ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

SCUOLA DI INGEGNERIA E ARCHITETTURA

CORSO DI LAUREA IN INGEGNERIA BIOMEDICA

CYBERSECURITY e DISPOSITIVI MEDICI: FASI di SVILUPPO e GOVERNANCE

Tesi in

Laboratorio di Ingegneria Biomedica

Relatore
PROF. ING. CRISTIANA CORSI

Presentato da
GIAN CARLO RAFFAELE TONTINI

Anno Accademico 2016-2017

Alla mia famiglia

"Le case felici sono costruite

con mattoni di pazienza"

Harold E. Kohn

Indice generale

Introduzione

Sicurezza informatica, cybersecurity sono tematiche entrate a far parte di prepotenza dell'ambito sanitario. Questa crescente attenzione è giustificabile dal fatto che le moderne tecnologie informatiche hanno e continueranno ad avere, un forte impatto sulla cura della salute dell'individuo. Tramite l'utilizzo di sensori, dispositivi indossabili, tecnologie di monitoraggio a distanza per la cura ed il benessere si è giunti a quella che viene definita salute digitale. Concetti come la cifratura dei dati o la protezione dei sistemi da eventuali attacchi hanno iniziato a fare parte del sistema salute perchè questo nuovo spazio cibernetico dove circolano dati ed informazioni sulla salute rappresentano una nuova ed estesa superficie d'attacco per gruppi di hacker. I dati statistici degli ultimi anni confermano questa tendenza che non sembra, almeno per ora, destinata a diminuire. Lo scopo del lavoro è approfondire lo standard di sicurezza dei dispositivi medici ed anche delle reti IT medicali per affermare che il rischio cibernetico venga considerato alla stregua delle altre situazioni pericolose per la salute ed il benessere dei pazienti. In questa tesi sono state analizzate le linee guida fornite dagli standard, dal processo di gestione del rischio dei produttori e di tutti gli altri attori del settore, evidenziando la necessità di implementare una governance di cybersecutity che assicuri un duraturo ed elevato standard qualitativo di sviluppo futuro.

Capitolo 1

1.1 - Dispositivi Medici

Nel 2007, con la direttiva 2007/47/CE, recepita in Italia nel 2010, è stata rivista la definizione di dispositivo medico DM, che ora recita:

Si definisce dispositivo medico (DM) ": *qualunque strumento, apparecchio, impianto, software, sostanza o altro prodotto, utilizzato da solo o in combinazione, compreso il software destinato dal fabbricante ad essere impiegato specificamente con finalità diagnostiche e/o terapeutiche e necessario al corretto funzionamento del dispositivo, destinato dal fabbricante ad essere impiegato sull'uomo a fini di:*

- *diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia;*
- *diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap;*
- *studio, sostituzione o modifica dell'anatomia o di un processo fisiologico;*
- *intervento sul concepimento la cui azione principale voluta nel o sul corpo umano non sia conseguita con mezzi farmacologici né immunologici né mediante metabolismo, ma la cui funzione possa essere assistita da tali mezzi.[1]*

Questa definizione ha reso possibile diversificare il DM a bordo di un'apparecchiatura, ma anche *stand-alone*, quando non dipende da altre unità di elaborazione.
Questa nuova normativa introduce soprattutto novità per quanto riguarda la ***validazione*** dei prodotti come DM: è necessario dimostrare che hanno un'azione positiva e quindi "*fanno del bene*".
Veniamo ora a due sotto-categorie del DM: i ***DM diagnostici in vitro*** (DM IVD) e i ***DM attivi***.
La definizione dei primi è la seguente:

"dispositivo medico – diagnostico in vitro: qualsiasi dispositivo medico composto da un reagente, da un prodotto reattivo, da un calibratore, da un materiale di controllo, da un kit, da uno strumento, da un apparecchio, un'attrezzatura o un sistema, utilizzato da solo o in combinazione, destinato dal fabbricante ad essere impiegato in vitro per l'esame di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, unicamente o principalmente allo scopo di fornire

informazioni su uno stato fisiologico o patologico, o su una anomalia congenita, o informazioni che consentono la determinazione della sicurezza e della compatibilità con potenziali soggetti riceventi, o che consentono il controllo delle misure terapeutiche.
I contenitori dei campioni sono considerati dispositivi medico-diagnostici in vitro. Si intendono per contenitori di campioni i dispositivi, del tipo sottovuoto o no, specificamente destinati dai fabbricanti a ricevere direttamente il campione proveniente dal corpo umano e a conservarlo ai fini di un esame diagnostico in vitro.
I prodotti destinati ad usi generici di laboratorio non sono dispositivi medico – diagnostici in vitro a meno che, date le loro caratteristiche, siano specificamente destinati dal fabbricante ad esami diagnostici in vitro;"[2]

La definizione dei secondi è invece la seguente direttiva (MEDDEV 2,1/6):

"dispositivo medico attivo: qualsiasi dispositivo medico legato per il suo funzionamento a una fonte di energia elettrica o a qualsiasi altra fonte di energia diversa da quella prodotta direttamente dal corpo umano o dalla gravità;" [3]
a livello esemplificativo, possiamo considerare:
DM attivi terapeutici i *Software per la pianificazione della dose di insulina.*

DM attivi diagnostici i Software di acquisizione ed elaborazione di immagini TC.
La certificazione del Software come quella di ogni altro DM deve essere a regola d'arte, cioè realizzata sfruttando tutte le conoscenze scientifiche e tecniche disponibili sul momento.
La realizzazione di un DM richiede un *fascicolo di progetto*, un *prototipo* e *un'analisi di rischio,* in cui è scritto che cos'è il prodotto che si vuole certificare, a che cosa serve esattamente e i rischi che derivano dal suo impiego, espressi anche come assegnazione ipotetica ad una *classe di rischio.*
È possibile quindi definire un ciclo di vita di sviluppo ed un vero e proprio ciclo di vita analogo al Software.

1.2 - Cybersecurity

La rapida evoluzione delle tecnologie, ha avuto un impatto importante sulla nostra vita e sulla nostra società.

Il collegarsi alla rete, oltre a permettere l'accesso ad una infinita mole d'informazione, rende i nostri dispositivi e *noi stessi* vulnerabili ai dati sensibili, social network e servizi bancari.

- Ad essere a rischio però, non siamo solo *noi stessi,* ma tutto ciò che potrebbe collegarsi alla rete, alterando vita economica e società dell'intero Paese.

È necessario quindi essere protetti, e proteggere tutto ciò che ci circonda, garantendo una sicurezza informatica all'avanguardia.

Di pari passo alla crescita del Software come DM, i rischi associati ad esso si riflettono in quelle che sono le tematiche e problematiche affrontate dalla cybersecurity.

Come possiamo definire il rischio?

Una risposta adeguata viene fornita dal National Institute of Standard and Technology (NIST):

"La protezione offerta a un sistema informativo per conseguire gli obbiettivi applicabili per preservare l'integrità, la disponibilità e la riservatezza delle risorse del sistema (hardware, software, firmware, informazioni/dati e telecomunicazioni)".

Questa definizione introduce i tre obbiettivi chiave che sono il fulcro della sicurezza informatica:

- *Riservatezza*: assicura che informazioni non vengano divulgate a persone o enti non autorizzati, introducendo il concetto di *privacy;*
- *Integrità*: assicura che le informazioni e i programmi siano modificati solo in modo specifico e autorizzato;
- *Disponibilità*: assicura che il sistema funzioni tempestivamente e che i servizi non siano negati agli utenti autorizzati.

La *cybersecurity* deve offrire *misure di protezione e* un livello di sicurezza informatico, riducendo o eliminando il danno introdotto da una minaccia.

Fig.1 : Numero dei cybercrimini nelle diverse tipologie di servizi dal 2011 al 2016 e relativi dati di distribuzione delle vittime di cybercrimini in aumento.

VITTIME PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2017
Institutions: Gov - Mil - LEAs - Intel	153	374	402	213	223	220	-1,35%	↘
Other targets	97	194	146	172	51	38	-25,49%	↓
Entertainment / News	76	175	147	77	138	131	-5,07%	↘
Online Services / Cloud	15	136	114	103	187	179	-4,28%	↘
Research - Education	26	104	70	54	82	55	-32,93%	↓
Banking / Finance	17	59	108	50	64	105	64,06%	↑
Software / Hardware Vendor	27	59	46	44	55	56	1,82%	↗
Telco	11	19	19	18	18	14	-22,22%	↓
Gov. Contractors / Consulting	18	15	2	13	8	7	-12,50%	↓
Security Industry	17	14	6	2	3	0	-100,00%	↓
Religion	0	14	7	7	5	6	20,00%	↑
Health	10	11	11	32	36	73	102,78%	↑

A livello globale, secondo quanto riportato dalla tabella 1, il trend del cyber attacco, risulta avere un picco nella sanità.

Negli ultimi anni, strutture sanitarie sono state affette dal *ransomware,* un tipo *di malware (cybercrimine)* che limita l'accesso del dispositivo che infetta, penetrando nel sistema attraverso, ad esempio, un file scaricato o una *vulnerabilità* del servizio di rete, richiedendo una somma (*ransom),* da pagare per rimuovere la limitazione. [4]

Secondo le cifre del *Presbyterian Medical Center* di Los Angeles, sono stati pagati *17.000 dollari in bitcoin,* al fine di ripristinare l'accesso ai propri sistemi medici elettronici

Per quanto riguarda il nostro paese nel 2016, numerose strutture sanitarie hanno subito un attacco informatico attraverso i ransomware e hanno chiesto aiuto a esperti del settore per innalzare i sistemi di sicurezza e mettersi al riparo da nuovi attacchi. [5]

1.3 - Sicurezza in ambito sanitario

Una recente indagine condotta dai *Lloyd's* sui comportamenti adottati nel settore sanitario europeo contro le minacce informatiche ha rivelato che il "cyber risk" non viene tenuto in considerazione da oltre il 70% delle aziende. Nonostante il 96% di esse abbia subito negli ultimi cinque anni una violazione telematica generica, solo il 32% di esse pensa che l'aggressione possa ripetersi in futuro adottando quindi appropriate misure di sicurezza informatica.

La gravità delle conseguenze che si possono verificare nell'ambito sanitario in caso di mancato rispetto delle adeguate misure di sicurezza contro cyber-attacchi sono sotto gli occhi di tutti, anche per il notevole risalto mediatico che è stato dato recentemente, portando all'attenzione del grande pubblico alcuni episodi di *ransomware* o di altri cyber-incidenti verificatisi in strutture sanitarie di livello internazionale.

Secondo il *Data Breach Investigation Report 2017* di Verizon (leader mondiale di soluzioni innovative per le tecnologie e la comunicazione), nel settore *Healthcare* si sarebbero verificati ben 458 incidenti, dei quali 296 con rivelazione confermata di dati.

I sistemi sanitari erano già vulnerabili in formato cartaceo, e, con la diffusione di sistemi informatici, è aumentato il rischio di attacchi hacker e quindi questi sistemi richiedono controlli accurati e rigorosi. A questo proposito alla fine del 2016 la *Food and Drug Amministrattion (FDA)* ha pubblicato la sua ultima guida sulla sicurezza informatica dei dispositivi medici dopo la messa in commercio. La guida tratta ovviamente dell'importante tema della cybersecurity e chiede alle aziende di operare in modo strutturato per pensare e agire su problemi di prodotto, hardware, software di rete, in modo che il rischio sia controllato e minimizzato. Il documento ricorda inoltre quelli che sono gli strumenti più a rischio dal punto di vista della cybersecurity come i dati personali e medici, l'uso di dispositivi Mobile e l'*Internet of Things*. Nel prossimo paragrafo analizzeremo brevemente le linee guida fornite dagli standard, seguendo quello che è il processo di gestione del rischio da parte dei produttori di dispositivi medici e di tutti gli altri *stakeholder* del settore, mettendo in evidenza come sia ancora necessario implementare una *governance* di security per assicurare salute e benessere sotto tutti i punti di vista. [6]

1.4 - Gestione del rischio

La valutazione del rischio è un processo in continuo miglioramento, in quanto nel tempo i fattori di rischio, esterni o interni, possono cambiare o presentarsi in forme impreviste. La struttura del processo di gestione del rischio passa attraverso le risposte alle seguenti domande:

- Cosa può succedere? (evento o minaccia);
- Se succede, quanto può essere negativo? (impatto);
- Con che frequenza può verificarsi tale evento?
- Quale è la probabilità che si verifichi? [7]

Al termine di tale attività dovremmo essere in grado di capire quali comportamenti/azioni sono da evitare. Questo non è, però, sufficiente in quanto occorre anche identificare quali azioni è opportuno attuare come fattori fondamentali di successo. Anche qui strutturalmente si possono sintetizzare tre domande:

- Cosa posso fare? (mitigazione o minimizzazione del rischio);
- Quanto mi costa? (non solo in termini economici, ma anche di risorse, capacità, mezzi).
- Ne vale la pena?

Da quanto detto fino ad ora, emerge chiaramente una integrazione indissolubile tra gestione del rischio e gestione dei processi da parte dell'Organizzazione. Per questa ragione si fa riferimento alla norma *UNI EN ISO 9001* come modello minimo da utilizzare per attuare un Sistema di Gestione per la Qualità che aiuti anche alla gestione del rischio, appare indispensabile.

Il numero dei DM integrati e collegati in rete sta rapidamente aumentando, comportando *criticità* in caso di malfunzionamento.

Secondo quanto riporta la direttiva *IEC 80001-1:2010,* per la gestione dei rischi:

- Si definiscono i ruoli, le responsabilità e le attività necessarie per la gestione del rischio delle reti IT delle strutture sanitarie per assicurarne la sicurezza e l'efficacia informatica [8]
- Si applica dopo che un dispositivo medico è stato acquistato da una organizzazione che vuole incorporarlo nella sua rete IT e durante tutto il ciclo di vita della rete stessa.

La gestione del rischio della rete IT richiede il coinvolgimento dell'organizzazione responsabile della rete, dei fabbricanti dei dispositivi medici in rete e di tutti gli altri fornitori di dispositivi/software IT utilizzati per, o nella rete.
Il produttore deve stabilire, documentare e tenere traccia attraverso il *ciclo di vita del DM* un processo per identificare i rischi a questo associati, stimando e valutando i rischi che potrebbero derivarne, controllandoli e monitorando l'efficacia di tali controlli. Questo processo dovrebbe includere i seguenti elementi:

- analisi del rischio;
- valutazione del rischio;
- controllo del rischio;
- produzione e post-produzione di informazioni

In questo scenario è opportuno stilare un piano di gestione del rischio, considerando il software come parte integrante del dispositivo medico, che includa :

- una descrizione del DM includendo le sue funzionalità all'interno del software;
- una dichiarazione che il software sarà sviluppato secondo la direttiva *IEC 62304;*
- i criteri di accettabilità del rischio correlati al software*,* diversi dai criteri di accettabilità utilizzati per le altre componenti del DM;
- includere un file di gestione del rischio che tenga traccia di tutti i cambiamenti a cui il software sarà soggetto durante il ciclo di vita. [9]

A tal proposito lo standard ISO 14971 analizza l'applicazione della gestione del rischio ai dispositivi medici stabilendo i requisiti per la gestione del rischio per determinare la sicurezza di un dispositivo medico da parte del costruttore durante il ciclo di vita del prodotto. In particolare, l'ISO 14971 è uno standard a nove parti che stabilisce innanzitutto un quadro per l'analisi, la valutazione, il controllo e la gestione dei rischi e specifica inoltre una procedura di revisione e monitoraggio durante la *produzione e la post-produzione.*

1.5 - Minaccia degli attacchi

Le minacce cyber sulle strutture sanitarie possono essere suddivise in due categorie:

- attacchi *non mirati* non discriminano tra i beni. Pertanto, gli avversari scelgono gli obiettivi che massimizzano il loro rapporto di guadagno / costo in primo luogo.

- attacchi *mirati* hanno asset specifici nei *crosshairs*. In questo caso, gli avversari hanno obiettivi precisi e sono disposti a mobilitare le risorse necessarie per raggiungerli.

Uno dei temi principali da prendere in considerazione è la molteplicità degli attori che gestiscono il record pazienti e quindi i numerosi obiettivi potenziali.

Oltre la minaccia *ransomware,* la diffusione di varie tipologie di attacco si fa sempre più grande e di solito mostrano schemi ricorrenti:

- gli hacker possono accedere al sistema d'informazioni sulla struttura utilizzando metodi fisici, sfruttamento di software scaduti, furto di dispositivi mobili, ma anche phishing o email maligne.
- Una volta che gli hacker hanno accesso all'*Intermediate system (IS),* utilizzano un virus speciale che detiene l'ostaggio del sistema crittografando i dati che contiene, così da rendere il sistema completamnete inaccessibile, fino che gli hacker non vengono ripagati con un riscatto (*ransomware*);
- furti di sistema classici, attarverso il *by-pass* del sistema rubando il maggior numero d'informazioni e record. È un attacco più pericoloso del *ransomware*, ma richiede più tempo ed è più difficile da attuare.

Parlando di cifre, si pensi che secondo una stima dell'*ESSEC BUSINESS SCHOOL* i dati record di assistenza sanitaria completi sono valutati 50$ ciascuno, mentre i numeri di previdenza sociale sono valutati 15$.

La tipologia di attacco che colpisce può essere molteplice, ma allo stesso modo efficace su vari livelli:

- abbondanza di operatori che hanno accesso alle informazioni.
- vasta gamma di hardware utilizzata all'interno degli impianti ospedalieri: personal computer, hardware, sistemi di alimentazione, impianti di archiviazione dati ,ecc..

L'elenco sta rapidamente allargandosi insieme alla digitalizzazione e l'uso di dispositivi mobile all'interno delle strutture sanitarie.

È difficile perciò cercare di proteggere un particolare campo di difesa ed è proprio per questo motivo che gli hacker tendono a minacciare le strutture sanitarie.

L' Indicatore di situazione economica (ISE) nel 2016 ha indagato una gamma rappresentativa di ospedali americani e ha scoperto che in sanità le strutture hanno solitamente strategie per contrastare gli attacchi *non mirati* nei registri dei pazienti. Però, ignorano totalmente le motivazioni

e le strategie che sarebbero state impiegate qualora gli aggressori avessero designato la salute del paziente o i record pazienti precisi e quindi attacchi mirati.

Capitolo 2

2.1 - Quadro normativo DM

Il quadro giuridico per i dispositivi medici comprende tre Direttive:

- la Direttiva *90/385/CEE* sui dispositivi medici impiantabili attivi;
- la Direttiva *98/79/CEE* sui dispositivi medico-diagnostici in vitro;
- la Direttiva *93/42/CEE,* documento che riporta i criteri generali da utilizzare nella progettazione e realizzazione di alcune categorie di dispositivi medici, vigente negli stati dell'UE.

I requisiti che un DM deve rispettare ai fini della *marcatura CE (figura 2)* sono divisi in due sottocategorie: [10]

- *requisiti generali*: riguardano disposizioni finalizzate alla sicurezza del paziente e degli utilizzatori del DM e a minimizzare i potenziali rischi.
- *requisiti relativi alla progettazione e alla costruzione*:
- caratteristiche chimiche, fisiche e biologiche
- infezione e contaminazione microbica
- caratteristiche relative alla fabbricazione e all'ambiente
- dispositivi con funzione di misura
- protezione contro le radiazioni
- requisiti per i dispositivi medici collegati o dotati di una fonte di energia

Fig. 2: Marchio CE

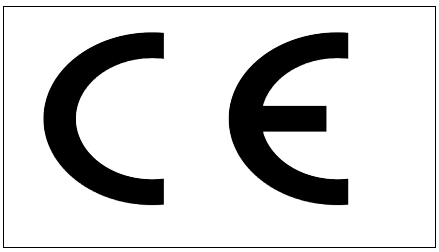
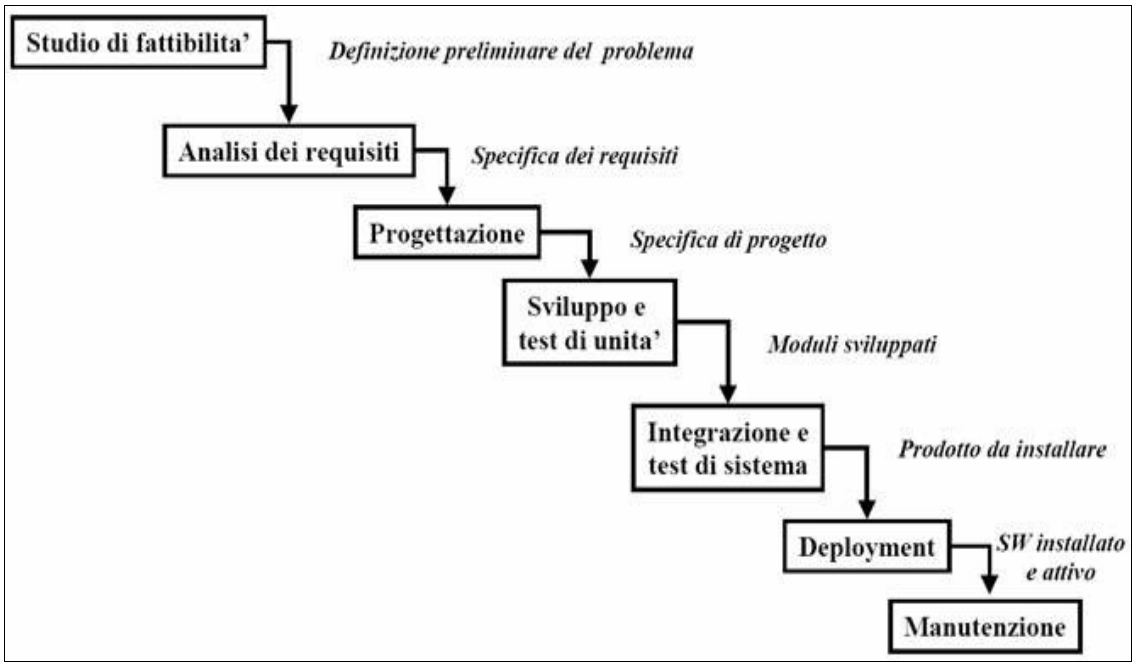


Fig. 3: Fasi di sviluppo del software



Dal punto di vista del *processo di sviluppo del software la direttiva EN 62304*, è diretta sia ai fabbricanti sia agli utilizzatori e introduce un approccio sistematico per la progettazione e il mantenimento del software durante tutto il suo ciclo di vita. *Non tratta la validazione e l'immissione del software a scopi medicali.*

Lo scopo di questa norma è di raccomandare un processo per lo sviluppo di software dispositivo medico di alta qualità, in linea con le direttive ed il sistema di qualità nel settore dei dispositivi medici.

La IEC 62304 definisce 3 classi per i software in base alla loro sicurezza:

- classe A: Nessuna lesione o danno alla salute;
- classe B: Lesioni non gravi;
- classe C: Morte o lesioni gravi.

2.2 - Quadro normativo sicurezza informatica (storico e direttive allo stato dell'arte)

Dal punto di vista della sicurezza, varie direttive sono state pubblicate di recente, di pari passo all'evoluzione del tema della *cybersecurity.*

Nel seguito vengono elencate le direttive più rilevanti in ordine cronologico:
Direttiva 2002/58 / CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva sulla privacy e le comunicazioni elettroniche).

Direttiva (UE) 2016/680 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati che abroga la decisione.

il 6 luglio 2016 il Parlamento Europeo ha adottato la *DIRETTIVA UE 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS)***.** La direttiva si colloca all'interno di una strategia europea che mira a rafforzare la *cybersecurity* e resilienza informatica dell'UE e muove dalla considerazione che le reti, *i sistemi e i servizi informativi svolgono un ruolo vitale nella società* e, pertanto, è essenziale che essi siano affidabili e sicuri per le attività economiche e sociali, in particolare ai fini del funzionamento del mercato interno.
Per fare ciò, e per fornire una risposta efficace alle sfide in materia di sicurezza delle reti e dei sistemi informativi, si è reputato necessario *un approccio globale* a livello di Unione, che contemplasse la creazione di una capacità minima comune e disposizioni minime in materia di pianificazione, scambio di informazioni, cooperazione e obblighi comuni di sicurezza per gli *operatori di servizi essenziali per i fornitori di servizi digitali.* Nulla impedisce, però, che gli operatori di servizi essenziali e i fornitori di servizi digitali applichino misure di sicurezza più rigorose di quelle previste dalla direttiva.
La Direttiva è entrata in vigore nell'*Agosto del 2016* e gli stati membri da allora hanno tempo sino al *9 maggio 2018* per trasporla, attraverso la normativa nazionale nei rispettivi ordinamenti e altri 6 mesi per identificare gli "operatori dei servizi essenziali". Possiamo classificare come operatore dei servizi essenziali il soggetto pubblico o privato, nel settore energia, trasporti, bancario, *sanitario*, di fornitura e distribuzione di acqua potabile, infrastrutture digitali, infrastrutture dei mercati finanziari.

Si tratta di una *specifica univoca* a livello dell'UE.

L'obiettivo della direttiva è raggiungere un livello di sicurezza dei sistemi, delle reti e delle informazioni comune a tutti i *Paesi membri dell'UE*. Si possono definire alcuni punti cardine:

- migliorare la capacità di cybersecurity dei singoli stati dell'UE;
- aumentare il livello di cooperazione tra gli Stati dell'unione;
- obbligo di gestione dei rischi.

La cooperazione tra i vari Stati è un dei punti più importanti della *direttiva NIS*.

È stato stabilito un gruppo di cooperazione che faciliti i rapporti tra gli Stati membri e che aumenti la fiducia. Questo gruppo di cooperazione sarà composto da rappresentati degli Stati membri, dalla Commissione e dall'European Union for Network and Information Security Agency (ENISA). Le *quattro aree* di lavoro del gruppo saranno: pianificazione, guida, segnalazione e condivisione.

La direttiva NIS quindi, rappresenta di sicuro un fondamentale passo verso un mercato unico digitale, un'opportunità di crescita economica oltre che una difesa da minacce sempre più presenti nella vita quotidiana dei cittadini e delle imprese europee. Ovviamente però la reale efficacia della direttiva dipenderà da come sarà implementata dagli Stati membri, e da quanto questa implementazione sarà in linea con gli obiettivi originali della direttiva stessa. [11]

Ricercatori del *FortiGuard Labs* hanno contato circa due milioni di tentativi di hackerare un sistema operativo *usato in sanità* per far funzionare dispositivi medici, pompe di infusione, monitor e monitor personali. Device salvavita pilotabili da remoto, in uno scenario dove la fantascienza diventa realtà. Una minaccia reale anche nelle corsie degli ospedali italiani.

Nel progetto UE c'è la necessità di dover dare un'impronta definitiva e concreta. A tal proposito la Commissione europea vuole rafforzare la sicurezza informatica nell'Ue incrementando gli investimenti in tecnologia, introducendo misure di tutela più severe e rafforzando la diplomazia per evitare gli attacchi da parte di altre nazioni. Nel testo si afferma inoltre la necessità di una maggiore cooperazione nazionale e dell'applicazione della legge per fermare gli attacchi in arrivo. Il documento richiede a breve termine una spesa aggiuntiva dell'Ue per raggiungere una massa considerevole di investimenti e superare la frammentazione all'interno della regione, e definisce il precedente piano del 2016 (che prevedeva una spesa di 1,8 miliardi di euro entro il 2020), un "primo passo". La relazione cita anche stime pubbliche e private secondo le quali l'impatto del crimine informatico sull'UE sarebbe aumentato cinque volte tra il 2013 e il 2017 e potrebbe salire ancora di quattro entro il 2019. L'Europol valuta queste perdite in 265 miliardi di euro l'anno. *Berlaymont* chiede una maggiore capacità tecnica per indagare gli attacchi informatici e per effettuare investimenti al fine di per promuovere un settore informatico regionale più forte. Un tema specifico che si prefigge di affrontare è quello di sviluppare una capacità di crittografia europea che

utilizzi tecnologie quantistiche di nuova generazione come base per sistemi di identificazione digitali sicuri, protezione delle proprietà intellettuali e sicurezza dell'e-commerce. L'UE sta cercando anche di istituire un principio di *"dovere di cura"* per i fornitori che sviluppano software e prodotti in questo settore, e ha promesso di presentare all'inizio del 2018 proposte concrete per dare alle autorità legali l'accesso transfrontaliero alle prove elettroniche. Un'altra proposta prevede la creazione di un Centro europeo per la ricerca e la competenza in materia di cybersecurity, per coordinare le soluzioni proposte, come parte del piano di rafforzare l'attuale Agenzia dell'UE per la sicurezza delle reti e dell'informazione (Enisa).

La revisione, annunciata nel mese di maggio (quando sarà definitivamente attuata la Direttiva Nis), fa parte della correzione a medio termine della strategia digitale dell'UE. Alcune proposte tuttavia, dovranno prima essere approvate dagli Stati membri e dal Parlamento Europeo.

2.3 - Fase di sviluppo del Software (pre-market)

Al fine di rimuovere ostacoli tecnici agli scambi nel mercato interno europeo risultanti dall'esistenza di norme e regolamentazioni tecniche nazionali divergenti tra loro, nel 1985, con la risoluzione del Consiglio EU, è stata adottata una nuova strategia in materia di armonizzazione tecnica e normalizzazione detta *"nuovo approccio"*.

Essa garantisce che gli stessi requisiti essenziali vengano richiesti ai prodotti nei diversi paesi europei e che, di conseguenza, le Autorità Competenti di ciascuno Stato Membro permettano la libera circolazione di dispositivi fabbricati in altri Stati Membri, avendo la certezza giuridica che tali prodotti siano equivalenti con quelli che rispondono alla normativa applicabile nel loro paese. La "conformità" ai requisiti imposti dalle normative è dimostrata dalla presenza sul prodotto del *marchio CE*.

I requisiti essenziali che i dispositivi medici devono soddisfare per poter circolare liberamente nell'UE sono divisi in *requisiti generali* e *requisiti di efficacia*:

- sicurezza e salute del paziente e degli operatori;
- prestazioni del dispositivo assegnate dal fabbricante;

- inalterabilità delle caratteristiche del dispositivo durante l'uso, il trasporto e l'immagazzinamento;
- minimizzazione dei rischi associati all'uso;
- analisi dei rischi;
- valutazione clinica per dimostrare la conformità ai requisiti essenziali (in particolar modo a quelli d efficacia); [12]

Di particolare importanza è la previsione nei *requisiti generali*, di una valutazione clinica di tutti i dispositivi medici per la dimostrazione della conformità ai requisiti essenziali (in particolare quelli relativi all'efficacia). Molte direttive di "nuovo approccio" fanno esclusivamente riferimento ai requisiti essenziali di sicurezza per consentire la libera circolazione dei prodotti nel territorio dell' UE; anche nelle direttive che prevedono la corrispondenza ai *requisiti di efficacia* (oltre a quelli di sicurezza), quali appunto quelle sui dispositivi medici, in effetti tali requisiti, seppure non trascurati, apparivano relativamente in secondo piano rispetto a quelli di sicurezza e, spesso, non erano espressi in maniera compiuta ed esplicita.

La progettazione di un DM diverge da quella di un componente in senso ingegneristico. Infatti in alcuni casi il dispositivo è destinato a replicare le funzioni di un componente umano (organo, arto, tessuto, ecc.) definendo in maniera specifica ingombri, masse, forme ed interfaccia, con un numero elevato di vincoli. In questa fase molto delicata in cui è necessario rendere evidenti e correggere in anticipo le eventuali lacune nella definizione degli input alla progettazione e le discrepanze tra il progetto proposto e i requisiti iniziali. Occorre quindi aumentare la probabilità che il progetto, una volta trasferito alla produzione, si realizzi in un prodotto adeguato alla propria destinazione d'uso e dare maggiore visibilità al processo di progettazione; migliorare la gestione delle risorse necessarie alla progettazione.

In questo processo è fondamentale definire il sistema di controllo della progettazione in modo documentato e dettagliato, per permettere a chi è coinvolto nelle attività di capire i requisiti, il processo, le aspettative e come la qualità della progettazione è assicurata dal sistema. Questo costituisce anche una linea di base per effettuare periodicamente riesami e miglioramenti del processo considerando la storia, i problemi e gli eventuali insuccessi del sistema.
In fase di *integrazione di sistema* il fabbricante deve definire e documentare l'architettura software, che descriva la struttura del software e ne definisca i *"software item"*. L'architettura software deve

evidenziare come i vari software item si interfacciano tra di loro e come si interfaccia con eventuali componenti esterni al software.

Inoltre essa deve esplicitare i collegamenti relativi a componenti software che hardware.

Nel corso dell'*integrazione di sistema* vengono assemblati i vari sottosistemi a partire dai moduli componenti, effettuando parallelamente il test di integrazione, che verificano la corretta interazione fra i moduli. Dopo che il sistema è stato assemblato completamente, viene eseguito il test di sistema.

Nell'ultima fase di *test di sistema (validazione del software)* bisogna fare una verifica generale e dimostrare che il software abbia sia requisiti iniziali richiesti dal cliente, in termini di funzionalità e prestazioni, sia requisiti derivanti dall'analisi dei rischi, in termini di efficacia del controllo dei rischi.

L'attività di *manutenzione* del dispositivo sta evolvendo verso una vera e propria funzione manageriale volta alla riduzione dei rischi connessi all'uso, alla diminuzione dei tempi di utilizzo e alla prevenzione dei guasti ed alla garanzia delle qualità delle prestazioni erogate.

L'obbligatorietà della manutenzione è imprescindibile e da quanto riporta il Paragrafo della "Gestione delle risorse tecnologiche" del DPR 14 Gennaio 1997 "Deve esistere un piano per la *manutenzione ordinaria e straordinaria delle apparecchiature biomediche "*.

Le azioni frequenti messe in campo per migliorare la sicurezza del dispositivo dovrebbero comprendere:

- manutenzione correttiva: installazione periodica di programmi più aggiornati (patch) per ovviare a possibili malfunzionamenti (bug) comunicati tipicamente dal Ministero della Salute o dalle Autorità Competenti di altri Paesi (cfr. segnalazioni di "incidente" e "mancato incidente") o derivanti da test effettuati a seguito dell'introduzione del dispositivo sul mercato;
- manutenzione perfettiva: installazione di aggiornamenti software che migliorino le prestazioni del dispositivo o la sua manutenibilità .
- manutenzione adattativa: interventi mirati a preservare le funzionalità del software del dispositivo a seguito di variazioni dell'ambiente in cui esso opera.

Va evitata la tentazione di conseguire risparmi di budget trascurando lo svolgimento della manutenzione preventiva che, operando su apparecchiature in apparente buono stato di funzionamento, potrebbe apparire meno pressanti rispetto alla manutenzione correttiva (che viene eseguita a seguito della rilevazione di una avaria).

Di particolare interesse risulta l'implementazione della *Raccomandazione* per la prevenzione degli eventi avversi conseguenti al malfunzionamento dei dispositivi/apparecchi elettromedicali.

Gli eventi sentinella dovuti a malfunzionamento dei dispositivi/apparecchi elettromedicali devono essere segnalati secondo il protocollo di monitoraggio degli eventi sentinella del Ministero del Lavoro, della Salute e delle Politiche sociali.
Al fine di migliorare la Raccomandazione nella pratica clinica, le strutture sanitarie sono invitate a fornire suggerimenti e commenti rispondendo alle domande del questionario accluso "*Insieme per migliorare la prevenzione degli eventi sentinella"*. [13]
Opportuni interventi di manutenzione preventive e correttive devono essere segnalate e documentate da un rapporto tecnico dettagliato.
Deve esistere infatti per ogni apparecchiatura una cartella la quale riporti tutti i dati significativi relativi ad ogni intervento di manutenzione subito.
Le schede di manutenzione devono riportare alcuni indicatori obbligatori come: tempo d'intervento, tempo di risoluzione guasti, tempo medio di fermo macchina, frequenza dei guasti, costo di manutenzione e costo delle parti di ricambio.

2.4 - Fase di sviluppo cybersecurity (pre-market)

Nel documento del *Food and Drug Administration (FDA) "Submissions for Software Contained in medical devices"* vengono sviluppate le linee guida per assistere il medico e l'industria dei dispositivi individuando le problematiche legate alla sicurezza informatica che i produttori dovrebbero considerare nella preparazione di presentazioni *pre-market* per i dispositivi medici. La richiesta di un'efficiente sicurezza informatica per assicurare funzionalità del dispositivo medico è diventata più importante con l'aumento dell'utilizzo di dispositivi *wireless e Internet e di rete* collegati per il frequente scambio elettronico di informazioni sanitarie correlate al dispositivo medico.
La guida fornisce le *raccomandazioni* per esaminare e documentare le presentazioni *pre-market* dei dispositivi medici FDA per assicurare una efficace *gestione della sicurezza* della rete e ridurre il rischio che la funzionalità del dispositivo sia intenzionalmente o involontariamente compromessa.

Si cerca quindi di evitare:

- modifiche non autorizzate;
- uso improprio o negativo dell'uso o l'uso non autorizzato di informazioni memorizzate, accessibili o trasferite da un dispositivo medico a un destinatario esterno;

e di assicurare che i produttori garantiscano:

- *riservatezza* delle informazioni, richiedendo che i dati, le informazioni o le strutture del sistema siano accessibili solo alle persone e alle entità autorizzate e siano trattati in tempi e modalità autorizzati, contribuendo in tal modo alla sicurezza dei dati e del sistema;
- *l'integrità delle informazioni*, richiedendo che i dati e le informazioni siano accurati e completi e non modificati in modo improprio;
- *disponibilità* di informazioni, richiedendo che i dati, le informazioni e i sistemi di informazione siano disponibili quando necessario. [13]

La guida invita i produttori a considerare la sicurezza della cyberecurity durante la fase di progettazione del dispositivo medico, definire e *documentare* i componenti della loro analisi e definire un *piano di gestione del rischio di cybersecurity* come parte dell'analisi del rischio per l'approvazione del prodotto.

Nello specifico viene richiesto*:*

- *analisi dei rischi*: Un elenco specifico di tutti i rischi di sicurezza in Internet che sono stati considerati nella progettazione del dispositivo;
- un elenco specifico e una giustificazione per tutti i controlli di sicurezza della rete che sono stati stabiliti per il dispositivo;
- una matrice di tracciabilità che collega i veri controlli di *cybersecurity* ai rischi di *cybersecurity* che sono stati considerati.

2.5 - Principi di validazione del Software

A causa della grande varietà di dispositivi medici, processi e impianti di produzione, non è possibile affermare in un documento tutti gli elementi di validazione specifici che sono applicabili. Tuttavia, un'applicazione generale di diversi concetti generali (definita nel documento "*General Principles of Software Validation; Final Guidance for Industry and FDA Staff")* può essere utilizzata con successo come guida per la convalida del software. Questi concetti generali forniscono un quadro accettabile per costruire un approccio globale alla validazione del software.

La verifica del software fornisce una prova oggettiva che le uscite di progettazione di una fase

particolare del ciclo di vita del software di sviluppo soddisfino tutti i requisiti specificati per quella fase. Tale *verifica* ricerca la coerenza, la completezza e la correttezza del software e della relativa documentazione di supporto in fase di sviluppo e fornisce il supporto per la successiva validazione. [15]

Il test del software è una delle molte attività di verifica intese a confermare che l'output di sviluppo software soddisfa i requisiti di input. Altre attività di verifica includono varie analisi statiche e dinamiche, ispezioni di codice e documenti, passaggi e altre tecniche.

La convalida del software è parte della convalida di progettazione di un dispositivo finito, ma non è definita separatamente nella regolazione del sistema di qualità. Ai fini di questa guida, *la FDA* intende per la convalida del software la *"conferma mediante l'esame e la fornitura di prove obiettive che le specifiche del software siano conformi alle esigenze dell'utente e agli usi previsti e che i requisiti particolari implementati attraverso il software possono essere rispettati in modo coerente."* In pratica, le attività di convalida software possono attuarsi sia durante, sia alla fine del ciclo di vita del software per garantire che siano soddisfatti tutti i requisiti. Poiché il software è solitamente parte di un sistema hardware più grande, la convalida del software include tipicamente la prova che tutti i requisiti software siano stati implementati correttamente e in modo completo e siano rintracciabili ai requisiti di sistema. Una conclusione secondo cui il software è convalidato dipende in larga misura dal test completo, dalle ispezioni, analisi e altre attività di verifica eseguite in ogni fase del ciclo di vita del software. Il test di funzionalità del software di periferica in un ambiente di utilizzo simulato e nel sito utente sono tipicamente inclusi come componenti di un programma di convalida generale per un dispositivo software automatizzato.

La verifica e la convalida del software sono processi complessi e dinamici in cui la procedura di validazione deve essere ripetuta nel tempo. In larga misura, la convalida del software è una questione di sviluppare un "livello di fiducia" che il dispositivo soddisfi tutti i requisiti e le aspettative dell'utente per le funzioni e le funzionalità automatizzate che il dispositivo deve svolgere. Misure come i difetti trovati nei documenti specifici, le stime dei residui di difetti, la copertura di test e altre tecniche sono tutti utilizzati per sviluppare un livello di fiducia accettabile prima di spedire il prodotto.

2.6 - Fase di sviluppo cybersecurity (post-market)

L'orientamento post-market per la sicurezza informatica suggerisce che un programma di gestione dei rischi del settore della sicurezza in rete risolva vulnerabilità che possono consentire *l'accesso, la modifica, l'abuso o la negazione di un dispositivo o l'uso non autorizzato di informazioni memorizzate*, accessibili o trasferite da un medico dispositivo a un destinatario esterno e ciò può causare danni al paziente. In particolare, la FDA raccomanda che un tale programma includa i seguenti componenti critici:

- *monitorare le fonti di informazione* in materia di sicurezza della rete per l'identificazione e la rilevazione delle vulnerabilità e dei rischi della sicurezza in Internet;
- *mantenere robusti processi di ciclo di vita* del software che includono meccanismi di monitoraggio di componenti software di terze parti per nuove vulnerabilità e esecuzione di convalida e convalida del progetto per aggiornamenti software e patch utilizzati per risolvere le vulnerabilità;
- c*omprendere*, valutare e rilevare le vulnerabilità;
- s*tabilire* e comunicare i processi per l'assunzione e la gestione delle vulnerabilità di cyberecurity;
- definire e saper controllare i rischi *controllati e incontrollati.* A tal proposito la FDA spiega che, in assenza di rimedi, un dispositivo con un rischio *incontrollato* del danno del paziente può essere considerato in violazione del Federal Food, Drug and Cosmetic Act e essere soggetto ad azioni di esecuzione. [16]

Uno dei criteri per la politica di discrezione dell'applicazione della FDA sulla re-portabilità delle modifiche del dispositivo non correlate alla routine di cybsecurity e prevedere che il produttore sia membro attivo di un *ISAO* (Standard Organization, improving Nation's cybesecurity). L'FDA considera il produttore membro dell'ISAO solo se garantisce alcuni criteri:

- *condivide* le informazioni sulla vulnerabilità con l'ISAO, incluse le comunicazioni con i clienti riguardanti le vulnerabilità della sicurezza in Internet;

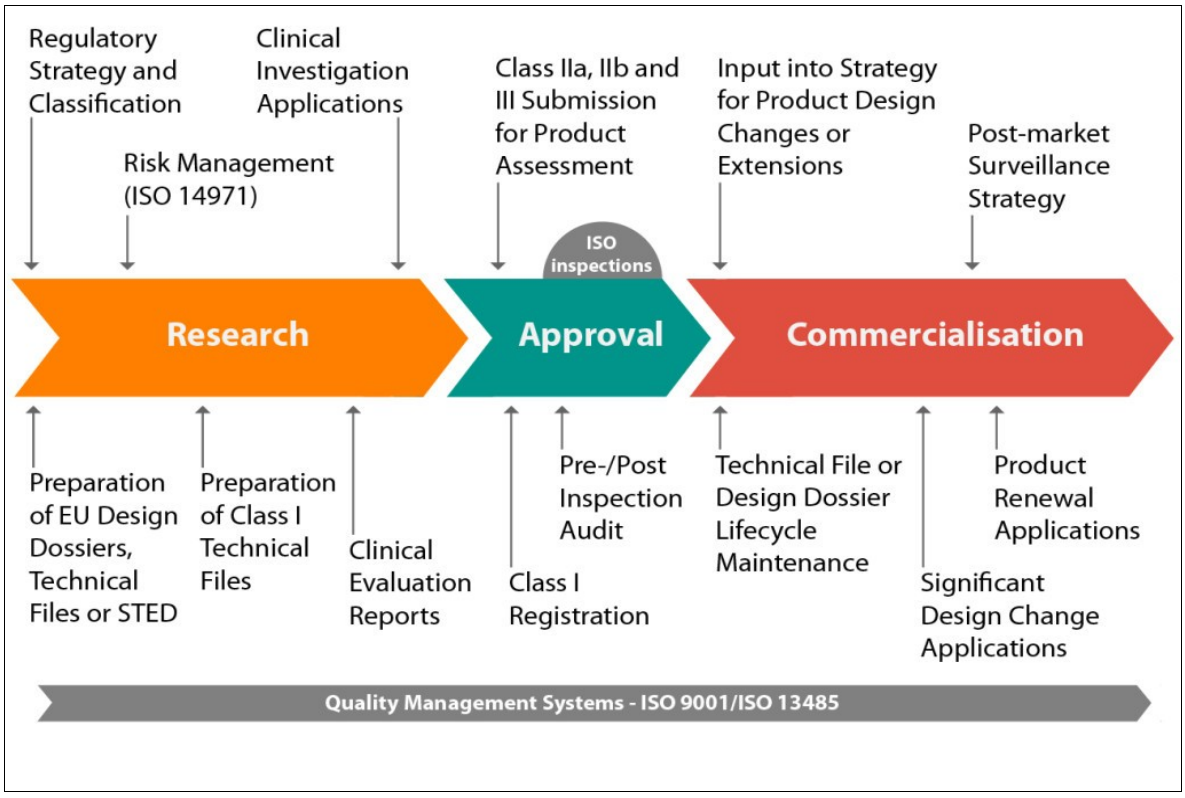
- *documenta* processi per valutare e rispondere alle informazioni sulla vulnerabilità e sulle minacce ricevute dall'ISAO.

A differenza della fase pre-market, ci sono degli aspetti diversi da tenere in considerazione, per quanto riguarda la gestione del rischio, infatti il post-market prevede di:

- *monitorare* le fonti di dati della sicurezza in rete per rilevare eventuali vulnerabilità
- *valutare* l'impatto di eventuali vulnerabilità del dispositivo.
- i*mpostare* processi per gestire le vulnerabilità
- *definire* le prestazioni cliniche essenziali di un dispositivo per mitigare i rischi di sicurezza in rete
- *crea* una politica coordinata di divulgazione delle vulnerabilità (ISAO)
- *impostare pratiche di mitigazione* per risolvere i rischi della sicurezza in rete prima di sfruttare eventuali vulnerabilità

Si prospetta quindi un quadro propenso a valutare, analizzare e risolvere prestazioni di ritorno dal mercato. La figura 4 riassume quanto illustrato nei precedenti paragrafi.

Fig. 4: Fasi di pre-market, validazione e post-market del software



Capitolo 3

3.1 - Sanità e cybesecurity, scenari percorribili

L'entrata in vigore della *DIRETTIVA UE 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (Direttiva NIS) (cap 2.1),* sancisce un passo fondamentale per rafforzare i diritti fondamentali dei cittadini nell'era digitale. Le modifiche introdotte da questa direttiva consentiranno:

un maggior controllo dei propri dati personali e un accesso più semplice. Sono progettate per assicurare che le informazioni personali siano protette ovunque vangano inviate, elaborate o memorizzate, anche al di fuori dell'UE, come spesso avviene utilizzando Internet.

Il vantaggio principale di cui usufruiranno i cittadini a seguito dell'introduzione della direttiva sarà il *diritto all'oblio* che consiste nell'eliminazione dei dati che un individuo condivide in rete, se non vi sono ragioni legittime per mantenerli. Questo diritto se, per esempio, la conservazione dei dati è necessaria per l'esecuzione di un contratto o per l'adempimento di un obbligo legale, i dati potranno essere conservati per quanto necessario per tale scopo.

Relativamente alle violazioni die propri dati, le aziende e le organizzazioni devono notificare all'autorità nazionale di controllo le violazioni dei dati che mettono a rischio i soggetti e devono comunicare al soggetto interessato tutte le violazioni ad alto rischio quanto possibile affinché gli utenti possano adottare misure appropriate.

Udo Helmbrecht, direttore dell'*Enisa*, l'agenzia di sicurezza informatica europea, ha evidenziato che l'obbligo di notifica degli attacchi informatici imposto dalla *NIS* a infrastrutture critiche e servizi digitali potrebbe contribuire ad alimentare questo trend.

Ciò ha determinato l'adozione di polizze informatiche che richiedono agli operatori di servizi essenziali quali energia, trasporti e *sanità* di riferire entro 72 ore alle pubbliche autorità qualsiasi episodio di attacco informatico.

L'*OCSE (Organizzazione per la cooperazione e lo sviluppo economico)* sta progettando di pubblicare nel corso dell'anno tre report sulla situazione del mercato europeo delle polizze informatiche. Lo scopo è quello di "*verificare se le compagnie assicurative sono in grado di*

quantificare i rischi", nonché "*esaminare i modelli di valutazione del rischio attualmente utilizzati*". L'*Enisa* si accinge invece ad organizzare un gruppo di lavoro che si occuperà di analizzare le coperture assicurative in ambito informatico.

L'era dei Big Data e dell'Internet delle cose trovano terreno fertile in un ambito caratterizzato da tecnologie chiuse e di laboratorio in cui ogni ente, ospedale, azienda sanitaria o istituto di ricerca produce ed elabora, in proprio, una quantità enorme di informazioni. La nuova frontiera rappresenta l'accesso diretto ad informazioni o per dare istruzione a dispositivi vitali direttamente nel corpo del paziente. [17]

La convergenza tra telecomunicazioni, informatica, fisica e biologia, apre prospettive rivoluzionarie che stanno modificando profondamente gli equilibri in grandi settori industriali e le equazioni del welfare da cui dipende l'equilibrio precario delle società occidentali. Senza questa convergenza, e senza l'utilizzo di tutte le tecnologie offerte, i sistemi sanitari potrebbero non riuscire a gestire il crescente numero di persone anziane affette da patologie croniche.

Blockchain, il sistema sicuro, efficiente e scalabile che consente lo scambio di dati mediati dal proprietario provenienti da diverse fonti, quali cartelle cliniche elettroniche, sperimentazioni cliniche, dati genomici e dati sanitari generati da dispositivi mobili, dispositivi indossabili e *Internet of Things***.**

L'accordo fra *Ibm Watson Health* e la *Food and Drug Administration* (FDA) degli Stati Uniti si fonda anch'esso su questa tecnologia.

Secondo il quadro di Agenda Digitale "In Europa, l'annuncio dell'accordo americano ha avuto impatto anche sulle politiche di finanziamento della **Strategia Europa 2020** in materia di innovazione tecnologica applicata alla sanità e della ricerca scientifica.

Nell'individuare le nuove sfide per la **Società 4.0** in termini di salute, cambiamento demografico e well-being, gli investimenti europei nelle aree di *leadership industriale* ed e*ccellenza scientifica*, permetteranno infatti di rendere disponibili a tutti nuove cure, interconnettere i sistemi sanitari e di far triangolare gli scienziati dei Centri di Ricerca con i laboratori in cui si creano nanomedicine e tessuti intelligenti. Una nuova "*cassetta degli attrezzi 4.0*" da cui i medici potranno scegliere con quale strumento prevenire e curare in modo sempre e personalizzato i malati". [18] Per quanto riguarda la *sicurezza* dei pazienti*,* nuove forme di *autenticazione* sono in vigore nella società 4.0:

- *fase di registrazione:* l'utente si registra con il fornitore dei servizi healt TMIS fornendo informazioni personalitità. Una password può essere scelta in una fase successiva o all'indirizzo fase di registrazione ed è soggetto a modifiche dopo il primo login.
- *login e autenticazione di fase:* l'utente accede ai servizi forniti dal TMIS fornendo la sua

identità.

- *modifica della password di fase:* Questa fase viene introdotta in modo che l'utente può aggiornare regolarmente la propria password, che minimizza la probabilità di attacchi dovuti all'utilizzo la stessa password.
- *fase di revoca:* le credenziali dell'utente sono revocate in caso di qualsiasi momento.

L'adozione della tecnologia sanitaria è un processo arduo che richiede una grande pianificazione e tempo. Dopo *l'implementazione*, il software deve essere aggiornato costantemente per mantenersi al passo con il programma. Le organizzazioni stanno spendendo grandi importi di finanziamento per diventare più integrati.

A tal proposito il *Cyber Threats to Health Information Systems*, si propone di fornire una revisione sistematica delle tendenze della sicurezza in Internet, incluse le minacce recenti e la sua relazione con l'industria sanitaria attraverso la letteratura accademica.

Metodologia di aggiornamento:

- *fonti di informazione:* Tre database separati sono interrogati per raccogliere la letteratura appropriata relativa alla sicurezza della cyberecurity. I database selezionati dai ricercatori hanno incluso l'indice cumulativo dell'infermiera (CINAHL) e PubMed (MEDLINE) tramite la società Ebson B Stephens (Host EBSCO) . L'operatore di ricerca a stringa (Cybersecurity AND Healthcare) o Ransomware, ha permesso di unire a fattor comune e filtrare tutti i risultati d'interesse per essere d'aiuto all'IT sanitario.
- *processo di raccolta dati e sintesi dei risultati*

l'estratto di ricerca è comunque fonte di analisi per i ricercatori, permettendo una serie di selezioni tra gli articoli d'interesse per la *manutenzione* informatica.

La politica del blockchain è perciò importante, unione di forze e materiale per rraggiungere uno scopo unico di preservare e protteggere i metadati dai cyberattacchi.

Occorre quindi avere idee concrete e possibili, per la realizzazione di un DM , a livello di software inteso come programma, a anche a livello "*astratto*", per quanto riguarda le informazioni all'interno dei DM stessi.

3.2 - Cybersecurity, mercato e nuove prospettive di lavoro

"Decolla in tutto il mondo il mercato della sicurezza informatica. Non solo dal punto di vista aziendale, ma anche da quello delle offerte di lavoro. Una serie di rapporti recenti di ricercatori del settore rilevano che il tasso di disoccupazione attuale per i professionisti della cybersecurity è pari a 0. Inoltre, ci sono circa un milione di posizioni legate alla sicurezza informatica" [18]

Secondo questo breve estratto dell'articolo su *Difesa&Sicurezza*, il nuovo mercato della cybersecurity, non punta a ridurre i costi e tagliare i professionisti, ma al contrario dovrebbe incrementare il numero degli occupati con 6 milioni di nuovi posti in tutto il mondo.

Negli USA nei primi sei mesi dell'anno sono 12 le startup che hanno tagliato l'ambìto traguardo del miliardo di dollari di valutazione. Tra i settori più gettonati dalle imprese emergenti spiccano healthcare e benessere, con aziende presenti in questa speciale classifica, tra cui quella con la valutazione più alta (circa 5,5 miliardi di dollari). La prerogativa di queste aziende è fornire soluzioni e strumenti tecnologici per elevare la qualità della condizione dei pazienti all'interno di ospedali e ambulatori. Di pari passo alla gestione dei dati sensibili, spiccano varie aziende con l'obiettivo di garantire proteizione e tutela di dati sensibili. [20]

In Italia si stima che il mercato complessivo della CyberSecurity (comprendendo le principali declinazioni commerciali, dal software alle applicazioni hardware fino ai servizi) vale 850 milioni di euro. Secondo un articolo del quotidiano online *key4biz, "Nel futuro prossimo il nostro modo di accedere ai servizi sanitari sarà profondamente mutato rispetto al passato. L'invecchiamento della popolazione, lo sviluppo dell'ecosistema digitale e nuovi servizi e tecnologie per medici e pazienti, faranno in modo che gran parte delle funzionalità ospedaliere siano ottimizzate in favore del ricovero domestico".*

Lo studio evidenzia che le *reti di nuova generazione saranno cruciali nella trasformazione del settore sanitario*, perché forniranno la necessaria efficienza nelle trasmissioni di dati all'interno di un ecosistema composto da *feedback, avvisi, mobilità e bassa latenza*. Le reti diventeranno un veicolo in grado di abilitare numerose applicazioni, tra cui il monitoraggio remoto tramite dispositivi medicali indossabili, l'interazione virtuale medico-paziente e la chirurgia robotica a distanza. Lo sviluppo del 5G permetterà un uso di dispositivi connessi che utilizzeranno sempre meno energia , con connessioni *affidabili* ed un accesso più sicuro ai dati. [21]

Conclusioni

La cybersecurity è diventata una questione di importanza rilevante per le strutture sanitarie. Hacker e malintenzionati non esitano ad attaccarle al fine di ottenere qualsiasi profitto paralizzando i sistemi con tecniche ransomware, hacking nelle banche dati ospedaliere con la vendita di infrmazioni sensibili al miglior offerente.

Su questo scenario la scarsa consapevolezza dei rischi dei dipendenti e la mancanza di finanziamenti adeguati alla sicurezza informatica, rendono questo problema molto rilevante.

Contemporaneamente, la molteplicità di tecniche di hacking ha aumentato il numero di potenziali autori di cybercrimini e la varietà del loro profilo.

Se il clamore mediatico di questi incidenti, ha determinato un crescente interesse su questo tema motivando nuove iniziative per modificare lo stato attuale mediante corsi di formazione del personale sanitario per il corretto utilizzo dei dispositivi, conferenze, presentazioni che cercano di spingere tutto il settore verso un totale coordinamento, aumentando così la consapevolezza riguardo le minacce informatiche tese a garantire la loro conformità con le policy (polizze) di sicurezza.

Questo è il primo passo per un efficiente "muro" al cybercrimine, ma non sarà sufficiente contro i sempre più sofisticati hacker e gruppi organizzati. Infatti domande quali come le strutture sanitarie possono implementare strutture in grado di proteggere i loro beni a lungo termine, o come possiamo proteggere i pazienti al fine di garantire un utilizzo delle risorse in modo sicuro, rimangono molto attuali e saranno certamente oggetto di nuove direttive non solo a livello europeo per rispondere alle numerose questioni ancora aperte che caratterizzano questo scenario in forte evoluzione.

Bibliografia

[1] http://www.italcert.it/medicali.aspx

[2] http://www.bioingegneria.uniba.it/

[3] https://www.theguardian.com/technology/

[4] http://www.salute.gov.it/portale/temi/

[5] http://www.ransomware.it/

[6] http://www.assiteca.it/

[7] http://www.innovazionepadova.it/

[8] http://www.salute.gov.it/

[9] https://www.certifico.com/

[10] http://www.trovanorme.salute.gov.it/

[11] http://www.techeconomy.it/

[12] https://www.fda.gov/

[13] https://www.salute.gov.it/

[14] https://www.fda.gov/

[15] https://www.fda.gov/

[16] https://www.fda.gov/

[17] https://www.agendadigitale.eu/

[18] https://www.agendadigitale.eu/

[19] http://www.difesaesicurezza.com

[20] https://www.economyup.it/

[21] https://www.key4biz.it

Fonti delle immagini

Fig. 1: Webinar realizzato da Stefania Tonutti : Privacy e Cybersecurity nella Sanità

Fig. 2: Marchio CE ; sito web : http://www.bioingegneria.uniba.it

Fig. 3: Fasi di sviluppo del software ;sito web http://www.mokabyte.it

Fig. 4: Fasi di pre-market,validazione e post-market del software; web www.realregulatory.com