

# Economia, 'Dati sensibili in sanità e sicurezza informatica'

**Autore :** Redazione

**Data :** 20 Agosto 2019



**A Lignano Sabbiadoro (UD) nel terzo incontro di 'Economia sotto l'Ombrellone', gli esperti in sicurezza informatica hanno sottolineato l'importanza di un confronto aperto tra programmatori e utilizzatori per difendere un patrimonio di dati prezioso**

*Riceviamo e pubblichiamo.*

Garantire la sicurezza dei dati sensibili in sanità, per ridurre i *data breach* che ogni anno costano all'Italia 3,5 milioni di dollari e la perdita o il furto di oltre 24.500 documenti sanitari, è principalmente una questione culturale e di consapevolezza, anche se, ovviamente, servono strumenti tecnici e normativi adeguati e maggiori controlli.

Nel nostro Paese negli ultimi anni si sono fatti molti passi in avanti, ma molto c'è ancora da fare perché in troppi, sia nel sistema sanitario, sia fra gli utenti, sottovalutano il problema.

Lo hanno sostenuto i relatori intervenuti al terzo incontro della nona edizione di 'Economia sotto l'Ombrellone' svoltasi ieri, lunedì 19 agosto, al Beach Aurora di Lignano Pineta (UD) sul tema 'Dati sensibili in sanità e sicurezza informatica', moderati dal giornalista Carlo Tomaso Parmegiani: il *data protection officer* dell'IRCCS 'Burlo Garofolo' di Trieste, Michele Bava, l'amministratore delegato di Karmasec, nonché uno dei principali esperti italiani di sicurezza informatica, Manuel Cacitti e Riccardo Furlanetto, socio e responsabile commerciale di Zulu Medical, azienda trevigiana che ha realizzato un sistema mobile *wireless* per la raccolta e gestione dei dati in emergenza che da oltre due anni è utilizzato con successo dal 118 dell'azienda sanitaria universitaria integrata di Udine e che sta venendo progressivamente adottato da altre aziende sanitarie.

Ha precisato Bava:

Quello che si può fare nelle aziende sanitarie per contrastare la perdita e il furto di dati sensibili è sicuramente alzare il livello di consapevolezza.

Ci sono, poi, aspetti normativi che possono aiutarci a seguire un percorso utile a proteggere le

informazioni che riguardano le persone.

Va anche detto che il ramo della sicurezza informatica è uno di quelli in cui le aziende fornitrici stanno investendo di più e, quindi, per fortuna, abbiamo a disposizione sempre migliori soluzioni tecnologiche per cercare di arginare il problema degli attacchi ai sistemi informatici sanitari che, purtroppo, sta dilagando non solo in Italia, ma in tutto il mondo.

Ha sostenuto Cacitti:

L'aspetto principale è rendersi consapevoli che oggi il dato assume un'importanza fondamentale, al punto che qualcuno parla del dato come quinto elemento dopo acqua, aria, terra e fuoco.

I dati, infatti, permettono di descrivere chi siamo e al contempo possono essere "monetizzati", tant'è che l'economia digitale si basa principalmente sulla capacità di generare valore dai dati, compresi quelli sanitari e sensibili di ciascuno di noi.

Può non piacere, ma è fondamentale esserne consapevoli. Va detto, comunque, che in tutto il settore sanitario ci sono diverse figure professionali che lavorano costantemente per garantire al meglio la sicurezza dei dati sensibili.

Riccardo Furlanetto, dal canto suo, ha sottolineato come lo sforzo principale da fare per migliorare la sicurezza dei dati in generale, e di quelli sanitari in particolare, sia soprattutto culturale:

Qualsiasi gestore di dati sensibili, dal privato al pubblico, deve crearsi una cultura di attenzione alla sicurezza dei dati. Fino a pochi anni fa, infatti, la sicurezza dei dati digitali sensibili era un tema che non veniva considerato.

Oggi, invece, viviamo di dati: pensiamo solo alla facilità con cui scarichiamo app o entriamo in siti lasciando in nostri dati in rete, spesso in modo molto "leggero".

Dal punto di vista di un'azienda come la nostra, dobbiamo utilizzare tutti gli strumenti giuridici e di controllo esistenti certificandoci secondo gli standard più elevati disponibili e dobbiamo aggiornarci giorno dopo giorno sulle minacce possibili per rendere i device che produciamo sempre più sicuri.

Prendendo spunto dal fatto che i *data breach* che colpiscono la sanità derivano per oltre il 50% non da attacchi informatici esterni, ma da perdite di dati generati da errori umani, i tre relatori intervenuti a *'Economia sotto l'Ombrellone'* hanno sostenuto che sicuramente c'è bisogno di una maggior formazione informatica del personale sanitario, soprattutto di quello meno giovane, ma è, forse, ancor più importante che gli strumenti informatici messi a disposizione di medici e infermieri siano semplici da usare.

Ha affermato Furlanetto:

Il mondo della sanità e quello dell'informatica sono mondi che hanno approcci e vivono situazioni spesso opposte. I sanitari sono, giustamente, concentrati sulla cura dei pazienti e non possono, né vogliono perdere tempo con "sofisticazioni" informatiche che fanno spesso la felicità dei programmatori e degli esperti del settore.

Chi, come noi, sviluppa i prodotti deve fare uno sforzo notevole operando in stretta sinergia con medici e sanitari per evitare di creare soluzioni "bellissime", ma che, poi, rischiano di rivelarsi poco

utilizzabili nella pratica quotidiana e, quindi, con il rischio di portare alla perdita di dati importanti a causa delle difficoltà di inserimento e trasmissione degli stessi.

Con il sistema adottato prima dall'Elisoccorso e poi dal 118 di Udine, sviluppato insieme ai medici e agli operatori, sono stati raccolti i dati relativi a oltre 25mila interventi in emergenza, in una situazione in cui, quindi, la facilità di utilizzo degli strumenti è assolutamente irrinunciabile.

Secondo Manuel Cacitti, spesso l'errore umano incide non necessariamente sulla perdita completa del dato, ma sulla sua disponibilità e/o integrità, il dato esiste, ma non è più leggibile o è parzialmente corrotto.

Questo avviene

perché spesso i sistemi sono complessi da gestire. Sono, cioè, magari progettati bene per quanto riguarda l'efficienza, i costi, la scalabilità, ma senza tenere conto della sicurezza.

È un aspetto più importante di quanto si pensi comunemente, tant'è che l'ultimo regolamento europeo sul tema sottolinea l'importanza di concetti come quelli della security by design e security by default per indicare come spesso la sicurezza dipenda in buona parte da come le architetture informatiche sono progettate.

Lo stesso si può dire per quanto attiene all'usability di un sistema. Se volete un sistema usabile non fatelo progettare a un informatico che lo farà secondo logiche che capisce solo lui, ma chiedete che sia progettato insieme al futuro utente.

A portare l'esperienza diretta di chi tutti i giorni ha a che fare con gli strumenti informatici utilizzati negli Ospedali è stato Michele Bava:

Il programmatore spesso non è interessato all'usabilità di ciò che progetta, mentre i medici hanno bisogno di qualcosa di molto semplice, facile e veloce da utilizzare.

Inoltre, per mentalità gli informatici lavorano sulla fisiologia dei sistemi, cioè sul mantenimento quotidiano dell'efficienza degli stessi, mentre i medici sono abituati a intervenire sulle patologie, ovvero su "sistemi" che si sono danneggiati e che vanno "riparati" subito; solo che non sempre un sistema informatico danneggiato è riparabile con un intervento immediato. Ovviamente, sono due visioni quasi antitetiche, non facili da conciliare.

Spesso, poi, non è semplice conciliare le esigenze di sicurezza con le abitudini degli operatori che non di rado considerano le password e le altre procedure di sicurezza come noiosi fastidi, mentre la cultura della privacy va vista non come un impedimento ma come un'opportunità. Davanti a singoli comportamenti poco attenti, infatti, non c'è norma o sistema di controllo tecnologico che possa garantire sicurezza.

La nona edizione di *'Economia sotto l'Ombrellone'* è organizzata da Eo Ipso - comunicazione ed eventi ed ha il patrocinio del Comune di Lignano Sabbiadoro e Turismo FVG.

*Main sponsor:* Greenway Group. *Sponsor:* Ombrellificio Ramberti, IS Copy Trieste, Dvs, Glp, Confindustria Udine, Zulu Medical, RealComm e Karmasec. *Sponsor tecnici:* Fondazione Villa Russiz, Lignano Pineta, Porto Turistico Marina Uno e Hotel Ristorante President.

Il prossimo incontro:

Lunedì 26 agosto ore 18:30

*'Il lavoro c'è. Come trovarlo?'*

Daniele Arman - Responsabile risorse umane Bofrost Italia Spa

Denis Magro - Amministratore unico di Run4job Srl

Giorgio Ardito - Presidente Lignano Pineta Spa

Modera: Carlo Tomaso Parmegiani, giornalista e responsabile editoriale Nordest di Eo Ipso

L'ingresso è libero e gratuito.

Al termine, aperitivo offerto da Fondazione Villa Russiz.