Alma Mater Studiorum · Università di Bologna

Campus Di Cesena
Scuola di Ingegneria e Architettura

Corso di Laurea in Ingegneria Biomedica

La cybersecurity delle reti IT Medicali e dei Dispositivi Medici

Elaborato in:
Informatica Medica e Reti di Telemedicina

Relatore:
Prof. Ing.
Giovanni Arcuri

Presentato da:
Silvio Di Santi

I Sessione
Anno Accademico 2017/2018

Indice

Introduzione

Si sente parlare sempre più spesso di sicurezza informatica, tematica che recentemente è entrata a far parte anche dell'ambito sanitario. Una tale attenzione è giustificabile dal fatto che le moderne tecnologie abbiano, e continueranno ad avere, un forte impatto sulla cura della salute. Tramite l'utilizzo di sensori, dispositivi indossabili, tecnologie di monitoraggio a distanza(*home caring*) per la cura e 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 attaccanti hanno iniziato a fare parte del sistema salute. Questo nuovo spazio cibernetico, all'interno del quale circolano dati e informazioni sulla salute, altro non rappresenta che 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.
In questo lavoro si è voluto approfondire quello che è lo standard in merito alla sicurezza, intesa sotto tutti i suoi aspetti, dei dispositivi medici e delle reti IT medicali per verificare che l'eventualità da rischio cibernetico venga considerata alla stregua delle altre situazioni pericolose per la salute e il benessere dei pazienti. Sono state prese in analisi 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 first per assicurare salute e benessere sotto tutti i punti di vista.

Capitolo 1

Reti di calcolatori

La costruzione di reti di calcolatori può essere fatta risalire alla necessità di condividere le risorse di calcolatori potenti. La tecnologia delle reti, e in seguito l'emergere dei personal computer a basso costo, ha permesso rivoluzionari sviluppi nell'organizzazione delle risorse di calcolo. Internet è una rete di calcolatori che interconnette dispositivi di calcolo in tutto il mondo, oggi è presumibilmente il più grande sistema ingegnerizzato che sia mai stato creato: centinaia di milioni di calcolatori connessi, collegamenti e commutatori, miliardi di utenti che si connettono tramite computer portatili, tablet e smartphone [14]. Complessivamente è stato stimato che un terzo della popolazione mondiale è on-line[2]. Tutti i dispositivi connessi sono detti *host* o *end system* e sono in grado di comunicare reciprocamente grazie a una rete di collegamenti(*communication link*) a commutatori di pacchetti(*packet switch*) che possono essere di diverse tipologie a seconda del mezzo fisico utilizzato(cavi coassiali, fibre ottiche, onde elettromagnetiche, ecc.).

1.1 Architettura di rete

L'architettura di rete è una tipologia di architettura software che descrive il complesso delle funzionalità logiche della rete stessa, cioè come sono strutturate e interconnesse tra loro. In particolare le architetture di rete sono organizzate a livelli o strati, ciascuno dei quali fornisce al livello supe-

riore o inferiore i servizi o funzionalità richieste. Nel termine architettura di rete è in realtà compreso anche il concetto di architettura a livello fisico di infrastruttura cioè a livello di interconnessioni tra *host* ovvero la cosiddetta topologia della rete. Tale insieme di funzionalità in buona parte non sono visibili o percepibili dall'utente finale, cioè nel terminale, il quale vede solo l'interfaccia di utenza con l'applicazione e parte dell'intera infrastruttura fisica, ma si nascondono all'interno del software di funzionamento del sistema sia esso un terminale di rete oppure nodi interni di commutazione o nelle rispettive interfacce di trasmissione lungo i collegamenti fisici di rete. Tipicamente ciascuno strato rappresenta un'astrazione di uno o più aspetti o funzionalità di rete con lo strato superiore che rappresenta lo strato che coinvolge i processi applicativi di rete, mentre quello più in basso è quello relativo alla trasmissione dell'informazione sul canale fisico di comunicazione. Il motivo del perché esistono varie funzionalità di rete è che la semplice trasmissione sul canale fisico non è tutto ciò che serve per una comunicazione efficace e affidabile tra due o più utenti avendo dunque bisogno di altre funzionalità per superare anche l'inaffidabilità del canale. Le regole e le convenzioni usate nel dialogo tra livelli omologhi sono conosciute come protocolli di rete che rappresentano l'implementazione logica delle funzioni dei vari strati di rete. Un insieme di livelli e protocolli è detto quindi architettura di rete.

1.1.1 Struttura e funzionamento

Tutte le architetture di rete sono strutturate a livelli. Il livello n su un *host* porta avanti una comunicazione logica col livello n su di un altro *host* finalizzata allo scambio di informazione. Le regole e le convenzioni che governano la conversazione sono collettivamente indicate col termine di protocollo di livello n. Le entità (processi) che effettuano tale conversazione tra due livelli n si chiamano *peer entity* (entità di pari livello). Nel caso di reti a commutazione di pacchetto il dialogo fra due *peer entity* di livello n viene realizzato attraverso lo scambio di *PDU (Protocol Data Unit)* o pacchetto composta dalla parte di dati utili o *payload (SDU Service Data Unit)* e dall'intestazione specifica del livello (*PCI Protocol Control Information* o *header*) ovvero l'informazione aggiuntiva di servizio (*overhead*) associata al

protocollo stesso. Lo scambio di informazioni tra due *peer-entity* è in realtà solo il frutto di una comunicazione logica tra i due livelli. In realtà a livello fisico non c'è trasferimento diretto di dati dal livello n di *host 1* al livello n di *host 2*: in trasmissione ogni livello di *host1* passa i dati e le informazioni di controllo al livello sottostante. Al livello 1 c'è il mezzo fisico ovvero il canale attraverso il quale i dati vengono trasferiti da *host 1* ad *host 2*. In ricezione, cioè quando arrivano a *host 2*, i dati vengono passati da ogni livello (a partire dal livello 1) a quello superiore fino a raggiungere il livello delle applicazioni. Ogni livello n comunica con quello direttamente superiore n+1 o inferiore n-1 attraverso un'interfaccia detta *SAP (Service Access Point)* e identificata da un indirizzo univoco (indirizzo SAP) che si rende utile per capire a quale strato o livello di destinazione è indirizzato il pacchetto.

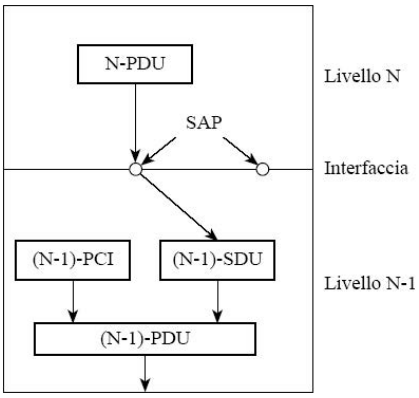

Figura 1.1: Interfacce e servizi tra livelli

Ogni livello si occuperà quindi di formare il rispettivo pacchetto (*framing*) delimitandolo dagli altri. Ciascun livello prevede generalmente un campo dati ovvero una SDU di lunghezza variabile con un limite massimo di dati (*MTU Maximum Transmission Unit*), operando quindi eventuali frammentazioni o segmentazioni su pacchetti troppo lunghi, e spesso anche un limite minimo, operando eventuali aggregazioni o riempimenti aggiuntivi (*padding*) su pacchetti troppo corti. L'intestazione (*header*) ovviamente è sempre fissa contenendo informazioni di servizio del rispettivo protocollo.

In trasmissione ciascuno strato incapsula i pacchetti informativi provenienti dagli strati superiori in un nuovo pacchetto di dimensioni via via più grandi aggiungendovi le informazioni di protocollo del rispettivo strato così che alla trasmissione di dati utili si aggiungono dunque via via sempre maggiori informazioni: per ogni funzionalità introdotta da un protocollo di un certo strato si aggiunge un rispettivo campo dati di *overhead* nell'intestazione del nuovo pacchetto. Tanto più alto è il numero di livelli e protocolli tanto maggiore sarà l'*overhead* totale finale. In ricezione, avviene il processo inverso: a partire dai livelli più bassi ogni protocollo riconosce ed analizza il rispettivo *header* del pacchetto ricevuto, compie le funzioni di controllo o elaborazione preposte (realizzando così la comunicazione logico-paritaria tra protocolli omologhi di dispositivi diversi) ed infine passa il restante pacchetto al protocollo di livello superiore e così via fino al livello di destinazione. In sostanza dunque in trasmissione l'aggiunta delle informazioni di protocollo per ciascuno strato prepara in maniera duale il rispettivo strato protocollare di ricezione all'espletamento del servizio ad esso preposto su ciascun pacchetto dati inviato utilizzando le informazioni di *overhead*.

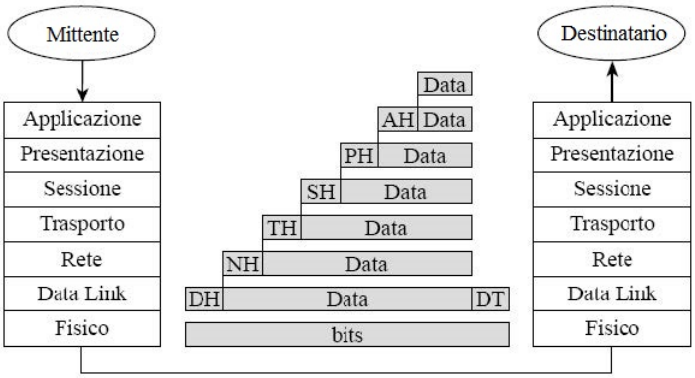

Figura 1.2: Invio e ricezione dati

Un modello standardizzato di architettura di rete che rappresenta lo standard *de iure* per reti di calcolatori è il modello ISO-OSI.

1.2 Il modello ISO/OSI

L'*Open Systems Interconnection*, meglio conosciuto come modello ISO/OSI, è uno standard per reti di calcolatori stabilito nel 1978 dall'*International Organization for Standardization* (ISO), il principale ente di standardizzazione internazionale. L'organizzazione sentì la necessità di produrre una serie di standard per le reti di calcolatori ed avviò il progetto OSI, un modello standard di riferimento a formato aperto per l'interconnessione di sistemi di computer. Il documento che illustra tale attività è il *Basic Reference Model* di OSI, standard ISO 7498[13]. Il modello ISO/OSI è costituito da una pila(*stack*) di protocolli attraverso i quali viene ridotta la complessità implementativa di un sistema di comunicazione per il networking. In particolare ISO/OSI è costituito da livelli(*layer*) che definiscono e racchiudono in sé a livello logico uno o più aspetti fra loro correlati della comunicazione fra due nodi di una rete. I livelli sono in totale sette e vanno dal livello fisico fino al livello delle applicazioni, attraverso cui si realizza la comunicazione di alto livello seguendo un modello logico-gerarchico.

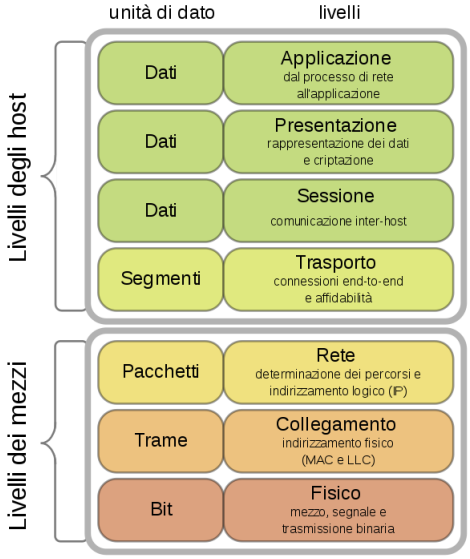

Figura 1.3: Modello ISO/OSI

I vantaggi proposti dal modello ISO/OSI risultano essere svariati:

- fornire una base per lo sviluppo di standard di interconnessione
- viene introdotto il concetto di sistema come un insieme di uno o più elaboratori con relativo software, periferiche, operatori umani, ecc. che complessivamente è in grado di elaborare dati
- nell'ambito del sistema viene definita l'applicazione come quella entità che effettivamente elabora i dati

Lo scopo di ciascun livello è quello di fornire servizi al livello superiore, tramite un protocollo di comunicazione specifico per quel livello, mascherando il modo in cui essi sono effettivamente implementati. In tal modo si realizza una comunicazione multilivello, che conferisce modularità al sistema con maggiore semplicità di progettazione e gestione della rete ovvero possibilità di migliorare, sviluppare e dunque eventualmente sostituire i protocolli dei vari strati.

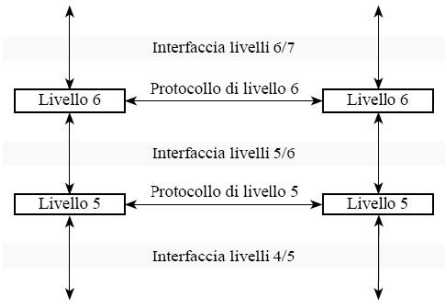

Figura 1.4: Protocolli e interfacce

1.3 Architettura del modello ISO/OSI

Seguendo il percorso di un ipotetico pacchetto di dati inviato da un sistema ad un altro sistema si vanno a descrivere i livelli attraversati e i relativi servizi offerti.

1.3.1 Livello 7: Applicazione

La sua funzione è quella di interfacciare e fornire servizi per i processi delle applicazioni: in trasmissione inoltra, quindi, le richieste al sottostante livello di presentazione, mentre in ricezione le riceve. Un programma applicativo interagisce con uno dei protocolli di livello di trasporto per ricevere dati o inviarli passandoli nella forma richiesta. Alcune tipiche operazioni implementate dai protocolli di questo livello sono:

- trasferimento file (FTP-*File Transfer Protocol*)
- terminale virtuale (connessione interattiva ad un calcolatore remoto)
- X.500 (*Directory Service*)

1.3.2 Livello 6: Presentazione

Ha come obiettivo quello di trasformare i dati forniti dal livello di applicazione in un formato standard e offrire servizi di comunicazione comuni, quali la crittografia, la compressione del testo e la riformattazione. Il livello di presentazione consente la gestione della sintassi e della semantica delle informazioni trasmesse, diversamente dagli altri livelli che gestiscono una sequenza di bit. Sono previste tre diverse tipologie di sintassi:

- astratta: definizione formale dei dati che gli applicativi si scambiano
- concreta locale: come i dati sono rappresentati localmente
- trasferimento: come i dati sono codificati durante il trasferimento

1.3.3 Livello 5: Sessione

Offre i servizi che consentono ad utenti operanti su macchine differenti di colloquiare tra loro attraverso la rete di comunicazione. In particolare, in questo livello vengono definite le regole per aprire e chiudere una connessione logica (protocolli di connessione) e quelle indispensabili al trasferimento dei dati (protocolli di comunicazione). Il compito principale è quindi di coordinare il dialogo tra utenti basandosi sul servizio offerto dal

livello di trasporto. Consente di aggiungere a connessioni end-to-end servizi più avanzati quali:

- la gestione del dialogo (mono/bidirezionale)
- la gestione del token
- la sincronizzazione

1.3.4 Livello 4: Trasporto

Fornisce trasferimento trasparente di informazione tra entità del livello sessione, in particolare fornisce un canale logico-affidabile di comunicazione end-to-end per pacchetti. I servizi forniti dal livello 4 sono diversi:

- la frammentazione dei dati provenienti dal livello superiore in pacchetti detti segmenti *transport-layer segment*
- realizzare una connessione persistente che viene poi chiusa quando non è più necessaria
- la correzione degli errori
- la prevenzione della congestione di rete
- multiplazione attraverso l'astrazione delle porte

1.3.5 Livello 3: Rete

Questo livello riceve segmenti dal soprastante livello di trasporto e forma pacchetti che vengono passati al livello sottostante. Il compito del livello di rete è la trasmissione logica di pacchetti tra due *host* arbitrari, che in generale non sono direttamente connessi. Nel modello ISO/OSI, il livello di rete è l'ultimo livello presente nei commutatori della rete ovvero nei nodi interni, mentre i livelli architetturali superiori sono presenti solo nei nodi terminali. É responsabile di:

- inoltro *(forwarding)*: ovvero ricevere un pacchetto su una porta, immagazzinarlo e ritrasmetterlo su un'altra

- frammentazione e riassemblaggio: se un pacchetto ricevuto ha una dimensione eccessiva per la rete su cui deve essere trasmesso, il livello di rete lo divide in frammenti e si occupa di riassemblare i frammenti ricevuti al momento della consegna

- instradamento *(routing)*: scelta ottimale del percorso di rete da utilizzare per garantire la consegna delle informazioni dal mittente al destinatario (scelta svolta dal router attraverso dei particolari algoritmi di routing e tabelle di routing)

1.3.6 Livello 2: Collegamento

Questo livello si occupa in primis di formare i dati da inviare attraverso il livello fisico, incapsulando il pacchetto proveniente dallo strato superiore in un nuovo pacchetto provvisto di un nuovo *header* (intestazione) e *tail* (coda), usati anche per sequenze di controllo. Come controllo di errore, per ogni pacchetto ricevuto, il destinatario invia al mittente un pacchetto di conferma ACK (*acknowledgement*) contenente lo stato della trasmissione: il mittente deve ripetere l'invio dei pacchetti mal trasmessi e di quelli che non hanno ricevuto riscontro/risposta. Per ottimizzare l'invio degli ACK, si usa una tecnica detta *Piggybacking*, che consiste nell'accodare ai messaggi in uscita gli ACK relativi ad una connessione in entrata. I pacchetti ACK possono anche essere raggruppati e inviati in blocchi. Questo livello si occupa anche di controllare il flusso di dati: in caso di sbilanciamento della velocità di trasmissione tra mittente e destinatario, si occupa di rallentare l'opera della macchina più veloce, accordandola all'altra e minimizzando così le perdite dovute a sovraccarico sul destinatario.

Il progetto IEEE 802

L'*IEEE 802 LAN/MAN Standards Committee (LMSC)* è una commissione dell'IEEE preposta a sviluppare standard per le reti locali (LAN) e per le reti metropolitane (MAN). Introduce l'idea che LAN e MAN debbano fornire un'interfaccia unificata verso il livello rete, pur utilizzando tecnologie trasmissive diverse. Per ottenere questo risultato il progetto IEEE 802 suddivide il livello di collegamento in due sottolivelli:

- **LLC(Logical Link Control)**: costituisce la parte superiore del livello di collegamento, può fornire servizi di controllo di flusso, conferma, rilevazione/correzione degli errori

- **MAC(Media Access Control)**: rappresenta il sottolivello inferiore, si occupa dell'incapsulamento dei frame prima della loro trasmissione e del decapsulamento alla loro ricezione; inoltre si occupa della rivelazione degli errori di trasmissione e di delimitare il frame per favorire la sincronizzazione tra il trasmettitore e il ricevitore. Infine controlla l'accesso ai media, comunicando direttamente con in livello fisico.

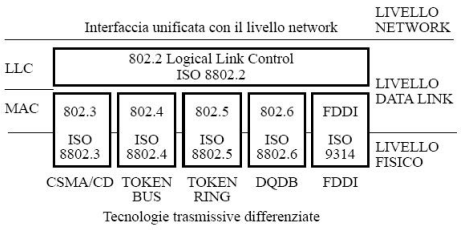

Figura 1.5: IEEE 802: sottolivelli LLC e MAC

1.3.7 Livello 1: Fisico

Questo livello riceve dal livello collegamento la sequenza di bit pacchettizzata da trasmettere sul canale e la converte in segnali adatti al mezzo trasmissivo come cavo coassiale, fibre ottiche o onde radio. In particolare, uno standard di livello fisico definisce:

- le caratteristiche fisiche del mezzo trasmissivo come forma, dimensioni, numero di piedini di un connettore e specifiche meccaniche

- le caratteristiche funzionali come il significato dei pin di un componente

- le caratteristiche elettriche, come i valori di tensione per i livelli logici, la codifica e la durata di ogni bit

1.4 Il modello TCP/IP

Sebbene il modello ISO/OSI rappresenti lo standard *de iure*, il modello TCP/IP rappresenta lo standard *de facto* nell'ambito delle reti dati. Nei primi anni '70, la *Defense Advanced Research Project Agency (DARPA)* finanziò l'Università di Stanford e la BBN (Bolt, Beranek and Newman) per lo sviluppo di un insieme di protocolli di comunicazione da utilizzarsi per lo sviluppo di reti a commutazione di pacchetto, per l'interconnessione di calcolatori eterogenei. Fu così che nacque l'*Internet Protocol Suite* i cui due protocolli più noti sono il TCP (*Transmission Control Protocol*) e l'IP (*Internet Protocol*). Tale modello può essere descritto per analogia con il modello ISO/OSI, il modello Internet è stato prodotto come una soluzione ad un problema ingegneristico pratico in quanto si è trattato di aggiungere via via strati protocollari all'architettura di rete delle reti locali per ottenere un'interconnessione efficiente ed affidabile. Il modello ISO/OSI, invece, è stato l'approccio più teorico-deduttivo ed è stato anche prodotto nel più vecchio modello di rete.

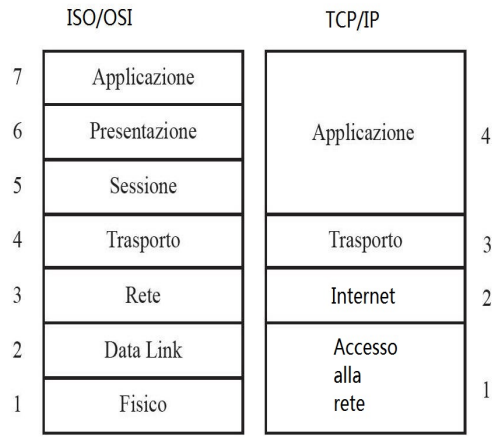

Figura 1.6: Confronto tra modello ISO/OSI e TCP/IP

Il modello ISO/OSI è basato sostanzialmente sui tre concetti di servizi, protocolli e interfacce, mentre il modello TCP/IP non fa distinzioni fra i tre.

Si vanno quindi a descrivere i livelli del modello TCP/IP come già fatto per il modello ISO/OSI.

1.4.1 Livello Applicazione

Questo livello rappresenta l'interfaccia con l'utente ed abilita, ad esempio, la consultazione di pagine web, stabilendo e gestendo le sessioni di lavoro dei processi client tra il nostro browser ed il server web. Il protocollo di trasporto TCP mette in coda i messaggi generati da client e server e li trasmette sotto forma di pacchetti su di una connessione bidirezionale; il buon fine della spedizione è attestato da una ricevuta di ritorno o riscontro (*acknowledgment*). Anche questo è un collegamento virtuale tra le due applicazioni, i cui dettagli sono demandati al successivo livello.

1.4.2 Livello Trasporto

Il livello di trasporto offre un servizio al livello delle applicazioni avvalendosi dei servizi del sottostante livello di rete. Per gestire molteplici processi attivi nel trasferimento dati sul medesimo nodo (o computer), cioè più sessioni di navigazione attive, il livello di trasporto (TCP o UDP) utilizza più numeri di porta. TCP nell'invio dei pacchetti usa il meccanismo dello *sliding window*. Una serie di pacchetti viene inviata da TCP seguendo delle regole ben precise:

- ad ogni finestra di pacchetti spedita il trasmettitore fa partire un timeout
- il ricevitore invia per ogni pacchetto ricevuto un ACK indicando il successivo pacchetto atteso
- il trasmettitore considera quindi spediti tutti i pacchetti precedenti
- se il timeout scade oppure sono ricevuti 3 ACK duplicati, TCP presume che si sia verificata la perdita di uno o più pacchetti e provvede ad implementare opportune strategie di ritrasmissione dei dati e di controllo della congestione

Questa è una tecnica molto importante perché fornisce un canale di comunicazione affidabile. Inoltre TCP contiene meccanismi per gestire la congestione ed il controllo di flusso.

1.4.3 Livello Rete

Esso si occupa di gestire l'indirizzamento dei nodi e l'instradamento attraverso il protocollo IP. A ciascun nodo viene infatti assegnato un indirizzo IP che lo identificherà in modo non ambiguo in rete. Le funzionalità di instradamento, invece, consentono di selezionare il percorso migliore per veicolare un messaggio verso un dato nodo destinatario, noto che sia il suo indirizzo IP.

1.4.4 Livello Fisico

Sotto il livello di rete, il modello di riferimento TCP/IP specifica solo che ci deve essere un livello di accesso alla rete in grado di spedire i pacchetti IP. Al livello di collegamento si decide come fare il trasferimento del messaggio per ogni singolo tratto del percorso: questo è un collegamento virtuale tra due computer (o router) adiacenti. Anche in questo caso le interfacce di comunicazione dei nodi adiacenti saranno individuate per mezzo di un indirizzo univoco (indirizzo MAC). Il livello fisico trasmette il messaggio sul canale di comunicazione usualmente sotto forma di segnali elettrici o elettromagnetici.

Capitolo 2

La sicurezza delle reti

Internet è l'esempio più lampante di come le tecnologie messe a disposizione dalle reti di calcolatori siano diventate sempre più presenti nelle nostre vite. Allo stato attuale tali tecnologie sono diventate di uso comune a tutti i livelli: istituti bancari, aziende sanitarie, servizi per il cittadino ecc., di conseguenza i dati digitali hanno assunto sempre maggiore valore parallelamente alla diffusione dei servizi a loro associati. Ma questi dati sono al sicuro?

2.1 Concetti di Sicurezza

La domanda sorge spontanea, cosa è la sicurezza informatica? Una risposta adeguata viene fornita dal *NIST(National Institute of Standard and Technology)*:

> "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)".[7]

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

- **Riservatezza**:
  - Riservatezza dei dati: assicura che informazioni private o riservate non siano disponibili o divulgate a persone non autorizzate.
  - Privacy: assicura il controllo su quali informazioni personali possano essere raccolte e memorizzate e da chi e a chi queste informazioni possano essere divulgate.
- **Integrità**:
  - Integrità dei dati: assicura che le informazioni e i programmi siano modificati solo in modo specifico e autorizzato.
  - Integrità del sistema: assicura che un sistema esegua in modo opportuno la sua funzione, libero da manipolazione non autorizzata, deliberata o involontaria, del sistema.
- **Disponibilità**: assicura che il sistema funzioni tempestivamente e che i servizi non siano negati agli utenti autorizzati.

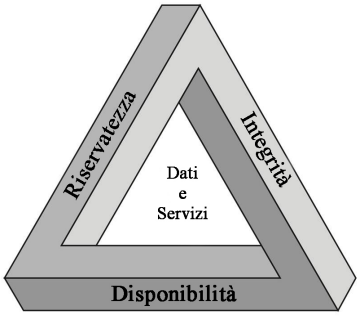

Figura 2.1: La triade dei requisiti di sicurezza

Le sfide che la sicurezza informatica si trova ad affrontare sono molteplici: nello sviluppo di particolari meccanismi di sicurezza bisognerebbe sempre considerare potenziali attacchi su quelle caratteristiche di sicurezza, in molti casi, gli attacchi di successo sono progettati osservando il problema

in una maniera completamente differente.
Avendo progettato diversi meccanismi di sicurezza è necessario decidere dove usarli: a partire dal collocamento fisico fino a quello logico(es. a quale livello di un'architettura di rete come ISO/OSI dovrebbe essere inserito uno specifico meccanismo). C'è una tendenza naturale, da parte degli utenti e degli amministratori di sistema, a percepire pochi vantaggi da investimenti in sicurezza fino ad un fallimento della stessa; la sicurezza richiede un controllo regolare e costante, obbiettivo difficile da raggiungere in ambienti e sistemi sempre più sottoposti a grandi carichi di lavoro da gestire[19]. La sicurezza è troppo spesso un obbiettivo non perseguito durante le fasi di progettazione di un sistema: in questo modo si genera più impedimento ad utenti e amministratori di sistema a causa della costante necessità di aggiungere quei meccanismi di sicurezza necessari a rispettare gli obbiettivi chiave di riservatezza, integrità e disponibilità, sarebbe sufficiente un approccio che includa la sicurezza nella fase di progettazione(*security by design*) per ottenere un livello di sicurezza minimo che riesca a contenere almeno le problematiche più ricorrenti e conosciute, garantendo così i tre obbiettivi chiave.

2.2 Architettura di sicurezza

Per soddisfare a tutti gli effetti le necessità di sicurezza di un'organizzazione e per valutare e scegliere differenti prodotti e politiche di sicurezza, il manager responsabile della sicurezza ha bisogno di un modo sistematico per definire e caratterizzare i requisiti di sicurezza. La *ITU(International Telecommunication Union)* ha stilato uno standard che definisce proprio questo approccio sistematico, all'interno della *Reccomendation X.800, Security Architecture for OSI*[17], troviamo ciò che serve ai manager per organizzare la sicurezza. Sebbene X.800 si focalizzi sulla sicurezza nel contesto delle reti e delle comunicazioni, i concetti sono applicabili anche alla sicurezza informatica. L'architettura di sicurezza OSI si concentra su attacchi di sicurezza, meccanismi di sicurezza e servizi di sicurezza, che possiamo definire brevemente come:

- **attacco di sicurezza**: qualsiasi azione che comprometta la sicurezza delle informazioni possedute da un'organizzazione.

- **meccanismo di sicurezza**: un meccanismo che è progettato per individuare, prevenire o risanare da un attacco di sicurezza(es. cifratura, firma digitale, controllo degli accessi).

- **servizio di sicurezza**: un servizio che migliora la sicurezza dei sistemi di elaborazione dati e del trasferimento dati di un'organizzazione. I servizi sono destinati a contenere gli attacchi di sicurezza facendo uso di uno o più meccanismi di sicurezza(es. autenticazione, riservatezza dei dati, integrità dei dati).

2.3 Minacce e Attacchi

Basandoci sul contenuto del documento RFC2828[18], diamo delle definizioni che saranno utili nelle successive discussioni. Nell'ambito della sicurezza il nostro interesse riguarda le vulnerabilità delle risorse di sistema o di rete(hardware, software, dati), che possono essere racchiuse nelle seguenti categorie generali:

- il sistema può essere **corrotto** in modo che non risponda correttamente, ad esempio i dati memorizzati in esso potrebbero essere diversi da come dovrebbero essere a causa di una modifica inappropriata
- il sistema può essere soggetto a **perdita di informazioni**, ad esempio qualcuno che non dovrebbe avere accesso ad alcune o tutte le informazioni disponibili attraverso la rete ottiene comunque tale accesso
- il sistema può essere reso **non disponibile**, che in altre parole significa che l'utilizzo del sistema o della rete è impossibile

In corrispondenza alle varie tipologie di vulnerabilità delle risorse di un sistema ci sono le minacce capaci di sfruttare queste vulnerabilità, le minacce altro non sono che dei potenziali danni alla sicurezza dei sistemi. Un attacco è quindi una minaccia portata a termine e, se riuscito, conduce a violazioni della sicurezza indesiderate. Gli attacchi possono essere distinti in due categorie:

- **attacco attivo**: un tentativo di alterare le risorse di sistema o influenzare le sue operazioni.
- **attacco passivo**: un tentativo di acquisire o utilizzare le informazioni del sistema che non riguarda direttamente le risorse di sistema.

Possiamo classificare gli attacchi anche in base alla provenienza degli stessi:

- **attacco interno**: avviato da un'entità all'interno del perimetro di sicurezza(un "interno"), l'agente interno è autorizzato ad accedere alle risorse di sistema ma le utilizza in maniera non approvata da chi ha garantito tali autorizzazioni.
- **attacco esterno**: avviato dall'esterno del perimetro di sicurezza da un utente non autorizzato del sistema.

Infine, una contromisura è qualsiasi mezzo utilizzato per affrontare un attacco. Idealmente, una contromisura può essere progettata per prevenire il realizzarsi di un particolare tipo di attacco.

Quando la prevenzione non è possibile, o in alcuni casi fallisce, l'obbiettivo è individuare l'attacco e poi ripristinare le risorse dagli effetti dell'attacco. Una contromisura potrebbe introdurre nuove vulnerabilità, in ogni caso anche dopo l'applicazione delle giuste contromisure potrebbero risultare presenti delle vulnerabilità residue; queste vulnerabilità potrebbero essere sfruttate da agenti malintenzionati rappresentando un livello residuo di rischio per le risorse di sistema.

2.3.1 Tipologie di attacchi

Andiamo quindi a descrive, sempre basandoci sul modello fornito dal documento RFC2828, i tipi di attacco e le relative conseguenze.

Divulgazione non autorizzata Rappresenta una minaccia alla riservatezza.

- **Esposizione**: può essere intenzionale, come quando un interno rilascia informazioni sensibili, ad esempio numeri di carta di credito, ad un attaccante esterno(ingegneria sociale). Può anche essere il risultato di un errore umano, hardware o software, che risulta nell'ottenimento di dati sensibili da parte di un agente non autorizzato.

- **Intercettazione**: questa è una tipologia di attacco comune nel contesto delle comunicazioni. All'interno di una rete condivisa, come ad esempio LAN o Ethernet, qualsiasi dispositivo collegato può ricevere una copia dei pacchetti destinati ad un altro dispositivo. In Internet, un determinato hacker può ottenere accesso al traffico e-mail e ad altri servizi di trasferimento dati(*MITM-Man In The Middle Attack*). Tutte queste situazioni creano il potenziale per degli accessi non autorizzati ai dati.

- **Analisi del traffico**: in questo caso l'attaccante è in grado di ottenere informazioni dall'osservazione dei pattern di traffico su una rete, come ad esempio la quantità di traffico tra due particolari *host* sulla rete(*sniffing*).

- **Intrusione**: un esempio di intrusione è un attaccante che riesce ad ottenere accesso non autorizzato a dati sensibili superando le protezioni di controllo degli accessi del sistema(*privilege escalation*).

Truffe In questa tipologia rientrano gli attacchi riguardanti l'integrità di sistema e/o dei dati.

- **Finzione**: un esempio di finzione può essere il tentativo da parte di un utente non autorizzato di ottenere accesso ad un sistema fingendosi

appunto un utente autorizzato. Un ulteriore esempio è fornito dalle logiche maligne, come i Trojan, che fingono di svolgere funzioni utili ma in realtà ottengono accesso non autorizzato alle risorse di sistema o ingannano l'utente facendogli eseguire altre logiche maligne.

- **Manipolazione**: si riferisce all'alterazione o sostituzione di dati validi oppure all'introduzione di dati falsi all'interno di file o database.

Interruzione di servizio Le minacce di questo tipo riguardano la disponibilità e/o l'integrità di sistema.

- **Disattivazione**: questo è un attacco alla disponibilità del sistema. Può risultare nella distruzione fisica o nel danneggiamento dell'hardware del sistema. Più tipicamente, software malevolo, come ad esempio Trojan, virus o worm, può operare in maniera tale da disattivare l'intero sistema o alcuni dei suoi servizi.

- **Corruzione**: attacco all'integrità di sistema. In questo contesto il software malevolo può operare in maniera tale da alterare le risorse di sistema o il funzionamento di determinati servizi. Un esempio di questa metodologia è quello di un agente che inserisce una *backdoor* all'interno del sistema per ottenere successivamente accesso al sistema e alle sue risorse in maniera differente dalla procedura usuale.

- **Ostruzione**: un modo di ostruire le operazioni di un sistema è quello di interferire con le comunicazioni disabilitando i collegamenti o alterandone le informazioni di controllo. Un'altra metodologia è quella di sovraccaricare il sistema con richieste superiori a quelle sopportabili(*buffer overflow*).

Usurpazione Minacce riguardanti l'integrità di sistema.

- **Appropriazione indebita**: può includere il furto del servizio. Un esempio è un attacco *DDos(Distributed Denial of Service)*, ovvero quando del software malevolo viene installato su un numero ingente di host(*botnet*) che saranno utilizzate come piattaforma per eseguire altrettante richieste su una macchina obbiettivo. In questo caso, il

software malevolo utilizza in maniera non autorizzata le risorse del sistema operativo ospite.

- **Abuso**: può accadere per mezzo di software malevolo o tramite un hacker che riesca ad ottenere accesso non autorizzato al sistema. In entrambi i casi, le funzioni di sicurezza possono essere disabilitate.

Da questa semplice schematizzazione ci è già possibile capire la complessità dei problemi legati alla sicurezza informatica, esistono tipologie di attacco specializzate per aggirare ogni tipologia di barriera posta a protezione di dati e sistemi. I requisiti di sicurezza si modificano ogni qualvolta un attaccante trova il modo di aggirarli, si potrebbe dire che è un costante bilanciamento delle forze tra chi pone dei limiti e chi tenta di superarli.

2.4 Trend della sicurezza informatica

Prendiamo a titolo di esempio i dispositivi "intelligenti", basti pensare agli oggetti di uso domestico che rientrano nella categoria IoT(*Internet of Things*), che rendono la nostra vita più facile e comoda. Queste "cose" una volta connesse, sono in grado di raccogliere e trasferire dati automaticamente, senza alcuna interazione umana; un mondo di oggetti di uso quotidiano sempre connessi, comporta, tuttavia, una maggiore superficie di attacco per i cybercriminali. I produttori sono numerosi e, in un mercato altamente competitivo tendono ad avere la precedenza quegli elementi concepiti per rendere più facile e comoda la vita dell'acquirente. Come già detto, quindi, la sicurezza non viene considerata durante la fase di progettazione.
Questo uno degli esempi più recenti che ha portato, nel corso degli ultimi anni, a porre attenzione proprio alle tematiche della cybersecurity. Un'attenzione così forte ha portato queste tematiche a tutti i livelli della società, ponendo nuove sfide soprattutto a governi e aziende che hanno dovuto fronteggiare una nuova tipologia di minaccia. Sono state istituite delle agenzie nazionali ed internazionali: tra le più conosciute ricordiamo il *NIST(National Institute of Standard and Technology)* con una divisione dedicata alla cybersecurity, l'*ENISA(Agenzia Europea per la Sicurezza delle Reti e dell'Informazione)* e nell'ambito del nostro territorio nazionale il

Framework Nazionale per la Cybersecurity, *CERT* e *CERT-PA*. Queste e tante altre aziende hanno come scopo principale quello di diffondere degli approcci, corredati da buone pratiche, per affrontare preventivamente le problematiche legate alla sicurezza.
Per dare consistenza alla discussione fatta fin qui ci baseremo sul *Rapporto 2016 sulla sicurezza ICT in Italia* stilato da *CLUSIT-Associazione Italiana Sicurezza Informatica*, basato su un campione complessivo di oltre 5.200 incedenti noti, che hanno avuto un impatto particolarmente significativo per le vittime in termini di perdite economiche, reputazione, diffusione di dati sensibili, avvenuti nel mondo dal primo gennaio 2011 al 30 giugno 2016. Nel rapporto si legge che il problema non è tanto che si verrà attaccati, ma quali saranno gli impatti degli attacchi andati a buon fine sulla sicurezza di organizzazioni, utenti, clienti e partner, e come impedire al maggior numero possibile di incidenti di verificarsi[4]. Nel primo semestre del 2016 sono stati analizzati 521 attacchi a fronte dei 495 del secondo semestre 2015 con un incremento del +5%, tendenza che gli esperti dicono sia destinata ad aumentare. Delle 18 categorie di servizio in cui il CLUSIT classifica le diverse realtà aziendali, nel primo semestre del 2016 la crescita maggiore degli attacchi gravi si è osservata nei settori bancario/finanza e salute; complessivamente, su 18 categorie considerate, due rimangono invariate, 5 appaiono in calo ed altrettante risultano stabili, mentre 6 mostrano un aumento nel numero di attacchi.

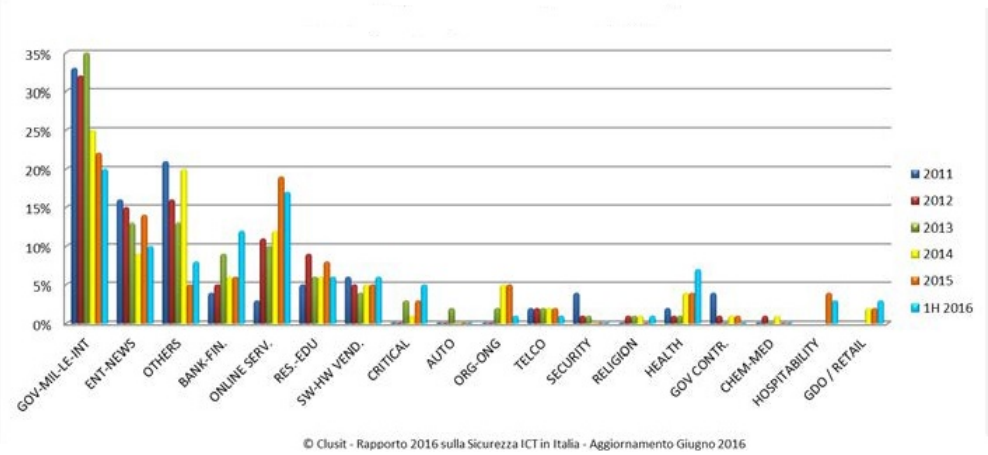

Figura 2.2: Attacchi per tipologia di servizio

Al primo posto troviamo il settore governativo con un quinto degli attacchi(20%), al secondo posto i servizi online/cloud(17%), al terzo posto, come già accennato, il settore bancario/finanziario con un incremento del +93% rispetto al semestre precedente fa registrare il maggior numero di attacchi degli ultimi 11 semestri. Rispetto al semestre precedente crescono anche il settore salute(+143%), sempre più sotto attacco con finalità di furto di informazioni ed estorsione tramite Ransomware, e la categoria infrastrutture critiche(+84%).
Alla luce di questi dati è evidente come la tematica della sicurezza informatica debba diventare sempre più centrale e correre al fianco dei futuri sviluppi delle tecnologie digitali.

Capitolo 3

Quadro normativo

Abbiamo visto come l'anno 2016 sia iniziato con un numero piuttosto rilevante di incidenti di sicurezza correlati ad operazioni di hacking compiute a danno di ospedali e apparecchiature mediche. Nel tempo il trend non si è invertito affatto, se facciamo riferimento a vicende ben più recenti - il Ransomware WannaCry che ha messo in ginocchio i sistemi sanitari Inglese e Spagnolo oltre che tante altre infrastrutture critiche[3] - , bensì si è andato accentuando. L'industria dell'IoT è in piena crescita; inoltre, il settore delle apparecchiature mediche può generare notevoli ed evidenti preoccupazioni in termini di sicurezza informatica. Ma perché? Cominciamo col dare una definizione di 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 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; di diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap; di studio, sostituzione o modifica dell'anatomia o di un processo fisiologico; di intervento sul concepimento, il quale prodotto non eserciti l'azione principale, nel o sul corpo umano, cui è destinato, con mezzi farmacologici o immunologici

> né mediante processo metabolico ma la cui funzione possa essere coadiuvata da tali mezzi".[1]

Risulta immediato dalla definizione appena fornita che le preoccupazioni in termini di sicurezza informatica relativamente ai DM siano fondate, dato che gli strumenti dell'ICT utilizzati a fini diagnostici rientrano appieno nella suddetta definizione. A fronte di quanto appena detto, all'interno della direttiva 2007/47/CE del Parlamento Europeo e del Consiglio troviamo una ulteriore chiarificazione:

> "Occore chiarire che un software è di per sé un dispositivo medico quando è specificamente destinato dal fabbricante ad essere impiegato per una o più delle finalità mediche stabilite nella definizione di dispositivo medico. Anche se utilizzato in un contesto sanitario, il software generico non è un dispositivo medico".[5]

L'accesso non autorizzato a questi dispositivi potrebbe produrre effetti gravi: potrebbe infatti comportare non solo il furto dei dati personali ma potrebbe pregiudicare direttamente la salute, se non la vita dei pazienti. Immaginiamo ad esempio uno scenario dove l'attaccante, una volta ottenuto il pieno accesso all'infrastruttura medica, possa manipolare i risultati dei sistemi di diagnosi o di trattamento; le attività condotte dai medici, in alcuni casi, dipendono da questi dispositivi medici: una manipolazione del genere potrebbe comportare la prescrizione di un trattamento errato ad un paziente, peggiorando le condizioni di salute di quest'ultimo.
In aggiunta a questo, all'interno dell'allegato II del D.lgs. 97/46, punto 12.1-bis troviamo una precisazione:

> "Per i dispositivi che incorporano un software o costituiscono in sé un software medico, il software è convalidato secondo lo stato dell'arte, tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione dei rischi, della validazione e della verifica".[1]

É chiaro quindi come il software DM sia normato per essere definito tale, successivamente andremo ad analizzare proprio quella che è la normativa in merito alla gestione del rischio del software dispositivo medico.

Bisogna inoltre ricordare che all'interno dei sistemi di elaborazione dei dispositivi medici e nell'infrastruttura che li ingloba circolano le informazioni riguardati lo stato di salute dei pazienti. Queste informazioni sono classificate come dati sensibili e sono normate dal *Codice in materia di protezione dei dati personali*, del quale vengono qui riportati i comma 6, 7 e 8 per dare un'idea generale sull'importanza acquisita dalle informazioni sullo stato di salute:

> "6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
> 7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche dati senza l'ausilio di strumenti elettronici.
> 8. I dati idonei a rivelare lo stato di salute non possono essere diffusi."[16]

Con questa ulteriore precisazione risulta chiaro come sia necessario un approccio che tenga in considerazione tutte e tre le proprietà chiave di sicurezza, disponibilità e sicurezza dei dati e del sistema.

Capitolo 4

La sicurezza in ambito sanitario

4.1 Gestione del rischio per software DM

Il software è spesso una parte integrante dei DM, stabilire la sicurezza e l'efficacia di un dispositivo medico contenete software richiede la conoscenza dell'ambito di impiego di tale software e la dimostrazione che quel software soddisfi quelle richieste senza causare rischi inaccettabili. É importante chiarire che il software in sé non rappresenta un rischio, ma potrebbe contribuire a situazioni rischiose. Bisognerebbe sempre considerare il software in una prospettiva di sistema poiché la gestione del rischio non può prescindere dalla visione d'insieme.
Per la successiva analisi ci baseremo sul report IEC/TR 80002-1:2009[9], andando quindi a discutere dell'applicazione dei requisiti contenuti nello standard ISO 14971:2007[6], su cui questo technical report si basa implementando appunto il processo di gestione del rischio.

4.1.1 Requisiti generali per la gestione del rischio

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

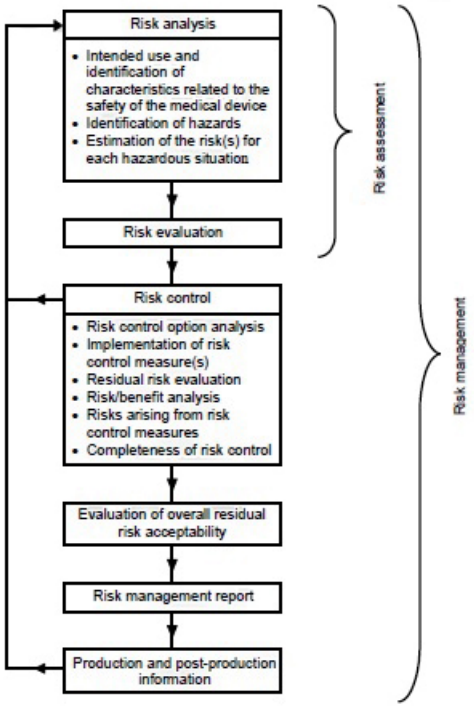

Figura 4.1: Processo di gestione del rischio

Bisogna sottolineare che gli aspetti di gestione del rischio legati al software devono essere focalizzati sui rischi del dispositivo medico, non solo sul rischio di fallimento del software, per essere efficaci. La gestione del rischio dovrebbe cominciare già nelle prime fasi di progettazione, ad esempio una progettazione pro-attiva è preferibile rispetto ad una reattiva.

Con un approccio pro-attivo, la sicurezza è tenuta in considerazione insieme alle altre esigenze del cliente. Mentre l'approccio reattivo si focalizza sulla destinazione di utilizzo del dispositivo medico e, solo in una fase tardiva, valuta i rischi e considera la sicurezza.
I vantaggi di un approccio pro-attivo sono:

- le specifiche di sistema, fin dall'inizio, includono non solo la destinazione d'uso del DM ma identificano i comportamenti che dovrebbero essere evitati per ridurre il rischio
- massimizza la sicurezza intrinseca per progettazione

Le caratteristiche maggiormente desiderabili di un sistema sicuro includono:

- utilizzo di meccanismi di sicurezza hardware semplici per evitare richieste eccessive sugli elementi software di sicurezza
- gestire le condizioni di guasto in maniera appropriata:
  - spegnimento sicuro in condizioni di guasto
  - metodi di rilevamento e/o prevenzione dalla corruzione di dati

É necessario inoltre stilare un piano di gestione del rischio, considerando il software come parte del dispositivo medico, che includa:

- una descrizione del DM includendo quali delle sue funzionalità saranno implementate nel software
- una dichiarazione attestante che il software sarà sviluppato secondo le regole presenti in IEC 62304[8]
- un riferimento al piano di sviluppo del software
- i criteri di accettabilità del rischio per i rischi correlati al software, se diversi dai criteri di accettabilità utilizzati per le altre componenti del DM
- attività di verifica

Infine, viene richiesto anche un file di gestione del rischio grazie al quale sia possibile tenere traccia di tutti i cambiamenti a cui il software sarà soggetto durante il proprio ciclo di vita.

4.1.2 Analisi del rischio

L'analisi del rischio è un'attività da cui il produttore non può prescindere, essa è composta di tre attività distinte:

- identificazione della destinazione d'uso
- identificazione dei pericoli conosciuti e prevedibili insieme alle loro cause
- stima del rischio per ogni pericolo e situazione pericolosa

Identificazione della destinazione d'uso

Ogni dispositivo medico ha una destinazione d'uso ben specifica, c'è comunque una probabilità di un uso improprio di questo; sebbene questa non sia una preoccupazione specifica del software, il suo utilizzo può comportare un aumento del rischio di abuso in quanto:

- il comportamento del DM è più complesso e quindi più difficile da controllare o capire
- l'utente potrebbe affidarsi troppo al software, senza capirne le limitazioni
- il DM potrebbe essere configurabile e l'utente potrebbe non essere al corrente della configurazione

L'utilizzo del software nei dispositivi medici rende possibile una gamma di interconnessioni tra DM e dispositivi non DM. É probabile che queste connessioni diano origine a nuovi utilizzi del sistema comprendente il dispositivo medico e gli altri dispositivi interconnessi. É quindi importante per il produttore specificare un insieme limitato di usi previsti per le interfacce di comunicazione del dispositivo medico e di progettare tali interfacce in maniera tale da limitare le interconnessioni a quelle sicure.

Identificazione dei pericoli

A differenza di calore, energia elettrica e similari, il software di per sé non rappresenta un pericolo ma potrebbe contribuire a situazioni pericolose. Elenchiamo alcune di queste situazioni pericolose a cui può contribuire il software:

- il software può implementare correttamente un requisito di sistema pericoloso, portando a comportamenti la cui natura pericolosa non viene apprezzata finché non si verifica un danno effettivo
- la specifica del software potrebbe implementare in modo non corretto un requisito di sistema, portando ad un comportamento indesiderato corretto in base alla specifica del software
- il progetto e l'implementazione del software potrebbero essere difettosi, portando a comportamenti contrari alla specifica del software

Table B.1 – Examples of causes by software function area

Software Function Area	Example causes for HAZARDS	Questions to ask
Data		
Clinical Information	SYSTEM accesses wrong patient RECORD and user interface display does not make it apparent, SYSTEM stores data from patient in wrong archive	Can there be display of multiple independent identifiers to put the user in the loop of detecting mix-ups? Can critical identifiers be embedded with actual data as a cross-check?
Reports	Report provides incorrect data or identifies it in the wrong sequence or without units.	What reports will be used for clinical purposes? What is the SEVERITY of HARM if the data is incorrect? How likely is it that a clinician would notice the problem?
Databases	Data corruption due to side-affects from SYSTEM level failures or SOUP.	How can data corruption be detected prior to use of the data? Can this be done with each use instead of only at start-up?
Diagnostics		
Decision-making Diagnosing SW	Artifact detection indication suppresses asystole indication on the display.	Has the alarm indication hierarchy been thoroughly reviewed and also reviewed with clinical staff?
Data Reduction	Arithmetic precision errors result in invalid result. Algorithm uses or displays incorrect units.	What arithmetic precision is required? How should mathematical formulas be coded to ensure adequate precision?
Automated PMs	Background diagnostic modifies data temporarily but while application code is retrieving the data for actual use. Background diagnostic interferes with proper timing.	Are application PROCESS locked out during diagnostics at appropriate times? Are diagnostics locked out during critical timed cycles?
SECURITY		
	No or inadequate protection of access to critical configuration parameters or data.	What data is critical and should not be modifiable by the user or should require supervisory authorization to do so? Is an audit trail needed?
	No or inadequate protection of access to controls of therapy or instrument operation.	Should operators be required to login before operation? Can patients inadvertently operate the MEDICAL DEVICE?
	No or inadequate protection from data and commands submitted through communications interfaces or networks.	What should be allowed remotely? Should assumed controls at the remote SYSTEMS be relied on and if so why?

Figura 4.2: Esempi di aree funzionali nel software correlate a rischio

Inoltre, il software presenta la particolare sfida della complessità, incluse eventuali interfacce utente complesse. Pertanto l'identificazione dei rischi del software non può essere svolta in maniera a sé stante ma dovrebbe essere svolta a livello di sistema da un team multidisciplinare composto da esperti clinici, ingegneri informatici, progettisti di sistemi ed esperti in usabilità.

Stima del rischio

Per stimare il rischio relativo al software è necessario prima di tutto identificare le situazioni di pericolo che includo il software. Il software potrebbe essere sia la causa iniziale della sequenza di eventi che portano ad una situazione pericolosa, o potrebbe essere in qualsiasi punto della catena di eventi. Esistono delle metodologie per identificare il ruolo del software in situazioni pericolose:

- **FTA(Fault Tree Analysis)**: è un metodo top-down utilizzato spesso a partire dal sistema del DM, il cui obbiettivo primario è individuare le cause di danno. Assume che si sia verificata una situazione pericolosa e procede all'indietro per identificare come sia potuta accadere. FTA può essere utilizzato per identificare componenti software coinvolte in una sequenza di eventi che ha portato ad una situazione pericolosa.

- **FMEA(Failure Modes and Effects Analysis)**: approccio bottom-up che comincia dai singoli componenti chiedendosi quali sarebbero le conseguenze se quel componente fosse danneggiato. In questo caso l'anomalia software è nota e può essere analizzata per il suo contributo alla catena di eventi che risulta in una situazione pericolosa.

Quando si identificano le sequenze di eventi che possono provocare una situazione pericolosa la correlazione tra il software per un DM(es. algoritmo di misurazione livelli di glucosio nel sangue) e le cause specifiche per i pericoli a questo collegati è di facile intuizione. Bisogna però porre attenzione anche a quelle situazioni di pericolo causate da anomalie software meno comuni. Nell'identificare misure di controllo del rischio, sarebbe improduttivo cercare di tracciare ogni possibile situazione pericolosa per ogni anomalia software; generalmente è meglio identificare i tipi di sequenze per ricavare

dei meccanismi di rilevazione e controllo del rischio per ognuno in modo da minimizzare il rischio.

4.1.3 Controllo del rischio

All'interno di un sistema complesso possono presentarsi molte sequenze di eventi che potrebbero portare a situazioni di pericolo, non è necessario né possibile applicare ad ognuna di queste delle misure di controllo del rischio; è sufficiente applicare tali misure a eventi selezionati in maniera tale da ridurre la probabilità generale di danno ad un livello accettabile.
All'interno di IEC/TR 80002-1 troviamo tre misure di controllo del rischio che il produttore può applicare.

Sicurezza intrinseca In questo caso la sicurezza fa parte della progettazione, ovvero, vengono rimosse funzionalità poco sicure del DM o modificata l'implementazione di tali funzionalità in una maniera più sicura. Nello sviluppo del software si cerca sempre di includere tutte le specifiche richieste dell'utente senza discriminazione, portando ad un eccessivo numero di interazioni tra le diverse componenti software, introducendo inevitabilmente situazioni di pericolo inaspettate. Nella maggioranza dei casi, la sicurezza intrinseca applicata al software, coinvolgerà:

- l'eliminazione di funzionalità superflue
- cambiamenti nell'architettura software per evitare sequenze di eventi che portino a situazioni pericolose
- semplificazione dell'interfaccia utente per ridurre la probabilità dell'errore umano
- specificità delle regole di progettazione del software per evitare anomalie dello stesso

Un esempio di quest'ultimo punto potrebbe essere il solo utilizzo di allocazione statica della memoria per evitare i problemi software connessi ad un'allocazione dinamica.

Misure protettive Le misure protettive per un dispositivo medico che fa uso del software possono essere implementate sia via hardware che via software. Il progetto di una misura protettiva deve essere indipendente dalla funzione alla quale viene applicata, obbiettivo relativamente semplice da ottenere quando si implementano misure protettive per il software via hardware e viceversa. Nel selezionare misure protettive software che si applicano ad altro software è necessario che il produttore dimostri un'adeguata segregazione tra la misura protettiva e le funzionalità specifiche del software. Ad esempio, il software utilizzato per fornire il trattamento al paziente può funzionare su un processore, mentre il software che implementa le misure protettive funziona su un processore differente.

Informazioni per la sicurezza L'esperienza utente rispetto all'utilizzo del software in un dispositivo medico può risultare complessa, questo causa una maggiore dipendenza dalle informazioni per la sicurezza, che vanno dai semplici avvisi su schermo a manuali complessi e corsi di formazione specifici. La complessità di tutti questi fattori può essere ridotta ponendo attenzione ad una buona progettazione dell'interfaccia utente.

Risulta chiaro che gli ambiti di intervento per le misure di controllo del rischio sono diversi, i punti evidenti ai quali queste misure sono applicabili risultano essere:

- **input al software**,limitare il numero di possibili input utilizzando misure di controllo del rischio hardware o software

- **output del software**, verificare che in uscita siano presenti valori inclusi in un intervallo sicuro e internamente consistenti

- **interfacce interne tra i moduli software**

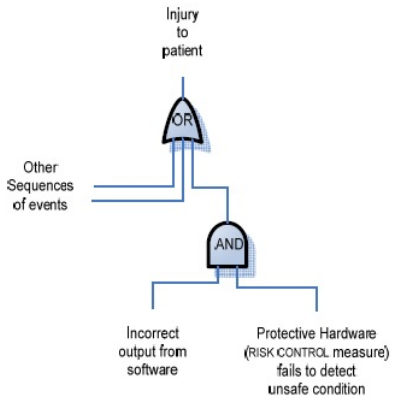

Figura 4.3: FTA che mostra le misure di controllo del rischio per gli output

4.1.4 Produzione e post-produzione di informazioni

Il produttore deve stabilire, documentare e mantenere un sistema per acquisire e revisionare le informazioni in merito al dispositivo medico durante la produzione e la post-produzione. La gestione del rischio software continua attraverso l'intero ciclo di vita del software, viene richiesto al produttore di stabilire dei piani di manutenzione che riguardano l'utilizzo delle procedure per ricevere, documentare, valutare, risolvere e tenere traccia delle risposte dopo il rilascio del software DM.

Abbiamo potuto vedere, seppur in forma molto ridotta, quanto lo standard riguardante la gestione del rischio del software dispositivo medico sia completo ed esaustivo per i produttori. La cybersecurity di questi dispositivi è garantita da altri standard più propriamente orientati al ciclo di sviluppo del software e dal fatto che la sicurezza all'interno di questo standard è considerata nella maniera più ampia possibile, includendo inevitabilmente anche i concetti propri della sicurezza informatica.

4.2 Gestione del rischio per reti IT Medicali

La convergenza di dispositivi medici e infrastrutture IT ha provocato un grande mutamento nel modo in cui sicurezza ed efficacia di un DM vengono gestiti. In questa sezione daremo un'idea di quelli che sono i rischi, e come si gestiscono, quando si integrano dispositivi medici all'interno di reti IT; passeremo quindi dal singolo DM visto in precedenza ad una visione di sistema vera e propria. Ci baseremo su quello che è lo standard che per primo ha considerato come connettere dispositivi medici e reti IT, ovvero la norma tecnica IEC 80001-1[10].

Alcuni dei principi base su cui è fondato lo standard sono:

- l'incorporazione o l'eliminazione di un dispositivo medico o di altri componenti di una rete IT è un compito che richiede un intervento progettato
- la gestione del rischio dovrebbe essere applicata prima dell'incorporazione di un DM all'interno di una rete IT e durante l'intero ciclo di vita della rete IT, per evitare rischi inaccettabili, compreso il possibile pericolo per i pazienti
- la documentazione annessa dovrebbe fornire istruzioni su come incorporare il DM nella rete IT, su come il dispositivo medico trasferisce le informazioni sulla rete IT e sulle caratteristiche minime della rete IT necessarie per rispettare la destinazione d'uso del DM, quando questo è incorporato nella rete IT. La documentazione annessa dovrebbe avvisare dei pericoli associati all'uso improprio del collegamento della rete IT o dei dati trasferiti attraverso di essa
- la gestione del rischio dovrebbe essere utilizzata per garantire le tre proprietà chiave di sicurezza, efficacia e sicurezza dei dati e del sistema

4.2.1 Ruoli e responsabilità

La norma ci introduce a quelli che sono ruoli e responsabilità riassunti nell'immagine seguente tratta dalla norma stessa.

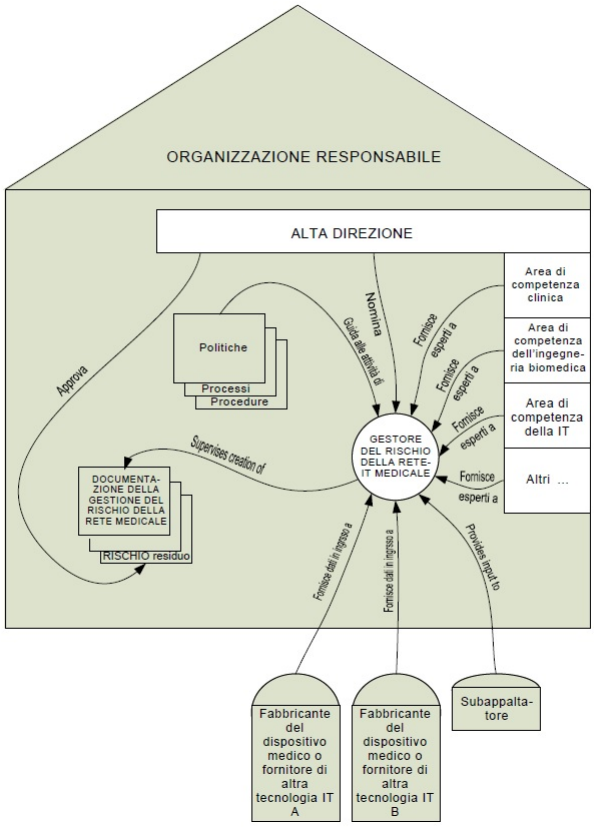

Figura 4.4: Panoramica ruoli e relazioni

Vediamo quindi quali sono gli aspetti più caratterizzanti di ognuno degli attori coinvolti in questo processo di integrazione tra IT e dispositivi medici.

L'intera responsabilità della gestione del rischio per una rete IT medicale deve risiedere all'interno della organizzazione responsabile(es. la struttura ospedaliera). Questa deve farsi carico del processo di gestione del rischio per la rete IT medicale, della pianificazione complessiva, la progettazione, l'installazione, il collegamento dei dispositivi, la configurazione, il funzionamento, la manutenzione e la messa fuori servizio dei dispositivi.

Per la gestione del rischio delle reti IT medicali, l'alta direzione deve assumere la responsabilità di:

- definire una politica per la gestione del rischio per incorporare i dispositivi medici
- definire la politica per determinare il rischio accettabile
- assicurare la reperibilità di risorse adeguate
- riesaminare i risultati delle attività della gestione del rischio a intervalli definiti

Il risk manager della rete IT medicale viene nominato dall'alta direzione e deve avere la responsabilità della gestione del processo di gestione del rischio; inoltre, deve supervisionare l'esecuzione del processo di gestione del rischio per il mantenimento delle proprietà chiave della rete IT medicale.

Ciascun fabbricante di dispositivi medici, in conformità alle corrispondenti norme, deve fornire all'organizzazione responsabile la documentazione annessa disponibile, che descrive la destinazione d'uso e fornisce le istruzioni necessarie per un uso sicuro ed efficace del dispositivo medico. Nel caso di dispositivo medico collegabile ad una rete IT, il fabbricante deve fornire le istruzioni per realizzare tale collegamento specificando:

- lo scopo del collegamento
- le caratteristiche richieste alla rete IT
- la configurazione richiesta alla rete IT
- le specifiche tecniche del collegamento di rete del DM, comprese le specifiche di sicurezza
- il flusso di informazioni tra il dispositivo medico, la rete IT medicale e gli altri dispositivi collegati a tale rete

I fornitori di altri prodotti(non DM) del comparto IT possono fornire:

- i componenti e i servizi delle infrastrutture
- i server
- il software intermedio(*middleware*)

Inoltre, ciascun fornitore di prodotti IT deve fornire la documentazione applicabile alla tecnologia fornita:

- descrizione tecnica e manuali
- caratteristiche richieste dalla rete IT
- configurazioni raccomandate dei prodotti
- incompatibilità e limitazioni note
- requisiti di funzionamento
- informazioni relative alla sicurezza cibernetica(vulnerabilità note)

4.2.2 Requisiti generali per la gestione del rischio

Una volta definito il contesto e gli agenti che vi partecipano, vediamo come il processo di gestione del rischio si sviluppa.
L'organizzazione responsabile deve preservare le proprietà chiave della rete IT medicale durante tutto il ciclo di vita. Per supportare il ciclo di vita della rete IT medicale, l'alta direzione deve definire e documentare la politica di gestione del rischio utilizzata per incorporare i dispositivi medici in una rete IT. La politica di gestione del rischio deve includere:

- il bilanciamento delle tre proprietà chiave rispetto alla missione aziendale dell'organizzazione responsabile
- mezzi per definire i criteri di accettabilità del rischio per ciascuna delle proprietà chiave

- una descrizione del o il riferimento ai processi che si applicano alle reti IT medicali includendo almeno
  - la gestione degli eventi
  - la gestione del rilascio delle modifiche
  - la gestione della configurazione
  - il monitoraggio

Il risk manager della rete IT medicale deve definire e mantenere un processo per identificare i pericoli, stimare e valutare i rischi associati, controllare tali rischi e monitorare l'efficacia del controllo del rischio, tenendo conto dell'uso definito della rete IT medicale.
L'organizzazione responsabile deve pianificare la gestione del rischio della rete IT medicale fornendo:

Descrizione delle risorse rilevanti per il rischio Un insieme non esaustivo di risorse potrebbe includere l'hardware, il software e le informazioni necessarie per la destinazione d'uso del dispositivo medico e all'uso definito della rete IT medicale. Sono inclusi:

- i componenti specifici della rete IT medicale, tutti i dispositivi medici incorporati e le altre apparecchiature dell'infrastruttura IT
- applicativi software medicali
- la caratterizzazione dei dati riferibili a pazienti sulla rete IT medicale o utilizzati dal dispositivo medico incorporato, compresa la loro natura, dimensione e grado di sensibilità
- le informazioni di supporto alle procedure sanitarie, inclusa la cronologia di utilizzo e i dettagli dell'operatore/utilizzatore
- una descrizione dello stato di sicurezza dei dati e del sistema e di altri contenuti importanti per le considerazioni sulla sicurezza generale del sistema

Documentazione della rete IT medicale Necessaria a supportare la gestione del rischio della rete IT medicale per le interfacce tra i dispositivi medici e tutti i componenti della rete. Questa documentazione deve includere:

- configurazione fisica e logica della rete
- struttura fisica e logica dei sistemi client/server
- sicurezza, affidabilità e integrità dei dati della rete
- requisiti di comunicazione di rete per ciascun dispositivo medico così come specificati dal fabbricante
- modifiche, aggiornamenti e miglioramenti futuri

Piano di gestione del rischio per la rete IT medicale É necessario fornire e mantenere un piano di gestione del rischio che deve comprendere:

- la descrizione della rete IT medicale
- una descrizione dell'attività, dei ruoli e delle responsabilità di tutte le parti coinvolte nel funzionamento della rete IT medicale
- le prescrizioni per il monitoraggio della rete IT medicale
- i criteri per l'accettabilità dei rischi, basati sulla politica per determinare il rischio accettabile dell'organizzazione responsabile

Le attività di gestione, analisi, valutazione e controllo del rischio, la valutazione del rischio residuo e di stesura del rapporto ed approvazione devono essere documentate. Tale documentazione può essere parte integrante del piano di gestione del rischio, oppure può essere costituita da documenti separati all'interno della documentazione relativa alla gestione del rischio associata alla rete IT medicale.

4.2.3 Analisi del rischio

L'organizzazione responsabile deve identificare i possibili pericoli derivanti dalla rete IT medicale, per ciascun pericolo deve poi stimare i rischi associati.

4.2.4 Valutazione del rischio

Per ciascun pericolo identificato, l'organizzazione responsabile deve decidere se:

- i rischi stimati sono abbastanza bassi da non necessitare riduzioni
- i rischi stimati non sono accettabili

Nel caso in cui i rischi stimati risultino inaccettabili bisogna implementare delle misure di controllo del rischio.

4.2.5 Controllo del rischio

L'organizzazione responsabile deve identificare e documentare le misure per il controllo del rischio proposte per ciascun rischio inaccettabile, finché i rischi residui possano ritenersi accettabili. Una o più opzioni di seguito elencate devono essere utilizzate per un corretto controllo del rischio:

- controllo intrinseco tramite progetto(es. separazione fisica di una rete da minacce esterne)
- misure di protezione(es. allarmi)
- informazioni per la sicurezza(es. documentazione per l'utilizzatore)

Nel momento in cui il controllo del rischio preveda dei compromessi in merito alle proprietà chiave, queste vanno preservate in un ordine di priorità che è sicurezza, efficacia e protezione dei dati e del sistema. Sono previste poi delle fasi di verifica delle misure di controllo del rischio per valutare eventuali nuovi rischi a seguito delle misure di controllo del rischio.

A fronte di questo ulteriore excursus fatto in merito alla sicurezza di sistemi complessi che integrano dispositivi medici e tecnologie proprie dell'IT anche in questo caso la normativa è completa ed esaustiva. In aggiunta a quella appena discussa sono presenti degli ulteriori documenti tecnici come ad esempio IEC/TR 80001-2-1[12] e IEC/TR 80001-2-2[11] che ne specializzano gli aspetti generali qui discussi.

4.3 Un esempio esplicativo

Si è visto come il rischio, in entrambe le norme che ne regolano la gestione, sia considerato principalmente da una prospettiva di probabilità di danno fisico al paziente e/o di danno al dispositivo medico. Questo implica che nell'analisi del rischio, al fine di prevenirlo, vengano considerate soprattutto quelle cause che potrebbero condurre alle situazioni pericolose prima definite. La proprietà chiave di protezione dei dati e del sistema viene preservata per ultima nel caso in cui siano necessari dei compromessi in merito alle tre proprietà chiave per rendere il rischio accettabile. Ma se da questa proprietà dipendessero in maniera retroattiva le altre due?
Nell'articolo di Marin et al.,[15] troviamo un buono spunto per poter rispondere a questa domanda. Il loro lavoro si è concentrato su una classe specifica di dispositivi medici individuata nei dispositivi ICD(*Implantable Cardioverter Defibrillator*, utilizzati per monitorare e supportare il controllo delle aritmie), avendo come punto di partenza una scatola nera e approcciando il problema in maniera inversa: sono state così analizzate le proprietà di sicurezza del sistema e di privacy relative a tali dispositivi. A partire dall'acquisizione dei segnali scambiati tra dispositivo impiantabile e dispositivo atto alla programmazione di questo, il team di ricercatori è riuscito a risalire ai pattern di dati e, di conseguenza, alle informazioni che transitavano tra uno e l'altro dispositivo. Una volta ottenute tutte le informazioni sulla logica comunicativa e sulle modalità di funzionamento del dispositivo le conseguenze negative sono più che prevedibili, dato che ne va della vita stessa del paziente.

Inoltre viene fatto notare come molti produttori spesso facciano affidamento nel non divulgare le specifiche dei protocolli di comunicazione per fornire la sicurezza, approccio conosciuto come *security-by-obscurity* e ritenuto molto dannoso dagli autori.
Questo caso di studio ha dimostrato come la proprietà chiave di sicurezza dei dati e del sistema debba diventare sempre più centrale nell'ambito del dibattito sulla sicurezza, poiché potrebbe influenzare in maniera retroattiva quelle proprietà chiave che sono già ampiamente perseguite, al fine di garantire un ambiente più sicuro sotto tutti i punti di vista.

Conclusioni

Come già sottolineato in precedenza, il mondo della sanità sta subendo un processo di massiccia digitalizzazione. Grazie all'ingresso in questo ambito di tecnologie embedded e soluzioni di home caring, la cura della salute ha acquisito nuove e rivoluzionarie forze che ci pongono altrettante sfide. Si è potuto vedere come l'interesse da parte di hacker sia cresciuto e continui a crescere nei confronti di un settore che non si sarebbe mai pensato potesse richiamare questo genere di attenzioni.
Il rischio cibernetico per le organizzazioni che forniscono servizi sanitari è ormai argomento di grande attualità, per citare un esempio a noi vicino basti pensare ai nuovi requisiti introdotti per il Fascicolo Sanitario Elettronico(FSE) che introducono tematiche come la cifratura e il controllo degli accessi. Per quanto riguarda i dispositivi medici e le reti IT medicali che li accolgono, la normativa è matura. Ci sono però delle criticità in merito ad interfacce e protocolli di comunicazione in quanto i produttori sviluppano i loro dispositivi medici attenendosi alle linee guida ma su base proprietaria, rendendo così l'interoperabilità difficile da realizzare: sarebbe auspicabile un processo di standardizzazione su questo fronte. Come conseguenza i risk manager sono obbligati a scendere dei compromessi riguardo aggiornamenti di sistema e sicurezza che spesso inficiano la proprietà chiave di sicurezza dei dati e del sistema. Quello che fino a qualche anno fa era appannaggio dei soli clinici, allo stato attuale necessita di un approccio multidisciplinare che includa tecnici IT ed esperti in sicurezza, in modo da garantire l'interoperabilità senza rinunce riguardo le proprietà chiave e di conseguenza la sicurezza a tutti i livelli.
Un tale obbiettivo è raggiungibile solo grazie ad una politica di security first che preveda la formazione di tutto il personale coinvolto al fine di renderlo

più consapevole e di arginare l'incidenza del fattore umano. É inoltre necessario che vengano implementate delle misure di controllo delle reti più stringenti come il filtraggio degli indirizzi, la cifratura delle comunicazioni secondo standard più rigorosi, una raffinata differenziazione dei privilegi di accesso degli utenti e tutte quelle tecniche di protezione già consolidate nel mondo IT. Forse trattare la sicurezza informatica al pari della sicurezza vera e propria dei pazienti è la via per una corretta gestione delle nuove sfide poste dalla salute digitale.

Bibliografia

[1] Decreto lgs. del 24 febbraio 1997, n.46. *Gazzetta Ufficiale*.

[2] D. Battu. Measuring the information society (11 october 2012)–itu. *Communication Networks Economy*, pages 253–253.

[3] Z. Chang. Cyberwarfare and international humanitarian law. 2017.

[4] Clusit. Rapporto sulla sicurezza ict in italia. *Milano: CLUSIT*, 2016.

[5] P. E. e Consiglio dell'Unione Europea. Direttiva 2007/47/ce. *Gazzetta Ufficiale dell'Unione Europea*.

[6] I. O. for Standardization. *ISO 14971 Medical devices-Application of risk management to medical devices*. ISO, 2007.

[7] B. Guttman and E. A. Roback. *An introduction to computer security: the NIST handbook*. DIANE Publishing, 1995.

[8] I. IEC. Iec 62304 medical device software-software life cycle processes. *IEC: Geneva, Switzerland*, 2006.

[9] I. IEC. Iec/tr 80002-1 medical device software-part 1: Guidance on the application of iso 14971 to medical device software. *IEC: Geneva, Switzerland*, 2009.

[10] I. IEC. 80001-1-application of risk management for it-networks incorporating medical devices-part 1: Roles, responsibilities and activities. *International Electrotechnical Commission, Geneva*, 2010.

[11] T. IEC. 80001-2-2-application of risk management for it-networks incorporating medical devices-part 2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls. *International Electrotechnical Committee*, 2011.

[12] T. IEC. 80001-2-1-application of risk management for it-networks incorporating medical devices-part 2-1: Step by step risk management of medical it-networks; practical applcations and example. *International Electrotechnical Committee*, 2012.

[13] I. ISO. 7498. *Reference Model for OSI.*

[14] J. F. Kurose and K. W. Ross. Reti di calcolatori e internet. *Un approccio top-down (III edizione)*, 2013.

[15] E. Marin, D. Singelée, F. Garcia, T. Chothia, R. Willems, and B. Preneel. On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. *ACSAC '16 Proceedings of the 32nd Annual Conference on Computer Security Applications Pages 226-236*, 2016.

[16] G. per la privacy. Codice in materia di protezione dei dati personali. 2003.

[17] P. Recommendations. International standards equivalent in technical content–ccitt recommendation x. 800 (1991). *Security architecture for Open Systems Interconnection for CCITT applications.*

[18] R. Shirey. Rfc 2828: Internet security glossary (may 2000). *Status: Informational.*

[19] S. William and B. Lawrie. *Computer Security: Principles And Practice.* Pearson Education, 2012.

Elenco delle figure