IBM rende disponibili i cifrari post-quantistici sui mainframe z16

https://www.hwupgrade.it/i/n/IBM_logo_720.jpg,

IBM ha annunciato che renderà disponibili sui nuovi mainframe z16 i cifrari post-quantistici standardizzati dal NIST a luglio. L’intento è di far sì che le aziende familiarizzino con i nuovi algoritmi in vista dell’implementazione su scala globale

di Riccardo Robecchi pubblicata il **05 Agosto 2022**, alle **12:51** nel canale Innovazione

Computer QuantisticoIBMCloud Security

Uno degli aspetti su cui **IBM** ha puntato i riflettori alla presentazione dei nuovi mainframe z16 è stata la compatibilità con la crittografia resistente agli attacchi da parte dei computer quantistici. L'azienda ha ora affermato che sarà possibile sfruttare i quattro nuovi cifrari standardizzati dal NIST grazie a un aggiornamento dell'adattatore **Crypto Express 8S**.

La cifratura post-quantistica arriva sui mainframe IBM z16

IBM è stata coinvolta direttamente nella creazione di tre dei quattro nuovi algoritmi di cifratura oggetto di standardizzazione da parte del NIST e non sorprende, dunque, che sia già pronta a integrarli all'interno dei propri prodotti.

Nello specifico, i mainframe z16 sono già pensati per

sfruttare gli algoritmi **CRYSTALS-Kyber**, pensato per lo scambio di chiavi tramite crittografia a chiave pubblica, e **CRYSTALS-Dilithium**, sviluppato per le firme digitali.

I cifrari sono già utilizzabili, ma la loro inclusione attuale è più tesa non tanto al loro uso immediato, ma al dare la possibilità alle aziende di **sperimentare e di aggiornare i propri software** per una compatibilità futura. Servirà infatti molto tempo perché tutti i sistemi vengano aggiornati ai nuovi algoritmi, ma tale lavoro deve partire ora per essere pronti in futuro. Come scrive Anne Dames, *distinguished engineer* nella divisione delle tecnologie crittografiche in IBM, *"[i mainframe] IBM z16 vi mettono nelle condizioni di iniziare a usare la crittografia* quantum safe *insieme a quella classica, mentre iniziate a modernizzare le applicazioni esistenti e a costruirne di nuove."*

"Documenti legali come mutui e prestiti che dovranno ricevere protezione per 20 anni o più, ad esempio, necessitano di nuovi algoritmi quantum safe *oggi"*, continua Dames. E proprio questo è il nocciolo della questione: bisogna farsi trovare preparati all'arrivo dei computer quantistici, anche se ciò dovesse avvenire fra 20 anni.

Read More