الخليج

اقتصاد, تقنية وسيارات

24 مايو 2024 17:27 مساء

من مسؤولي أمن المعلومات قلقون بشأن التطبيقات % 87

دبي: «الخليج»

أصدرت «داياناتريس»، الشركة العاملة في المراقبة الموحدة والأمن، استطلاعها السنوي لرؤساء أمن المعلومات تحت عنوان «حالة أمن التطبيقات في عام 2024». ويكشف هذا التقرير أن المؤسسات تعاني وجود حواجز اتصال داخلية تعيق قدرتها على معالجة تهديدات الأمن السيبراني. وتشير النتائج إلى أن كبار مسؤولي أمن المعلومات في الشرق الأوسط، كما هي حال نظرائهم في جميع أنحاء العالم، يواجهون صعوبات في التوفيق بين فرق الأمن والمسؤولين التنفيذيين، ما يخلق فجوات في فهم الشركة للمخاطر السيبرانية.

وركزت الشركة على استكشاف فجوات الاتصال هذه للحصول على رؤى أعمق، حول كيفية اعتماد نهج موحد لقابلية المراقبة والأمن، من شأنه أن يعزز تعاون الفريق ويقلل احتمالات التعرض للمخاطر.

ويستند هذا التقرير إلى دراسة استقصائية عالمية شملت 1,300 من كبار مسؤولي تكنولوجيا المعلومات، (بما في ذلك 150 مشاركاً في الشرق الأوسط)، وعشر مقابلات مع الرؤساء التنفيذيين والمديرين الماليين في الشركات التي يعمل فيها أكثر من 1,000 موظف.

النتائج في الشرق الأوسط •

1- عدم التوافق بين المستوى التنفيذي ومجلس الإدارة يؤدي إلى مخاطر إلكترونية: يبذل كبار مسؤولي أمن المعلومات جهوداً كبيرة لتحقيق التوافق بين فرق الأمن والمديرين التنفيذيين، حيث يقول 87% من هؤلاء المسؤولين، إن أمن التطبيقات يمثل مجالاً مجهولاً، ولا يحظى بالاهتمام الكافي على مستوى الرئيس التنفيذي ومجلس الإدارة.
2- فرق الأمن تتبع نهجاً تقنياً أكثر من اللازم: يقول سبعة من كل عشرة مسؤولين تنفيذيين تمت مقابلتهم، إن أعضاء فرق الأمن يستخدمون مصطلحات فنية من دون الاستعانة بالسياق المناسب للعمل. ومع ذلك، سلط 77% من كبار مسؤولي أمن المعلومات الضوء على أن المشكلة متجذرة في الأدوات الأمنية، التي لا يمكنها تقديم رؤى وأفكار يمكن للمديرين التنفيذيين ومجالس الإدارة على المستوى التنفيذي استخدامها، لفهم مخاطر الأعمال ومنع التهديدات.
3-الذكاء الاصطناعي يؤدي إلى المزيد من التهديدات السيبرانية المتقدمة: أصبحت معالجة هذه الفجوة في التكنولوجيا والاتصالات مهمة للغاية، بخاصة مع ظهور الهجمات، التي تعتمد على الذكاء الاصطناعي والتهديدات السيبرانية، التي تزيد بشكل كبير من مخاطر الأعمال.
وفي ضوء هذه الخلفية، يقول أكثر من ثلاثة أرباع (76%) مديري أمن المعلومات في الشرق الأوسط، إن مؤسساتهم تعرضت لحادث أمني متصل بالتطبيقات في العامين الماضيين. وتترتب على هذه الحوادث مخاطر كبيرة، حيث يقوم كبار مسؤولي أمن المعلومات حول العالم بتسليط الضوء على العواقب الشائعة، التي تعرضوا لها، بما في ذلك الإيرادات المتأثرة (47%)، والغرامات التنظيمية (36%)، وفقدان حصة السوق (28%).
وقال بيرند جريفيندر، الرئيس التنفيذي للتكنولوجيا في «داينا تريس»: «قد تترتب على حوادث الأمن السيبراني عواقب وخيمة تطال المؤسسات وعملاءها، لذلك أصبحت المشكلة تمثل مصدر قلق بالغ الأهمية على مستوى مجلس الإدارة. ومع ذلك، يسعى العديد من مديري تكنولوجيا المعلومات بكل جهد ممكن، لتحقيق التوافق بين فرق الأمن وكبار المديرين التنفيذيين، لأنهم غير قادرين على الارتقاء بلغة الحوار المتخصصة، والتركيز على مخاطر أعمال محددة.

نتائج الأبحاث الإضافية •

أصبحت الحاجة ماسّة إلى تعزيز المشاركة الوثيقة بين فرق الأمن والمسؤولين التنفيذيين، لاسيما وأن ظهور الذكاء الاصطناعي يعرّض المؤسسات لمخاطر إضافية. ويشعر مديرو تكنولوجيا المعلومات حول العالم بالقلق، بشأن قدرة الذكاء الاصطناعي على تمكين مجرمي الإنترنت من إنشاء برمجيات استغلال جديدة بشكل أسرع، ومن ثم إطلاقها على نطاق أوسع (52%). ويعرب هؤلاء أيضاً عن قلقهم بشأن قدرة الذكاء الاصطناعي لإتاحة المجال أمام المطورين، لتسريع تطوير البرامج مع قدر أقل من الإشراف، ما يؤدي إلى ظهور المزيد من نقاط الضعف (45%).
وفي أثناء بحثهم عن الحلول، يقول 81% من مسؤولي تكنولوجيا المعلومات في الشرق الأوسط، إن أتمتة «التطوير والأمن والعمليات» مهمة جداً لإدارة مخاطر نقاط الضعف، التي يسببها الذكاء الاصطناعي.
وعلى المستوى العالمي، يقول 71% من كبار مسؤولي تكنولوجيا المعلومات، إن أتمتة التطوير والأمن والعمليات» مهمة جداً لضمان اتخاذ تدابير معقولة، لتقليل المخاطر الأمنية للتطبيقات.
ويقول 80% من مديري تكنولوجيا المعلومات في الشرق الأوسط أن أتمتة التطوير والأمن والعمليات، ستكون ضرورية لتعزيز قدراتهم على مواكبة اللوائح الناشئة، مثل تفويض الأمن السيبراني الصادر عن هيئة الأوراق المالية والبورصات، وأبحاث وتقييم التطوير والأمن والعمليات (NIS2) والتوجيه الثاني لأنظمة الشبكات والمعلومات في الاتحاد الأوروبي في حين يقول 79% آخرون إن الحاجة إلى أدوات أمن التطبيقات المتعددة، تؤدي إلى عدم الكفاءة (DORA) التشغيلية بسبب الجهد المطلوب لفهم مصادر البيانات المتباينة.