TECNOLOGIE E MANAGEMENT PER LA SANITÀ

ISSN 0392-4831 - Mensile - Anno LII

9
NOV023

Tecnica Ospedaliera

Con il patrocinio di

EXPOSANITA'
MED • CARE • INNOVATION

AIIC associazione italiana ingegneri clinici

LIUC BUSINESS SCHOOL

CREMS Centro di Ricerca in Economia e Management in Sanità e nel Sociale

LIUC Università Cattaneo

CONFINDUSTRIA Dispositivi Medici

tecniche nuove
healthcare

ISSN 0392-4831 - Mensile - Anno LII

TECNOLOGIE E MANAGEMENT PER LA SANITÀ

9
NOV023

Tecnica Ospedaliera

www.tecnicaospedaliera.it

Con il patrocinio di

EXPOSANITA'
MED • CARE • INNOVATION

AIIC associazione italiana ingegneri clinici

LIUC BUSINESS SCHOOL

CREMS
Centro di Ricerca in Economia e Management in Sanità e nel Sociale
LIUC Università Cattaneo

CONFINDUSTRIA Dispositivi Medici

OSPEDALI DI COMUNITÀ
NUOVE TIPOLOGIE EDILIZIE

PRONTO SOCCORSO
ORGANIZZAZIONE E PERFORMANCE

REPROCESSING DI ENDOSCOPI
INTEGRAZIONE E OTTIMIZZAZIONE

ADVICE, LA TELEMEDICINA NEL LAZIO

01health. SANITÀ DIGITALE

tecniche nuove
healthcare

SOMMARIO NOVEMBRE 2023

Tecnica Ospedaliera

In copertina:
Nuova BN
via Nessa, 19/21
10048 Vinovo (TO)
tel. 011.9654446
www.nuovabn.it

La sicurezza informatica dei dispositivi medici

La sicurezza informatica è una delle prerogative più importanti per le organizzazioni sanitarie. Poiché attacchi informatici e violazioni dei dati dei pazienti sono sempre più diffusi, le strutture sanitarie si impegnano a proteggere in modo sempre più rigoroso la privacy dei pazienti. I dispositivi medici connessi a una rete di comunicazione possono offrire numerosi vantaggi rispetto ai dispositivi non connessi, come l'accesso a cure sanitarie più convenienti e tempestive. Tuttavia, quando un dispositivo medico è connesso a una rete di comunicazione, la vulnerabilità informatica può rischiare di essere violata, con prevedibili conseguenze e disagi per il paziente. La sicurezza informatica è una responsabilità condivisa con l'industria dei dispositivi medici, le organizzazioni di assistenza sanitaria, i pazienti, i ricercatori sulla sicurezza e altre agenzie governative

KEYWORDS

sicurezza informatica, dispositivi medici, rischio per il paziente

cyber security, medical devices, patient risk

Armando Ferraioli
Bioingegnere, Studio di Ingegneria Medica e Clinica, Cava de' Tirreni (SA)

Cybersecurity is one of the most vital concerns for healthcare organizations around the globe. Hospitals and other care facilities are working harder to protect patients privacy as cyber attacks and patient data breaches become more common. Medical devices connected to a communications network can offer numerous advantages over non-connected devices, such as access to more convenient or more timely health care. However, when a medical device is connected to a communications network, there is a risk that cybersecurity vulnerabilities could be exploited by an attacker, which could result in patient harm. The cybersecurity is a shared responsability with the medical device industry, health care delivery organizations, patients, security researchers and other government agencies.

La crescente incorporazione in sanità di una tecnologia sempre più innovativa porta a una meticolosa precisione nell'assistenza sanitaria, pur essendo ancora necessari ulteriori progressi nella sicurezza informatica. La frequenza delle violazioni di dati è in aumento e la sanità è il settore che subisce gli attacchi informatici maggiori a livello globale. A causa della loro immutabilità, le informazioni alle quali si accede sono di particolare interesse per i criminali. Poiché le cartelle cliniche includono dati privati come nome, data di nascita, informazioni sull'assicurazione e sull'operatore sanitario, informazioni sanitarie e genetiche, non è più possibile ripristinare la privacy o annullare il danno psicosociale allorché i dati privati siano stati violati. Questi attacchi sono una minaccia per l'identità e le finanze dei pazienti e possono ostacolare il regolare svolgimento delle operazioni ospedaliere e mettere a rischio la salute e il benessere dei pazienti. Dal punto di vista degli ospedali, queste violazioni, oltre a causare ritardi operativi, possono avere effetti dannosi a lungo termine sulla reputazione e sui profitti. Il ransomware è una minaccia significativa per la riservatezza, l'integrità e la disponibilità delle informazioni. Quando una macchina o un dispositivo ne è colpito,i dati vengono in genere crittografati, l'accesso è negato ed è richiesto un riscatto, il cui pagamento, però, non garantisce il ripristino dei dati. Oltre al ransomware, esistono altri tipi di malware che rappresentano una minaccia per le organizza-

zioni sanitarie. Questi includono furti di credenziali in base ai quali nomi utente, password e altri token vengono rubati da criminali informatici e wiper con cui intere unità disco possono essere cancellate, senza possibilità di recuperare i dati.

E-mail e phishing

Il phishing è in genere il punto iniziale di compromissione per incidenti di sicurezza significativi; è particolarmente efficace perché è preso di mira il singolo utente, indotto con l'inganno a divulgare informazioni riservate, cliccare su un collegamento dannoso o aprire un allegato dannoso. Il phishing si verifica più spesso attraverso e-mail, benché possa verificarsi anche tramite siti web, social media, messaggi di testo, chiamate vocali. Fra i tratti distintivi delle e-mail di phishing vi sono ortografia e grammatica scadenti, allegati dubbi, affermazioni troppo enfatiche per essere vere e un tono di urgenza o che agisce sulla paura o sull'avidità degli utenti. Le e-mail di phishing generali non vengono inviate a destinatari specifici e non hanno contenuti personalizzati. Sicurezza informatica e protezione delle informazioni sono vitali per il funzionamento delle organizzazioni sanitarie. Molte di esse dispongono di vari sistemi informativi specializzati, come il sistema EHR (Electronic Health Records), sistemi di prescrizione elettronica, sistemi di supporto alla gestione dello studio, sistemi di supporto alle decisioni cliniche, sistemi informativi radiologici e sistemi computerizzati di immissione degli ordini dei medici, oltre a migliaia di dispositivi interconnessi via internet che necessitano di protezione. Questi includono, per esempio, ascensori intelligenti, sistemi intelligenti di riscaldamento, ventilazione e condizionamento dell'aria, pompe per infusione, dispositivi di monitoraggio remoto del paziente. L'e-mail è uno dei principali mezzi di comunicazione nelle organizzazioni sanitarie. La capacità di archiviazione delle caselle di posta tende ad ampliarsi grazie all'archiviazione di tutti i tipi di informazioni preziose. La sicurezza della posta elettronica è quindi parte integrante della sicurezza informatica della struttura. La formazione e la sensibilizzazione alla sicurezza sono fondamentali per contrastare i tentativi di phishing.

LA PROTEZIONE FISICA DEL DISPOSITIVO È IMPORTANTE PER SALVAGUARDARNE IL FUNZIONAMENTO, LA CORRETTA CONFIGURAZIONE E I DATI

Sicurezza fisica

L'accesso fisico non autorizzato a un computer o a un dispositivo può determinarne la compromissione. Esistono tecniche fisiche per hackerare un dispositivo che possono vanificare i controlli tecnici altrimenti in atto. La protezione fisica del dispositivo, quindi, è importante per salvaguardarne il funzionamento, la corretta configurazione e i dati. Un esempio è lasciare un laptop incustodito: azioni negligenti possono portare sia al furto sia alla perdita del laptop o al suo sabotaggio in modo non rilevabile, tale che diventi accessibile all'hacker previa installazione di un keylogger per la registrazione di informazioni sensibili (es. credenziali).

Sistemi legacy

Sono sistemi o componenti obsoleti che restano in uso al posto delle relative versioni aggiornate disponibili sul mercato. Un sistema legacy richiede un'elevata manutenzione, in genere è incompatibile con i sistemi di nuova generazione e la sua riconversione è costosa e complessa. Una sfida alla sicurezza informatica in sanità consiste nell'impronta significativa che molte organizzazioni hanno nell'uso di sistemi legacy. Essi possono permanere nelle organizzazioni sanitarie sia perché non sempre si è in grado di sostenere i costi rilevanti che comporta l'installazione di nuovi sistemi sia perché possono essere integrati in un livello di tecnologia agile che consente di appropriarsi di nuove funzioni in tempi brevi, alla velocità di oggi, evitando investimenti non sempre appropriati all'uso.

Stakeholders sanitari

Lo stakeholder di un'organizzazione sanitaria è anzitutto il paziente, ovvero il consumatore di servizi

sanitari erogati profit o no profit. I pazienti devono essere in grado di comunicare telematicamente e in sicurezza con gli operatori sanitari, mediante telemedicina, messaggistica sicura ecc. Devono acquisire le indispensabili politiche di privacy e di sicurezza nel merito e saper mantenere le informazioni inviate e ricevute in forma strettamente privata. Il coinvolgimento degli stakeholders può generare opportunità per migliorare la gestione e le performance dell'azienda sanitaria. Il personale sanitario preposto al trattamento dei dati sensibili deve essere dotato di un'adeguata formazione relativa alla cyber security, che gli consenta di alzare il livello di sicurezza dei dati sensibili ricevuti e trasmessi. Un attacco informatico che violi un sistema sanitario e scambi, alteri o cancelli informazioni su diagnosi, terapie e cure da somministrare ai pazienti, ne impedisce il recupero, determinando danni che, oltre al disagio fisico, possono portarlo finanche alla morte. Le organizzazioni sanitarie dovrebbero formare e istruire adeguatamente il personale sulle misure di sicurezza informatica da rispettare con ciclicità di aggiornamenti sulle nuove minacce. È sempre più frequente che la semplice ricezione di una mail determini blocco e inaccessibilità ai dati sensibili, bloccando l'operatività di un ospedale, con le conseguenze del caso. Lo stakeholder più evoluto permette di allineare la performance sociale, ambientale ed economica alla strategia attraverso partecipazione attiva e ascolto. I C-Suite sono il livello più elevato di responsabilità manageriale. Il titolo che li identifica inizia sempre per C (chief) e sono direttamente responsabili di un settore definito dell'azienda che rappresentano. Essi hanno il compito di coordinare e mettere in relazione vari ruoli aziendali, ricevendo e trasmettendo informazioni tra colleghi e collaboratori di cui sono garanti e responsabili. Un numero sempre maggiore di organizzazioni sanitarie si avvale della collaborazione di un Chief Information Security Officier (CISO) o di un Chief Risk Officier (CRO) a protezione della propria cyber security. Alcune organizzazioni sanitarie, pur avendo una cyber security informatica soddisfacente, nell'interazione con i vari fornitori dell'azienda (che non sempre applicano politiche di sicurezza informatica rigorose) subiscono problematiche tali da compromettere la cyber security dell'azienda stessa. Per ovviare a ciò, l'azienda sanitaria deve garantire il controllo di quattro punti chiave:

- riservatezza: le informazioni possono essere lette soltanto da chi è autorizzato

LE ORGANIZZAZIONI SANITARIE DOVREBBERO FORMARE E ISTRUIRE CICLICAMENTE IL PERSONALE SULLE MISURE DI SICUREZZA INFORMATICA DA RISPETTARE

- autenticità: discernere la validità delle informazioni
- integrità: completa leggibilità e attinenza delle informazioni
- disponibilità: accessibilità motivata dalle informazioni stesse.

Valutazione del rischio (cyber risk)

La sicurezza informatica richiede il massimo livello di misure preposte a proteggere le informazioni digitali, i dispositivi, le risorse e le informazioni personali desumibili da account, file, foto, intermediazioni finanziarie ecc. La gestione del rischio informatico si avvale di un processo atto a individuare la vulnerabilità del sistema informativo, che potrebbe paventare il rischio di ingenti perdite finanziarie e danni sia economici sia di immagine dell'azienda. La sicurezza informatica infallibile è purtroppo ancora una chimera ed è pertanto necessario un approccio basato sulla gestione del rischio aziendale. Anche con infrastrutture e pratiche IT di qualità, insieme a una protezione proattiva e misure di sicurezza delle informazioni, il rischio di un attacco persisterà. Il valore di un bene per l'organizzazione sanitaria e la sua esposizione al rischio ne determinano la priorità nei processi di protezione. L'IT di qualità è importante in questo caso, poiché la gestione della configurazione sarà parte integrante di questa fase di identificazione. L'analisi del rischio deve valutare un giusto compromesso tra rischi e benefici, oltre che tra rischi diversi, considerando non solo le potenziali conseguenze per la sicurezza del paziente ma anche l'impatto sulla protezione dei dati e della privacy, sulla disponibilità delle informazioni e sulla loro integrità. Quest'ultima è particolarmente importante in quanto la non integrità dei dati sani-

tari può avere gravi conseguenze sulla sicurezza del paziente (che da soggetto passivo è diventato protagonista del suo percorso di cura). Le strutture sanitarie possono gestire i rischi attraverso vari metodi, dall'attenuazione all'evitamento, al trasferimento e all'accettazione del rischio. Poiché gli esseri umani sono l'anello più debole alla base della sicurezza informatica, gli approcci delle strutture sanitarie alla sicurezza informatica dovrebbero tenere conto della necessità di sensibilizzare in tal senso gli utenti, il che non garantisce la sicurezza ma segna un passo importante che porta nella giusta direzione. Gli utenti finali, dai medici al personale addetto alla pianificazione, nonché i pazienti e gli operatori sanitari che collegano i propri dispositivi personali alla rete ospedaliera, possono involontariamente minacciare la sicurezza informatica della struttura sanitaria.

Controlli di sicurezza

La maggiore connettività alle reti informatiche ha esposto le amministrazioni sanitarie a nuove vulnerabilità perché possono verificarsi furti d'informazioni sanitarie, attacchi ai dispositivi medici, attacchi ransomware che possono arrivare a paralizzare i sistemi sanitari ed è per questo che tutte le organizzazioni sanitarie devono disporre di controlli di sicurezza di base avanzati. Non tutti gli incidenti di sicurezza, però, possono essere prevenuti. Un solido piano di risposta in tal senso è indispensabile per la sicurezza informatica nell'assistenza sanitaria, così da bloccare ogni tentativo di attacco se affrontato in modo tempestivo e risolutivo. I controlli di sicurezza di base includono: antivirus, backup e ripristino di file/dati, prevenzione della perdita di dati, gateway di posta elettronica, crittografia a riposo, crittografia per file/dati archiviati, crittografia in transito, firewall, piano di risposta agli incidenti, sistema di rilevamento e prevenzione delle intrusioni, gestione dei dispositivi mobili, politiche e procedure, smaltimento sicuro, formazione alla sensibilizzazione alla sicurezza, programma di gestione delle vulnerabilità/programma di gestione delle patch, gateway web. I controlli di sicurezza avanzati includono: dispositivo antifurto, piano di continuità aziendale e ripristino di emergenza, condivisione di informazioni sulle minacce (chiamata anche condivisione di informazioni), scientifica digital, scansioni delle vulnerabilità, autentificazione a più fattori, segmentazione della rete, test di penetrazione.

Avvalersi di professionisti

I professionisti della sicurezza informatica sono necessari per progettare elementi di sistemi che proteggano i dati dei pazienti, come firewall migliorati, soluzioni di crittografia e reti segmentate. Questi professionisti testano le vulnerabilità del sistema, indagano sugli incidenti, sostituiscono hardware e software obsoleti o rischiosi e sviluppano protocolli di sicurezza. Essi devono essere all'avanguardia nelle competenze tecniche analitiche e orientate ai dettagli avanzati, con capacità di leadership e risoluzione dei problemi. Tali competenze includono la capacità di gestire: monitoraggio della rete; test di sistema (comprese le simulazioni d'attacco); programmazione software; installazione di hardware, software e applicazioni; gestione account utente; indagine sulle violazioni e sulla denuncia dei danni; nuove tendenze di sicurezza informatica (compresi i nuovi strumenti di sicurezza); aggiornamento sulle tendenze tecnologiche tra cui intelligenza artificiale e apprendimento automatico; sviluppo e comunicazione di protocolli di sicurezza e best practice; formazione dei dipendenti su rischi, politiche e procedure per la sicurezza; conformità normativa e rendicontazione.

Raccomandazioni per i dispositivi medici connessi

Dispositivi medici come monitor, pompe endovenose ecc. nonché dispositivi impiantabili e connessi possono propagare difetti o causare incidenti nella sicurezza informatica e agire come elementi deboli nella catena di sicurezza attraverso la quale il malware può diffondersi. Anche se la diversità dei dispositivi può rendere difficile l'adozione di politiche di sicurezza rigorose, la loro sicurezza informatica è fondamentale. I dispositivi medici so-

L'IT DEVE MANTENERE UN INVENTARIO SEMPRE AGGIORNATO DEI DISPOSITIVI SULLA RETE

no in genere a diretto contatto con i pazienti e possono aumentare i rischi negli interventi chirurgici e in tutto ciò che concerne la sicurezza dei pazienti. I progressi come IoMT – Internet of Medical Things (Internet collegato alla tecnologia da indossare) consentono di effettuare cure mediche a distanza e di assicurare una elevata precisione nell'erogazione dell'assistenza sanitaria. Tuttavia, l'utilità e la sicurezza dell'assistenza clinica devono essere bilanciate sia con la sicurezza dei dati sensibili che della privacy. Anche se i dispositivi utilizzati sono altamente interconnessi nella rete ospedaliera e raccolgono grandi quantità di dati clinici che devono essere trasferiti in modo sicuro, detengono limitazioni intrinseche che li espongono a vulnerabilità. Frequentemente essi non dispongono di misure di sicurezza adeguate come ad es. risorse integrate atte a consentire l'impiego di misure di sicurezza quali crittografia e processi forensi, attività di modellazione delle minacce e rilevamento di malware. I dispositivi progettati per espletare la loro funzione in isolamento spesso finiscono per essere integrati nella rete, mentre risulta quasi impossibile garantire la sicurezza fisica dei dispositivi indossabili perché avendo una durata limitata, il loro sistema operativo o le relative piattaforme finiscono per diventare obsoleti in tempi relativamente brevi e la manutenzione dell'apparecchiatura risulta critica per la sicurezza del dispositivo medico.

È inoltre essenziale che l'IT mantenga un inventario regolarmente aggiornato dei dispositivi sulla rete (autorizzati e non). Le reti ospedaliere hanno spesso numerosi dispositivi personali integrati. Pazienti e medici spesso collegano dispositivi mobili e dispositivi indossabili, aumentando così le esposizioni al rischio e inficiando le politiche che permettono di portare il proprio dispositivo. L'organizzazione sanitaria deve adottare misure e politiche ragionevoli atte a bloccare la connettività di dispositivi personali non approvati, anche utilizzando la gestione dei dispositivi mobili o dei sistemi di distribuzione del software, applicando la crittografia dei dati locali, quando possibile, in una posizione preventiva.

Terminologia

Cybersecurity: insieme di mezzi, tecnologie, procedure, tese alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità esplicitati da due concetti fondamentali: 1) sicurezza; 2) affidabilità. Un programma è tanto più sicuro quanto minori sono le probabilità che si verifichi un guasto.
Malware (software malevolo): termine generico riferito ad un programma, a un documento oppure a un messaggio di posta elettronica in grado di sabotare disturbandole, le operazioni svolte da un utente di un computer.
Phishing: truffa operata da soggetti malintenzionati ai danni di vittime impegnate in comunicazioni digitali (di solito e-mail) a cui si chiede di fornire dati sensibili (password, codici fiscali, PIN ecc.).
Ransomware: definito "virus del riscatto", è considerato il peggior attacco informatico degli ultimi anni (blocca il computer e lo rende inutilizzabile). La posta elettronica è il canale di diffusione prediletto dagli hacker che richiedono all'utente il pagamento di un riscatto per ottenere la chiave di sblocco dell'algoritmo crittografico.
Keylogger: strumento hardware o software in grado di effettuare la registrazione (logging) della tastiera di un computer, cioè in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente se ne accorga.
Stakeholder: insieme dei soggetti coinvolti direttamente o indirettamente in un progetto o in un'azienda in cui hanno un interesse specifico e sono per questo interessati a determinare un buon andamento dell'attività stessa.
Wiper: classe di malware distruttivo destinato a cancellare il disco rigido del computer che infetta, eliminando dati e programmi.
Crittografia informatica: base della protezione dei dati che utilizza metodi per rendere un messaggio non comprensibile a quanti non siano autorizzati a leggerlo. Sistema che si fonda sull'utilizzo di algoritmi matematici a sequenze di caratteri in trasformazione e che garantisce la riservatezza nella trasmissione dei dati, tipica della sicurezza informatica.
Gateway: dispositivo di rete che collega due reti informatiche di tipo diverso; specifiche combinazioni hardware e software atte a effettuare conversione di protocollo di rete.
Patch: piccola porzione di software (fix o bugfix) progettata per aggiornare o migliorare un programma e per risolvere un problema di vulnerabilità della sicurezza chiamato in genere bug, all'interno di un programma software o di un sistema operativo.
Firewall: componente di difesa perimetrale, hardware e/o software, che utilizza un insieme di regole per controllare il traffico dati in entrata e in uscita e che fornisce una protezione di sicurezza informatica della rete stessa.

Conclusione

Nell'assistenza sanitaria, la prevenzione di solito è la cura migliore. Questo vale per il mondo reale come per quello digitale. La salute digitale di un individuo può essere direttamente legata alla sicurezza informatica dei sistemi sanitari. Costruire la resilienza informatica di una struttura sanitaria è vitale ed è responsabilità condivisa. Medici e personale amministrativo devono seguire una formazione adeguata e praticare l'igiene digitale (insieme di pratiche quotidiane per evitare virus, furti d'identità, malware); i responsabili devono applicare politiche appropriate e considerare la sicurezza informatica nelle decisioni di acquisto. I produttori devono dotare i prodotti di misure di sicurezza informatica appropriate. I team di sicurezza informatica delle strutture sanitarie devono adottare strumenti atti alla salvaguardia della struttura sanitaria e dei pazienti. La formazione continua dei dipendenti, la consapevolezza delle minacce moderne alle quali si è esposti in rete e la costituzione di gruppi di caccia alle minacce (threat hunting) in grado di individuare minacce nascoste che sfuggono ai controlli automatizzati possono contribuire a limitare gli attacchi.