Progettare per la Sanità

Organizzazione, tecnologia, architettura

04_18

CNETO
Centro Nazionale
per l'Edilizia
e la Tecnica Ospedaliera

Spazio e architettura ospedaliera: quando le attività funzionali innescano quelle sociali / Organizzazione e funzionalità all'insegna dell'high-tech all'ospedale **Rey Juan Carlos** di Madrid / La **costruzione modulare prefabbricata:** l'Azienda sanitaria dell'Alto Adige sceglie i moduli Cadolto / Le corrette scelte progettuali dell'impianto elettrico nei **DEA** / Modelli organizzativi dell'Ospedale di Comunità / Come garantire la **sicurezza nel sistema informativo sanitario** e nei dispositivi medici collegati / **Human Technopole,** la scommessa italiana / Antibiotico-resistenza: intervista a **Francesco Menichetti** Presidente GISA / Il modello **NextVision** per ottimizzare il PDTA per il trattamento della degenerazione maculare

L'ospedale Rey Juan Carlos di Madrid
Progetto di Rafael de La-Hoz

edra

Promuovere l'innovazione con ricerca e prevenzione

L'ospedale Rey Juan Carlos di Madrid
Progetto di Rafael de La-Hoz

Nei Paesi avanzati, si stima che l'80% delle risorse sanitarie venga speso nella gestione delle malattie croniche. Gli scenari futuri, tutt'altro che ottimistici, sottolineando l'incremento di tutte le patologie legate all'invecchiamento della popolazione e alla crescente esposizione a fattori di rischio ambientali e sociali, evidenziano l'urgenza di affrontare il problema della sostenibilità economica dei nostri sistemi sanitari.

In questo complesso e articolato contesto di fragile equilibrio tra risposte alla malattia e risorse disponibili, è universalmente riconosciuto il ruolo importantissimo della prevenzione e della gestione del paziente attraverso piani di cura personalizzati. Servono quindi centri altamente specialistici, con una stretta interconnessione con la ricerca, e in cui si insegni al cittadino a prendersi cura di sé, promovendo stili di vita sani.

Già da parecchi anni, in Paesi all'avanguardia come gli Stati Uniti, sono stati realizzati importanti modelli di riferimento in tal senso; ambienti favorevoli alla condivisione della conoscenza in cui mettere in atto la "concentrazione dei saperi", attraverso la creazione di team multiprofessionali che collaborano fianco a fianco.

È la direzione che si sta perseguendo con il progetto lanciato nel 2015, alla chiusura dell'esposizione universale di Milano, di Human Technopole. Un progetto che, con la sua struttura altamente innovativa costituita da 7 centri di ricerca, sarà operativo entro il 2024 e concentrerà 1500 persone all'interno di un'area di 30.000 mq. Un hub di riferimento per gli istituti di ricerca, le università e gli ospedali in cui si utilizzeranno tecnologie e metodologie innovative, quali la genomica e l'analisi dei big data, al fine di sviluppare nuovi percorsi diagnostici e terapie indirizzate alla persona. Ma l'impegno di Human Technopole sarà anche quello di promuovere quel rinnovamento culturale, in cui i cittadini siano educati a stili di vita più sani e alla prevenzione e i pazienti abbiano accesso a nuove cure più velocemente.

Un passo importante verso quelle eccellenze che sovente invidiamo al di fuori del contesto italiano.

Margherita Carabillò

Progettare per la Sanità

Organo ufficiale del C.N.E.T.O.: Centro Nazionale per l'Edilizia e la Tecnica Ospedaliera

Direttore Responsabile
Giorgio Albonetti

Direttore Scientifico
Margherita Carabillò

Coordinamento Editoriale
Chiara Scelsi

Redazione
Fabio Chiavieri

Comitato scientifico
Stefano Capolongo, Margherita Carabillò, Albert de Pineda, Eric de Roodenbeke, Gilles Dussault, Tiziana Ferrante, Giuseppe Manara, Maurizio Mauri, Paolo Pettinelli, Walter Ricciardi, Aymeric Zublena

Comitato di redazione
Architettura: Cristina Donati
Nuove tendenze: Stefano Carera
Impiantistica: Simone Cappelletti
Information Technoloy:
Fabrizio Massimo Ferrara
Organizzazione e management:
Federico Lega
Servizi e facility management:
Maurizio Pedrini

Hanno collaborato a questo numero:
L. Baldessin, R. Boerci, M. Capponi, S. Carera, L. Cavazzana, F. M. Ferrara, R. Guccione, M. Miserendino, N. Paltrinieri, N. Principi, L. Ricci, M. Violante, A. Zenorini

Coordinamento Stampa & Produzione
Walter Castiglione (Responsabile rivista)
w.castiglione@lswr.it Tel. 02 88184.222

Pubblicità
Stefano Busconi (responsabile vendite)
dircom@lswr.it - Tel. 02.88184.404

Archivio immagini
Shutterstock

Traffico
Donatella Tardini (Responsabile)
d.tardini@lswr.it Tel. 02 88184.292
Stefania Bruno
s.bruno@lswr.it Tel. 02 88184.261

Abbonamenti
Tel. 02 88184.233 | Fax 02 56561173
e-mail: abbonamentiedra@lswr.it
Costo copia singola: euro 2,50
(Presso l'Editore, fiere, manifestazioni)
2016: abbonamento annuale Italia euro 30,00
abbonamento annuale Europa euro 60,00

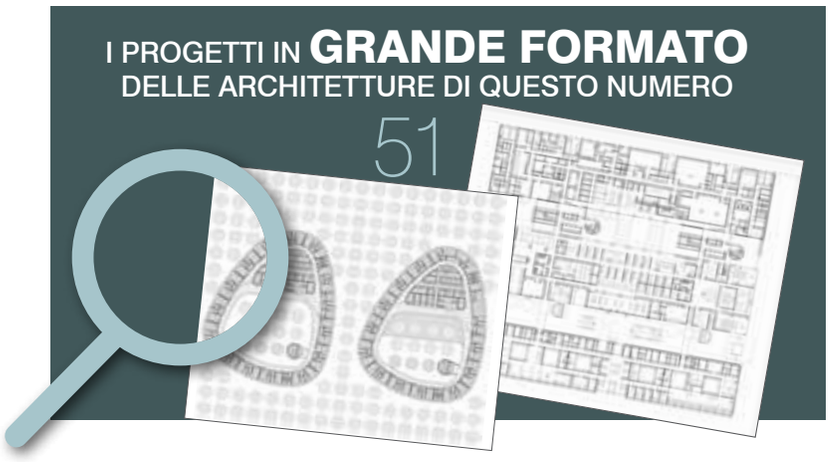
Stampa
mccgraphics
Pol. Ind. Txirrita Maleo Pab 11
20100 Errenteria (Gipuzkoa), Spain

Progettare per la sanità - bimestrale
Reg. Trib. Milano n. 767 del 09/11/1998
Iscrizione al ROC n. 23531 del 06/05/2013

Testata Associata
A.N.E.S.
ASSOCIAZIONE NAZIONALE
EDITORIA PERIODICA SPECIALIZZATA

Testata volontariamente sottoposta a certificazione di tiratura e diffusione in conformità al Regolamento CSST - Certificazione Editoria Specializzata e Tecnica

Sommario **di settembre**



Le aziende presenti in questo numero

Abbiamo parlato di:

di Massimo Capponi, Fabrizio Massimo Ferrara, Mariachiara Violante

La sicurezza dei dispositivi medici nel **sistema informativo sanitario**

Le attività sanitarie si basano sempre più sull'impiego di dispositivi medici. La sicurezza complessiva del binomio "sistema informativo + dispositivo medico" influenza, direttamente e indirettamente, la protezione dei dati, la qualità del servizio erogato e -in definitiva- la salute del paziente

È ormai ampiamente riconosciuto che in una azienda sanitaria moderna il sistema informativo non può essere un semplice insieme di tecnologie e programmi software più o meno correlati fra loro, ma deve rappresentare uno strumento completo e integrato per il governo della struttura, sia dal punto di vista della gestione corrente, sia sotto il profilo della strategia evolutiva, assicurando la continuità dei processi aziendali attraverso i diversi settori e l'integrazione e la disponibilità del patrimonio informativo sotto il profilo sia clinico che amministrativo. E questo sia all'interno dell'azienda che nel contesto della rete territoriale per la continuità del percorso assistenziale del paziente.

In una tale visione, una valenza particolare assume ovviamente la gestione della "sicurezza" (includendo in questo termine anche gli aspetti di protezione dei dati personali, secondo quanto prescritto dal recente Regolamento UE 2016/679), che va intesa non solo dal punto di vista prettamente tecnologico, ma in quadro più ampio, tale da garantire l'esecuzione sicura e corretta dei processi aziendali, minimizzando e prevenendo – per quanto possibile– tutti i rischi ai quali l'azienda può essere esposta. Rischi che – nel settore sanitario – assumono una rilevanza particolare in quanto possono avere implicazioni anche sulla stessa salute del paziente.

Anche per quanto riguarda il profilo normativo, vale la pena di sottolineare come il Regolamento UE sulla protezione dei dati personali definisca principi e regole di ampio respiro, non circoscrivibili a singole attività o procedure ma di rilevanza per tutte le attività dell'organizzazione. Il loro rispetto nell'ambito del sistema informativo, pertanto, richiede un approccio organico e integrato che tenga conto di tutti gli aspetti in tutti i settori: dall'organizzazione dei dati, alle funzionalità, alle tecnologie.

In questa visione maggiormente strategica, anche le caratteristiche funzionali ed informative del sistema informativo costituiscono quindi elementi fondamentali e qualificanti ai fini della sicurezza e della gestione del rischio nell'azienda sanitaria.

In estrema sintesi l'obiettivo finale di un "sistema informativo sicuro" può essere individuato nella capacità di seguire e supportare senza soluzione di continuità i processi dell'organizzazione (sia quelli che si esauriscono all'interno di un singolo settore che – soprattutto – quelli che si articolano attraverso settori diversi) e di rendere disponibili tutte le informazioni di potenziale rilevanza nei tempi e nei modi appropriati per le diverse esigenze, assicurando che le tutte le attività possano essere condotte nel rispetto dei requisiti di:

- SAFETY, ovvero evitare di fare danno per errore;
- SECURITY, ovvero evitare di fare danno per dolo;
- RESILIENCE, ovvero capacità di operare in tutte le condizioni;
- TRUST, ovvero garantendo affidabilità ed il rispetto delle norme.

In un tale scenario, la gestione della sicurezza nei sistemi informativi e la definizione di strategie evolutive che tengano conto sia delle possibilità connesse a nuovi modelli organizzativi, a nuovi protocolli clinici e a nuove tecnologie (e dei rischi connessi), sia delle normative sempre più precise e stringenti si deve necessariamente basare su un approccio multidimensionale.

Nel 2016, in collaborazione con la Direzione Generale dei sistemi informativi del Ministero della Salute, l'ALTEMS (Alta Scuola di Economia e Management dei Sistemi Sanitari) ha condotto una indagine a livello nazionale sulla sicurezza dei sistemi informativi sanitari coniugando la "tradizionale" analisi degli aspetti – organizzativi, informativi, funzionali e tecnologici – del sistema informativo con le prospettive proprie dell'approccio dall' Health Technology Assessment, quali il rischio clinico, l'impatto sul paziente, l'aspetto economico, le implicazioni etiche, la rispondenza alle normative ecc. come schematizzato in fig. 1.

Fig. 1: L'approccio multidimensionale alla sicurezza nel sistema informativo

Secondo questo approccio e partendo da questo quadro di validità generale in qualsiasi sistema informativo sanitario, è stato recentemente avviato un nuovo studio finalizzato a dettagliare un modello di riferimento per gli aspetti di sicurezza specifici dei contesti – sempre più rilevanti – in cui i dispositivi medici elettronici rivestono un ruolo significativo nel processo assistenziale e di cura. Va infatti considerato che sempre di più le prestazioni erogate in ambito ospedaliero sono basate su un impiego intensivo di apparecchiature e dispositivi medici, il cui grado di efficienza e di efficacia può influenzare, direttamente ed indirettamente sia la qualità del servizio erogato che la sicurezza del paziente e degli operatori. Per valutare l'impatto del rischio sulla salute, la FDA suggerisce l'approccio basato su cinque livelli qualitativi di gravità per determinare se il rischio per le prestazioni cliniche del dispositivo è controllato (accettabile) o non controllato (inaccettabile):

- **Trascurabile:** disagio o disagio temporaneo
- **Minore:** lesioni o menomazioni temporanee che non richiedono un intervento medico
- **Serio:** lesioni o menomazioni che richiedono un intervento medico professionale
- **Critico:** lesioni critiche, menomazioni permanenti o lesioni pericolose per la vita
- **Catastrofico:** morte del paziente

Fig. 2: Valutazione del rischio in funzione del livello di sicurezza

Questi livelli di rischio rappresentano il termine di riferimento ultimo ai quali relazionare i vari aspetti della sicurezza, considerati nel loro insieme e tenendo conto che l'affidabilità di un sistema complesso è determinata dall'affidabilità del componente più debole.

Con questo approccio è necessario implementare un processo per valutare il rischio relativo relazionando il livello della sicurezza complessiva (ovvero tenendo conto di tutti gli aspetti) del binomio sistema informativo + dispositivo medico con la possibile gravità dell'impatto sulla salute dei pazienti, come schema-

tizzato in fig. 2. Agendo sui vari aspetti (organizzativi, informativi, funzionali e tecnologici) della sicurezza si deve ridurre il rischio ad un livello accettabile.

AUMENTO DEL RISCHIO CIBERNETICO NEL SETTORE SANITARIO

Negli ultimi anni, si riscontra un aumento continuo del numero di attacchi informatici alle organizzazioni sanitarie e queste, in genere, non risultano adeguatamente preparate. La velocità di cambiamento nelle tecnologie ha superato la capacità delle strutture politiche, legali e normative di adattarsi, lasciando il settore sanitario senza una struttura di sicurezza univoca e chiara da seguire.

Ciò ha portato la maggior parte delle aziende e dei produttori, ad adottare un proprio approccio nella progettazione dei dispositivi causando problemi di interoperabilità e obsolescenza dei sistemi che continuano a essere usati poiché (di solito) le organizzazioni non intendono o non possono rimpiazzarli.

La convergenza tecnologica ha reso commercialmente disponibili moltissimi dispositivi medici che incorporano al loro interno comuni infrastrutture di rete, sistemi operativi, software, interfacce con dispositivi mobili intelligenti, computer e sistemi di controllo. Quindi oggi molti dispositivi medici potrebbero essere vulnerabili alle violazioni della sicurezza informatica poiché spesso incorporano sistemi operativi datati e vulnerabili, non più compatibili o addirittura non più supportati.

Inizialmente, la motivazione principale degli attacchi informatici era il valore delle informazioni relative ai pazienti sul mercato nero; di recente invece, si assiste a un drammatico aumento dei crypto-ransomware con cui i criminali utilizzano del malware per crittografare le informazioni e poi richiedere un riscatto alle organizzazioni sanitarie per recuperare le informazioni segretate e per ripristinare l'operatività della struttura. Sfortunatamente, una scarsa sicurezza informatica potrebbe anche influire sulla salute del paziente oltre a rivelare impropriamente le sue informazioni sensibili.

Le aziende produttrici di dispositivi medici e soprattutto le organizzazioni sanitarie, oggi devono affrontare nuove minacce informatiche, sempre più complesse e sofisticate:

- interruzione dell'assistenza/servizio sanitario (con rischio di decesso dei pazienti);
- inganno del personale operativo tramite mail contraffatte o falsi siti Web per ottenere credenziali di accesso al sistema, apparati, reti e/o installare malware sui dispositivi;
- minacce interne (insider threat), involontarie o intenzionali, che possono rappresentare una minaccia significativa per la posizione privilegiata all'interno dell'organizzazione;
- perdita di dati sensibili e/o informazioni sui pazienti, in particolare quelle sanitarie protette elettronicamente;
- perdita e/o violazione dei dati, appropriazione indebita delle informazioni, perdita di beni e/o dell'operatività;
- ricatto, estorsione e/o costrizione attraverso lo sfruttamento dei dati riservati sottratti;
- furto di proprietà intellettuale.

Inoltre, la sicurezza informatica continua a focalizzarsi sulla protezione dei dati sanitari dei pazienti senza affrontare le vere minacce e proteggere adeguatamente la salute dei pazienti. La riservatezza delle informazioni è una priorità per i sistemi ospedalieri mentre la protezione dell'individuo è una priorità quando i pazienti dipendano da dispositivi medici come parte integrante della loro cura. In quest'ultimo caso, la vera priorità è la corretta funzionalità operativa dei dispositivi, in un contesto sempre più ampio, come rappresentato in fig. 3.

I DISPOSITIVI MEDICI NEL CONTESTO TECNOLOGICO DEL SISTEMA INFORMATIVO

Recenti ricerche hanno dimostrato che gli incidenti dovuti a dispositivi connessi non-computing (come i dispositivi medici) si classificano tra le prime tre cause di impatto finanziario grave e che questo tipo di incidenti è destinato ad aumentare.

L'ECRI Institute, ha recentemente pubblicato la lista dei 10 principali rischi (generici) relativi alle tecnologie medicali emergenti per il 2018 da cui emerge che almeno la metà delle cause sono direttamente riconducibili a vulnerabilità dei dispositivi medici o dei sistemi e apparati cui essi sono collegati:

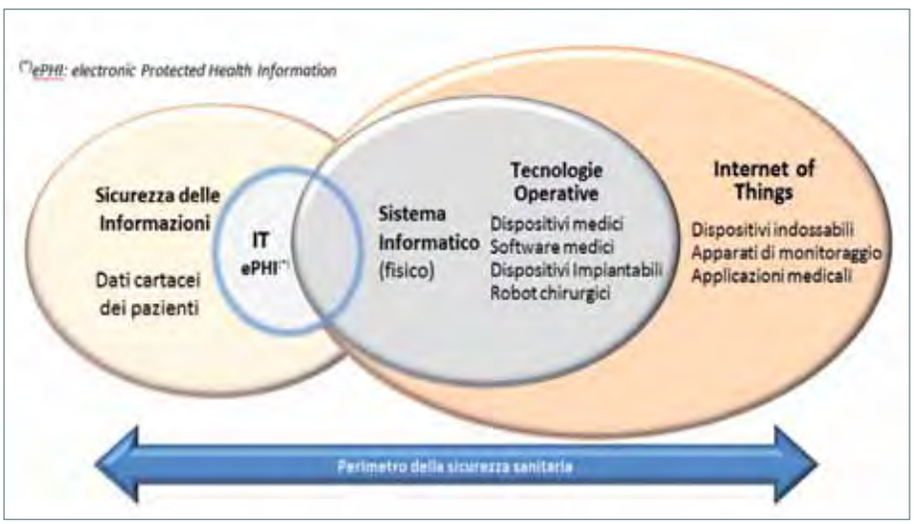


Fig. 3: Il perimetro della sicurezza sanitaria

- ransomware e altre minacce alla sicurezza informatica (con potenziale impatto sui pazienti);
- mancata rilevazione degli allarmi per inappropriata configurazione di dispositivi e sistemi;
- errata manutenzione causa di malfunzionamenti dei dispositivi, guasti alle apparecchiature (e potenziali lesioni al paziente);
- errori di impostazione e/o utilizzo (workarounds, modalità operative alternative) che possono annullare la sicurezza dei dispositivi e sistemi (i.e., somministrazione automatizzata di medicinali);
- impatti (di qualsiasi tipo) sulla rete dei dispositivi medici che possono portare a cure ritardate e/o inappropriate.

Relativamente al software, poiché la sua sicurezza dipende prima di tutto dalla sicurezza del dispositivo su cui esso è installato, lo si deve considerare componente fondamentale nel caso dei dispositivi medici connessi in rete, situazione che rappresenta anche uno degli attuali scenari possibili dell'IoT e ancor più di quelli futuri. Un software affetto da vulnerabilità che controlli un dispositivo connesso alla rete e che venga considerato a basso rischio (Classe I), potrebbe essere sottovalutato (se non ignorato) nell'analisi dei rischi ma diventare il punto di accesso per gravi azioni malevole contro l'intero sistema.
Inoltre, la connessione di molteplici dispositivi alla rete implica una superficie di attacco maggiore e quindi, maggiori possibilità di diventare bersaglio dei criminali informatici; pertanto, oltre alla sicurezza dei sistemi centrali, si devono considerare attentamente altri aspetti (i dispositivi, l'infrastruttura e la rete) affinché il sistema complessivo possa ritenersi intrinsecamente sicuro.
La sicurezza IoT, fino a poco tempo fa sostanzialmente ignorata, è diventata ora argomento di grande preoccupazione. Sono state prese alcune misure per evitare problemi e rischi principali nei sistemi complessi ma molto resta da fare sui dispositivi più piccoli e soprattutto per quelli obsoleti.
In risposta alla crescente diffusione delle minacce e alla domanda di standard per il settore delle infrastrutture critiche, è stata sviluppata la Raccomandazione ITU-T Y.4806 "Security capabilities supporting safety of the Internet of Things", allo scopo di determinare quali siano le funzionalità di sicurezza specifiche che supportano l'esecuzione sicura delle applicazioni.
Per contrastare le vulnerabilità, si deve partire dalla loro identificazione e determinare i tipi di impatto oltre a eseguire l'analisi e la modellizzazione delle minacce alla sicurezza funzionale del sistema per individuare le misure di sicurezza che consentano quanto meno di mitigarne il rischio.
Molti dispositivi hanno capacità di archiviazione, memoria ed elaborazione limitate e spesso devono essere in grado di funzionare a potenza ridotta (i.e., dispositivi portatili alimentati a batteria) perciò l'approccio alla sicurezza basato sulla crittografia deve essere ripensato, non disponendo della potenza di elaborazione necessaria per elaborare rapidamente le informazioni e per trasmetterle in tempo reale in modo sicuro. Uno dei metodi più utilizzati per proteggerli e aumentare la sicurezza complessiva del sistema, è utilizzare più livelli di difesa, segmentare la rete e inserire i dispositivi su intervalli separati da apparati firewall che compensino i limiti dei dispositivi e consentano di isolarli in caso di intrusione (vedi anche fig. 3, Architettura del Point of Care secondo ISO 11073).
Inoltre, è fondamentale che ogni dispositivo abbia una propria identità e si autentichi prima di accedere alla rete tramite opportuni punti di accesso (gateway). L'infrastruttura dovrebbe fornire un livello di sicurezza predefinito imponendo l'uso di password e certificati forti per ogni dispositivo connesso, impostando i privilegi di accesso consentiti per ciascun dispositivo al minimo indispensabile sulla base delle sue funzioni specifiche e impedendo comunque l'accesso completo all'intero sistema. È altrettanto fondamentale che i dispositivi supportino gli aggiornamenti del firmware e consentano l'installazione di patch come elemento irrinunciabile per la gestione e la manutenzione della rete: un singolo dispositivo che non possa essere aggiornato o che non consenta l'installazione di patch, può compromettere l'intera operatività della rete e consentire l'accesso a persone malintenzionate.
Per questi motivi, una volta protetti i dispositivi, è necessario proteg-

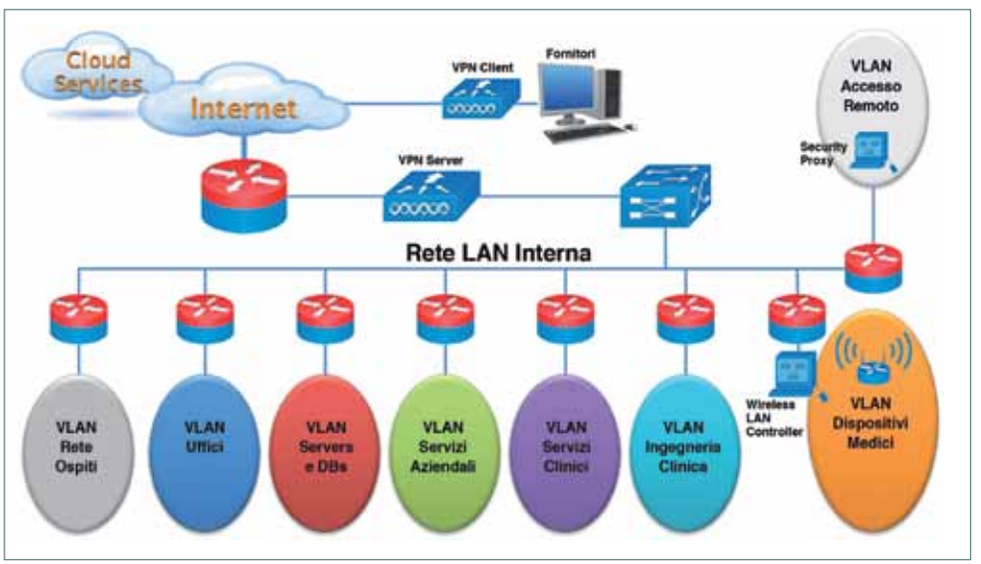


Fig. 4: Fonte: IEEE 11073-00101TM:2008[1]

gere la comunicazione all›interno della rete, quella tra i dispositivi e l'applicazione e i messaggi tra la periferia e il centro.
Tuttavia, nonostante i notevoli rischi per la sicurezza, i sistemi dotati di dispositivi connessi alla rete devono consentire un elevato accesso alle informazioni (senza il quale si perderebbero i vantaggi operativi). Quello che deve essere limitato è la possibilità di infiltrazioni e l'accesso indiscriminato ai dati.
Poiché i malfunzionamenti nel sistema sono inevitabili, è comunque fondamentale analizzare costantemente le vulnerabilità e monitorare le comunicazioni alla ricerca di comportamenti anomali in modo da poter distinguere le diverse situazioni.
Questo approccio richiede un nuovo modo di pensare, progettare e utilizzare reti e sistemi: è il concetto di Security by Design (pensare alla sicurezza fin dalla fase di progettazione del prodotto), fondamentale per garantire che dispositivi e reti siano il più possibile protetti dagli attacchi, lo siano in ogni parte componente il sistema complessivo e per tutto il loro ciclo di vita.

CONVERGENZA TRA PROTEZIONE E SICUREZZA

La protezione nei dispositivi medici fa riferimento ai guasti e come questi possono essere evitati o mitigati per renderli non dannosi. I dispositivi o i sistemi che attuano funzioni di protezione agiscono sul processo sotto controllo per evitare che si verifichino eventi pericolosi ben identificati. Quindi, l'eventualità che un errore non previsto comporti la mancata esecuzione di una funzione di protezione quando invece sarebbe richiesta, è probabilistica, quantitativa e cambia raramente. Viceversa, la sicurezza affronta scenari di attacchi intelligenti e dannosi identificando avversari, loro capacità, intenzioni e risorse, metodi e vulnerabilità che possono essere sfruttate. Quindi la probabilità che una minaccia possa sfruttare una vulnerabilità è un risultato qualitativo che cambia dinamicamente in funzione dei parametri identificati e/o della loro evoluzione man mano che vengono scoperte nuove vulnerabilità e sviluppati metodi per sfruttarle.
Il tradizionale approccio di sicurezza delle informazioni, tipico dell'ambiente IT, Riservatezza/Integrità/Disponibilità (Confidentiality–Integrity–Availability, CIA), non enfatizza questi fattori.
Per i Sistemi Cyber Physical (CPS), come i dispositivi medici e l'ambiente operativo dell'Ingegneria Clinica, è necessario considerare anche la Salvaguardia/Affidabilità/Disponibilità (Safety–Reliability–Availability, SRA) dei processi, dei dispositivi, della rete e dei sistemi connessi. Questa diversità di visione del dominio evidenzia anche come le medesime parole possono essere usate riferendosi ad obiettivi differenti: quando il team di sicurezza IT considera i rischi (i.e., della disponibilità), generalmente si riferisce alle informazioni da una prospettiva di sicurezza informatica o di sicurezza ICT mentre per l'ingegneria clinica e per la funzionalità dei dispositivi medici, la disponibilità si riferirà ai sistemi/dispositivi medici, ai processi e alle funzioni di protezione potenzialmente utilizzate per prevenire operazioni pericolose e controllare i rischi che comportino danni fisici.
Il nuovo approccio deve inoltre includere tutte le funzioni di protezione e valutare le conseguenze di guasti e/o malfunzionamenti con impatto su persone, apparecchiature e ambiente operativo, consapevole della responsabilità legale dei produttori, degli integratori, dei fornitori ICT e delle organizzazioni sanitarie per tutto il ciclo di vita del sistema. Partendo da quanto definito in ambito legislativo (D.Lgs. 196/03[2], UE 679/2016[3]) e normativo (ISO/IEC 27001 ISO/IEC 80001 e ISO 31000), si dovrebbe attribuire ad ogni apparecchiatura o dispositivo medico, una valutazione del relativo livello di sicurezza nelle condizioni d'uso tipiche (IVR: Indice di Valutazione del Rischio) tenendo conto sia delle tematiche tipiche dell'ingegneria clinica (i.e., documentazione e manutenzione delle apparecchiature, rischi collegati al paziente ecc.) sia degli aspetti informatici solitamente trascurati nell'analisi del rischio delle tecnologie biomediche.
Questo valore, ottenuto attraverso metodi statistici e una stima oggettiva dei pesi che renda il modello consistente e ripetibile, potrebbe essere poi inserito nel contesto più ampio di valutazione del livello di sicurezza dell'intera struttura sanitaria.
L'estensione del suo utilizzo a livello territoriale permetterebbe di centralizzare l'archiviazione dei dati relativi ai dispositivi medici delle strutture ospedaliere e l'aggregazione di una grande quantità di questi dati, consentirebbe di applicare il modello al dominio dei Big Data ottenendo risultati dell'IVR sempre più attendibili e un sensibile miglioramento nell'attività decisionale.
Attraverso lo studio di una adeguata mole di dati si potrebbero poi analizzare le variazioni dell'IVR e individuare quei fattori che permettano di prevenire i guasti, garantendo un ciclo di vita più lungo delle macchine e/o inviare avvisi alle ASL interessate prima che la criticità diventi rilevante. Tutto ciò consentirebbe anche di ottenere notevoli benefici dal punto di vista economico (costi legali, risarcimento danni, protezione degli investimenti, manutenzione preventiva ecc.).

APPROVVIGIONAMENTO DI SISTEMI E DISPOSITIVI MEDICI

Per quanto riguarda il tema dell'approvvigionamento, le organizzazioni sanitarie e i produttori di dispositivi medici potrebbero beneficiare dello sviluppo congiunto e condiviso di una serie di specifiche in materia di sicurezza; ciò potrebbe essere facilitato anche dall'utilizzo di un linguaggio di "procurement" condiviso e di linee guida comuni che definiscano e garantiscano la sicurezza integrata nei sistemi e nei dispositivi medici.
In questo modo, le organizzazioni sanitarie avrebbero la possibilità di definire più efficacemente le richieste di offerta mentre i fornitori potrebbero dimostrare che i prodotti proposti adottano processi di sviluppo sicuri, i dispositivi o sistemi soddisfano le specifiche funzionali richieste, garantiscono la sicurezza informatica oltre a quella del paziente e che la gestione del ciclo di vita copre tutti gli aspetti

relativi alla sicurezza, inclusi test di accettazione, verifica, integrazione, manutenzione e qualsiasi tipo di riferimento di supporto (i.e., linee guida, normative o standard).
Naturalmente, anche con l'impegno più attento nell'analizzare e contrastare i potenziali rischi di cyber-sicurezza prima di collocare un dispositivo medico sul mercato, non si possono prevenire le vulnerabilità future derivanti dall'introduzione di nuove tecnologie e conseguenti modalità di attacco.
Si può però valutare la qualità del prodotto proposto, verificando che siano stati rispettati dai fornitori gli standard di produzione e di sicurezza informatica più attuali come, ad esempio, quelli sviluppati per gli ICS ovvero i sistemi di controllo industriali (IEC 62443-4-1 e IEC 62443-4-2).
In molte analisi del rischio, l'equilibrio tra sicurezza, protezione e privacy è ottenuto indirettamente valutando l'impatto e le conseguenze sul business; però i perimetri di sicurezza delle informazioni (sul paziente e sulla sua salute) non affrontano esplicitamente i rischi riguardanti la protezione del paziente né l'approccio alla sicurezza che si deve avere per gestire gli aspetti di tutela della sua incolumità nel caso di dispositivi medici con funzioni di controllo fisico (CPS).
La possibilità di collaborare e condividere un lessico e una comprensione comuni tra le parti, porterebbe ad utilizzare controlli o contromisure per mitigare i rischi relativi alla sicurezza che vengono valutati in base al loro impatto, in particolare sulle funzionalità di protezione e salvaguardia, evitando di introdurre nuovi rischi. Ciò può richiedere la riprogettazione delle funzioni di protezione per affrontare i rischi indotti dalla sicurezza come requisito specifico delle norme di sicurezza funzionale (cfr. IEC 61508).
È anche possibile che le valutazioni del rischio per la sicurezza non debbano più focalizzarsi sull'informazione come la risorsa primaria da difendere ma debbano considerare esplicitamente il contesto operativo per i dati e i risultati oltre ai sistemi e i processi sanitari nei quali tali informazioni vengono utilizzate.

CONCLUSIONI

Per garantire la sicurezza nel sistema informativo e nei dispositivi medici collegati, tutte le parti coinvolte nei processi decisionali ed operativi del perimetro sanitario devono collaborare per identificare e valutare rischi e minacce, definire piani per la loro mitigazione e dare una adeguata risposta agli incidenti, garantendo prima di tutto la sicurezza e l'incolumità dei pazienti (fig. 5)
All'interno dell'organizzazione, nell'ambito della sicurezza e privacy, è determinante stabilire una chiara definizione dei ruoli e delle responsabilità per il sistema interno di controllo e gestione dei rischi di cui l'ente si è dotato o intende dotarsi, nel rispetto dei princìpi di segregazione funzionale dei compiti. La gestione della sicurezza e delle conformità alla privacy necessitano di competenze distintive, di leve gestionali e anche della corretta assegnazione delle funzioni agli opportuni livelli gerarchici affinché i soggetti preposti possano prendere decisioni consapevoli ed essere efficaci nelle azioni da perseguire, rispettando le prerogative assegnate, le disposizioni regolamentari e quelle interne.

Fig. 5: "Framework for Improving Critical Infrastructure Cybersecurity"

Gli autori

MASSIMO CAPPONI
CEO and Cofounder I2oT srl (Italy Internet of Things).
FABRIZIO MASSIMO FERRARA
Docente di Informatica e Sistemi Informativi presso il Corso di Laurea in Economia e Gestione delle Aziende e dei Servizi Sanitari, Università Cattolica del Sacro Cuore
Coordinatore scientifico del "Laboratorio sui sistemi informativi sanitari dell'ALTEMS
MARIACHIARA VIOLANTE
Laboratorio sui sistemi informativi sanitari ALTEMS