I Requisiti di Cybersecurity secondo il Medical Devices Regulations MDR 2017/745

In un mondo sempre più interconnesso grazie agli avanzamenti tecnologici portati avanti nel campo della progettazione dei dispositivi elettronici, la cybersecurity occupa un ruolo centrale nella protezione degli stessi da attacchi che ne minerebbero l'integrità.

Qual è la definizione di Cybersecurity?

La Cybersecurity è definita dalla CISA (America's Cyber Defense Agency) come "L'arte di proteggere reti, dispositivi, e informazioni da accessi non autorizzati o da usi criminali, e la pratica di garantire confidenzialità, integrità, e disponibilità dell'informazione" [1]. La Cybersecurity, quindi, è un'insieme di pratiche che permettono di assicurare la difesa dei dispositivi elettronici, e si caratterizzano per la possibilità di essere declinate, in maniera dettagliata, in diversi ambiti applicativi.

In particolare, in campo medtech, le specifiche relative alla cybersecurity sono elencate nell'Annex I del Medical Devices Regulations (MDR 2017/745) [2]: queste definiscono i requisiti minimi di sicurezza da essere soddisfatti sia in fase di progettazione che di commercializzazione dei dispositivi medici, inclusi IVD ("*In Vitro* Diagnostic" medical devices).

Quali sono i concetti chiave quando si parla di Cybersecurity nei dispositivi medici?

La sicurezza IT nei dispositivi medicali fa riferimento principalmente ai concetti di:

- Confidenzialità delle informazioni, sia statiche che in transito;
- Integrità, necessaria a garantire autenticità e accuratezza dei dati;
- Disponibilità di processi, dispositivi, dati e sistemi connessi.

Queste tre nozioni cardine sono sintetizzate dall'acronimo *CIA*: "Confidentiality, Integrity and Availability". Il manufacturer ha quindi il compito di sviluppare i dispositivi medici in accordo con lo stato dell'arte, tenendo in considerazione il principio della riduzione del rischio anche nel campo della information security. D'altronde, non tutti i rischi collegati alla sicurezza dei sistemi informatici impattano solamente sull'aspetto tecnologico di suddetti dispositivi, ma potrebbero avere dei risvolti negativi in ambito safety. È quindi di vitale importanza mettere in atto misure di riduzione del rischio

tramite le pratiche di cybersecurity durante tutto il ciclo di vita del dispositivo medico, attraverso un processo iterativo che richiede aggiornamenti regolari del sistema [3].

Le misure di cybersecurity possono avere un risvolto sulla safety, secondo MDCG 2019-16 [3]

Per chiarire il concetto di rischio con impatto sulla sicurezza, si può analizzare il seguente esempio: un ventilatore per la respirazione assistita viene attaccato da un malware tramite accesso fisico al dispositivo via interfaccia USB. L'attacco risulta in una mancata funzionalità del dispositivo, che può ledere la sicurezza del paziente durante un trattamento. La protezione quindi delle porte di accesso al medical device è di vitale importanza, in quanto non solo la mancanza di essa rappresenta un rischio per il dispositivo stesso, ma anche per il suo corretto funzionamento e quindi la salute del paziente durante il suo *intended use*. Le tecniche messe in atto tramite la cybersecurity sono volte a proteggere il dispositivo da accessi indesiderati, garantendone la funzionalità.

Esistono gruppi di lavoro focalizzati sull'armonizzazione dell'approccio alla Cybersecurity per i dispositivi medici?

L'armonizzazione dell'approccio alla cybersecurity dei medical devices è l'obiettivo di un gruppo di lavoro internazionale dell'International Medical Device Regulators Forum (IMDRF), che si occupa di redigere il Medical Device Cybersecurity Guide [4]. Questo documento chiarisce gli aspetti fondamentali relatiamente alla sicurezza dei dispositivi, fornendo una guida per la progettazione di tali che possa conciliare innovazione, performance e sicurezza.

In conclusione, i requisiti minimi di cybersecurity sono da tenere in considerazione durante tutto il ciclo di vita del dispositivo medico, dalla sua progettazione alla sua distribuzione e maintenance, per garantirne la massima performance e proteggere la salute e la sicurezza dei diversi attori che prendono parte al suo utilizzo.

Fonti:

[1] www.cisa.gov

[2] Regulation (EU) 2017/745 of the European Parliament and of the Council

[3] MDCG 2019-16 Rev.1, Guidance on Cybersecurity for medical devices

[4] Medical Device Cybersecurity Guide, www.imdrf.org