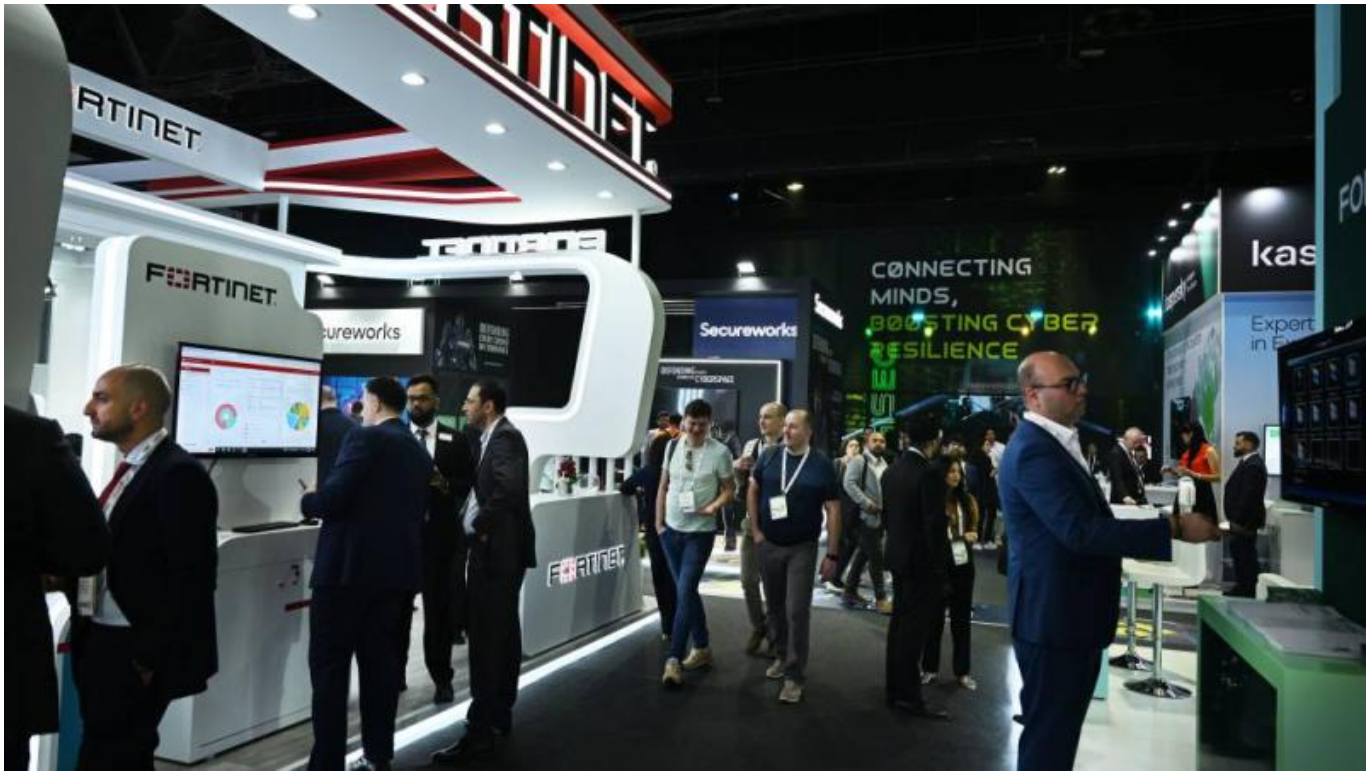
الخليج

اقتصاد, تقنية وسيارات

27 مارس 2024 12:31 مساء

اختراق 30 مليار سجل منذ بداية 2024.. الشرق الأوسط أول المستهدفين



دبي: «الخليج»

في الوقت الذي يستعد فيه المجتمع الدولي للأمن السيبراني، لانطلاق فعاليات معرض ومؤتمر «جيسيك جلوبال 2024»، المؤتمر الأكبر للأمن السيبراني والأكثر تأثيراً في الشرق الأوسط وإفريقيا، والذي سيعقد في الفترة من 23 إلى 25 إبريل في مركز دبي التجاري العالمي، يسلط الخبراء في هذا المجال المتسارع الضوء على اختراق البيانات، والطرق التي يمكن للشركات والحكومات توحيد جهودها لتعزيز قدرة الأمن السيبراني العالمي على التكيّف مع الظروف الجديدة.

في منطقة الشرق الأوسط على وجه التحديد، كانت عمليات النفط والغاز والهيئات الحكومية والمؤسسات المالية الأكثر تأثراً، وتظهر دوماً باعتبارها أهدافاً رئيسية لهجمات اختراق البيانات، وعلى الصعيد العالمي، تم اختراق أكثر من 30 مليار سجل معروف حتى الآن في عام 2024، وهو ما يمثل أكثر من 5000 حادثة تم الكشف عنها علناً، وفقاً لشركة استشارات السوق في المملكة المتحدة «آي تي غافورنيس».

كل عملية اختراق تصاحبها تكلفة معينة، وتستمر هذه التكلفة في الارتفاع عاماً بعد عام مع ظهور أساليب هجوم جديدة ونقاط ضعف جديدة ومخاطر جديدة، حيث يعكس تقرير «تكلفة اختراق البيانات لعام 2023» الصادر عن شركة «آي بي إم» اتجاهاً تصاعدياً في تكاليف اختراق البيانات، حيث وصل متوسط تكلفة عملية الاختراق في عام 2023 إلى 4.45 مليون دولار بزيادة قدرها 2.3% عن عام 2022.

استعداد الشركات

تعكس الزيادة في حالات الخروقات القياسية حول العالم، والتكاليف المرتبطة بها، الفجوة بين البرمجيات الخبيثة سريعة التطور، واستعداد الشركات لتجنب الحوادث الناشئة، وسيقوم الخبراء في معرض ومؤتمر «جيسيك جلوبال» ببحث تأثير هذه الفجوة عبر مناقشات وحوارات عدة تعتلي المنصة الرئيسية للمعرض، حيث سيطرحون أفكارهم ورؤاهم وخبراتهم الفريدة خلال الحدث العالمي.

التنسيق المكثف

الذي يُزعم أنه يحتوي (MOAB) «كانت الأخبار المتواترة مؤخراً حول وجود ملف يحمل اسم «أم جميع الاختراقات

على 1.2 تيرابايت وأكثر من 3,800 ملف من البيانات، تتضمن المعلومات الشخصية وبيانات الاعتماد لأكثر من 26 مليار سجل، مثيرة للقلق بشكل خاص لمجتمع الأمن السيبراني الدولي.

في حين قال خبراء الصناعة منذ فترة طويلة: إن تسرب البيانات المركزية أمر لا مفر منه، فهو ليس من الضروري أن يكون أمراً حتمياً، كما تسهم الحكومات بدور حاسم في وضع وإنفاذ اللوائح والمعايير لحماية خصوصية بيانات المواطنين، كما تتحمل مسؤولية مواجهة المشهد المتصاعد لاختراق البيانات.

ولمكافحة التهديدات المتطورة والبرامج الضارة، تتطلب الشراكات العامة والخاصة تنسيقاً مكثفاً، فالتخصيص الدقيق للموارد والتصميم الشامل لاستراتيجيات المرونة، إلى جانب الاستثمار في تطوير التقنيات وتبادل المعلومات، يتيح للشركات إمكانية الوصول إلى الإجراءات التي تم اختبارها على مستوى الأمن القومي والأساليب المجربة والحقيقية لإدارة المخاطر.

سيف ذو حدين

من الأمور المهمة لكل من الحكومات والمؤسسات التي تسعى إلى تعزيز موقعها في مجال الأمن السيبراني، هو ظهور تقنيات الذكاء الاصطناعي والتعلم الآلي، وكلاهما يستعد لإحداث ثورة في استراتيجيات الدفاع للمؤسسات والأفراد على حدٍ سواء.

ونظراً لطبيعته التكيفية، التي تمكنه من التعلم والتطور، أصبح الذكاء الاصطناعي قادراً على أن يكون متقدماً على التهديدات السيبرانية المعقدة إلى حدٍ كبير، وهذا ما يجعله حلاً واعداً بشكل خاص لتعزيز دفاعات الأمن السيبراني.

وتعد الحوسبة الكمومية مذهلة بالقدر ذاته، حيث تعمل على تعزيز حل المشكلات بسرعات معالجة غير مسبوقة وتقديم تحليلات تنبؤية.