Security Management ospedaliero: la Regione Lazio apre all'istituzione di una figura fondamentale

Date : 29 Luglio 2020

Chi non osa nulla, non speri in nulla
Friedrich von Schiller

Ho affrontato più volte, in questi anni, il tema della **security** in ambito ospedaliero; un mondo, quello dei servizi sanitari, straordinariamente complesso sotto l'aspetto della sicurezza anticrimine, informatica, dell'incolumità personale (sia dei dipendenti che dei pazienti ricoverati), senza contare le problematiche connesse al furto di oggetti personali.

Peraltro, quello della sanità rappresenta uno dei settori strategici di un **sistema paese**: un insieme di risorse, assetti, personale e istituzioni finalizzato a tutelare la salute pubblica, e dunque un'alterazione delle sue capacità nell'erogare prestazioni produrrebbe un impatto negativo e diretto sulla collettività.

In un settore dove la spesa pubblica ha un peso significativo, circa il 9% del PIL, la sicurezza diventa un requisito di primaria importanza, come la protezione dei suoi assetti assume una connotazione di interesse nazionale; un comparto appartenente alle cd. **Infrastrutture Critiche** (IC), secondo quanto indicato nella **Direttiva 114/2008**: *"sono infrastrutture critiche tutti quegli elementi e sistemi essenziali per il mantenimento delle funzioni vitali della società, della salute della sicurezza e del benessere economico e sociale dei cittadini..."*

Un'azienda ospedaliera, al di là delle sue dimensioni, ha delle **vulnerabilità intrinseche** di difficile gestione, dal punto di vista *safety* e *security*; ad esempio il *triage*, struttura operativa della medicina e chirurgia di accettazione e di urgenza (MeCAU), caratterizza un'area decisamente critica da gestire, dal punto di vista della sicurezza pubblica e dello stesso personale medico, dove il rischio di manifestazioni estreme, che sfociano puntualmente in vere aggressioni fisiche, sono avvenimenti quotidiani.

Altro esempio: in ogni struttura sanitaria sono presenti i servizi di ristorazione per i dipendenti e i pazienti residenti; inoltre, la relativa giacenza di merci e alimenti espone un ospedale a diversi rischi criminogeni, come reati predatori o, peggio ancora, atti di sabotaggio; e qui si apre uno scenario decisamente particolare, perché si entra nella sfera della *food safety* e *security*, due concetti tra loro complementari, che rappresentano due accezioni di sicurezza differenti ma

strettamente correlate.

Per non parlare poi della vulnerabilità delle farmacie ospedaliere, vere e proprie casseforti - in termini di valore economico – dove sono custoditi farmaci, presidi sanitari, attrezzature e apparecchiature sanitarie per la diagnostica, di appetibile valore sul mercato della ricettazione.

Tuttavia, nell'attuale contesto sociale colpito dalla pandemia da Covid-19, è estremamente importante occuparsi anche della *cyber security* del settore sanitario, perché qui si pone un problema ancora più importante del "solo" rischio che vengano sottratti beni materiali o cartelle cliniche dagli archivi; quello che preoccupa maggiormente il *management* ospedaliero sono gli apparati medici, di cura e diagnostica - soprattutto quelli della medicina nucleare – esposti ormai a continui **attacchi informatici**, sia esterni che interni.

Dunque nel settore *Healthcare*, l'emergenza pandemica evidenzia nuovamente un nervo da sempre scoperto, che stavolta non è solo sanitario o di carenza nelle risorse professionali mediche: stavolta la problematica è contestualmente di *physical* e *cyber security*, due elementi che la dicono lunga sulla **convergenza**, spesso sottovalutata, tra sicurezza **fisica** e **logica**.

D'altronde, basterebbe riflettere sull'allarme, comunicato lo scorso aprile dall'FBI, sul pericolo di attacchi al sistema sanitario, informazione raccolta e rilanciata poi dall'Europol; in buona sostanza, i federali statunitensi focalizzano l'attenzione sull'*escalation* di attacchi portati a segno con una tipologia di *malware* nota come **Kwampirs**, un **patogeno informatico** che colpì anche in Italia: ne fu vittima illustre l'ospedale Spallanzani di Roma, come pure l'ospedale universitario di Brno (Repubblica Ceca), che si ritrovò con l'intera rete IT *off*!

Come non potremmo mai dimenticare un altro attacco, quello subito dal sistema sanitario Britannico, pesantemente aggredito nella primavera 2017 dall'epidemia informatica da virus WannaCry; una **tecnoinfezione** veicolata attraverso una vulnerabilità di Microsoft Windows contenuta nei sistemi sanitari non aggiornati, e costata al *National Health Service (NHS)* circa 100 mln di £.

Come visto fin qui, non c'è solo un aspetto di sicurezza fisica delle infrastrutture e di salvaguardia dell'incolumità fisica da considerare: è l'accesso alle informazioni e ai dati clinici del paziente che consente, non solo di rubare, ma di modificare le cartelle cliniche personali, inquinando pericolosamente la diagnostica.

Cosa fare, allora?

Appare evidente come una tale risposta la possa dare solo un **professionista della sicurezza ospedaliera**, figura oggi pressoché assente dal panorama sanitario nazionale, salvo rarissimi e virtuosi casi.

L'istituzione obbligatoria del *Security Manager* presso le grandi aziende ospedaliere è cosa ormai irrimandabile, perché rappresenta l'interfaccia specializzata – nello scambio delle informazioni con le altre istituzioni - che raccoglie, analizzandoli, tutti gli elementi necessari per impostare programmi di sicurezza - *cyber, security e safety* -, che vanno dall'utilizzo di

tecnologie specializzate applicabili al perimetro della sicurezza logica, fino all'uso di infrastrutture tecniche e risorse umane per garantire il perimetro della sicurezza fisica, a tutto vantaggio della sicurezza pubblica.

Ciononostante, solo con un approccio trasversale e integrato, progettato e realizzato da un professionista della *security*, possiamo trarre tutti quei benefici attesi da un programma ben articolato e incisivo; peraltro, avere un unico referente a stretto contatto con il *management*, evitando pericolosi errori comunicativi provenienti dai diversi reparti e sottostrutture ospedaliere, rappresenterebbe un'ulteriore e robusta garanzia.

Difatti, la prova di quanto detto fin qui è nei risultati tangibili conseguiti da tutte quelle strutture ospedaliere – ancora poche - che hanno scelto questo percorso, dimostrando come l'**approccio unitario** sia l'unico che consente di ottenere risultati estremamente efficaci, con ricadute economiche decisamente concrete.

Ecco perché, immediatamente dopo l'esplosione epidemica, siamo tornati - con altri professionisti del settore - a riparlare per l'ennesima volta della figura del *manager* della *security* all'interno degli ospedali. Una figura che va resa obbligatoria, al pari dei DPO, in tutte le strutture mediche complesse, pubbliche e private, perché in questi mesi emergenziali l'assenza di una tale professionalità nella gestione dei protocolli di *security* all'interno dei nosocomi si è fatta sentire: pochi sapevano gestire una procedura di sicurezza, mettere in campo un normalissimo assetto di vigilanza, o semplicemente interfacciarsi con gli stessi IVP, con le FF.OO., gli uffici della prefettura o il dipartimento di protezione civile!

Già sette anni fa, il problema fu messo all'attenzione del ministero competente; nel gennaio 2014 fu presentata alla Camera, a firma dell'On. Alessio Villarosa, un'**interrogazione** all'allora Ministro dell'interno proprio sulla mancata integrazione della figura del *Security Manager* all'interno della filiera della **sicurezza** nazionale del sistema paese.

In questi mesi di *lockdown,* parlando della questione con l'On. Giancarlo Righini, del Consiglio regionale del Lazio, spiegavo quale delicato e importante ruolo rimaneva ancora scoperto all'interno delle caselle che compongono l'architettura gestionale della sanità ospedaliera regionale. Ne parlavamo commentando una **legge** approvata dal parlamento qualche mese prima, che istituiva obbligatoriamente la figura del *Security Manager*, ma solo all'interno del generico "perimetro cibernetico".
Da questa nostra discussione capimmo l'importanza, anche alla luce di quanto accaduto con l'emergenza Covid, di portare la cosa anche all'attenzione del Consiglio regionale, perché un argomento così strategico, vitale per la sicurezza sociosanitaria nel complesso sistema sanitario regionale, andava affrontato in aula: elaborammo così un testo di **mozione** che fu presentato per la discussione di rito e, dopo un'attenta analisi, approvato all'unanimità!

Auguriamoci che questo nuovo atto politico possa far scuola a livello nazionale, riempiendo il vuoto normativo che ancora permane nell'ambito della *security* ospedaliera.

Articolo a cura di **Giovanni Villarosa**