

CyberSEC2025, Mattei (IBM Italia): 'Le Sfide per la sicurezza con l'avvento dei computer quantistici'

La rapida evoluzione delle minacce quantistiche mette a dura prova i sistemi di contrasto, che spesso e volentieri arrivano tardi per rispondere adeguatamente. *“Se ci sono dei criminali che copiano dei dati oggi per poterli decriptare domani è ovvio che i dati che hanno una rilevanza per i prossimi due anni mi interessano poco ma per quei dati per i quali devo garantire che siano inaccessibili per i prossimi 10 anni ebbene, per quei dati noi dobbiamo cominciare fino da oggi a criptarli in una maniera che sia in grado di contrastare un attacco quantistico.* Lo ha detto **Federico Mattei**, Business Development EMEA, IBM Quantum nel suo intervento alla 4^a edizione di #CyberSEC2025Rome, la Conferenza internazionale promossa e organizzata dal nostro giornale, in corso il 5 e il 6 marzo a Roma presso i Saloni di Rappresentanza della Caserma Salvo D'Acquisto organizzata da nostro giornale.

L'importanza di cominciare a prepararsi da oggi è fondamentale, *“ma, come ha chiesto di fare Biden nel 2022 a tutte le agenzie Usa, serve una mappatura completa di tutti gli algoritmi crittografici in uso e serve una strategia di crypto agility, vale a dire la capacità di cambiare l'algoritmo in un tempo certo, 60 o 90 giorni”*, prosegue Mattei.

Biden già sapeva nel 2022 che gli Stati Uniti, ma anche la Ue, avrebbero dovuto rispondere a qualche executive order che

ordina di deprecare determinati algoritmi.

Ma quanto tempo ci vuole per effettuare questo tipo di mappatura e di sostituzione? In media per le grandi istituzioni e le grandi aziende ci vogliono in media 10 anni.

“Spero davvero che non sia vero che la minaccia quantistica si presenterà nel 2030, perché altrimenti siamo in grosso ritardo”, aggiunge Mattei, sperando altresì che ciò non sia vero nemmeno nel 2035.

Ma quel che è certo è che bisogna cominciare a lavorarci da subito. *“Plaudiamo al fatto che la settimana scorsa il Mimit e il Mur hanno pubblicato la strategia quantistica italiana. Era necessaria, la maggior parte dei paesi europei l’avevano già da 2020. Sappiamo che il sottosegretario Butti ha stanziato anche una task force per l’implementazione di questa strategia. E’ fondamentale collaborare tutti insieme per mettere in sicurezza i sistemi nei tempi giusti per l’arrivo della computazione quantistica”,* chiude Mattei.

Leggi le altre notizie sull’home page di Key4biz

<https://www.key4biz.it/cybersec2025-mattei-ibm-italia-le-sfide-per-la-sicurezza-con-lavvento-dei-computer-quantistici/523712/>