PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4929 di Venerdì 07 maggio 2021

La vera sicurezza informatica nella sanità è ancora molto lontana

I lettori ormai sanno come il mondo della sanità sia quello nel quale più frequentemente si verificano situazioni informatiche critiche, da un punto di vista della sicurezza. Ecco un'analisi più approfondita dei problemi maggiori.

L'esame afferente a situazioni di crisi informatica nel mondo della sanità, negli ultimi anni, per non dire un decennio, dimostra come molto spesso le strutture sanitarie siano più preoccupate di tutelare la salute dei pazienti, che di tutelare i loro preziosi riservati dati personali. La diffusione crescente di tecnologie Internet of Things non ha fatto che accrescere il problema, richiamando l'attenzione di esperti e strutture specializzate.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0330] ?#>

Vediamo la situazione.

Una recente ricerca mette in evidenza come gli apparati utilizzati nelle reti ospedaliere appartengano, per almeno il 50%, alle seguenti tre categorie.

- Apparati non classificati operanti in un contesto Internet of Things- IoT,
- apparati medici operanti in un simile contesto- IoMT,
- generiche tecnologie operative- OT.

Traducendo questi percentuali in numeri, si stima che esistano più di 250 milioni di apparati medici presenti sul mercato, con una crescita esponenziale, che potrà portare il numero degli apparati, nel 2025, a 500 milioni.

Davanti a questi numeri, sorprende il fatto che non siano state attivate appropriate misure di sicurezza informatica di questi stessi apparati.

Uno studio recente ha messo in evidenza che più della metà degli apparati utilizzati correntemente è vulnerabile ad attacchi di medio ed alto livello, mentre quasi tutti i sistemi di visualizzazione delle immagini, ad esempio utilizzati in apparati radiografici, sono pilotati da applicativi che sono ormai vicini al termine della loro vita utile. Si tratta pertanto di applicativi per i quali spesso il fornitore ha cessato di offrire supporto, in fase di aggiornamento, e quindi con crescenti e gravi lacune in termini di sicurezza.

Se a questa considerazione aggiungiamo il fatto che molto spesso questi apparati sono collegati in una rete ospedaliera informatica, appare evidente come la probabilità che attacchi su un apparato possano essere trasferiti ad altri apparati, collegati

alla stessa rete, sia del tutto realistica.

A fronte di questa drammatica situazione, in molte strutture ospedaliere i responsabili informatici non godono del supporto, in termini di risorse umane ed economiche, che sarebbe necessario per raggiungere un livello appena sufficiente di sicurezza.

Gli esperti, a questo proposito, raccomandano di cominciare ad attivare un piano organico di sicurezza, articolato come di seguito descritto.

Tanto per cominciare, occorre avviare una rassegna di tutti gli apparati informatici di tipo IoT collegati in rete, con puntuale descrizione dell'apparato e delle condizioni di aggiornamento software, se previsto, e di funzionamento.

A questo punto si ha a disposizione un quadro di riferimento, che permette di effettuare una valutazione di vulnerabilità non solo dei singoli apparati, ma anche della intera rete, proprio perché, come accennato in precedenza, un apparato "debole" può essere la via preferenziale di ingresso per attaccare l'intera rete.

Anche se la soluzione di una rete integrata sembra attraente, considerazioni di sicurezza informatica ritengono invece sia più opportuno suddividere e raggruppare questi apparati in reti separate, creando un solo punto di interfaccia fra le reti, che potrà così essere meglio controllato.

Le ormai diffuse tecniche di Zero Trust possono essere adottate, con sufficienti garanzie di efficienza ed efficacia.

Un'attenta analisi degli attacchi perpetrati negli ultimi anni mette in evidenza, ancora una volta, che l'utilizzo di parole chiave deboli rappresenta il più frequente punto di debolezza dell'intera rete.

In parallelo, occorre attivare una rete di contatti con i fornitori degli apparati, precedentemente classificati, per essere certi che aggiornamenti informatici, seppure disponibili, siano regolarmente inseriti dell'apparato in questione.

Un'altra ricerca, recentemente sviluppata, ha messo in evidenza come, nella stragrande maggioranza dei casi, la mancanza di collegamento organizzativo e logico tra chi compra questi apparati e chi li mette in servizio, informando tempestivamente il responsabile informatico, favorisce l'opera degli attaccanti.

Il consiglio da dare ai responsabili informatici del settore della sanità è quello di creare al più presto dei memorandum, da inviare all'alta direzione, in modo che, ove si abbia a verificare una violazione dei dati, il riparto di responsabilità venga effettuato in modo accurato e proporzionato, come d'altronde prevede il regolamento generale sulla protezione dei dati, agli ormai famosi articoli 82 ed 83.

Adalberto Biasiotti

 Questo articolo è pubblicato sotto una Licenza Creative Commons.

www.puntosicuro.it