الخليج

اقتصاد, تقنية وسيارات

27 يناير 2023 15:06 مساء

تضاعف الهجمات الإلكترونية على وسائل الإعلام.. وإيران والتشيك الأبرز

عرض خبراء كاسبرسكي توقعاتهم بشأن التحديات الماثلة أمام مراكز العمليات الأمنية. وأشار الخبراء إلى ارتفاع عدد حوادث الأمن الرقمي التي استهدفت قطاعي الحكومة ووسائل الإعلام في عام 2022، مشيرين إلى استمرار هذا التوجه في العام الجاري. ورجّح الخبراء أن مراكز العمليات الأمنية في هذه القطاعات وغيرها، تواجه المزيد من الهجمات الموجهة المتكررة، إضافة إلى هجمات سلاسل التوريد عبر مقدمي خدمات الاتصالات. وهناك تهديد آخر ينتظر مراكز العمليات الأمنية، يتمثل في المزيد من حوادث اختراق التطبيقات العامة. وقد تواجه المؤسسات المهددة بهجمات برمجيات الفدية أيضاً احتمالات تدمير بياناتها. وجهة نظر المؤسسات إلى مراكز العمليات الأمنية فيها لا تشير إلى أكثر من وجود نقص في الموظفين وزيادة في الطلب على الكفاءات.

وتتمتع مراكز العمليات الأمنية بأهمية بالغة، نظراً لأن دور الأمن الرقمي في الشركات الكبيرة يزداد بشكل ملحوظ كل عام. ويمكن للفرق ذات التنظيم الجيد العاملة في هذه المراكز تأمين مؤسساتها في وجه البرمجيات الخبيثة وأساليب الهجوم السريعة التطوّر. وتشتمل نشرة كاسبرسكي الأمنية لهذا العام على تنبؤات مخصصة لمراكز العمليات الأمنية.

هجمات متكررة •

لاحظ خبراء كاسبرسكي، أن متوسط عدد الحوادث في قطاع الإعلام قد تضاعف في عام 2022؛ إذ ارتفع إلى 561 هجوماً بعد أن وصل إلى 263 في 2021. وشهد العام الماضي، عدداً من الحالات البارزة، بينها انقطاع البث التلفزيوني الحكومي الإيراني من قبل قراصنة خلال الاحتجاجات التي عصفت بالبلاد. كذلك تعرضت منافذ إعلامية لهجمات (DDoS) الحرمان من الخدمة الموزعة كان من بينها مؤسسات إعلامية في جمهورية التشيك.
وأصبح الإعلام هدفاً رئيسياً لمجرمي الإنترنت ضمن أهداف شملت 13 قطاعاً خضعت لتحليل خبراء كاسبرسكي، بينها قطاعات الغذاء والتنمية والمالية، إلى جانب القطاع الحكومي الذي شهد زيادة في متوسط عدد الحوادث بنسبة 36% في عام 2022.

ومن المتوقع أن يستمر النمو في عام 2023، مع تكرار الهجمات الموجهة من قبل الجهات التي تحظى برعاية بعض الحكومات، ويُرجّح أن تُلاحظ هذه الهجمات كثيراً. وبينما سيطغي هذا التوجه على الجهات الحكومية، فإن وسائل الإعلام يزداد استهدافها خلال النزاعات الدولية التي تقترن تقليدياً بحرب المعلومات، نظراً للدور الحيوي الذي يلعبه الإعلام في النزاعات.

ولطالما ظلّت الشركات الكبيرة والجهات الحكومية أهدافاً لمجرمي الإنترنت والجهات التخريبية التي ترعاها الحكومات، بحسب ما أكد سيرجي سولداتوف رئيس مركز العمليات الأمنية لدى كاسبرسكي، الذي أشار في المقابل إلى أن الاضطرابات السياسية «زادت من دوافع المهاجمين، وأعادت تنشيط القرصنة، والتي لم يواجهه مختصو الأمن الرقمي وفق سياسات تنظيمية واضحة حتى عام 2022».

وقال: «للموجة الجديدة من الهجمات دوافع سياسية، ولذا فإنها تستهدف القطاعين الحكومي والإعلامي تحديداً، ومن الضروري لحماية المؤسسات تنفيذ كشف شامل عن التهديدات ومعالجتها من خلال الخدمات المُدارة الخاصة بالكشف عن التهديدات والاستجابة لها».

هجمات سلاسل التوريد عبر مقدمي خدمات الاتصالات •

قد يستهدف مجرمو الإنترنت في عام 2023 سلاسل التوريد من خلال تكثيف هجماتهم على شركات الاتصالات، لذا فإن التهديد المتزايد يلوح في الأفق. وشهد قطاع الاتصالات في عام 2021 لأول مرة انتشاراً للحوادث العالية الخطورة على مدار العام. وعلى الرغم من أن متوسط نسبة هذه الحوادث في 2022 كان أقل؛ إذ بلغ نحو 12% لكل 10 آلاف نظام مراقب مقابل 79% في 2021، فإن هذه الجهات تظل أهدافاً جذّابة لمجرمي الإنترنت.

مدمرات برمجيات الفدية: حوادث اختراق التطبيقات العامة •

لاحظ خبراء كاسبرسكي طوال عام 2022 توجهاً جديداً لبرمجيات الفدية من المنتظر أن يستمر في عام 2023، ويتمثل في عدم اكتفاء الجهات التخريبية بتشفير بيانات المؤسسات؛ بل بإتلافها أيضاً. وهو توجه ينسجم مع الهجمات ذات الدوافع السياسية.

وهناك تهديد آخر ينتظر مراكز العمليات الأمنية، يتمثل في المزيد من حوادث اختراق التطبيقات العامة التي يستخدمها الجمهور؛ إذ يتطلب الاختراق من المحيط استعدادات أقلّ من التصيد عندما تكون الثغرات القديمة لا تزال مكشوفة.

- **ماذا ستواجه مراكز العمليات الأمنية داخلياً؟**

تتزايد القيمة التي يحملها كل عضو في الفريق (حتى الأعضاء غير المهرة) في مراكز العمليات الأمنية. ويُعد تطوير مهارات الفريق الطريقة المثبتة لمواجهة الكمّ المتزايد من التهديدات، ما يُضفي أهمية كبيرة على التدريبات حول TTX فحوص الأجهزة، وأشكال التمارين الأخرى، مثل والفرق الأرجوانية، والمحاكاة الاستشارية للهجمات.
ويؤدي مشهد التهديدات المتزايدة إلى زيادة الموازنات المخصصة لمراكز العمليات الأمنية، وارتفاع الطلب على المزيد من الكفاءات. وتتحول أعداد الحوادث والتهديدات المتزايدة إلى حاجة إلى التنبؤ بالهجمات والأساليب، ما يرفع قيمة استقصاء معلومات التهديدات وملاحقتها.