تشفير رسائل Microsoft 365 يسمح بتسريب معلومات حساسة

وجد باحثون أن التشفير الافتراضي لرسائل الإيميل في سحابة مايكروسوفت يستخدم Electronic Codebook (ECB) وهو وضع يسمح بتسريب معلومات هيكلية عن الرسالة. وقد اعتبروا من وجهة نظرهم أن ذلك يندرج ضمن تصنيف الثغرات الممكن استغلالها

بروتوكولات التشفير

TLS هو بروتوكول طبقة النقل الآمنة و يستخدم للتشفير بين نقطتين لمجموعة من تطبيقات الإنترنت

النسخة المعتمدة حاليا TLS 1.3 منذ عام 2018 تبني على أساسات بروتوكول SSL الذي بدأ الاستغناء عنه في عدد من التطبيقات

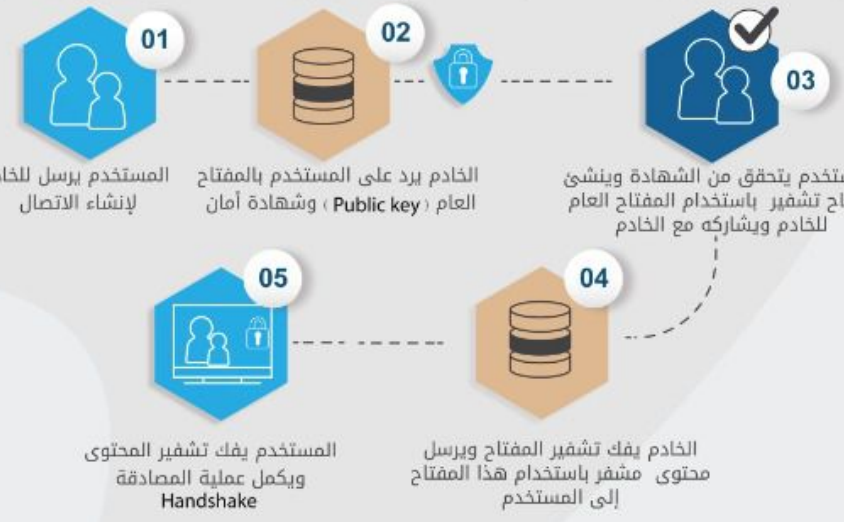
هيئة الاتصالات: عقدت ملتقى التقنيات التنظيمية في نسخته الأولى

عقدت هيئة الاتصالات ملتقى التقنيات التنظيمية في نسخته الأولى، وذلك بمشاركة العديد من الخبراء والمختصين؛ بهدف تسليط الضوء على التقنيات التنظيمية وإبراز دورها وأهميتها في إدارة الحوكمة والمخاطر والامتثال، ومناقشة مجموعة من الموضوعات المتعلقة بالأدوار التنظيمية والرقابية للشركات والمؤسسات والفرص الواعدة للشركات الناشئة.

المصدر https://www.citc.gov.sa

التشفير

عملية تحويل بيانات أصلية إلى بيانات مشفرة باستخدام أحد خوارزميات تقنيات التشفير والمفتاح الخاص بذلك



يستخدم التشفير في عدد من بروتوكولات الإنترنت BGP-SEC,DNS-SEC,HTTPS

المخاطر المحتملة

الثغرات الأمنية: مثل ثغرة HeartBleed لمكتبة التشفير OpenSSL التي تسببت في عام 2014 لتعرض ملايين الأجهزة حول العالم لخطر الاختراق.

تعرض هيئة الشهادات (CA) للاختراق: مثل تعرض شركة ديجي نوتار في 2011 لاختراق نتج عنه إصدار 500 شهادة أمان مزيفة عرّضت ما يقارب من 300 ألف مستخدم لخطر الاختراق.

الحوسبة الكمية: مثل تعرض بروتوكولات الأمان المعتمدة على مفاتيح التشفير بين نقطتين إلى خطر عالي بحكم القدرات الهائلة التي تملكها الحواسب الكمية في إمكانية فك هذه المفاتيح.

"تم إصدار هذه النشرة من جمعية الإنترنت في السعودية برعاية مركز الإنترنت السعودي"