اقتصاد, آراء وتحليلات, مقالات

12 فبراير 2023 21:34 مساء

توجهات الأمن السيبراني

الكاتب

نيكولاي سولينغ

***نيكولاي سولينغ**

شهدت دولة الإمارات زيادة بنسبة 151% في الهجمات السيبرانية خلال الربع الثالث لعام 2022، قياساً بزيادة قدرها 28% على مستوى العالم، ما يمثل الزيادة الأكبر في الهجمات على أساس سنوي وفق أحد الأبحاث. لذا من الواضح أن المهاجمين يستهدفون الشركات في الإمارات، مما يؤكد على أهمية تطبيق استراتيجيات قوية لضمان الأمن السيبراني.

ولتنفيذ هذه الاستراتيجيات بفعالية، يجب على المؤسسات فهم التحولات القادمة في مشهد الأمن السيبراني في المنطقة وتوقعها لحماية نفسها بما يقتضيه الموقف. وفيما يلي توقعات لأبرز توجهات الأمن السيبراني التي سترسم ملامح عام 2023.

يوفر الدور المتنامي للذكاء الاصطناعي في العالم السيبراني الكثير من الفرص، إلا أنه يرفع من مستوى الأخطار كذلك، حيث سيشهد عام 2023 زيادة التهديدات التي تستخدم تقنيات تصيد متطورة وتدمجها مع الذكاء الاصطناعي لاستهداف المستخدمين بطرق أكثر ذكاءً. ووجدت إحدى الدراسات أن هجمات التصيد في الإمارات ازدادت بنسبة 230% خلال الربع الثاني من عام 2022، وهو ما يشكل تهديداً تحتاج الشركات في الدولة والمنطقة عموماً إلى الحذر منه.

وغيّر الذكاء الاصطناعي هجمات التصيد بصورة جذرية، حيث أتاح للمهاجمين الاستفادة من ميزات مثل معالجة اللغة الطبيعية لإنشاء رسائل تصيّد مُقنعة وصعبة الكشف، بضغطة زر وبدون جهد يُذكر. ويُظهر أحد الأبحاث إمكانية إساءة استخدام المهاجمين لروبوتات الدردشة، مثل دردشة «جي بي تي» لكتابة رسائل التصيّد والتعليمات البرمجية. ويمكن للمهاجمين أيضاً إطلاق حملات تصيّد أكثر استهدافاً وتعقيداً من خلال دمج الذكاء الاصطناعي مع قواعد بيانات

.المعلومات المُخترقة والتي توجد على الإنترنت المظلم

ويؤثر تطور اللوائح التنظيمية وقوانين الامتثال على مقاربة المؤسسات في إدارة البيانات في عام 2023، لا سيما وأن الحكومات في المنطقة تعمل على تطبيق قوانينها الخاصة لخصوصية البيانات، من بينها دولة الإمارات والسعودية وعُمان. وستبدأ فرق تكنولوجيا المعلومات والمؤسسات بصورة عامة بتغيير وجهة نظرها عن جمع البيانات وتخزينها، .بالتزامن مع تطبيق مزيد من اللوائح التنظيمية محلياً

وتعتقد الكثير من المؤسسات أن البيانات التي تجمعها تشكل مورداً يمكن الاستفادة منه وتخزينه بدون أي عواقب، إلا أننا سنشهد تغير هذه النظرة بالتزامن مع إدراك المؤسسات للمسؤولية المُترتبة على بعض البيانات التي تجمعها، مما .سيضطرها إلى مراجعة وتحديث ممارساتها لضمان معالجة البيانات بطريقة أخلاقية وقانونية

وهنا يبرز دور مزودي خدمات الأمن السيبراني لإدارة أمان البيانات وجوانب الامتثال، لتمكين عملائهم من التركيز على .مهامهم وأعمالهم الأساسية

سنشهد في عام 2023 مزيداً من الهجمات على سلسلة التوريد والتي تستهدف مزودي البرمجيات ومطوريها، حيث سُجلت العديد من الهجمات التي تستهدف تطبيقات المراسلة والبريد الإلكتروني المستخدمة بكثرة في مجموعة كبيرة .من المؤسسات

ويمكن للمؤسسات العمل مع مزودي خدمات الأمن السيبراني، الذين يعملون على دراسة عمليات تكنولوجيا المعلومات والاتصالات في المؤسسة لمعرفة نوع المكتبات البرمجية المُستخدمة، وفيما إذا كانت عرضةً للاستغلال، ثم .إجراء تقييم للمخاطر بهدف معرفة جودة شيفرة المصدر لهذه المكتبات البرمجية وإجراء التغييرات اللازمة

في الإمارات خلال الربع الثالث لعام 2022 نفس العدد المُسجل (DDoS) بلغ عدد الهجمات الموزعة لحجب الخدمة .خلال النصف الأول من العام تقريباً

ويمكن للمؤسسات التخفيف من هذه الهجمات بشكل فعال من خلال فهم ردة فعل أنظمتها عليها. وتحتاج إلى حلول التخفيف من الهجمات الموزعة لحجب الخدمة إلى تحديث السياسات والتقنيات باستمرار مع الاستفادة من تحليلات .دقيقة في الوقت الحقيقي، لا سيما في ضوء المتطلبات دائمة التطور التي تفرضها مساعي التحول إلى الرقمنة

يشكل الأمن السيبراني عنصراً حاسماً وضرورياً في جميع مراحل مشوار التحول إلى الرقمنة. ويسعى المهاجمون باستمرار لتطوير أساليبهم لتجاوز الإجراءات الأمنية، غالباً من خلال استغلال التقنيات الناشئة مثل الذكاء الاصطناعي، لذا لا بد للمؤسسات من بذل جهود واعية والتعاون مع مزود خدمة موثوق لتعزيز مرونتها السيبرانية والازدهار خلال .عام 2023

*** رئيس قسم التكنولوجيا في «هلب أي جي»**