In punta di anfibi

di ISABELLA RAUTI*

Tutti i rischi dai “data breach” sanitari

Rete sanitaria e sicurezza informatica: un binomio cruciale sul quale, purtroppo, abbiamo riflettuto troppo poco prima del Covid-19. Eppure la pandemia ci ha posto di fronte anche a tale scenario. In piena emergenza, il 23 marzo, in Spagna, la Polizia ha denunciato un invio massiccio di *email* al personale sanitario, contenente un virus molto pericoloso, tale da far saltare tutto il sistema informatico degli ospedali. Lo stesso giorno, un attacco Ddos aveva colpito gli ospedali di Parigi, sommergendo i *server* con false richieste allo scopo di impedirne il funzionamento. Pochi giorni prima, in Repubblica Ceca era stato colpito l’University Hospital Brno. Anche la nostra rete sanitaria nazionale non è stata esente. Il primo aprile le apparecchiature del laboratorio per test Covid-19 dell’azienda ospedaliera San Camillo di Roma risultavano sabotate. Una settimana prima, un attacco *hacker* aveva interessato il sistema informatico dell’ospedale Spallanzani, parte dello stesso complesso. “Alcuni attacchi informatici ai danni di strutture italiane di eccellenza attualmente impegnate nel fronteggiare l’emergenza sanitaria in atto relativa al Covid-19 sono stati oggetto di una riunione straordinaria del Nucleo sicurezza cibernetica”, ha rivelato l’Intelligence. “Alla luce delle evidenze disponibili – ha aggiunto – gli esperti del Nucleo hanno valutato che gli episodi rappresentano una ricaduta fisiologica della situazione in corso, che sollecita appetiti di varia natura, per lo più di matrice criminale”.
Ma la questione ha anche risvolti pregressi. Negli ultimi dieci anni la minaccia informatica nel settore sanitario ha avuto un’impennata. Secondo il Data breach investigations report di Verizon (Edizione 2019), tali violazioni sono da attribuire non a *hacker* esterni, ma a soggetti interni. Tale minaccia interna rappresenta una tendenza che sembra quasi un’esclusiva del settore sanitario, da fronteggiare con una strategia appropriata che faccia i conti con i radicali cambiamenti registrati negli ultimi anni dalle reti sanitarie. Si calcola che siano più di sette milioni i pazienti che utilizzano dispositivi medici connessi e con monitoraggio da remoto. Le strutture ospedaliere che affidano necessariamente i dati medici ai sistemi di archiviazione informatica e ad ambienti *multicloud* sono consapevoli che questa scelta – inevitabile per i vantaggi che offre – aumenti la sfida della sicurezza.
È necessario contestualizzare la *cyber-security* come questione di tutela del paziente. Le violazioni informatiche dei dispositivi medici, infatti, possono causare non solo il furto dei dati sanitari personali, ma anche diagnosi errate, con tutto quello che ne consegue sulla salute e sulla vita dei pazienti. Le minacce informatiche più ricorrenti sono il *phishing*, il *ransomware*, il furto o la perdita di dati o di apparecchiature. Gli attacchi informatici colpiscono registri sanitari, sistemi It, dispositivi medici in rete, e nessun ambiente ospedaliero, grande o piccolo che sia, pubblico o privato, può davvero ritenersi immune dalla minaccia.
Con l’innalzamento del rischio di attacchi informatici è aumentato, negli ultimi anni, anche lo sforzo della cura e dell’igiene informatica e la volontà di adeguamento normativo e di difesa. Le realtà che operano nel settore Health care devono adottare quotidianamente prassi di *cyber-hygiene* per tutelare la loro stessa operatività, per proteggere le informazioni dei pazienti e la loro salute. La sicurezza informatica nel settore sanitario sarà una delle sfide del futuro al *cyber-crime* e sarà considerata sempre più come parte integrante dell’assistenza ai pazienti. Ciò impone l’adozione di corrette *policy* di utilizzo dei sistemi informativi e di gestione delle informazioni, nonché strumenti di rilevamento degli accessi ai dati e soluzioni immediate rispetto a violazioni e attacchi.

*senatrice, giornalista e scrittrice, ufficiale dell’Esercito (Ris. Sel.)