La Cybersecurity dei dispositivi sanitari connessi e lo scenario normativo sulla cybersecurity e la Privacy
Massimo Montanile

**Il Rischio Cyber**

Il Global Risks Report 2020, emesso dal World Economic Forum nell'ambito dell'iniziativa "Global Risks", segnala, per il 2020, un incremento atteso di Cyberattack. Si teme che non siano state prese sufficienti misure per contrastare il rischio cyber e che la comunità globale è generalmente mal posizionata per affrontare le vulnerabilità che hanno affiancato gli avanzamenti del XX secolo.

Kaspersky. per il 2020, prevede un incremento di attacchi ai dati sanitari (Cybersecurity of connected healthcare 2020: Overview and predictions), nonostante abbia registrato che il numero di dispositivi medici attaccati - computer dei medici, server e attrezzature mediche - nel 2019 è diminuito a livello globale.

Tale previsione negativa risiede nelle ragioni principali degli attacchi cyber a dati sanitari: la mancanza di attenzione ai rischi della digitalizzazione e la mancanza di consapevolezza della sicurezza informatica da parte del personale delle strutture sanitarie.

Un sondaggio condotto da Kaspersky tra i dipendenti del settore sanitario negli Stati Uniti e in Canada ha rivelato che quasi un terzo di tutti gli intervistati (32%) non aveva mai ricevuto alcuna formazione sulla sicurezza informatica ed il 10% di top manager ha ammesso di non essere a conoscenza di una politica di cybersecurity nella propria organizzazione.

Un altro grave problema è la mancanza di standard di sicurezza adeguati implementati nei dispositivi medici IoT.

In particolare, secondo il forecast Kaspersky 2020:

- Crescerà l'interesse per le cartelle cliniche nel Dark Web. Sui forum clandestini le cartelle cliniche sono a volte anche più costose delle informazioni sulle carte di credito.
- L'accesso alle informazioni del paziente permette non solo di rubare, ma anche di modificare le cartelle. Ciò può portare ad attacchi mirati contro singoli individui: si sfrutta il fatto che gli errori diagnostici costituiscano la causa principale della morte di un paziente.
- Il numero di attacchi ai dispositivi delle strutture mediche nei Paesi che hanno appena iniziato il processo di digitalizzazione nel campo dei servizi medici

crescerà in modo significativo il prossimo anno. Kaspersky prevede attacchi mirati a scopo di riscatto contro gli ospedali nei Paesi in via di sviluppo.

- Un numero crescente di attacchi mirati contro gli istituti di ricerca medica e le aziende farmaceutiche che conducono ricerche innovative. La ricerca medica è estremamente costosa e alcuni gruppi APT specializzati in furti di proprietà intellettuale attaccheranno tali istituti con maggiore frequenza nel 2020.
- Pur non avendo ancora registrato attacchi a dispositivi medici impiantati (ad esempio i neuro-stimolatori), Kaspersky prevede che possano essere posti sotto attacco, date le numerose vulnerabilità di sicurezza in tali dispositivi. Inoltre, La creazione di reti centralizzate di dispositivi medici indossabili e impiantati (come nel caso degli stimolatori cardiaci) porterà alla nascita di una nuova minaccia: un unico punto di ingresso per attaccare tutti i pazienti che utilizzano tali dispositivi.

Oltre il 50% della popolazione mondiale è ora online, circa un milione di persone vanno online per la prima volta ogni giorno e due terzi della popolazione globale possiedono un dispositivo mobile. Se da un lato la tecnologia digitale sta portando enormi vantaggi economici e sociali per gran parte della popolazione, la mancanza di un quadro di governance globale della tecnologia rappresenta un rischio significativo.

Il quadro normativo nazionale ed europeo in tema di cybersecurity definisce in modo chiaro quali siano gli obblighi che le organizzazioni devono rispettare a fronte di un incidente di sicurezza, dettagliando cosa fare e quando farlo, lasciando tuttavia alle singole organizzazioni la scelta di come organizzare i propri processi interni per ottimizzare la gestione degli incidenti di sicurezza, nel rispetto della legge.

Il legislatore infatti, riconoscendo che rischi, minacce, vulnerabilità e tolleranze di rischio sono peculiari a ciascuna organizzazione, non impone le misure da adottare per la gestione del rischio cyber. Ciascuna organizzazione determina in autonomia le azioni da intraprendere, le priorità e l'entità degli investimenti necessari per ridurre e gestire tali rischi, in una logica classica di valutazione costi/benefici.

La cybersecurity è tuttavia un problema complesso che richiede l'attuazione di un modello strutturato di intervento per essere affrontato in modo efficace. Le organizzazioni devono necessariamente abbandonare la logica individualista e cooperare con le altre organizzazioni, affinché le esperienze di ciascuna siano portate a fattor comune, implementando processi organizzativi e tecnologici in grado di abilitare una tale vision.

La letteratura propone vari framework per il disegno e l'implementazione di sistemi di gestione per la cybersecurity, che potrebbero vantaggiosamente essere utilizzati da un'organizzazione per contrastare i rischi cyber.

Il Framework Nazionale per la Cybersecurity e la Data Protection, opportunamente integrato con le pratiche di sicurezza previste dallo standard internazionale ISO/IEC 27701 e da quelle dello Schema internazionale ISDP©10003, può costituire un ottimo strumento per chi opera in ambito Sanità per contrastare efficacemente i rischi Cyber.

Lo schema di certificazione ISDP©10003 è stato analizzato nell'ambito dello Studio della Commissione Europea sui meccanismi di certificazione GDPR ex art.42 e 43, condotto dalla Tilburg University, che ne ha sancito la conformità allo scopo di cui all'art. 42 del GDPR.

**Il Framework Nazionale per la Cybersecurity e la Data Protection**

In Italia nel 2015 è stato presentato il Framework Nazionale per la Cybersecurity, che è stato sviluppato grazie alla proficua collaborazione tra imprese private, accademia, enti pubblici. Esso si basa sul Framework del Nist, estendendolo con tre concetti (Priorità, Maturità, Contestualizzazioni) che lo rendono uno strumento di elevata efficacia applicativa.

I Livelli di Priorità (Alta; Media; Bassa) sono associati alle singole Subcategory e permettono di supportare le organizzazioni nella definizione del cronoprogramma da implementare per raggiungere il profilo atteso di cybersecurity.

I Livelli di Maturità, da specificare almeno per le Subcategory a priorità alta, consentono di valutare il grado di maturità raggiunto dallo specifico processo di sicurezza cui si riferiscono. Definiti secondo una scala crescente, abilitano percorsi incrementali di miglioramento.

Con la contestualizzazione si adatta il Framework alle caratteristiche della singola organizzazione, attraverso un processo di selezione delle Subcategory pertinenti, delle priorità, dei livelli di maturità.

La ISO/IEC 27701, che estende i controlli della ISO/IEC 27001 alla privacy, non è richiamata nel Framework, essendo stata pubblicata successivamente (ad agosto 2019) all'emissione dell'attuale Versione (2.0) del Framework, pubblicata a febbraio 2019, che, della famiglia ISO 27000, richiama solo la ISO/IEC 27001.

Si suggerisce di integrare le "Informative References" del Framework Core con i controlli della ISO/IEC 27701.

La ISO/IEC 27001 (e la sua estensione ISO/IEC 27701) non sono però in linea con l'art. 43 del GDPR; infatti esse sono riferite a Sistemi di Gestione e, come tali, possono essere certificate da Organismi di Certificazione accreditati secondo la ISO/IEC 17021-1, che definisce i requisiti degli organismi che forniscono audit e certificazione di sistemi di gestione.

Per questo motivo riteniamo opportuno introdurre nel contesto del Framework anche lo schema ISDP©10003. Le relative integrazioni si concentrano soprattutto sulle nuove Category e Subcategory introdotte successivamente nel core del Framework per estendere quegli aspetti riguardanti la protezione dei dati personali che non erano sufficientemente coperti nel Framework originale.