PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4901 di Lunedì 29 marzo 2021

Una garanzia di protezione per i dati sanitari

Le cartelle cliniche dei pazienti, per legge, debbono essere conservate per un tempo illimitato. Come si può conciliare questa imposizione con la adozione di idonee garanzie di protezione dei dati stessi da possibili violazioni?

Tra i tanti problemi che deve affrontare il mondo della sanità, forse non è stata ancora prestata sufficiente attenzione alle modalità di conservazione e protezione delle cartelle cliniche.

La legge impone che tali documenti vengano conservati per un tempo illimitato. Per evitare un sovraccarico dei depositi e degli archivi delle strutture ospedaliere, oggi sono molte le strutture che ricorrono alla digitalizzazione dei documenti stessi, secondo modalità garantistiche, che permettono la distruzione dei supporti cartacei originali, pur garantendo una piena validità delle copie informatiche.

A questo punto, ci si potrebbe domandare quali garanzie possono offrire le strutture sanitarie, circa il fatto che i documenti cartacei digitalizzati, seppure opportunamente protetti da algoritmi criptografici, non possano essere violati in un futuro più o meno lontano.

Oggi abbiamo a disposizione potenti algoritmi criptografici, come ad esempio lo AES-Advanced crypto system, del quale gli esperti affermano di poter essere in grado di garantire una sufficiente protezione da attacchi di decifrazione per i prossimi 30 anni.

Il motivo per cui si introduce questa limitazione temporale è legato alla crescente potenza di calcolo degli elaboratori, in particolare gli elaboratori quantici, oppure quantistici, che impongono di esaminare in una prospettiva temporale completamente diversa i tempi collegati ad un attacco sistematico alle chiavi crittografiche.

Da ciò discende che oggi l'attenzione deve sempre tenersi alta sugli algoritmi criptografici utilizzati, ma ancora più alta deve essere l'attenzione posta alle modalità di creazione, distribuzione ed utilizzo delle chiavi criptografiche, che potrebbero diventare il punto debole dell'intero sistema di protezione delle informazioni su supporto digitale.

Ecco perché occorre fare un salto di qualità nell'intero processo di creazione e gestione delle chiavi criptografiche, ricorrendo a tecniche quantistiche.

Questa esigenza è ovviamente ancora più sentita del mondo della sanità, proprio per i tempi assai lunghi di conservazione che sono imposti dalle vigenti normative, almeno in Italia.

In altri paesi la situazione è meno drammatica, perché ad esempio in altri paesi il limite temporale è posto a 30 anni, esattamente come a trent'anni è posto il limite temporale di conservazione delle cartelle sanitarie dei donatori di sangue, in Italia.

Gli specialisti hanno cominciato allora a studiare nuove tecniche di produzione, distribuzione ed utilizzo di chiavi criptografiche di altissima resistenza, basate appunto su tecniche quantistiche.

Una trasmissione di una chiave, prodotta e distribuita con questo sistema, è assai più resistente a possibili disturbi, presenti sul canale di trasmissione. L'adozione di ripetitori, anch'essi a tecnica quantistica, permette di ridurre in maniera drammatica la possibilità che la chiave venga alterata da disturbi di trasmissione.

Ma non è finita.

Uno dei grandi vantaggi di un processo di distribuzione di una chiave criptografica quantistica sta nel fatto che essa non può essere copiata. Inoltre, qualsiasi tentativo di accedere alla chiave stessa ne comporta l'immediata alterazione e successiva impossibilità di utilizzo, mettendo inoltre in evidenza il tentativo di attacco.

Sottolineo il fatto che stiamo parlando di tecniche di produzione e distribuzione delle chiavi criptografiche, e non degli algoritmi criptografici, sui quali queste chiavi verranno utilizzate.

Per questa ragione lo European Telecommunication Standard Institute ? ETSI, ad ottobre 2020 ha organizzato una conferenza sulla sicurezza delle applicazioni criptografiche a base quantica, seguita da un evento tecnico, a fine di gennaio 2021, che ha approfondito questi temi.

Tutti coloro che hanno l'esigenza di protezione criptografica dei dati devono prestare attenzione a queste nuove tecniche, tanto è vero che le aziende che vendono queste applicazioni si stanno già preparando a migrare le loro piattaforme ed i loro algoritmi verso soluzioni quantistiche, in modo da far compiere un salto di qualità a livello di protezione da decodifica di dati critici, proiettata nel lungo periodo.

Mi auguro che chiunque debba oggi affrontare questi problemi sappia guardare lontano, prescrivendo ed acquistando tecniche di protezione che sappiano resistere agli attacchi del tempo.

Naturalmente quanto illustrato in precedenza poco a che fare con le numerosissime sanzioni, recentemente applicate dall'autorità Garante nazionale a strutture sanitarie di vario tipo, per violazioni afferenti al trattamento di dati personali. In questo caso, le

violazioni erano decisamente meno gravi, in quanto facevano riferimento all'invio ad un errato destinatario di informazioni sanitarie. È questo il tipo di problema che tipicamente si verifica, quando non si è diligenti nella digitazione di un numero di facsimile, inviando un fax ad altro destinatario.

Adalberto Biasiotti

---

www.puntosicuro.it