الخليج

اقتصاد, أسواق الإمارات

27 أبريل 2024 22:40 مساء

خبراء: تضاعف الاستثمار لصد التهديدات السيبرانية في الإمارات

دبي: حمدي سعد

ضاعفت مؤسسات وشركات في الإمارات من الاستثمار بحلول وعمليات التأهيل البشري لمواجهة التهديدات السيبرانية والإلكترونية المتعاظمة، لاسيما الحلول التي تستخدم الذكاء الاصطناعي في التنبؤ ورصد الهجمات في بدايتها.

قال خبراء ومسؤلو شركات ل «الخليج» على هامش الدورة ال 13 لمؤتمر ومعرض الخليج لأمن المعلومات (جيسيك)، الذي اختتم اعماله الخميس في دبي: إن الاستثمار في العنصر البشري والشمول التقني عاملان ضروريان، لمواجهة أساليب قراصنة المعلومات لاختراق الشبكات وسرقة البيانات.

وأشار الخبراء إلى أن التحول الرقمي في الإمارات، لابد أن توازيه استعدادات كبيرة لحماية المعلومات من القراصنة والمخربين، الذين تتغير توجهاتهم بين لحظة وأخرى، بهدف الحصول على أموال أو التخريب لصالح دول أو جهات في

.بعض الأحيان

ستيفان بيرنر

ألف خطر 30 •

التابعة «إي آند انتربرايز» إن الشركة كشفت، (Help AG) «قال ستيفان بيرنر، الرئيس التنفيذي لشركة «هيلب إيه جي خلال 2023، نحو 30 ألف تنبيه للمخاطر الحرجة في دول مجلس التعاون الخليجي، فيما شكّلت تهديدات سرقة البيانات الشخصية نسبة 49%، وإساءة استخدام العلامات التجارية 39 %، مقابل 10% تسرّب بيانات، و1.5% .لمحاولات التصيّد الاحتيالي

وأضاف أثرت التهديدات السيبرانية إلى حدّ كبير في قطاعات التعليم بنسبة 36%، والطيران 29 %، والرعاية الصحية 15%، تلتها المؤسسات في قطاع الحكومة 8%، والاستثمار 7%، وقطاع البنوك والتمويل 4%، في ظلّ تزايد رقمنة .المعاملات في هذه القطاعات

وزادت هجمات حجب الخدمة بنسبة 42%، حيث سجلت الشركة 213 ألف هجمة من هذا النوع، في ما استهدفت 40% من الهجمات القطاع الحكومي، و29 % منها طالت قطاع الاتصالات، و 9% لقطاع الطيران، و5 % لقطاع النفط .والغاز

وأوضح بيرنر، أن توجّهات الاستثمار في الأمن السيبراني، شهدت تضاعفاً، خلال 2023، بالتزامن مع استمرار التحول الرقمي، حيث سجلت الشركات والحكومات في دول المجلس نمواً في: توحيد مجالات الأمن السيبراني بنسبة 100 % في مجال التكنولوجيا، وارتفع الاستثمار في الدفاع السيبراني المُدار بشكل كبير، بسبب التعقيد المتزايد للمخاطر .الرقمية

إميل أبو صالح

«التوليدي» •

فيما قال إميل أبو صالح، المدير الإقليمي لمنطقة الشرق الأوسط وإفريقيا في «بروف بوينت»: حققت دولة الامارات تقدماً كبيراً في التحول الرقمي, ولكن هذا التحول تواجهه التهديدات الإلكترونية والسيبرانية، التي تستهدف الشبكات والتقنيات، مشيراً إلى أن أكبر التهديدات وأكثرها استمراراً، لا تزال تتمثل في الاحتيال عبر البريد الإلكتروني والتصيد .الاحتيالي

مخاطر كثيرة، وتقوم (ChatGPT) وأضاف، تشكل الشعبية المتزايدة لأدوات الذكاء الاصطناعي التوليدي مثل .المؤسسات في دولة الإمارات بدمج البيانات الحساسة في هذه التطبيقات بشكل متزايد، ما يخلق ثغرة أمنية محتملة

ويظهر تقرير «بروف بوينت» الأخير، حول مشهد فقدان البيانات، أن الذكاء الاصطناعي التوليدي، هو المجال الأسرع

.نمواً، الذي يثير اهتمام المؤسسات في الدولة

وأكد أبو صالح، أن الطرق القديمة لحماية البيانات لم تعد فعالة، ما يتطلب بناء دفاع جماعي ولوائح تنظيمية قوية .وتطبيقاً استباقياً ومشاركة للمعلومات بين المنظمات، للتغلب على تحديات مشهد التهديدات

عزالدين حسين

إدارة نقاط الضعف •

قال عزالدين حسين، المدير الإقليمي الأول لهندسة الحلول في الشرق الأوسط وتركيا وإفريقيا في شركة «سينتينل وان»: تزود الحلول القائمة على الذكاء الاصطناعي المؤسسات بالأدوات والمعلومات اللازمة لتوقع التهديدات، وإدارة .نقاط الضعف وحماية أصولها الرقمية في أي مكان في العالم

وأضاف أن حلول الذكاء الاصطناعي تمنح المؤسسات إمكانية تحديد التهديدات في وقت مبكر، لتستجيب بسرعة أكبر، وقد أحدثت هذه التطورات تأثيراً كبيراً في قطاع الأمن السيبراني، وفرضت تغيرات في الطريقة، التي تقوم بها المؤسسات باكتشاف الهجمات السيبرانية ومنعها والرد عليها. وأوضح حسين أن تقنيات الذكاء الاصطناعي التوليدي، باتت الأكثر تقدماً في القطاع لاكتشاف التهديدات وتحليلها والاستجابة لها، حيث تعمل على تبسيط العمليات، من خلال .الجمع بين الأدوات وتجميع معلومات التهديدات

وأوضح حسين أنه ومن خلال الاستفادة من التحليلات المستندة إلى الذكاء الاصطناعي، وربط مجموعات البيانات، يتيح بعض الحلول للمؤسسات إمكانية الحصول على رؤية شمولية عبر كامل المؤسسة، وتحسين موقفها الأمني بشكل .عام

توم لاوندز

معايير صارمة •

ورأى توم لاوندز، المدير الإقليمي لشركة «سايبر أرك»:تعتبر دولة الإمارات متطورة عالمياً في حماية البنى التحتية الرقمية، كما تطبق معايير صارمة للأمن الإلكتروني، ولقد أدى نجاحها المتواصل إلى جعلها هدفاً رئيسياً لكمّ كبير من الهجمات، التي غالباً ما تكون معززة بالذكاء الاصطناعي. وأضاف، أن أمام قادة المؤسسات خيار مواصلة الإنفاق على البنية الرقمية والسحابية، دون إهمال الجوانب المرتبطة بالأمن الإلكتروني، فالاستثمار في مبادرات دفع عجلة الأعمال إلى الأمام، التي لا تأخذ بعين الاعتبار الإنفاق على أدوات الأمن الإلكتروني، سيؤدي في نهاية المطاف إلى مستويات غير .مقبولة من المخاطر

تقليص فجوة المهارات •

وقالت ديبتي غوبال، مديرة أبحاث في «جارتنر» للأبحاث: «مع الانتقال إلى ما هو أبعد من الذكاء الاصطناعي

التوليدي، تلوح فرص المساعدة في حل بعض المشاكل المستمرة، التي يشهدها الأمن السيبراني، وخاصة نقص المهارات والسلوك البشري غير الآمن. وأضافت غوبال بحلول عام 2028، سيسهم اعتماد الذكاء الاصطناعي التوليدي في تقليص فجوة مهارات الأمن الإلكتروني، ما يلغي الحاجة إلى توفير تعليم متخصص من 50% من الشواغر.

وتوقّعت جارتنر وصول حجم إنفاق المستخدم النهائي على الأمن الإلكتروني وإدارة المخاطر في منطقة الشرق الأوسط وشمال إفريقيا إلى 3.3 مليار دولار خلال 2024، بزيادة بنسبة 12.1 % عن 2023.

"حقوق النشر محفوظة "لصحيفة الخليج .2024 ©