الخليج

اقتصاد, تقنية وسيارات

22 نوفمبر 2022 20:24 مساء

من الهجمات الإلكترونية خلال الربع الثالث برامج فدية 40%

«دبي: «الخليج

أصدرت مجموعة «سيسكو تالوس»، أحدث تقرير فصلي لها يسلط الضوء على توجهات الاستجابة للحوادث والتهديدات السيبرانية العالمية.

للمرة الأولى منذ إصدار هذه التقارير، شهدت استجابة سيسكو تالوس للحوادث عدداً متساوياً من ارتباطات برامج الفدية وبرامج ما قبل الفدية، والتي تشكل ما يقرب من 40% من التهديدات هذا الربع. واستهدف المهاجمون قطاع التعليم أكثر من أي قطاع في هذا الربع، يليه قطاع الخدمات المالية والحكومية والطاقة على التوالي. ولأول مرة منذ الربع الرابع للعام 2021، لم يكن قطاع الاتصالات هو القطاع الأكثر استهدافاً. في حين أن سبب استهداف قطاع التعليم بشكل متكرر هذا الربع يبقى غير معروف، إلا أن هذا وقت شائع من العام للخصوم لاستهداف المؤسسات التعليمية تزامناً مع عودة الطلاب والمعلمون إلى المدرسة.

تميز الربع الثالث أيضاً بالمتغيرات التي طرأت على برامج الفدية عالية المستوى والتي تم رصدها في السابق، مثل ظهرت لأول مرة في أبريل (Black Basta) وعائلة جديدة من برامج الفدية تحت اسم «Hive and Vice Society» 2022 ولم تتم ملاحظتها بعد في عمليات الاستجابة للحوادث. واصلت مجموعة سيسكو تالوس أيضاً مراقبة التهديدات التي كانت موجودة باستمرار في الفترات السابقة، بما في ذلك التصيد الاحتيالي وتسوية البريد الإلكتروني للأعمال ومحاولات استغلال نقاط الضعف في التطبيقات العامة والتهديدات الداخلية.

على الصعيد الداخلي للشركات، فوفقاً للتقرير لا يزال الافتقار إلى المصادقة متعددة العوامل أحد أكبر العقبات التي تعترض أمن الشركات. وكانت 18% من الشركات إما لا تمتلك المصادقة متعددة العوامل أو تم تمكينها فقط على عدد قليل من الحسابات والخدمات الهامة، ما يسمح لمجرمي الإنترنت بتسجيل الدخول والمصادقة.

وقال فادي يونس، رئيس الأمن السيبراني لدى سيسكو في الشرق الأوسط وأفريقيا وقسم مزودي الخدمات في أوروبا الشرق الأوسط وأفريقيا: «نعيش اليوم في عصر متصل ورقمي أكثر من أي وقت مضى، حيث يعتبر الأمن السيبراني في يومنا هذا ذا أهمية قصوى. ونظراً لأن الشركات والحكومات في جميع أنحاء المنطقة تسعى إلى حماية بياناتها وأعمالها، نواصل في سيسكو جهودنا لدعم عملائنا، ما يساعد على دفع الاكتشاف السريع للمخاطر الإلكترونية والحماية منها».

وأضاف يونس: «يعرّف الأمن السيبراني بأنه قائم علي البيانات. فكلما زاد عدد الرؤى والمفاهيم التي نمتلكها في مشهد التهديدات، كلما كانت قدرتنا للقياس عن بُعد أفضل، وزادت احتمالية القدرة على منع الحوادث الأمنية. ويمكن لإمكانياتنا عند حدوث اختراق ما اكتشاف التهديدات والاستجابة لها ومعالجتها بأسرع وقت ممكن».