PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3880 di lunedì 24 ottobre 2016

IoT e USB: conciliare sanità e protezione dei dati personali

La stragrande maggioranza delle violazioni di dati personali si registra proprio nell'ambito di istituzioni sanitarie e ci si può domandare se questo fatto ha delle ragioni obiettive, cui bisogna porre con urgenza rimedio. Di Adalberto Biasiotti.

Ho già avuto modo di dare notizie ai lettori di una ricerca di mercato, sviluppata ogni anno, che conferma senza ombra di dubbio che il mondo delle istituzioni sanitarie è quello in cui si registrano le più frequenti e gravi violazioni nella tutela dei dati personali.

D'altro canto, se l'approccio alla tutela di questi dati è quello espresso da un noto primario ospedaliero, che mi dichiarò: "Fra salute e privacy, io mi preoccupo solo della salute!", non v'è dubbio che i risultati della ricerca di mercato trovano piena motivazione, anche se non evidentemente giustificazione.

Come se non bastassero i problemi legati quindi all'approccio che il mondo sanitario ha, nei confronti della protezione dei dati personali dei pazienti, vi sono cause esogene che non fanno altro che aggravare il problema.

Una prima causa esogena è indubbiamente legata all'utilizzo sempre più allargato di presidi terapeutici che sono collegati alla rete ospedaliera, utilizzando l'ormai famosa e pericolosa architettura IoT- Internet of Things.

I progettisti di questi presidi sanitari avanzati si preoccupano della integrità e rapidità della connessione, che permette di trasferire i dati prelevati dal sensore, che il paziente indossa o cui il paziente è collegato, al sistema informativo sanitario ospedaliero, in modo che eventuali anomalie possono essere immediatamente rilevate. Come seconda funzione primaria di questi dispositivi vi è la possibilità di archiviare i dati, in modo da mettere a disposizione dei sanitari l'evoluzione storica di parametri critici. L'analisi storica è preziosissima per valutare, ad esempio, l'effetto che alcuni principi attivi farmaceutici possono avere su determinate malattie.

Il problema sta nel fatto che i progettisti di questi apparati, proprio come i sanitari, di tutto si preoccupano, tranne della protezione della comunicazione da possibili interferenze.

Fortunatamente da qualche tempo altri specialisti si stanno occupando di questo problema e hanno messo a punto dei protocolli criptografici, che potrebbero permettere di proteggere la comunicazione fra il sensore e il server. Il problema, legato alla introduzione di questi algoritmi criptografici, discende dal fatto che la capacità di calcolo di questi sensori è molto bassa, mentre invece spesso gli algoritmi criptografici richiedono un'elevata capacità di calcolo, tanto più elevata quanto più resistente è l'algoritmo.

Un algoritmo pienamente soddisfacente deve essere tale da garantire l'autentica del sensore, l'integrità e la riservatezza dei dati che vengono scambiati.

Un'altra caratteristica che permette di valutare la resistenza all'attacco di un algoritmo è legata alla lunghezza della chiave. Ancora una volta, chiavi lunghe significano elevata sicurezza ma anche richiedono elevata capacità di calcolo, difficilmente reperibile sui microcircuiti installati su questi sensori.

Ecco perché una possibile soluzione nasce dall'incorporare nella circuiteria del sensore un microprocessore progettato appositamente per la gestione di protocolli criptografici avanzati. Quando ad un microprocessore si chiede di svolgere questa sola specifica funzione, esso può essere ottimizzato e ridotto in dimensioni, oltre a consentire un aumento della velocità di calcolo e quindi una riduzione dell'intervallo che passa tra il momento in cui il sensore ha acquisito il dato e il momento in cui il dato viene ricevuto dal sistema informatico sanitario.

Infine, non dimentichiamo che una parola chiave sicura deve essere modificata nel tempo e quest'operazione non può essere evidentemente fatta da tastiera, ma deve essere realizzata con una funzione evolutiva, incorporata nell'algoritmo criptografico stesso.

Come si vede, non sono problemi facili da risolvere ma sembra che, nonostante l'atteggiamento alquanto agnostico delle strutture sanitarie, delle soluzioni efficienti ed efficaci siano a disposizione del responsabile informatico della struttura ospedaliera.

Ma non abbiamo finito.

Un recente studio ha messo in evidenza un altro grave problema della movimentazione di dati in ambito sanitario.

Questo problema è legato alla presenza sempre più diffusa di supporti di memoria con connessione USB.

La presenza di una presa USB su un apparato sanitario permette la connessione di chiavette, che possono essere usate solo in forma passiva, ad esempio per estrarre dati, ma possono purtroppo essere usate anche informativa, ad esempio per inserire virus.

Una possibile soluzione, che in ambiente bancario è ancora oggi presente, è quella di bloccare la possibilità di connessione di chiavette USB, anche se evidentemente questo approccio può creare problemi operativi, cui bisogna pensare per tempo e cui bisogna dare una soluzione altrettanto per tempo.

Ancora una volta, bisogna trovare un compromesso tra facilità d'uso e sicurezza d'uso e, ancora una volta, non invidio i responsabili informatici del mondo della sanità, che oltretutto hanno a che fare con controparti, come dichiarato in precedenza, poco sensibili a questi problemi.

Può darsi che l'entrata in vigore del nuovo Regolamento Europeo 2016 /679, con le sanzioni pesantissime applicabili a coloro che non tutelano a sufficienza i dati personali degli interessati, potrà costituire un valido incentivo a fare di più e di meglio in questo delicatissimo settore.

Adalberto Biasiotti

Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

---

www.puntosicuro.it