PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5631 di Venerdì 31 maggio 2024

Per proteggere i nostri dati occorre guardare lontano

La commissione europea ha pubblicato, a metà aprile, una raccomandazione, che stimola i paesi europei a studiare fin da adesso soluzioni di sicurezza informatica, resistenti ad attacchi con i potentissimi computer quantistici.

I lettori mi perdoneranno se, quando ho letto questa notizia, la ho associata a quanto dovettero fare gli istituti di vigilanza, che si occupavano del trasporto valori. La crescente diffusione di armi potenti, come Kalashnikov, fece sì che le protezioni antiproiettile dei furgoni esistenti non fossero più sufficienti e fu necessario sviluppare ed acquistare tutta una nuova serie di furgoni, in grado di resistere a attacchi con queste temibili armi.

La situazione è simile a quanto sta accadendo adesso per la protezione delle reti di comunicazione e dei dati.

Tutti sappiamo che la straordinaria potenza dei computer quantistici permette non solo di sviluppare nuovi algoritmi, particolarmente resistenti ad attacchi di decifrazione, ma consente anche di usare gli stessi computer per attaccare questi stessi algoritmi, e cercare di decodificarli, violando quindi i dati e le comunicazioni, protetti da questi algoritmi.

Anche se infatti è vero che le tecnologie quantistiche porteranno notevoli benefici sociali ed economici, non v'è dubbio che lo sviluppo di questi computer renderà più agevole, per i malintenzionati, l'accesso a dati sensibili, non protetti da applicativi criptografici di elevatissimo livello.

La strategia della commissione europea, per fronteggiare questo rischio, è quella di stimolare le nazioni europee a mettere a punto, fin da adesso, degli applicativi criptografici in grado di resistere anche ad attacchi portati con i potenti computer quantistici.

Poiché si tratta di una soluzione a base software, non dovrebbero esservi grosse difficoltà nell'attivare queste protezioni, che risulterebbero compatibili con le attuali strutture informatiche.

La raccomandazione mira ad aiutare gli Stati membri a mettere a punto una strategia omogenea, nel mettere a punto sistemi di sicurezza oltremodo avanzati. La raccomandazione inoltre mira a rendere compatibili le varie soluzioni, in modo che la

migrazione di dati fra le varie nazioni europee non venga compromessa.

Questa raccomandazione si aggiunge a quelle già avanzate da altri enti, che hanno affrontato o stanno affrontando questo problema. Ad esempio, si pensi al recente rapporto della agenzia europea per la sicurezza cibernetica (ENISA), ed allo sviluppo di applicativi crittografici, in grado di resistere ad attacchi con i potenti computer quantistici.

Riporto in allegato il testo di questa raccomandazione, fortunatamente questa volta disponibile in lingua italiana, perché è indispensabile che i responsabili della sicurezza informatica sappiano guardare lontano e, soprattutto in fase di impostazione di nuove architetture informatiche, le predispongano per gestire avanzati strumenti di protezione.

RACCOMANDAZIONE DELLA COMMISSIONE del 11.4.2024 relativa a una tabella di marcia per l'attuazione coordinata della transizione verso la crittografia post-quantistica (PDF)

Adalberto Biasiotti