Capitolo 10

LO SMARTPHONE IN UN SONDAGGIO SULLE CONOSCENZE DI CYBERSECURITY IN SANITÀ

Daniele Giansanti (a), Mauro Grigioni (a), Lisa Monoscalco (b), Rosario Alfio Gulino (b)
(a) Centro Nazionale Tecnologie Innovative in Sanità Pubblica, Istituto Superiore di Sanità, Roma
(b) Facoltà di Ingegneria, Università di Tor Vergata, Roma

Cybersecurity in sanità

Recentemente si è assistito ad un crescente interesse verso la sicurezza informatica. Hanno fatto molto eco in passato gli attacchi informatici nel settore dell'industria e dei consumi e preoccupano i recenti attacchi informatici nel settore sanitario. Recentemente, ad esempio, al centro del dibattito sono stati gli attacchi, ad esempio di tipo *ramsonware*, nei sistemi sanitari e le potenziali vulnerabilità venute alla luce per alcune tipologie di dispositivi medici critici (per lo più impiantabili attivi) che possono essere connessi in rete. Nel delicato settore della sanità europeo si è generalmente registrato un ritardo nell'affrontare le tematiche di cybersecurity rispetto agli USA. Questo è dovuto al fatto che negli USA il mondo della Salute è senza ombra di dubbio un'industria, non solo a livello di percezione, ma nella pratica: l'approccio al problema è stato infatti in USA identico a quello avuto in generale verso il mondo dell'industria e dei consumi.

Solo recentemente in Europa, e quindi in Italia, si è iniziato ad affrontare il problema con la dovuta attenzione. Nel settore sanitario, oggi la criticità relativa alla straordinaria diffusione delle tecnologie innovative (es. pancreas artificiale) connesse in rete nell'ambito sanitario (oltre 300.000 classi di dispositivi medici) si intrecciano inevitabilmente con le caratteristiche di sicurezza ed efficacia dei servizi erogati e la protezione dei dati trattati, creando un contesto di elevata attenzione dove effettuare analisi quantitative dipende dalle informazioni inserite nei Sistemi sanitari, mentre l'analisi della sensibilità degli operatori può essere rilevante per i loro comportamenti.

Obiettivo dello studio

Una trattazione ampia della problematica esula naturalmente dagli obiettivi di questo lavoro in quanto necessiterebbe quanto meno il coinvolgimento di un ampio gruppo di esperti con competenze diverse nel sistema sanitario nazionale, nelle tecnologie, nella regolamentazione. L'obiettivo del lavoro, nello spirito del rapporto è quello di posizionare lo smartphone nel settore della cybersecurity in sanità. Non vi è dubbio che lo smartphone possa essere un veicolo di *cyber-risk* se connesso a dispositivi medici e questo meriterebbe una indagine mirata di ampio respiro con le premesse di cui sopra. Ma un ruolo che può sicuramente avere lo smartphone è anche quello sicuramente di attore in analisi sulla situazione e percezione del problema della cybersecurity attraverso lo sviluppo e la somministrazione di sondaggi.

In questo studio è stato pertanto sviluppato un questionario destinato agli operatori sanitari per analizzare la situazione e la percezione del problema della cybersecurity in sanità, ed è stato sottoposto ad un primo campione per testarne la robustezza.

Sviluppo e somministrazione di un questionario sulle conoscenze di cybersecurity in sanità

Il questionario elettronico composto di 30 domande, sviluppato utilizzando *Forms*, è stato sottomesso ad un primo campione di 55 soggetti operanti nel settore sanitario in uno studio in collaborazione tra il Centro Nazionale Tecnologie Innovative in Sanità Pubblica dell'Istituto Superiore di Sanità e l'Università di Tor Vergata condotto nel 2018-2019 a Roma.

La Figura 1 illustra la distribuzione della popolazione degli intervistati.

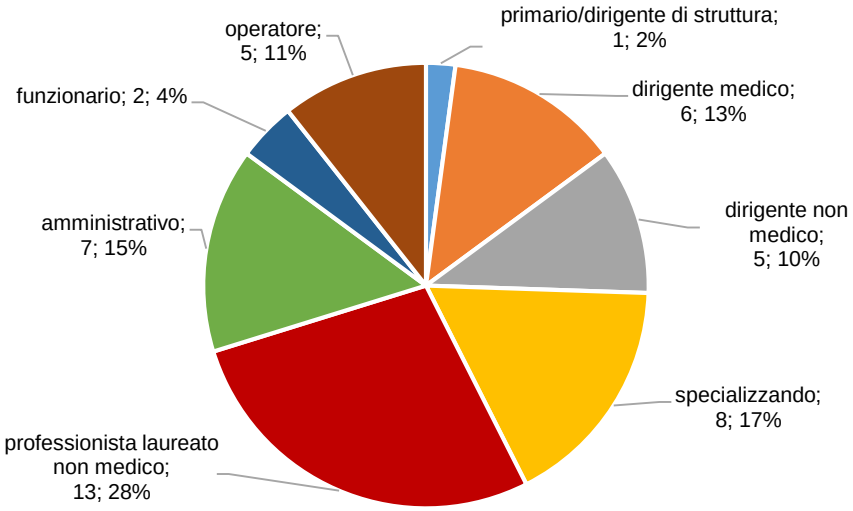

Figura 1. Composizione del campione intervistato

Diverse domande erano a valutazione con punteggio gradato (1 = minimo; 5 = massimo). La sottomissione a 55 operatori sanitari di diverse professionalità, condotta anche per verificare la robustezza della metodologia non ha mostrato criticità nella distribuzione e raccolta in rete. Al momento si sta ampliando il campione. Seguirà un *data mining* mirato

Da una prima analisi si evidenzia: a) una autopercezione di sicurezza nel proprio ambiente pari a 2,78 b) un desiderio di investire sulla formazione in questo ambito.

Le conoscenze generali relative alla cybersecurity hanno ricevuto un punteggio pari a 2,65. Sebbene la maggior parte degli intervistati (91%) affermi che "nonostante la digitalizzazione del settore sanitario abbia portato dei problemi a livello di sicurezza, i benefici che ha comportato siano superiori ai possibili rischi" (Figura 2); solamente il 35% ritiene che le iniziative destinate alla cybersecurity siano adeguate (Figura 3); solamente il 29% ha frequentato corsi di formazione (Figura 4) e il 64% auspica una introduzione di corsi specifici (Figura 5).

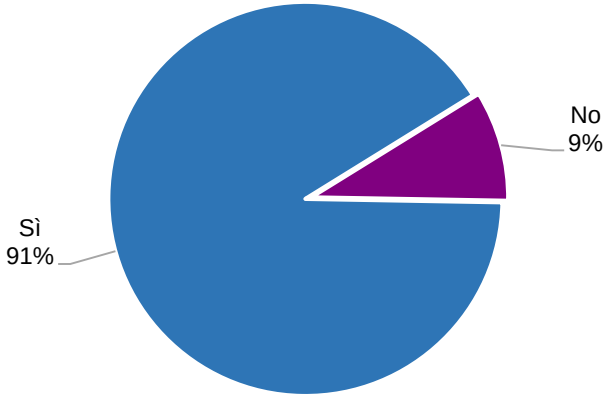

Figura 2. Percezione dei benefici della digitalizzazione nonostante i rischi informatici

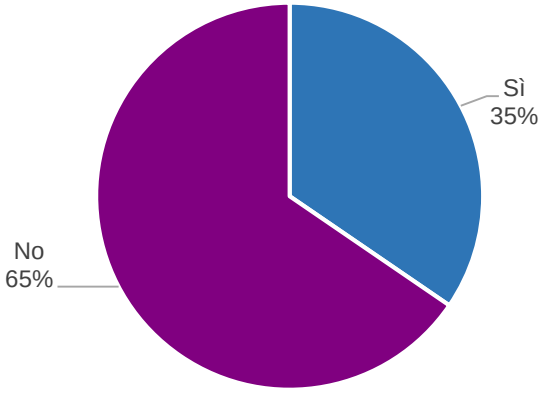

Figura 3. Percezione dell'adeguatezza delle iniziative sulla cybersecurity da parte degli operatori

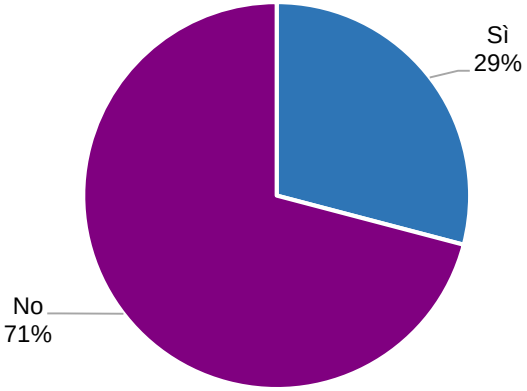

Figura 4. Partecipazione ad appositi corsi di cybersecurity da parte degli operatori

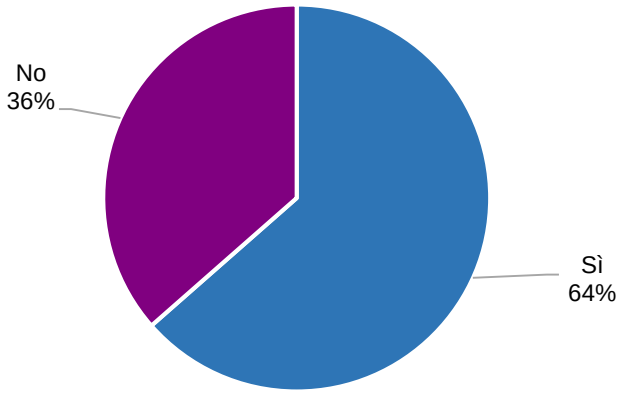

Figura 5. Necessità di introduzione di corsi sulla cybersecurity negli ospedali per gli operatori

Conclusioni e sviluppi futuri

Tale contributo è stato sviluppato tra il Centro Nazionale Tecnologie Innovative in Sanità Pubblica e la Facoltà di Ingegneria dell'Università di Tor Vergata in Roma, attraverso una collaborazione su tesi nel corso di laurea Magistrale in Ingegneria Medica. Nello studio è stato presentato un sondaggio destinato agli operatori sanitari per analizzare la situazione e la percezione del problema della cybersecurity in sanità. Tale questionario sviluppato elettronicamente in *Forms*, sottomesso ad un primo campione per testarne la robustezza, si è dimostrato robusto in ogni fase della somministrazione. Da una prima analisi focalizzata sulla conoscenza, formazione e pratiche di cybersecurity sono emersi alcuni aspetti interessanti relativi alla percezione di cybersecurity nel proprio ambiente di lavoro e un forte desiderio di formazione in questo ambito. Un ulteriore *data mining* permetterà di approfondire ulteriori aspetti relativi a problematiche ruotanti attorno alla cybersecurity.

La metodologia presentata sicuramente potrà essere utilizzata in applicazioni di ampio respiro nell'ambito della cybersecurity dove sicuramente un punto di partenza importante è quello dell'analisi delle conoscenze dei *desiderata* e delle preoccupazioni degli attori del Servizio Sanitario Nazionale.