PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 3988 di lunedì 10 aprile 2017

Sicurezza e sanità: ancora un buco nero

La sicurezza informatica nel mondo della sanità comporta un coacervo di addestramento dei dipendenti è di tecnologie, ma ad oggi sembra che soddisfacenti risultati siano ancora lontani. Di Adalberto Biasiotti.

Tempo addietro un primario di un ospedale milanese ebbe a dichiarare che per lui era assai più importante far recuperare ad un paziente la sua salute, rispetto alla garanzia di tutela dei suoi dati personali sanitari. Questo atteggiamento è molto diffuso nel mondo della sanità ed è questa la ragione per la quale i più clamorosi furti o perdite di dati, registrati in una parte qualsiasi del mondo, coinvolgono quasi sempre il mondo della sanità.

Purtroppo questo atteggiamento non permette di mettere sotto controllo i rischi effettivamente presenti, perché un clic sul link sbagliato, oppure il mancato rispetto di una prescrizione, inviata per via informatica e non correttamente trasferita, può portare ad un danneggiamento della salute del paziente, invece che al suo miglioramento.

Durante un recente incontro, a Boston, un responsabile della sicurezza e della protezione dei dati personali ha messo in evidenza ai partecipanti, perlopiù appartenenti al mondo della sanità, quali potrebbero essere le più appropriate strategie per conciliare l'ambizione di aiutare i pazienti a recuperare la propria salute con i fattori umani ed informatici, che possono compromettere questa ambizione.

L'esperto ha dichiarato che, a suo avviso, i problemi sono legati per il 70 percento al fattore umano per il 30 percento a fattori tecnologici. Ad esempio, se usate lo stesso codice identificativo personale e le stesse parole chiavi in gran numero di applicazioni, state costruendo un ambiente a rischio, che potrebbe, presto o tardi, essere compromesso, sia accidentalmente, sia dolosamente, con conseguenze negative sulla salute dei pazienti coinvolti.

Questa è la ragione per la quale una sicurezza informatica nel mondo della sanità, che abbia caratteristiche di efficienza ed efficacia, richiede una strategia multistrato, che include l'utilizzo di presìdi tecnologici efficaci e un appropriato addestramento dei soggetti coinvolti.

D'altro canto, a che serve uno strumento informatico efficace, se i soggetti coinvolti non sanno utilizzarlo in modo appropriato?

Il nuovo regolamento europeo prevede delle sanzioni elevatissime per tutti coloro che sono coinvolti in perdite di dati personali, sia di tipo accidentale, sia di tipo doloso. È certamente triste pensare che il livello di sicurezza informatica nel mondo della

sanità potrà crescere più a seguito di applicazioni di elevate sanzioni, che non ad un aumento della sensibilizzazione dei soggetti coinvolti e dopo una crescita delle disponibilità economiche, che permettono di attuare appropriate misure di protezione.

D'altro canto, un applicativo di ransomware, che riesca a entrare nel mondo della sanità, può creare problemi assolutamente drammatici, sia nel brevissimo termine, ad esempio bloccando l'erogazione di farmaci da parte di distributori automatici, sia a medio termine, impedendo di acquisire informazioni atte a rendere più efficiente ed efficace il protocollo terapeutico dei pazienti.

Durante un recente esame delle circostanze afferenti ad una violazione dei dati personali, in ambito sanitario, gli inquirenti hanno accertato che il sistema informatico non era dotato di misure di sicurezza soddisfacenti, per non dire elevate, e che perfino la protezione antivirus delle workstation non era stata aggiornata da lunghissimo tempo.

Davanti a queste drammatiche situazioni, ci si rende conto che la sicurezza informatica nel mondo della sanità ha ancora tanta, ma tanta strada da compiere!

Adalberto Biasiotti

---

www.puntosicuro.it