما يكون من الأفضل أن نشرحه من المنظور التجاري ورؤية الأعمال له بوصفه مجموعة من التقنيات والعمليات والممارسات المصممة خصيصاً لحماية الأصول المعلوماتية والبيانات في المؤسسة من المخاطر المحتملة، وتشمل هذه الأصول أجهزة الكمبيوتر والهواتف المتحركة والنظم القائمة على الحوسبة السحابية. يعني التعرضُ للخطر والاختراق فقدانَ مقومات السرية والسلامة والإتاحة الخاصة بالأصول المعلوماتية التي تؤدي في الغالب إلى الإضرار بالشهرة المؤسسية وخسارة الإيرادات وفقدان ثقة المساهم والعميل في المؤسسة.

تم اختراق مليار سجل من سجلات البيانات في عام ٢٠١٤ (جرائم الفضاء الإلكتروني في الولايات الأمريكية لعام ٢٠١٥ – دراسة أصدرتها شركة برايس ووتر هاوس كوبرز PWC). في الأيام الأولى من حوادث أمن الفضاء الإلكتروني، كانت المؤسسات ترغب في أغلب الأحيان في الإعلان عن أي اختراق عند حدوثه، ورغم ذلك، لم يعد الإفصاح المحدود أو عدم الإفصاح على الإطلاق خياراً صالحاً في وجود المتطلبات التنظيمية للإخطار فور حدوث مخالفة بناءً على الانتشار السريع للمعلومات عبر الصحافة والوسائط الاجتماعية. بالإضافة إلى ذلك، ظهر الآن على الساحة «الهاكتيفيست»

(قراصنة الكمبيوتر المتسللون بطريقة محظورة إلى ملفات أو شبكات الكمبيوتر طمعاً في تحقيق غايات اجتماعية أو سياسية) والجريمة المنظمة ومرتكبو الجرائم الإلكترونية الخبيثة عقب ارتكابهم لعمليات اختراق ناجحة وذلك ضمن مخططاتهم لجذب الانتباه، ويؤدي ذلك إلى أن تصبح المؤسسات عُرضة للمخاطر بسرعة كبيرة.

تغيير شكل مشاركة مجلس إدارة المؤسسة

لا نتفاجأ بظهور أمن الفضاء الإلكتروني على جداول أعمال مجالس إدارة المؤسسات، ويكمن التحدي الأكبر الذي تواجهه هذه المؤسسات في إجراء التعديلات اللازمة على طريقة تناولها لحوكمة أمن الفضاء الإلكتروني. اتجهت الشركات في الماضي إلى رؤية المخاطر الأمنية بوصفها جزءاً من مخاطر تكنولوجيا المعلومات بدلاً من اعتبارها جزءاً من الإدارة الشاملة للمخاطر على مستوى المؤسسة، وقد أنبأ عدم قدرة مجلس الإدارة على فهم كامل نطاق المخاطر المقترنة بحوكمة أمن الفضاء الإلكتروني إلى التأخير في طرح الأسئلة الرئيسية، ومن ثم عدم الإجابة عنها. لقد تمثلت النتيجة في بعض الحالات في حدوث خروقات أمنية غير متوقعة.

من أجل معالجة ذلك، شكلت العديد من المؤسسات الآن لجنة مستقلة لإدارة المخاطر المحتملة تعمل مستقلة عن لجنة إدارة المخاطر والتدقيق، ويعني هذا أن المؤسسة تستطيع التركيز بشكل أفضل على جميع جوانب إدارة المخاطر عبر الإدارات التي لها علاقة بالأصول المعلوماتية. والواقع أنه يلزم تزويد المؤسسات بالمعلومات الصحيحة وتحديد حدود قبولها المخاطر وإرساء مقومات ثقافة المخاطر داخل هيكل المؤسسة ولدى العاملين ويكون ذلك بإرساء الأمثلة العملية وإبقائهم مدركين لأهمية الأمر من خلال الحفاظ على مستوى مناسب من الوعي والتدريب لديهم.

هناك عدد من التطورات المحددة التي تُعزز مسؤولية الإدارة العليا ومساءَلتها في هذا المجال، فعلى سبيل المثال تم فرض نظام التفويض والإدارة العليا (SM&CR) في القطاع المالي في المملكة المتحدة (واجب التنفيذ منذ مارس ٢٠١٦) متطلباً قانونياً على عاتق مسؤولي الإدارة العليا لاتخاذ الخطوات الملائمة للحيلولة دون حدوث المخالفات التنظيمية داخل نطاق مسؤولياتهم، وتركز النسخة الحديثة من أيزو /ISO IEC ٢٧٠٠١ على أن تكون المساءَلة عن أمن الأصول ضمن واجبات أعلى المستويات التنظيمية الوظيفية في المؤسسة.

يحتاج مجلس الإدارة إلى إدراك ما إذا كانوا يوجِّهون الأسئلة الصحيحة، أو يرون الصورة بأكملها فيما يتعلق بالمخاطر الإلكترونية، لكن اتباع مجلس الإدارة لثقافة التبشير بالأخبار السعيدة والنفور من السيئة يعني في كل الأحوال فقدان أدق التفاصيل المطلوبة عن المخاطر الإلكترونية. إن التعويل المفرط على ضوابط التحكم التي ظلت محل استخدام لمدة طويلة يشير إلى تعريض الإدارة الفعَّالة والمراقبة الواجبة لخطر حقيقي علماً بأن ضوابط التحكم السارية لم تتعرض لاختبار عملي حقيقي وأصبحت جزءاً من عملية شكلية روتينية لا طائل منها وتصل في النهاية إلى مجلس الإدارة في شكل أرقام إحصائية. إن الحل الحقيقي لإنجاز نظام فعال يصمد أمام الاختراقات يكمن في البدء بالإجراءات التصحيحية على مستوى مجلس الإدارة أولاً.

منهج الدفاع في العمق

يعد المنهج المتعدد الطبقات للدفاع في العمق (أو ما يُسمى: إطار عمل حلقات البصل)، حيث توضع طبقات متعددة من الضوابط الأمنية حول الأصول المعلوماتية أحد الأسس الجيدة التي يجب أن ينطلق منها مجلس الإدارة لتوجيه الأسئلة. الطبقات الدفاعية الخمس هي: (١) المستخدم، (٢) التطبيق، (٣) المحيط (الشبكة/ المعدات والأجهزة)، (٤) الخادم الإلكتروني، (٥) قاعدة البيانات التي يتم تخزين الأصول المعلوماتية فيها.

على مستوى المستخدم، تستطيع المؤسسة التنقيب ووضع ضوابط متدرجة لوصول المستخدم صاحب امتياز الدخول على النظام، والوصول المرخَّص والوصول المحظور، ودراسة إحصائيات الامتثال على هذه المستويات. كما يجب أن توفر طبقات التطبيق الإلكتروني الإحصائيات حول ضوابط الوصول والتشفير الآمن والتحديثات والإصدارات الحالية، على أن تتوافر مستويات متماثلة من المعلومات لجميع الطبقات الأخرى.

تظل نقاط الضعف على مستوى الخوادم والشبكة الإلكترونية متمتعة بالأهمية الأمنية القصوى في ظل وجود العديد من المؤسسات التي لا تزال تحتفظ بنظم غير مدعومة أمنياً وتستخدمها في تنفيذ عملياتها اليومية، وهذا ما يجعل الاختراق أكثر يسراً وسهولة. أفصح تقرير شركة NOPSEC لعام ٢٠١٥ حول حالة إدارة المخاطر وأوجه الضعف عن أن أوجه الضعف في النظام وسوء تهيئته لا تزال هي السبب الرئيسي في وقوع المخالفات الأمنية. وعندما تستغرق المؤسسات ١٧٠ يوماً تقريباً لرصد المخالفات، فإنه يتضح أن الإدارة يجب عليها تركيز انتباهها إلى إدارة أوجه الضعف في هذه المجالات. ورغم وجود عدد أكبر من أوجه الضعف في كل أصل يتم تسجيله إلا أن مزوّدي خدمات الحوسبة السحابية رصدوا فترات أقصر للمعالجة ونقاط ضعف ثابتة خلال فترة أقل من ٣٠ يوماً.

من المهم الانتباه إلى الموردين حيث إنه مع وجود مخاطر في سلسلة التوريدات، وهي إحدى مقومات الأمن الرئيسية، يلزم مساءلة جميع مزوّدي الخدمات عن تقديمهم الأدلة الثبوتية على استخدامهم لأفضل الممارسات الأمنية.

إدارة المخاطر بناءً على الاتجاهات العالمية في المجال

أفصح تقرير الأمن السنوي لعام ٢٠١٦ الصادر من شركة سيسكو (Cisco) عن أن ٩٢٪ من إجمالي ١١٥,٠٠٠ جهاز من سيسكو موصول بالإنترنت تعمل عليه برمجيات لها نقاط ضعف معروفة بينما ٣١٪ من هذه الأجهزة «غير متاحة للشراء» و٨٪ منها وصلت إلى «نهاية عمرها الافتراضي»، مما يعني أنها لن تكون قادرة على الحصول على دعم وتحديث البرمجيات عن بعد عبر الإنترنت. يمكن استعراض تلك الإحصائيات إلى جانب الأرقام الواردة في تقرير NOPSEC الذي يوضح أن الأمر يستغرق من المؤسسات ١٠٣ أيام تقريباً لمعالجة أي مشكلة أمنية، بينما في قطاع البنوك يستغرق الأمر ١٧٦ يوماً تقريباً. لا بد أن تأخذ الإدارة تلك المخاطر في الحسبان وتدمج بينها وبين المخاطر الأخرى ذات الصلة مثل مخاطر سلسلة التوريدات أو عروض النطاق الترددي للاتصال من مصدر غير مناسب والقدرات والخبرات، من أجل تأكيد حجم المخاطر الكلية واتخاذ قرارات سليمة بخصوص المخاطر المحتملة سواء من خلال تخفيفها أو إدارتها أو تحويلها. يجب استخدام تلك المعلومات عند اتخاذ القرارات بشأن الاستهلاك أو من أجل التخطيط الإستراتيجي للأعمال وخاصة في مجال استهلاك البنية التحتية لتكنولوجيا المعلومات.

يتعين على الإدارة أيضاً الحصول على موجز بشأن الاتجاهات العالمية في المجال مما يساعد في تطبيق منهج الإدارة الاستباقية للمخاطر، ويشمل ذلك منظومة Blockchain وهي سجل حسابات لا مركزي يسمح لأجهزة الكمبيوتر من كل مكان في العالم كي تصبح جداول بيانات متسلسلة للمعاملات المالية ترتبط مع بعضها الآخر في كتل إلكترونية يتألف كل منها من بيانات خاصة منفصلة لكنه يستخدم رمزاً وعنواناً عاماً من أجل ربط كل كتلة وتأمينها ضد الخروقات. تعد عملة البيتكوين الإلكترونية من التطبيقات الأولى التي استخدمت هذه البنية التحتية ومنذ ذلك الحين تم ابتكار العديد من مثيلاتها. تحتل شركة ريبل (Ripple) المرتبة الثانية في هذا النوع من التطبيقات ذات الفائدة الكبرى في القطاع المالي نظراً لقدرتها على الارتقاء بمعاملاتنا المالية إلى أعلى مستويات توفير التكاليف والدقة في عرض تفاصيل البيانات المالية على أكثر من مستوى.

تلعب نظم التحليل الآني والمستقبلي للبيانات الضخمة دوراً مهماً حالياً في العديد من المؤسسات، حيث يُستخدم التحليل المنطقي للبيانات الضخمة للاستبصار بتوجهات العميل وميوله ويمكن أن تعرض أيضاً احتمالات متعددة على فريق العمل الأمني الإلكتروني لربط التهديدات المستقبلية المحتملة والتعامل مع الخروقات القائمة بالفعل.

الاعتبارات الرئيسية أمام مجلس الإدارة

• إجراء معالجة دورية للأحداث والاستجابة السريعة للخروقات الأمنية واعتبارها ممارسات روتينية على مستوى مجلس الإدارة.

• طرح الأمثلة وإرساء ثقافة الاستعداد للمخاطر وإرساء نظم الأمن المعلوماتي في المؤسسة.

• توجيه نفس الأسئلة أثناء الإدارة اليومية حول حوكمة أمن الفضاء الإلكتروني لنظم المؤسسة، بحيث يتم معرفة أماكن

وجود الأصول ومن يمكنه الوصول إليها وهل يمكن اختراقها وكيف حدثت الخروقات وأسبابها وكيفية التعامل مع الحدث والعمليات والإجراءات الواجب استخدامها عند وقوع خروقات.

• إدراك أن سرعة إصدار تحديثات البرمجيات عبر الإنترنت وتحديد نقاط الضعف في البرمجيات أمر سوف يستمر من قبل مزوِّدي النظم مثل مايكروسوفت وأوراكل وأدوب. وسوف تستمر أيضاً الهجمات الخبيثة التي تخرج النظم من الخدمة من خلال الاجتياح بالحركة المرورية العقيمة التي تجعلها مشغولة بالكامل ويتعذر التعامل معها وقد تزايدت في الآونة الأخيرة حالات استهداف العديد
من المسؤولين التنفيذيين الكبار من خلال حملات البريد الإلكتروني المزيفة (تصيُّد الضحية عبر الانتحال والحصول على بيانات حساباته المالية).

• معرفة ضرورة دراسة المخاطر الأمنية في نطاق إطار المخاطر على مستوى المؤسسة بدلاً من اعتبارها قائمة على أساس تكنولوجيا المعلومات بشكل محض.

• يصبح أمان الجهاز النهائي أكثر أهمية ويجب تعقبه وإدارته نظراً لأن حرية اختيار الجهاز المُستخدَم سوف تزيد أيضاً. ويتسم التشفير الفعَّال بالأهمية الشديدة لكنه يجب ألا يتمخض عن إهمال المجالات الأخرى في أمن الفضاء الإلكتروني.

• الجانب المادي (الأجهزة والمعدات) في أمن الفضاء الإلكتروني بوصفه خط الدفاع الأول، يجب ألا يتم إغفاله على أن يعد جزءاً من جميع إجراءات رفع التقارير.

• معرفة مسؤوليات التفويض بما في ذلك حوكمة أمن الفضاء الإلكتروني. تعقُّب التطور في النهوض بمستوى النضح الأمني في المؤسسة، بحيث يتم إرساء حالة من التحسين المستمر وألا تُعد استجابته إلى متطلبات أمن الفضاء الإلكتروني مجرد رد فعل لا أكثر بل يجب أن تكون استباقية.

• تعقُّب الإحصائيات من أجل ضمان مراعاة الأمن في بداية المشروعات بدلاً من إرجاء الإجراءات الأمنية إلى وقت لاحق أو حتى استبعادها استبعاداً كلياً.

• الإبقاء على مسألة الأمن بشكل دوري على رأس جدول اجتماعات مجلس الإدارة، وتخصيص الفترة الزمنية المناسبة لفهم القياسات والمقارنات المتوفرة.

• مواصلة إنشاء لجان إدارة المخاطر والتي تكون مستقلة عن لجنة إدارة المخاطر والتدقيق، وذلك لتسهيل إمعان النظر في أمن الفضاء الإلكتروني بطريقة أكثر تدقيقاً.

يشير الآن ٧٥٪ من المديرين التنفيذيين في المملكة المتحدة إلى أمن الفضاء الإلكتروني بوصفه أكبر ثالث تهديد بعد الرقابة المفرطة وعدم التيقُّن الجيوسياسي (تقرير شركة PwC لعام ٢٠١٥ حول الأمن) وقد تردد صدى ذلك لدى نظرائهم على مستوى العالم. رغم أنه يمكن استخدام الغير لنقل المسؤولية إليه، إلا أنها يجب أن تظل دائماً على رأس أولويات المؤسسة، وتستمر المسؤولية الأخلاقية لمجلس الإدارة في التعاظم حتى تشمل البُعد الرقمي وطريقة تعامل المؤسسة مع بياناتها وحمايتها وتأمينها لها.

وتبقى كفاءة مجلس الإدارة والتزامه في مواجهة تلك التحديات من الأمور الشديدة الأهمية والتي تكفل استعداد المؤسسة في حالة حدوث الخروقات.