Il giusto percorso di Cyber Security per la sanità

https://www.ictsecuritymagazine.com/wp-content/uploads/Napoli_Michele.mp4

Le informazioni di natura sanitaria rappresentano, per definizione, dati sensibili e altamente critici in un'ottica di sicurezza cyber.

Con la progressiva digitalizzazione del settore ospedaliero e l'introduzione del FSE (Fascicolo Sanitario Elettronico) assistiamo infatti allo sviluppo di una *Digital Healthcare* che oltre agli innegabili benefici – tra cui la possibilità di colmare, grazie alla Telemedicina, il divario esistente fra differenti accessi alle cure su base locale – implica **numerosi fronti di rischio.**

L'enorme quantità di dispositivi e dati necessariamente coinvolta nell'erogazione dei servizi si scontra, spesso, con infrastrutture obsolete o con personale non sufficientemente preparato a riconoscere e gestire una minaccia Cyber; con il significativo contributo dell'IoMT (*Internet of Medical Things*), che espande ulteriormente la superficie d'attacco a tutto vantaggio dei criminali informatici.

La cornice regolamentare: i paradigmi NIST

Nell'intenzione di fornire un'offerta sanitaria accessibile, paritaria ed efficiente aziende e istituzioni del mondo farmaco-ospedaliero devono sapersi evolvere per abbracciare ogni articolazione di questo nuovo e complesso panorama, in una stretta cooperazione che includa presidi territoriali, grandi hub specialistici e farmacie di quartiere; così

idealmente mettendo “in sicurezza” l’intero percorso terapeutico di ciascun paziente, dalla presa in carico fino alla guarigione e senza tralasciare gli aspetti di prevenzione.

Sul piano normativo una delle principali fonti di riferimento è rinvenibile nel Framework NIST (*National Institute of Standards and Technology*, USA) che individua cinque funzioni essenziali a cui deve assolvere un’efficace piano di sicurezza informatica in qualsivoglia settore:

1. *Identify* – l’identificazione e catalogazione dei dati da tutelare;
2. *Protect* – l’implementazione di tutti gli standard e protocolli concretamente volti alla loro difesa;
3. *Detect* – le operazioni tese a rilevare anomalie o attività malevole;
4. *Respond,* la fase di reazione da attivare in seguito a un Data Breach o altro tipo di attacco;
5. *Recover,* passaggio “postumo” teso a ripristinare i sistemi colpiti nonché ad analizzarne gli effetti così da prevenire simili casi in futuro.

Applicare tale cornice all’ambito della sanità significa assumere la complessità del quadro di riferimento e abbracciare, di conseguenza, una visione della cybersecurity sempre più integrata; sia come processo costante e trasversale, sia come responsabilità condivisa fra tutti gli operatori e gli utenti dei servizi erogati.

Ruoli e responsabilità nell’ambito dei servizi Cloud

Anche per la sanità l’avvento del Cloud, insieme al vantaggio di poter condividere informazioni essenziali in modo sempre più rapido, ha comportato un significativo aumento del rischio: il *Cyber Risk Management* dev’essere allora una priorità per evitare che la portata innovativa degli archivi

digitali sia vanificata da potenziali incidenti, soprattutto considerati gli altissimi costi – umani ed economici – che un'interruzione di servizio può causare in attività così critiche. È quindi necessario prevedere soluzioni di detection e response, rafforzare i sistemi di autenticazione e gestire le vulnerabilità dei propri asset in modo da non comprometterne privacy e sicurezza.

Nel video un breve commento di Michele Laurenzi, Regional Sales Manager per il centro-sud Italia di 7Layers, che durante l'evento Sanità 2030 appena conclusosi a Napoli, ha sottolineato che *"il rischio cyber in ambito sanitario è amplificato dal fatto che un'interruzione in servizi così critici causa un danno non solo per l'azienda, ma per un'intera collettività. Questo rende le aziende sanitarie particolarmente appetibili per organizzazioni che si occupano di cybercrime o cyberwar e lo fanno in modo assolutamente professionale. E' per questo necessario contrapporre altrettanta professionalità e competenza, rivolgendosi ad aziende come 7Layers che opera da un decennio come cybersecurity-only company e può mettere a disposizione anche delle aziende del settore sanitario la propria esperienza ed il proprio knowhow"*

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/il-giusto-percorso-di-cyber-security-per-la-sanita/