Corriere delle Comunicazioni
Quindicinale
Data 23-01-2012
Pagina 30
Foglio 1 / 2

Proposte

SICUREZZA E-HEALTH MANCA UN CAPITANO

PAOLINO **MADOTTO***

Dati sanitari e sicurezza. Un binomio inscindibile in un momento in cui si rende necessaria - per motivi economici e di efficienza del sistema sanitario nel suo complesso - la digitalizzazione della macchina amministrativa. Il punto sullo stato dell'arte delle aziende sanitarie (Asl) in Italia è fatto da una ricerca del Link Campus di Roma che fa capo all'Università di Roma "Tor Vergata". Attraverso questo lavoro si è cercato di porre luce su questo mondo somministrando un questionario alle Asl italiane. Gli assi portanti della ricerca sono stati quelli tipici della sicurezza Ict: "Disponibilità" intesa come la capacità dei sistemi di fornire in ogni momento i dati; "Integrità" intesa come la capacità di proteggere le informazioni da modifiche non autorizzate; "Confidenzialità" capacità del sistema di garantire l'accesso alle sole persone autorizzate.
La popolazione sotto esame è stata di 146 Asl di cui il 58% ha risposto; un dato importante anche se il 42% di aziende sanitarie che decidono di non rispondere apre un enorme interrogativo sulla trasparenza della pubblica amministrazione. Sembra infatti che la cultura della PA sia ancora troppo ancorata all'idea di coprire le proprie lacune anziché farle venire alla luce per colmarle.
I primi problemi cominciano dagli stanziamenti ed evidenziano - sulla base dei dati presenti sul sito del ministero della Salute - che la spesa pro-capite delle aziende sanitarie è di 1.800 euro anno, di cui solo 6,7 speso in IT: questo dato differisce da quanto indicato da Assinform 2011 perché questo è riferito su tutta la spesa sanitaria).

Asl, solo il 58% risponde ai questionari
Tiene duro una cultura che punta a coprire le lacune più che a superarle

Se poi leggiamo il dato procapite per macro-regioni scopriamo che al sud si spendono solo 5,0 euro mentre al nord 6,9 euro e che al sud vi sono circa 500mila abitanti per Asl contro i 362,636 del nord.
Per la sicurezza le Asl ogni anno spendono nel 73,5% dei casi meno di 0,25 euro procapite, con punte di 0,12 euro nel 45% dei casi. Una spesa insufficiente rispetto al rischio di perdere dati.
Ciò che è emerso dalla ricerca è una situazione preoccupante segnata da un approccio formale che nasconde una situazione molto simile a quella di cinque anni fa. Basta pensare che nel 38% dei casi non esiste alcun controllo diretto sui dati gestiti da strutture accreditate.
In questo panorama non possiamo stare tranquilli parlando di "cloud" e eHealth. Dall'indagine risulta che oggi le aziende sanitarie si rivolgono per il 69% a strutture esterne e per il 60% circa sono dati sensibili. La percentuale non è molto differente rispetto a cinque anni fa, anche se sono aumentati del 20% i dati sensibili gestiti all'esterno. Solo nel 58% dei casi si sentono confidenti che i dati non possono essere trafugati da maleintenzionati.
Questo malgrado l'esistenza di regole per l'accesso e, nel 65,5% dei casi, un programma di formazione specifico. Dal punto di vista della disponibilità, in un paese fortemente segnato da continui rischi idrogeologici, emerge che solo il 23% delle strutture è in grado di ripristinare i dati entro un giorno e il 40% entro tre giorni. Mentre solo il 39% delle aziende sanitarie ha un sito alternativo. Nel 70% dei casi non si prova mai la capacità della struttura di rispondere ad un evento catastrofico, eppure i dati sanitari sono quelli più necessari durante le situazioni di crisi.
La ricerca mette in luce una situazione marcata da un approccio formale, la 196/03 e il nuovo Codice dell'amministrazione digitale (Cad) appaiono nei fatti inapplicate. Ciò che più manca

Corriere delle Comunicazioni
Quindicinale
Data 23-01-2012
Pagina 30
Foglio 2 / 2

sono stanziamenti adeguati al rischio e, ancora più importante, la necessaria cultura della sicurezza e della governance del'IT. Sembra che si stia investendo in grandi soluzioni applicative (eHealth) senza porsi il problema di mettere qualcuno alla porta per proteggerle.

In questo contesto anche il Garante per la Protezione dei dati personali, Francesco Pizzetti ha evidenziato la funzione di supplenza dell'authority rispetto ad un organismo di governance dell'IT nella PA. Ciò che emerge dai dati è la mancanza di un organismo in grado di dare indicazioni sulla sicurezza e sulla governance, di avere un quadro unitario e sistemico. L'Aipa non ha saputo raggiungere tale obiettivo, mentre DigitPA non ha questa missione prioritaria. Manca una struttura in grado di emanare linee guida cogenti, buone pratiche, vigilare sul patrimonio di dati e applicazioni e la sua gestione, avere un master plan delle grandi progettualità in corso. Appare difficile mantenere una rotta senza un "cruscotto" e un capitano. ▲

Centro Alta Tecnologia Link Campus University


SICUREZZA E-HEALTH MANCA UN CAPITANO

I Garanti europei controllano Carrier IQ