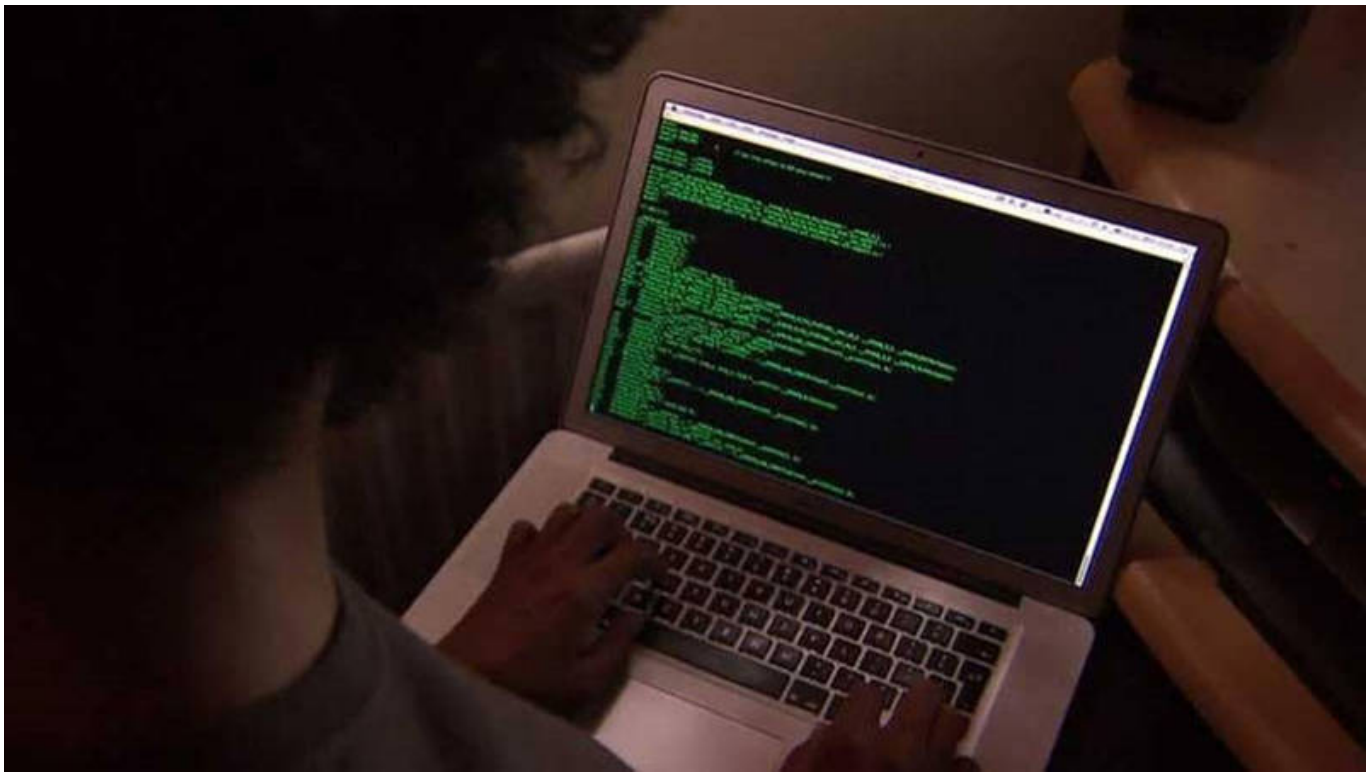
اقتصاد, تقنية وسيارات

1 يونيو 2021 20:05 مساء

زيادة في الهجمات الإلكترونية على الإمارات 250 %



«دبي: «الخليج

سلّط تقرير جديد أطلقته شركة «ديجيتل 14» الضوء على التهديدات والمخاطر الإلكترونية، التي تكتنف الشركات والمؤسسات الإماراتية، باعتبارها أهدافاً «عالية القيمة» لمنفذي الهجمات السيبرانية.

وبحسب التقرير الذي حمل عنوان «المرونة الإلكترونية: مشهد التهديدات الإلكترونية للشركات الإماراتية 2021» فإن التكلفة المرتفعة المرتبطة بالتهديدات والهجمات الإلكترونية الناجحة تحتّم على مؤسسات القطاعين العام والخاص بذل المزيد من الجهد لمواجهة التهديدات الأمنية الخطيرة، وحماية أعمالها وعملائها من اختراق البيانات.

وذكر التقرير أن الإمارات شهدت زيادة بنسبة 250% في الهجمات الإلكترونية في عام 2020، وزيادة هائلة في هجمات

.التصيد الاحتيالي وبرامج الفدية، مع تسجيل 1.1 مليون هجمة تصيد احتيالي خلال عام 2020

وتشير التقديرات إلى أن تكلفة اختراق البيانات في الشرق الأوسط تجعل المنطقة في المرتبة الثانية في العالم عند 6.52 .في عام 2020، بعد الولايات المتحدة مباشرةمليون دولار في المتوسط

ويكشف التقرير أن الجهات المنفّذة للتهديدات السيبرانية من دول أخرى أصبحت أكثر نشاطاً بين عامي 2017 و2020، حيث تزايد عددها، وأصبحت أكثر تعقيداً، كما بات التعرف إليها أكثر صعوبة. وتعتبر دولة الإمارات والشرق .الأوسط الأوسع أهدافاً لأنشطة الهجمات الإلكترونية من دول أخرى مدفوعة بأغراض اقتصادية وسياسية

وزادت برامج الفدية بشكل كبير في عام 2020؛ حيث أظهرت دراسة زيادة بنسبة 33٪ في عدد عائلات برامج الفدية الجديدة، مقارنة بعام 2019، وكانت القطاعات الحكومية وقطاعات البنية التحتية الحيوية من بين القطاعات الرئيسية .المستهدفة في الهجمات خلال عام 2020

وقال جوشوا نايت، النائب التنفيذي للرئيس لحلول الدفاع الإلكتروني في ديجيتل 14: «تشكل الإجراءات الاستباقية خطوة مهمة للغاية بالنسبة للشركات؛ حيث إن تكلفة تلك الإجراءات لا تقارن بالتكاليف التي ربما تضطر الشركات .لدفعها للاستجابة لهجمات إلكترونية ناجحة والتعافي منها

وقد فرضت جائحة «كوفيد– 19» تحديات مضاعفة فيما يتعلق بالتهديدات السيبرانية الحالية، كما أنها أدت إلى ظهور .«مجموعة جديدة من المخاطر الإلكترونية، التي ينبغي على الشركات تكثيف جهودها لمواجهتها والحد من تأثيراتها

وأوضح نايت، «لم تعد المنهجيات والاستراتيجيات التقليدية للأمن السيبراني كافية، ويجب تعزيز الحماية الإلكترونية المستمرة كعملية دائمة ومستدامة لتقوية وتحسين أمن المؤسسات بشكل مطرد، بدلاً من الاعتماد على حل واحد لمرة .«واحدة

الصورة