Innovation and Technology Transfer

Il ruolo del Centro TISP nella sicurezza dei cybersistemi dall'informazione/formazione alla ricerca.†

Daniele Giansanti,[a] Sandra Morelli,[a] Giuseppe D'Avenio,[a] Mirko Rossi,[a] Alessandro Spurio,[a] Maurizio Lucentini,[a] Giovanni Maccioni,[a] Mauro Grigioni.[a]

1 Evidenze di criticità nei sistemi interconnessi. Cybersecurity

Nella recente decade si è assistito ad un crescente interesse verso la sicurezza informatica. Nel recente passato gli attacchi informatici nel settore dell'industria e dei consumi hanno fatto molto clamore, e preoccupano i recenti attacchi informatici nel settore sanitario. Ad esempio, al centro del dibattito sono stati gli attacchi di tipo ramsonware che hanno colpito alcuni sistemi sanitari (specialmente in UK) 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. In Europa, nel settore critico della sanità 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 (ad 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 la possibilità di effettuare analisi quantitative dipende dalle informazioni inserite nei sistemi sanitari, mentre l'analisi della sensibilità e delle competenze informatiche degli operatori può essere rilevante per i loro comportamenti.

2 Il gruppo nazionale di cybersecurity

Nel marzo 2018 è nato il primo gruppo di studio a livello nazionale per la costruzione di un sistema di sicurezza dei dati informatici nei servizi sanitari. Il gruppo di studio, coordinato dall'Istituto Superiore di Sanità, é nato da un'iniziativa congiunta del Centro Nazionale per la Telemedicina e le Nuove Tecnologie Assistenziali e del Centro Nazionale di Tecnologie Innovative in Sanità Pubblica in collaborazione con vari enti ed organismi, la Polizia Postale e delle Comunicazioni e vede la partecipazione di molti esperti appartenenti a diverse università italiane. L'obiettivo è quello di sviluppare le conoscenze e le metodologie di difesa dei sistemi informativi utilizzati quotidianamente in ambito sanitario ed è per la prima volta perseguito in una sinergia tra Istituzioni. Il sistema sanitario italiano potrà infatti svilupparsi in modo ordinato e sicuro soltanto assicurando la protezione dei dati sanitari dei cittadini in modo uniforme su tutto il territorio nazionale, rispetto agli attacchi informatici. Il Gruppo studia strategie specifiche per migliorare costantemente la difesa delle strutture sanitarie del Paese da attacchi informatici di varia natura e si occuperà degli aspetti di formazione per le professioni sanitarie, con l'obiettivo di maggiore stimolare una adeguata consapevolezza dei rischi cyber in sanità, diffondere la conoscenza tecnica e raccomandare le migliori pratiche di protezione.

3 L'attività in ISS

Il termine cybersecurity è relativamente recente, ma in realtà riprende problematiche relative alla sicurezza dei sistemi di elaborazione connessi in rete in modo interoperativo. In passato in ISS tali problematiche sono state affrontate in diversi ambiti sia in modo specifico che perimetrale. A titolo non esaustivo si possono citare alcune esperienze di technology assessment in telemedicina[1] dove nelle metodologie proposte si è tenuto in conto anche di alcune problematiche che oggi afferirebbero alla cybersecurity, o altre sempre in telemedicina ma focalizzate sulla stesura di linee guida in teleradiologia,[2] dove naturalmente particolare rilevanza è stata data anche agli aspetti di sicurezza e privacy che oggi afferirebbero alla cybersecurity. Dalla costituzione del Gruppo nazionale sono state avviate in ISS anche una serie di attività specifiche che comprendono la formazione, l'informazione, la creazione di un laboratorio di cybersecurity, la focalizzazione su lavori di tesi specifici nell' ambito della terza missione, la disseminazione di risultati di ricerca interna all'ISS su aspetti ed elementi di cybersecurity. Tra queste attività si evidenziano (a) i progetti di Alternanza Scuola-lavoro volti a sensibilizzare i giovani adolescenti su queste problematiche,[3,4] e le mostre (b) tenute

[a] *Centro TISP, Istituto Superiore di Sanità (ISS), Roma email: mauro.grigioni@iss.it*

† presentato a @ITIM 2019 - 19° Congresso Nazionale Associazione Italiana di Telematica ed Informatica Medica 11-12 Novembre 2019, Matera/Potenza.

nella Notte Europea dei Ricercatori;[5] entrambe tali attività sono state svolte in collaborazione con il Centro TETA. Si sono svolte inoltre altre attività di terza missione quali quelle di tesi sviluppate in collaborazione con diverse università come l'Università di Tor Vergata e della Sapienza. In una di queste collaborazioni è stata sviluppata una survey sulla percezione del problema della cybersecurity. Tale survey si è basata su forms ed è stata diffusa attraverso Whatsapp a professionisti sanitari per analizzare la situazione e la percezione del problema della cybersecurity in sanità. I risultati sono consultabili in[6]. In un'altra collaborazione sono state analizzate inoltre molte problematiche connesse a dispositivi medici che si aprono a rischi di cyberattacchi proprio per il fatto che, per esigenze di adattamento terapeutico, si aprono al mondo esterno attraverso la condivisione in rete. Tra questi DM uno dei più critici è sicuramente il pancreas artificiale (PA),[7] che rappresenta una vera e propria palestra per la cybersecurity essendo un sistema eterogeneo e complesso connesso in rete. In un sistema eterogeneo quale è il PA la connessione wireless, che permette alle componenti di comunicare tra di loro e che utilizza anche uno smartphone, crea un ambiente suscettibile agli attacchi cibernetici. A titolo di esempio non esaustivo, se la connessione tra dispositivo wearable per il monitoraggio continuo del glucosio e il microcontrollore nello smartphone non fosse sicura, un malintenzionato potrebbe inviare dati deliberatamente errati all'algoritmo di controllo il quale potrebbe determinare il rilascio di un'elevata quantità di insulina determinando una situazione di ipoglicemia nel paziente; il corpo risponderebbe alla condizione di ipoglicemia attraverso il rilascio di glucagone ed epinefrina: perdurando tale situazione per un tempo sufficiente, verrebbero compromesse le funzionalità cerebrali, motorie e cognitive, fino anche a causare la morte.

Bibliografia

1 D. Giansanti, S. Morelli, V. Macellari, Telemedicine technology assessment part i: setup and validation of a quality control system, Telemedicine and e-Health 13 (2) (2007) 118–129.

2 A. Orlacchio, P. Romeo, M. Inserra, G.Grigioni, D.Giansanti, Guidelines for quality assurance and technical requirements in teleradiology. Istituto Superiore di Sanità, Rapporti ISTISAN 13/38 (2013).

3 S. Salinetti, P. D. Castro, M. Barbaro, E. Ambrosini, C. Agresti, Alternanza scuola lavoro in ISS. Riflessioni a tre anni di attività, Notiziario dell'Istituto Superiore di Sanità 31 (2018) 3–7.

4 Catalogo delle attività dell'Istituto Superiore di Sanità per le scuole, Vol. IV, 2019.

5 A. Rossi, M. Barbaro, S. Salinetti, B. Caccia, C. Agresti, E. Ambrosini, P. De Castro, La notte europea dei ricercatori: un successo in crescita. Notiziario dell'Istituto Superiore di Sanità (2018).

6 D. Giansanti, M. Grigioni, L. Monoscalco, R. A. Gulino, A smartphone based survey to investigate the cyber-risk perception on the health-care professionals, in: Mediterranean Conference on Medical and Biological Engineering and Computing, Springer, 2019, pp. 914–923.

7 U. Ferrante, M. Grigioni A.R. Gulino, Diabetes Technologies: Evolution, Modeling and Evaluation of Perspetives Through New Methods of HTA, International Congress ICEHTMC, Roma 20-23 ottobre 2019.