

## «أكرونيس»: الإمارات منيعة أمام تهديدات وبرمجيات الفدية»



دبي: «الخليج»

كشفت شركة «أكرونيس» العاملة في مجال الحماية السيبرانية في أحدث تقرير لها، عن قصة نجاح ملهمة حول قدرة دولة الإمارات العربية المتحدة ودول منطقة الخليج العربي على مواجهة الهجمات السيبرانية.

يستعرض تقرير «أكرونيس» للتهديدات السيبرانية 2023، رؤى وتحليلات مشهد الأمن السيبراني في دولة الإمارات ودول مجلس التعاون الخليجي، ليعكس المناعة القوية لهذه المنطقة في مواجهة هجمات برمجيات الفدية، مع ظهور علامات مبشرة بانحسار التهديدات.

ويتوقع التقرير حدوث استقرار واضح في وتيرة الكشف عن برمجيات الفدية طوال الربع الرابع من عام 2023 بفضل التزام المنطقة بتحسين المشهد الرقمي وحمايته من الهجمات. كما يتوقع عودة للمستويات الهادئة بعد القفزة التي حدثت في الربع الأول من عام 2023، الذي شهد زيادة الهجمات بنسبة 6٪ مقارنة بالربع الرابع من عام 2022.

عدم يقين

وفي ظل سرعة التطور وانعدام اليقين، تبرز دول مجلس التعاون الخليجي وفي مقدمتها الإمارات لتمثل واحة للأمن

السيبراني على الصعيد العالمي وفق ما أورده التقرير، حيث تصاعد تكاليف الهجمات السيبرانية في الشرق الأوسط، وتشير بيانات شركة «آي بي إم» بوضوح إلى أن متوسط تكلفة الهجمة السيبرانية على المؤسسات في دولة الإمارات والسعودية يقدر بحوالي 6.53 مليون دولار، بما يزيد على المتوسط العالمي بنسبة 69%.  
كذلك يتطرق التقرير إلى النجاح في مواجهة هجمات الفدية، والتحديات المستمرة لهجمات الاحتيال، والتعامل مع البرمجيات الخبيثة، وتشير البيانات، إلى احتفاظ دولة الإمارات بوضع أفضل نسبياً، إذ تبلغ نسبة الإصابة 10% ما يضعها في الترتيب 31 عالمياً. وأيضاً، الذكاء الاصطناعي الذي يعيد صياغة المشهد من جديد، حيث تتبنى ما يزيد على 70% من الشركات في دولة الإمارات لتقنيات الذكاء الاصطناعي في عمليات اتخاذ القرار.

مصدر قلق

وقال زياد نصر، المدير العام لمنطقة الشرق الأوسط في الشركة: «نظراً لموقع الشرق الأوسط على الصعيد العالمي وبالأخص دولة الإمارات وتحولها إلى مركز اقتصادي عالمي، أصبحت شركات القطاعين العام والخاص هدفاً أساسياً للهجمات السيبرانية. وعلى مدار السنوات القليلة الماضية، كانت هجمات الفدية هي مصدر القلق الرئيسي ولكن مع تبني العديد من الإجراءات والتدبير الحازمة وغير المكلفة لتفادي تلك الهجمات وتوفير حلول تقنية للتعامل معها، تمكن صناع القرار في المنطقة من التغلب على هذه الهجمات والحد من أثارها الخطرة. ومن المؤكد أن التعليم المستمر وزيادة القدرات والمهارات البشرية واستثمار الشركات في تدابير الحماية السيبرانية عبر مختلف القطاعات من أهم «المحاور لتأهيل المنطقة لمجابهة التهديدات السيبرانية المستمرة»