Lettere dalla terra di mezzo della sanità digitale (2) – 3 Gennaio 2018

# Cybersecurity nella sanità digitale ai tempi dell'IoT: la splendida opportunità di una tempesta perfetta (*ovvero: La Battaglia dei 5 Eserciti)*

Quando ho cominciato a scrivere queste note ero in treno e stavo tornando da Roma, dove avevo partecipato al "Forum sui dispositivi medici" organizzato dal Ministero della Salute. Avevo ancora negli occhi la saletta strapiena (con molte persone in piedi) e gli sguardi attenti dei partecipanti, nonostante uno slittamento di agenda che aveva fatto sì che il tema cybersecurity fosse stato relegato dalle 12:30 alle 14 (con tutti a digiuno, perché la pausa pranzo è stata concessa rigorosamente solo dopo le 14!). Anche ora, ripensando a mente fredda a quella giornata così ricca di contenuti e di stimoli (http://www.forumdispositivimedici.it/), non mi esce dalla testa il pensiero che probabilmente siamo alla vigilia di quello che qualcuno potrebbe definire "La battaglia dei cinque eserciti": uomini, nani ed elfi contro lupi mannari ed orchi. Il perché lo capirà chi avrà la pazienza di arrivare alla fine di queste righe.

La cybersecurity è da sempre uno dei temi che affascinano di più nell'Information Technology: un mix di tecnologia avanzata, di figure quasi leggendarie e romanzesche come gli hacker incappucciati, o gli attivisti con la maschera di Guy Fawkes di Anonymous, di luoghi comuni, di paure più o meno razionali e di aneddoti inquietanti. Quando qualcuno mi dice "voi informatici siete strani" (a chi di noi non è capitato?), di solito rispondo: dovresti provare a frequentare gli informatici esperti di cybersecurity. Lo dico con affetto, perché in questo ambito ho incontrato le figure professionalmente (e spesso anche umanamente) più interessanti in assoluto. Nell'ambito del forum sui dispositivi medici poi, l'interesse era acuito dagli ultimi eventi recenti, in particolare dalla Field Action dell'FDA americana sui pacemaker della Abbot[1], che si sono dimostrati vulnerabili. Il testo originale dell'FDA dice espressamente che: "queste vulnerabilità, se sfruttate, potrebbero permettere a un utente non autorizzato (i.e. qualcuno che non sia il medico del paziente) di accedere al dispositivo usando apparecchiature disponibili in commercio. Questo accesso potrebbe essere utilizzato per modificare i comandi di programmazione del pacemaker impiantato e ciò potrebbe causare danni al paziente dovuti a un rapido esaurimento della batteria, o alla somministrazione di stimolazione inappropriata"[2]. Inquietante, anche perché penso che molti altri produttori di impiantabili siano nella stessa situazione della Abbot. Il fatto che i dispositivi medici, tra cui anche gli impiantabili, siano tra i device informatici meno sicuri e più facili da manipolare o manomettere anche a distanza è un fatto noto. Se io fossi un hacker (o un cracker, direbbero i puristi) e volessi fare un danno ad una persona o un'azienda, non avrei dubbi: oggi è molto più facile hackerare un pace-maker o una pompa ad insulina, che un telefonino (e ovviamente non è per niente difficile hackerare un telefonino…). Situazione paradossale, anche se ci consoliamo dicendoci che non ci sono

[1] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm
[2] La traduzione è mia, il testo originale dell'FDA è: "These vulnerabilities, if exploited, could allow an unauthorized user (i.e. someone other than the patient's physician) to access a patient's device using commercially available equipment. This access could be used to modify programming commands to the implanted pacemaker, which could result in patient harm from rapid battery depletion or administration of inappropriate pacing."

ancora stati casi di questo tipo di attacchi (non so con quale consapevolezza lo si affermi). In realtà ci sono altri paradossi singolari su cui riflettere nell'ambito della sicurezza informatica in sanità. Ne cito tre:

- Paradosso #1: **«Ci son più cose in cielo e in terra, Orazio, che non sogni la tua filosofia» (Amleto). Ossia: ci sono più informazioni nello «shadow IT» che nell'IT Ufficiale.** Qualche esempio? Da un report CISCO del 2015[3] dall'originale titolo: "Conosci la strada per Ballylickey", si evince che i dipartimenti IT mediamente stimano in 51 i servizi cloud usati dalla propria azienda, mentre in realtà la media è di 730. Un errore di stima del 1300% circa. Per fare poi qualche esempio rispetto al contesto sanitario, i dati gestiti dai sistemi informativi attraverso i sistemi tradizionali ormai sono solo una piccola parte rispetto alle informazioni generate e gestite da altri dipartimenti, come l'Ingegneria Clinica o i servizi tecnici. Per non parlare dei dati "auto-gestiti" (in modalità cloud o meno) dai clinici e dagli altri utenti.

- Paradosso #2: **In sanità, i sistemi più critici e i dati più sensibili dal punto di vista della sicurezza (sia come security che safety) sono in una «terra di nessuno».** Il caso dei pacemaker citato è un esempio, ma non è l'unico. Durante il suo intervento M. Rizzetto di AIIC[4] ha citato il report: "Top 10 Health Technology Hazards for 2018" dell'istituto ECRI[5], una bibbia per gli ingegneri clinici, che mette come rischio tecnologico n. 1 per i pazienti: "Ransomware e altre minacce di Cybersecurity".

- Paradosso #3: **I C.I.O. stanno lavorando febbrilmente (pro GDPR e non solo) per fortificare la cittadella… ma non c'è più alcuna cittadella da difendere!** Gli attacchi alla sicurezza informatica sono sempre più pervasivi e organizzati. Per avere un'idea di cosa sta avvenendo in tempo reale, basta dare un'occhiata a siti come quello di Norse Corporation: http://map.norsecorp.com/. La sanità peraltro è uno degli ambiti in cui gli attacchi stanno crescendo con maggior intensità, come mostra il report di Clusit 2017 citato anche da Corrado Giustozzi di AGID nel suo intervento:


Il Prof. Baldoni, di recente nominato nuovo vicedirettore generale del DIS (Dipartimento delle Informazioni per la Sicurezza) con delega alla cybersecurity, ha ricordato che con l'esplosione dell'IoT (o internet delle cose) è cambiato drammaticamente il contesto, perché è diventata obsoleta l'idea stessa che ci sia un perimetro da difendere, con un "dentro" sicuro e un "fuori" ostile. Allora l'idea di difendere una "cittadella" va abbandonata (e qui lo dico soprattutto a noi C.I.O.) perché, benché sia rassicurante, è medioevale. Dobbiamo piuttosto rendere ragionevolmente sicura una città aperta e interconnessa, come avviene nella lotta al terrorismo dopo l'11 settembre. Le strategie, l'organizzazione, i processi e gli strumenti tecnologici a supporto della sicurezza vanno tutti ripensati in quest'ottica.

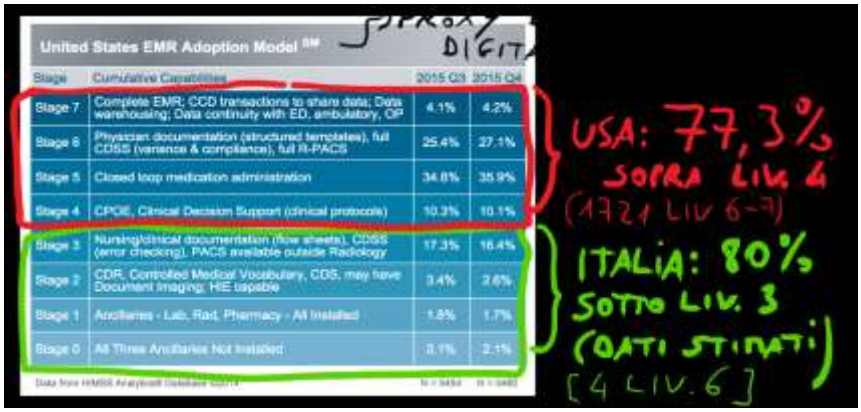
---

[3] "Do You Know the Way to Ballylickey? Shadow IT and the CIO Dilemma" – Nick Earle (https://blogs.cisco.com/cloud/shadow-it-and-the-cio-dilemma)

[4] http://www.aiic.it/

[5] https://www.ecri.org/Pages/2018-Hazards.aspx

Ora vorrei chiarire le affermazioni contenute nel titolo. Innanzitutto, ribadisco che a mio parere stiamo vivendo la splendida opportunità di ripensare la sanità digitale in modo da attuare veramente quanto previsto dal G.D.P.R., ossia la "security & privacy by design", coniugato con l'usabilità e l'utilità per gli utenti dei sistemi. Infatti, la trasformazione digitale della sanità italiana è come la Patagonia: alcuni picchi eccezionali in una pianura sterminata e un po' desolata. I dati non sono molti, ma se prendiamo come proxy il modello EMRAM di HIMSS e ci confrontiamo con gli Stati Uniti è evidente che noi siamo solo all'inizio di un cammino (di digitalizzazione prima e di trasformazione digitale poi):




Quale occasione migliore di impostare il cammino che abbiamo davanti in modo nuovo evitando i (tanti) errori commessi da chi ci ha preceduto, non solo in termini di sicurezza e privacy, ma anche di utilità e usabilità dei sistemi? Possiamo non cogliere l'occasione per passare da un approccio puntuale e frammentario (ma veramente crediamo che blindare una porta e lasciare le finestre aperte sia una buona strategia di difesa?) ad un approccio olistico alla sicurezza?

Certo il cammino non è semplice e richiede alleanze forti, come nella battaglia dei 5 eserciti de "Lo Hobbit". Da una parte i mannari e gli orchi, dall'altra uomini, nani ed elfi. Ora come allora, gli attaccanti sono diversificati: alcuni si muovono per puro tornaconto, altri (forse ancora più pericolosi) per ragioni ideologiche. Ora come allora, nessuno dei difensori può farcela da solo: non ha senso parlare di sicurezza dell'IT senza considerare l'Ingegneria Clinica o viceversa, così come non ha senso non includere nell'equazione i fornitori e le istituzioni. Ora come allora, mannari ed orchi sono forti, ma possono essere sconfitti grazie ad un'alleanza tra uomini, nani ed elfi. Per questo mi sono sentito di portare al Forum come AISIS alcune proposte concrete di collaborazione su tre temi:

1. **Competenze e consapevolezza:** l'e-HealthAcademy di AISIS (con SDA Bocconi) e i percorsi di certificazione delle competenze secondo e-CF (con AICA) saranno aperti anche a non soci AISIS. Fornitori, Ingegneri Clinici, e-Leader potranno partecipare al percorso formativo che nel 2018 avrà una parte specificamente dedicata alla cybersecurity. Per approfondimenti: segreteria@aisis.it
2. **Organizzazione e processi:** elaborazione di un documento congiunto su "Cybersecurity e IoT in sanità" tra Ingegneri clinici (AIIC) e C.I.O. (AISIS).
3. **Strategia e governance:** creazione di un tavolo di coordinamento e monitoraggio tra istituzioni, tecnici ed esperti di sicurezza.

Sui primi due punti come AISIS ci siamo già attivati, per il terzo punto stiamo lavorando per creare un tavolo con tutti gli attori coinvolti.

Concludo augurando (a tutti quelli che sono sopravvissuti alla fine del 2017) un 2018 all'insegna della nuova sanità digitale, ricca di sfide e di opportunità!

Giuliano Pozza