TREND

Cybesecurity in Sanità, il Cio figura centrale per battere gli hacker

Con la diffusione della telemedicina e dei dispositivi connessi è necessario accentrare le competenze e che sia solo il Chief Information Officer ad avere il controllo di tutte le "macchine". Nel 2023 sprint al metaverso per migliorare le cure in ottica "phygital" e alla blockchain per rendere più sicure e interoperabili le cartelle cliniche

11 Gen 2023

Federica Meta
Giornalista

Argomenti trattati

Aziende

A armis
M miodottore

Approfondimenti

B Blockchain
C Cio
D Digital Health
M Metaverso

Articoli correlati

NEW BUSINESS
Cio Agenda 2023: come monetizzare gli investimenti tecnologici
05 Gen 2023

L'INTERVISTA
Celli, Philips: "Sanità 4.0 alle porte, all'Italia serve una strategia data driven"
22 Dic 2022

ELEZIONI 2022
Cashback fiscale per battere l'evasione? Scontro Conte-Renzi
08 Set 2022

CONFERENZA DELLE REGIONI E DELLE PROVINCE AUTONOME
CORCOM
www.corrierecomunicazioni.it
Utenti unici: 10.189
Rassegna del 11/01/2023
Notizia del: 11/01/2023
Foglio:2/3

Anche nel 2023 la sanità dovrà affrontare delle sfide cruciali. Le carenze di personale, aggravate anche a causa del burnout creato dal Covid-19, stanno avendo un impatto sull'erogazione dei servizi sanitari in tutto il mondo. Inoltre, gli attacchi informatici continuano ad aumentare.

Armis, azienda attiva nella sicurezza degli asset, ha stilato i trend chiave che stanno emergendo nel settore della cybersecurity applicata alla sanità, alla luce dell'ascesa della medicina a distanza, con la conseguente diffusione dei dispositivi connessi e l'allargamento del campo d'azione degli hacker.

Una recente ricerca condotta da Ponemon ha individuato che il 12% degli attacchi ha avuto origine dai dispositivi IoT mentre in un recente focus group organizzato da Armis, è stato rilevato come i rischi di sicurezza informatica percepiti come più elevati nel settore sanitario riguardano i dispositivi IT tradizionali: i desktop e i laptop Windows che conservano le informazioni sanitarie personali (Phi). Un combinato disposto, quello tra device IoT e tradizionali, che può mettere a rischio la tenuta di un settore "sensibile" come quello sanitario.

Indice degli argomenti

Il Cio, unico punto di responsabilità per la sicurezza digitale

Con l'evoluzione delle tecnologie IoT, OT e IT, la responsabilità dei sistemi informatici è rimasta invariata. I sistemi OT (Operational technology) restano di competenza della gestione delle strutture, mentre i dispositivi medici rientrano nel reparto di ingegneria biomedica, che può riferire al Chief marketing officer.

Sebbene questi dispositivi utilizzino spesso un servizio condiviso fornito dal team IT, quando si tratta di esaminare le patch e la sicurezza dei dispositivi, questo compito spetta spesso ai singoli team, con l'IT che ha una visibilità molto limitata sui dispositivi che non possono avere sistemi di sicurezza installati.

L'assistenza sanitaria deve allineare tutti i sistemi digitali sotto un unico punto di responsabilità. Ecco perché è cruciale che ci sia una sola figura di riferimento ovvero il Cio (Chief information officer).

Aumento di servizi gestiti e in hosting

Come detto precedentemente, la tecnologia è spesso vista come la soluzione ad alcune delle principali sfide che la sanità deve affrontare. La tecnologia risolverà l'aumento dei costi dell'assistenza utilizzando i big data per promuovere un'assistenza basata sul valore, migliorerà l'efficacia delle diagnosi precoci e la qualità dei trattamenti, aiuterà a identificare i fattori di rischio per le malattie e migliorare la sicurezza dei pazienti attraverso una migliore previsione degli esiti, solo per citarne alcuni. Il monitoraggio remoto dei pazienti ha dimostrato di ridurre i tassi di riammissione, e si tratta solo di una piccola parte dei tipi di condizioni a cui viene applicata oggi.

Ciò che raramente emerge, però, è il modo in cui tutto questo verrà finanziato e dotato di personale. L'assistenza sanitaria è drammaticamente colpita dalla carenza di personale, ma non solo sul versante clinico: anche su quello informatico. Molte organizzazioni sanitarie hanno faticato ad attirare i migliori e più brillanti talenti IT, in particolare quelli situati vicino ai grandi datori di lavoro del settore tecnologico e finanziario. Purtroppo, il mondo