Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS
Analisi e prevenzione

15 novembre 2024

Valutazione dell'UFCS

Necessità d'intervento in relazione con la crittografia post-quantistica (PQC)

Alla luce degli sforzi in atto nella produzione di computer quantistici di dimensioni sufficienti e in considerazione delle possibili conseguenti ripercussioni sulle procedure e sugli algoritmi crittografici attualmente impiegati, l'UFCS ha redatto una valutazione tecnologica sui computer quantistici e sulla crittografia post-quantistica (PQC). La situazione e la conseguente necessità d'intervento possono essere riassunte come segue:

- i computer quantistici rappresentano un pericolo per la sicurezza di determinate procedure e determinati algoritmi crittografici[1]. Gli esperti non sono tuttavia ancora unanimi sulle reali possibilità e sulle tempistiche della produzione di computer quantistici di dimensioni sufficienti.
- Nel frattempo sono in fase di sviluppo procedure e algoritmi resistenti ai computer quantistici (crittografia post-quantistica, PQC) e il «National Institute of Standards and Technology» (NIST) statunitense sta procedendo alla loro standardizzazione. È molto probabile che gli standard in fase di elaborazione vengano adottati a livello internazionale.
- Non appena i suddetti algoritmi alternativi saranno disponibili, sarà opportuno riflettere sulla possibilità di passare[2] dagli algoritmi attuali agli algoritmi PQC e pianificare a medio termine la migrazione, per poter approfittare di algoritmi più potenti nella gestione dei rischi nella prospettiva di una strategia proattiva.
- Per i propri prodotti IT, i produttori e i fornitori possono pianificare e realizzare autonomamente la summenzionata migrazione; le organizzazioni, per contro, dipendono dai produttori e dai fornitori e devono convenire con essi piani di migrazione specifici ai prodotti.
- Se un'organizzazione non è in grado di realizzare internamente la pianificazione della migrazione, può rivolgersi a partner esterni provvisti delle corrispondenti conoscenze tecniche. Nella scelta di un partner bisognerà tuttavia assicurarsi che quest'ultimo conosca bene sia le attività sia l'infrastruttura IT dell'organizzazione.

[1] In particolare per le procedure e gli algoritmi crittografici rientranti nell'ambito della crittografia asimmetrica (Public Key).

[2] Per la migrazione sono disponibili modalità d'esercizio ibride, nel cui quadro gli algoritmi tradizionali e gli algoritmi PQC possono essere combinati e impiegati in maniera complementare.