الخليج

اقتصاد, أسواق عالمية

13 مارس 2022 21:29 مساء

توجهات لإدارة الأمن الإلكتروني والمخاطر أمام التهديدات الجديدة 7

«دبي:«الخليج

سلّطت شركة «جارتنر» للأبحاث الضوء على أبرز سبعة توجهات يتوجب على القادة المسؤولين عن إدارة الأمن الإلكتروني والمخاطر معالجتها لتأمين الحماية والتوسّعات في الأعمال الرقمية للمؤسسات الحديثة، لا سيما في ظل التهديدات الجديدة والناشئة خلال عام 2022 وما بعده.

وقال بيتر فيرستبروك، نائب رئيس الأبحاث لدى «جارتنر»:«تواجه المؤسسات حول العالم تحديدات تتمثّل في هجمات برامج الفدية المعقّدة، وهجمات على سلاسل الإمداد الرقمية، ومحاولات استغلال نقاط الضعف الأصيلة فيها. في حين أن الانتشار الواسع لأسلوب العمل المختلط بسبب ظروف الجائحة والتوجه نحو حوسبة السّحاب تزيد من صعوبة التحدّيات التي تواجه الرؤساء التنفيذيين لتقنية المعلومات في سعيهم نحو تأمين بيئة عمل المؤسسات المتوزّعة بشكل متزايد» ـ وذلك إلى جانب تعاملهم مع النقص الحالي في توفّر الكفاءات الأمنية.

1- توسّع سطح الهجوم

تسجّل المؤسسات توسّعات في إجمالي سطح الهجوم المحتمل. كما أن المخاطر المتعلقة باستخدام أنظمة تقليدية/سيبرانية، وإنترنت الأشياء، وحوسبة المصدر المفتوح، وتطبيقات حوسبة السّحاب، وسلاسل الإمداد الرقمية المركّبة، والتواصل الاجتماعي، وغيرها كانت قد أدّت إلى تعريض مزيد من الأسطح الخاصة ببعض الأصول المملوكة لدى هذه المؤسسات إلى مخاطر الهجمات الخارجية.

2- مخاطر سلسلة الإمداد الرقمي

اكتشفت الأطراف التي تقف خلف الهجمات الأمنية أن سلاسل الإمداد الرقمي يمكن أن توفر عائداً مجدياً لقاء الاستثمار سجّلت انتشاراً كبيراً عبر سلسلة الإمداد، ومن المتوقع ظهور المزيد من Log4j في استهدافها. فبعض الثغرات مثل الثغرات المشابهة. وتتوقع شركة «جارتنر» أنه وبحلول عام 2025 فإن 45% من المؤسسات حول العالم ستكون قد تعرضت لهجمات استهدفت سلاسل إمداد البرامج لديها، وهو ما يمثل زيادة بمعدّل ثلاثة أضعاف عن عام 2021.

3- تهديدات الهوية والاستجابة لها

تعمل الأطراف الفاعلة والتي تقف خلف هذه الهجمات المركبة على استهداف البنى التحتية لإدارة التعرف على الهوية وصلاحيات الوصول، حتى بات سوء استخدام صلاحيات الاستخدام الممنوحة سببا رئيسيا لنقل الهجمات. وهذا ما للإشارة إلى مجموع «ITDR دفع بشركة «جارتنر» لإطلاق مصطلح «الكشف عن تهديدات الهوية والاستجابة لها الأدوات والممارسات التي يمكن اتباعها لتأمين الحماية لأنظمة إدارة هوية المستخدم.

4- القرارات الموزّعة

مع تطور متطلبات وتوقّعات الأمن السيبراني لدى المؤسسات، ما يزيد من حاجة المسؤولين إلى حلول أمنية أكثر مرونة في ظل هذا التوسّع لأسطح الهجوم المحتمل. ولهذا، فإن مجال وحجم ومستوى تعقيد الأعمال التجارية يدفع بالحاجة إلى توزيع قرارات الأمن السيبراني، ومسؤوليتها، والمساءلة عنها عبر مختلف أقسام المؤسسة بدلاً من الاكتفاء بمركزيّة هذه المهمة.

5- أكثر من مجرد توعية

لا يزال الخطأ البشري يمثل عاملاً في العديد من الانتهاكات المتعلقة بالبيانات، ما يشير إلى أن الأساليب التقليدية للتدريب والتوعية بالمخاطر الأمنية ليست فعّالة كفاية. في حين أن المؤسسات التقدّمية تقدم على الاستثمار في برامج بدلاً من الاكتفاء بحملات التوعية الأمنية التقليدية والتي تركز على تحقيق SBCPs شاملة للسلوك والثقافة الأمنية متطلبات الامتثال.

6- توحيد شركات التزويد

مع تسارع وتيرة التقارب الرقمي على صعيد التقنيات الأمنية، مدفوعة بالحاجة إلى تبسيط هذه العمليات، والحد من نفقاتها الإدارية، وتعزيز الفاعلية. وتسهم عدّة منصات في تسريع الاستفادة من الحلول المتقاربة مثل حلول التعرّف SSE وحلول خدمات الأمن الطرفيّ extended detection and response (XDR) والاستجابة الممتدّة

.CNAPP ومنصات تطبيقات الحماية الأصيلة عبر حوسبة السّحاب

شبكة الأمن السيبراني –7

يدفع التوجه نحو دمج منتجات الأمان إلى الجمع ما بين مكونات المنظومة الأمنية. ومع ذلك، لا تزال هنالك حاجة إلى وضع سياسات أمنية ثابتة، وتمكين سير المهام والأعمال، وضبط تبادل البيانات بين هذه الحلول الموحّدة. تساعد بنية شبكة الأمن السيبراني CSMA في توفير هيكلية ووضعية أمنية مشتركة ومدمجة لتأمين جميع الأصول، سواء كانت في .مكان العمل، أو في مراكز البيانات أو عبر حوسبة السّحاب