الخليج

اقتصاد, تقنية وسيارات

23 مارس 2023 22:18 مساء

مايم كاست»: 60% من الشركات بحاجة إلى رفع إنفاقها على الأمن السيبراني

«دبي: «الخليج

أكد تقرير «حالة أمن البريد الإلكتروني 2023» الذي أصدرته مايم كاست، الشركة المختصة في أمن البريد الإلكتروني والعمل التشاركي، أن 60% من الشركات في الإمارات والسعودية بحاجة إلى رفع إنفاقها على الأمن السيبراني.

والتقرير هو دراسة عالمية تقوم على مشاركات 1,700 شخص من صانعي القرار في مجالات الأمن وتقنية المعلومات، لتزويد القراء بعدد من النتائج المهمة المتعلقة بمشهد التهديدات الراهن، وتقديم التوصيات التي تساعد المؤسسات على تحسين موقفها الأمني.

ويسلط التقرير العالمي الضوء على التهديدات التي تواجه الشركات في مختلف أنحاء العالم، بما فيها دولة الإمارات والسعودية. وقد قال 94% من المشاركين في الإمارات و100% من المشاركين في السعودية، إنهم تعرضوا للاستهداف في هجمات لسرقة الهوية عبر البريد الإلكتروني خلال العام الماضي، ولكنهم جميعاً قالوا إنهم إما لديهم نظام للرصد والحماية من الهجمات القادمة عبر البريد الإلكتروني، أو يخططون لتطبيق نظام من هذا النوع قريباً.

الوعي السيبراني في أوساط المديرين التنفيذيين

وفي ظل التعقيد المتزايد للهجمات السيبرانية، أظهر قادة الأعمال في المنطقة، إرادة أكبر لمواجهة تلك المخاطر والاستثمار في التدابير المناسبة للوقاية من الهجمات السيبرانية. وفي المتوسط، قالت 95% من الشركات في الإمارات بينما قال Google Workspaceو Microsoft 365 والسعودية إنها بحاجة إلى حماية أقوى لتطبيقات عملها من 61% إن شركاتهم بحاجة إلى إنفاق مزيد على الأمن السيبراني. ولكن جميع الشركات تحدثت عن تقديم التدريب للتوعية السيبرانية بشكل ما في مؤسساتها، ما يشير إلى قدر أكبر من التنبّه للهجمات المستقبلية. وفي ضوء ازدياد التركيز على الجاهزية السيبرانية لدى المسؤولين التنفيذيين، يشعر المديرون التنفيذيون لتقنية المعلومات، بتمكين أكبر

.للتعبير عن متطلباتهم وتنفيذ الاستراتيجيات والأساليب التكتيكية التي تجعل مؤسساتهم أكثر أمناً

أدوات العمل التشاركي.. ضرورتها والمخاطر المرتبطة بها

وما زالت فرق العمل موزعة بين المكاتب ومواقع العمل عن بعد، ما يعني استمرار أهمية أدوات العمل التشاركي واستمرار المخاطر التي تترتب على استخدامها، ضمن أدوات التواصل مع أفراد الفريق. ويتفق أربعة وثمانون في المئة من المشاركين في استطلاع تقرير حالة أمن البريد الإلكتروني في الإمارات، و94% منهم في السعودية، على أن أدوات ضرورية لإنجاز المهام المرجوة من عملهم، ويتوقع 82% من Slack أو Microsoft Teams العمل التشاركي مثل المشاركين في البلدين أن تسبب تلك الأدوات تعرّضهم لهجمة سيبرانية عام 2023. فالزيادة الحادة في انتشار واستخدام هذه الأدوات تجعلها محور تركيز مديري تقنية المعلومات ممن سيحرصون على تطبيق التدابير الأمنية الكافية .للتمكّن من مواصلة حماية عملهم أثناء استعمالها

تعزيز الجاهزية السيبرانية

هناك إدراك متزايد لحقيقة كون المخاطر السيبرانية لا ترتبط بتقنية المعلومات وحسب، وبأنها نقاط ضعف حرجة تشكل مخاطر مباشرة على الأعمال بشكل كامل. ولهذا السبب، تتخذ المؤسسات التدابير الضرورية للاستعداد لمواجهة الهجمات الوشيكة، حيث يستخدم نصف تلك المؤسسات تقنيات الذكاء الاصطناعي وتعلم الآلة لمساعدة فرق العمل في .مواكبة المستجدات على الرغم من نقص مواردها، بينما وضع النصف الآخر منها خططاً لتطبيق تلك التدابير

ولا شك في أن استخدام الذكاء الاصطناعي سيساعد فرق الأمن السيبراني في منع وقوع الهجمات وإدارة التهديدات، حيث قال المشاركون في الاستطلاع إن أهم المزايا التي حصلوا عليها من الذكاء الاصطناعي تمثلت في تحسين قدرتهم على حظر التهديدات (64%)، ودقة أكبر في الكشف عن التهديدات (56%)، وتسريع زمن معالجة التهديدات (56%). وبالإجمال تعتقد معظم الشركات أن أنظمة الذكاء الاصطناعي ستساعدها في تحقيق ثورة حقيقية في أسلوب ممارستها .للذكاء الاصطناعي

وقال ويرنو جيفرز، المدير الإقليمي لدى مايم كاست الشرق الأوسط: «تعد نقاط الضعف في سلسلة الإمداد وتزايد التعاون عبر الإنترنت ونمو حجم التشبيك الرقمي، من أبرز الأسباب التي تجعل المشهد السيبراني محفوفاً بمخاطر أكبر. فالتقاطع بين الاتصالات والأفراد والبيانات يحمل مخاطر ضخمة نظراً لاستغلال المهاجمين لهذا القدر من التداخل في مساحات العمل العاصرة. وتظهر أبحاثنا أن إدارات الشركات أدركت أخيراً أن المخاطر السيبرانية هي مخاطر تهدّد أعمالها بالكامل، ولهذا فقد حان الوقت ليتمكن مديرو تقنية المعلومات من إثبات أهمية رفع الميزانيات المخصصة .لهم، من أجل الوصول إلى مستوى أفضل من الصمود في وجه الهجمات السيبرانية