الخليج

اقتصاد, أسواق الإمارات

23 أبريل 2024 17:59 مساء

الذكاء الاصطناعي سلاح 91% من مؤسسات الإمارات لتعزيز الأمن السيبراني

«دبي: «الخليج

سلطت أحدث دراسة أجرتها شركة سيسكو، الضوء على الطفرة الكبيرة في استخدام تقنيات الذكاء الاصطناعي في استراتيجيات الأمن السيبراني للمؤسسات في دولة الإمارات العربية المتحدة. وتشير الدراسة إلى أن 91% من الشركات التي شملها استطلاع الرأي تقوم بدمج تقنيات ذكاء اصطناعي في دفاعاتها الأمنية، وخاصة في مجال الكشف عن التهديدات والاستجابة لها والتعافي منها.

وتم إعداد مؤشر سيسكو للجاهزية للأمن السيبراني لعام 2024 في ظل حقبة تتميز بالاتصال الفائق ومشهد تهديدات سريع التطور. وعلى الرغم من استمرار استهدافها بمجموعة متنوعة من الهجمات التي تتراوح من التصيد الاحتيالي وبرامج الفدية إلى هجمات سلسلة التوريد وهجمات الهندسة الاجتماعية، إلا أن الشركات اليوم تحاول بنشاط تعزيز

دفاعاتها وتقويتها. وبينما تقوم ببناء دفاعات ضد هذه الهجمات، فإن تعقيد أوضاعها الأمنية، التي تهيمن عليها حلول متعددة النقاط، يمثل تحدياً في سياق إحباط هذه التهديدات بشكل فعّال.

وتتفاقم هذه التحديات في بيئات العمل الموزعة التي تنتشر بشكل أكبر في أيامنا هذه، حيث يمكن نشر البيانات عبر كم هائل ولا حدود له من الخدمات والأجهزة والتطبيقات والمستخدمين. ومع ذلك، لا تزال 87% من الشركات تشعر بثقة تتراوح بين متوسطة إلى كبيرة في قدرتها على صد الهجمات السيبرانية باستخدام بنيتها التحتية الحالية، ويؤكد هذا التفاؤل على ضرورة اتخاذ موقف استباقي في التعامل مع التهديدات ومواجهة التحديات الناشئة بشكل مباشر.

مؤشر سيسكو للجاهزية للأمن السيبراني لعام 2024: بناء المرونة في الاستجابة لمشهد التهديدات المتطور

يقوم المؤشر بتقييم جاهزية الشركات عبر خمس ركائز رئيسية هي: ذكاء الهوية، ومرونة الشبكة، وجدارة الآلة، وتعزيز السحابة، وتحصين الذكاء الاصطناعي، تتكون بدورها من 31 حلاً وقدرة. ويستند هذا التقرير إلى استطلاع رأي مزدوج التعمية شمل أكثر من 8000 من قادة الأعمال والأمن في القطاع الخاص عبر 30 سوقاً عالمياً، وتم تنفيذه من قبل طرف ثالث مستقل. وقد طُلب من المشاركين الإشارة إلى أي من هذه الحلول والقدرات قاموا بنشرها ومرحلة النشر.

وتعليقاً على نتائج التقرير، قال فادي يونس، مدير عام الأمن السيبراني لدى سيسكو في منطقة الشرق الأوسط وإفريقيا: «في ظل استمرار تطور المشهد الرقمي بسرعة، لا يمكن أبداً التراخي في تعزيز تدابير الأمن السيبراني الاستباقية. ومن الضروري أن تعطي المؤسسات أولوية كبيرة للاستثمارات في مجال الأمن السيبراني، وأن تتبنى حلولاً مبتكرة للتخفيف من المخاطر بشكل فعّال. ويمكن للمؤسسات في دولة الإمارات العربية المتحدة من خلال تعزيز ثقافة المرونة السيبرانية، التنقل في المشهد الرقمي بثقة واطمئنان، وحماية عملياتها ضد التهديدات الناشئة.»

• ومن النتائج الرئيسية الأخرى للمؤشر:

· الحوادث السيبرانية المتوقعة في المستقبل: ذكر 85% من المشاركين من الإمارات العربية المتحدة إنهم يتوقعون أن تؤدي حادثة أمن سيبراني إلى تعطيل أعمالهم خلال ال 12 إلى 24 شهراً القادمة. ويمكن أن تكون تكلفة عدم الاستعداد لهذه الحادثة كبيرة جداً، حيث قال 65% من المشاركين إنهم تعرضوا لحادث أمن سيبراني خلال الأشهر ال 12 الماضية، وقال 52% من المتضررين إن ذلك كلفهم ما لا يقل عن 300 ألف دولار.

· الحمل الزائد لحلول النقاط: لم يحقق النهج التقليدي المتمثل في اعتماد حلول نقاط الأمن السيبراني المتعددة نتائج فعالة، حيث قال 82% من المشاركين من الإمارات العربية المتحدة إن وجود حلول نقاط متعددة عمل على إبطاء قدرة فريقهم على اكتشاف الحوادث والاستجابة لها والتعافي منها. وهذا يثير مخاوف كبيرة حيث قالت 78% من المؤسسات إنها قامت بنشر عشرة حلول نقاط أو أكثر في مجموعاتها الأمنية، في حين قالت 26% منها أن لديها 30 حل نقاط أو أكثر.

· استمرار فجوة المواهب السيبرانية: سلطت 90% من الشركات الإماراتية الضوء أيضاً على نقص المواهب كمشكلة رئيسية. وفي الواقع، ذكر 51% من الشركات أن لديها أكثر من عشرة وظائف مناصب أمن سيبراني شاغرة في وقت إجراء استطلاع الرأي. ومن اللافت للنظر أن 95% من الشركات الإماراتية تفكر بدمج تقنيات ذكاء اصطناعي في برامجها للأمن السيبراني لتغطية أكثر من 10% من وظائف الأمن السيبراني الشاغرة، مما يسلط الضوء على نهج استباقي تجاه معالجة نقص المواهب وتبني حلول مبتكرة.

تكثيف الاستثمارات السيبرانية المستقبلية: تدرك الشركات التحديات الماثلة وتعمل على تعزيز دفاعاتها، حيث يخطط ٠ 68% منها لترقية بنيتها التحتية لتكنولوجيا المعلومات بشكل كبير خلال ال 12 إلى 24 شهراً القادمة. وعلاوة على ذلك، تخطط المؤسسات لترقية حلولها الحالية (66%)، ونشر حلول جديدة (54%)، والاستثمار في تقنيات تعتمد على الذكاء الاصطناعي (54%). وإلى ذلك، تعتزم جميع الشركات تقريباً (99%) زيادة ميزانيتها للأمن السيبراني خلال الأشهر ال 12. المقبلة، حيث تتوقع 91% من هذه الشركات نمواً كبيراً بنسبة 10% أو أكثر في ميزانياتها للأمن السيبراني

وللتغلب على تحديات مشهد التهديدات الذي نعيشه اليوم، ينبغي على الشركات تسريع استثماراتها الهادفة في مجال الأمن، بما في ذلك اعتماد تدابير أمنية مبتكرة ونهج منصة أمنية، وتعزيز مرونة شبكاتها، وإنشاء استخدام هادف للذكاء الاصطناعي التوليدي، وزيادة عمليات التوظيف لسد فجوة مهارات الأمن السيبراني.