PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4718 di Lunedì 15 giugno 2020

I problemi del mondo della sanità non sono solo legati alla pandemia

Il carico di lavoro che grava sul mondo della sanità non può consentire di dimenticare altri problemi che affliggono questo mondo legati alla protezione sicurezza dei dati informatici: l'utilità di adottare procedure del tipo "zero trust".

Le statistiche confermano che il mondo della sanità ha una probabilità doppia, rispetto ad altri ambienti, di soffrire per perdita di dati o essere bersaglio di attacchi informatici. In particolare, nei primi nove mesi del 2019, gli attacchi informatici alle strutture sanitarie sono aumentati del 60%. Questa situazione scaturisce dall'elevato valore dei dati finanziari e sanitari, afferenti ai pazienti, che il mondo della sanità tratta.

Occorre tuttavia mettere in evidenza come il settore bancario e finanziario è anch'esso esposto a rischi di questo tipo, ma nel mondo della sanità la posta in gioco è ben più elevata. Dal momento in cui il mondo della sanità fa' un affidamento sempre maggiore sugli aspetti informatici alla tecnologia, per fornire assistenza al paziente, i tre parametri fondamentali del mondo informatico, vale a dire riservatezza, integrità e disponibilità, possono avere un impatto diretto sul livello di attuazione affidabile di protocolli terapeutici. In casi estremi, un attacco informatico ad un sistema informatico può perfino portare alla perdita di vite umane.

L'analisi delle più recenti tecniche di attacco ha portato ad una valutazione tanto semplice quanto preoccupante: le strutture sanitarie non possono ritenere che gli utenti, le apparecchiature elettroniche ed altre oggetti soggetti, coinvolti nella cura dei pazienti, siano davvero affidabili. È questo il concetto alla base di un'espressione, che oggi diventa sempre più frequente, vale a dire "zero trust".

Oggi tutti i responsabili dei sistemi informatici, sia a livello operativo, sia a livello di security, sanno bene cosa significa questa espressione. I motivi per cui le strutture sanitarie sono più esposte ai rischi informatici sono evidentemente legati all'esistenza di sistemi ormai superati, alla mancanza di personale informatico debitamente preparato, alla presenza di dati anche personali di grande valore, nonché alla disponibilità a pagare riscatti, a fronte dei rischi della salute che potrebbero essere legati alla perdita o non accessibilità dei dati.

Un esempio di approccio "zero trust" per le strutture sanitarie

Gli specialisti del settore offrono queste linee guida, che dovrebbero guidare gli specialisti di sicurezza informatica nell'ambito sanitario nell'applicazione di questo approccio:

- la rete deve sempre essere ritenuta come non affidabile

- si deve ritenere come dato di fatto la presenza di minacce interne ed esterne nell'arco delle ventiquattrore
- l'ubicazione dell'apparato informatico non rappresenta un elemento di garanzia circa la sua affidabilità
- qualsiasi apparato, utente e flusso di dati deve essere autenticato ed autorizzato
- le politiche di sicurezza devono essere dinamiche e aggiornate, sulla base di un panorama dettagliato degli scenari di attacco, rilevati a livello mondiale.

Per poter attuare questi schemi, le strutture sanitarie devono superare numerosi problemi, come ad esempio:

- applicativi, sistemi operativi a ed hardware obsoleti
- piattaforme informatiche obsolete, che mancano di strumenti di sicurezza aggiornati
- apparati medici che vengono progettati più per soddisfare alle esigenze sanitarie, che non alle esigenze di sicurezza informatica
- inaffidabilità dei rapporti informatici con organizzazione terze, come ad esempio laboratori di analisi, le cui caratteristiche di sicurezza dei sistemi informativi sono spesso ignote
- una insufficiente preparazione del personale coinvolto, che viene costantemente aggiornato sugli aspetti sanitari, ma assai di rado sugli aspetti di sicurezza informatica, nell'ambito della gestione quotidiana.

Ancora una volta, valga il messaggio che non è sufficiente curare la malattia di un paziente, ma occorre anche mantenere aggiornato e sicuro il suo profilo informatico, nel contesto della struttura informatica ospedaliera. Un virus può essere certamente pericoloso, ma anche un bit sbagliato, al posto sbagliato, può essere altrettanto pericoloso!

Adalberto Biasiotti

---

www.puntosicuro.it