CASE STUDY

INNOVAZIONE DIGITALE E CYBERSICUREZZA ALL'OSPEDALE ISRAELITICO: INTRODOTTI MEDIGATE DI CLAROTY CON LA GESTIONE CLINICALSOC DI MEAD NEI SISTEMI DI PROTEZIONE DELLA INFRASTRUTTURA ICT

La soluzione è il primo passo verso un progetto "health global security" per la messa in sicurezza dell'intero network ospedaliero

Reggio Emilia, 17 Luglio 2023
I dati relativi gli attacchi ai danni delle infrastrutture critiche sono sempre più allarmanti, soprattutto quando si parla del settore sanitario. Come confermato anche dal Rapporto Clusit 2023, gli ospedali sono tra i nuovi obiettivi prediletti dai criminali informatici. Vista la complessità dei sistemi operativi e del servizio di prima utilità che erogano verso il cittadino, possono essere certamente annoverati tra le infrastrutture critiche più vulnerabili e, di conseguenza, che necessitano di maggiore protezione.
È proprio in questo contesto che si inserisce l'innovazione tecnologica introdotta dall'Ospedale Israelitico - tra i più antichi di Roma con oltre 400 anni di storia - che va ad integrare la propria infrastruttura IT con soluzioni adeguate e maggiormente performanti a tutela della sicurezza.

"Da sempre, la nostra struttura ha dimostrato una spiccata sensibilità verso questo tema, pertanto abbiamo maturato sul campo, giorno dopo giorno, la consapevolezza che sia necessario avere un approccio alla sicurezza più ampio e non limitato alla protezione perimetrale dei dati, degli apparati IT e dei singoli processi gestiti. È indispensabile adottare soluzioni che garantiscano il monitoraggio ed una copertura cyber a 360° di tutto ciò che concorre alla erogazione del Servizio di Diagnosi e Cura del Paziente. È necessario sviluppare soluzioni che siano in grado sia di rilevare le vulnerabilità che di suggerire tempestivamente azioni di 'messa in sicurezza' e protezione delle informazioni che determinano il profilo di salute dei nostri pazienti e, soprattutto, dei dati che ne gestiscono le terapie. Queste soluzioni contribuiscano a salvaguardare la continuità e l'accesso ai servizi, non differibili, sempre più digitali, remoti ed informatizzati, che offriamo ai cittadini", afferma il Dott. Riccardo Fragomeni - Direttore Sistemi Informativi dell'Ospedale Israelitico.

Durante la fase di analisi del mercato, *Claroty* si è distinta per l'offerta di una soluzione unica, che garantisce il full-monitoring, combinando prodotti e servizi in grado di cyber-proteggere sia l'infrastruttura che i processi. Inoltre, la proposta si è presentata assolutamente compatibile ed integrabile con le altre soluzioni e applicazioni operative presso la struttura (CUP, ADT, Registro Operatorio, OE, ecc…).
Nell'aprile di quest'anno, l'Ospedale Israelitico ha implementato *Medigate di Claroty*, grazie al supporto di *Mead*, System Integrator titolato e certificato, che, con il servizio ClinicalSOC appositamente ingegnerizzato per il settore sanitario, è stato in grado di attivare la soluzione configurandola al meglio con le altre componenti di sistema.

Il *Servizio ClinicalSOC di Mead* è conforme alla ISO 27001 e risponde, anche, alle normative IEC 62443 e IEC 80001-1 a garanzia: della sicurezza, della disponibilità dei servizi e dell'integrità dei dati che transitano

MEAD INFORMATICA s.r.l.

Sede legale ed amministrativa:
Via G. Ferraris, 2 | 42122 REGGIO EMILIA
Tel +39 0522 265800 | **Fax** +39 0522 393306
info@meadinformatica.it
P.IVA 01604010353

Sede operativa
Via delle Industrie, 19/d | 30175 MARGHERA
Tel +39 041 5997411 | **Fax** +39 041 5997444

Sede operativa
Centro Direzionale Colleoni, Palazzo Liocorno A/2
Via Paracelso, 4 | 20864 Agrate Brianza (MB)
Tel +39 039 9899011 | **Fax** +39 039 9899020

Sede operativa
ROMA

nelle apparecchiature e nell'intera infrastruttura. Gestito da un reparto tecnico dedicato, segue le linee guida del framework NIST: identificare, proteggere, rilevare, rispondere e ripristinare.

La sinergia tra *Claroty* e *Mead* ha consentito all'Ospedale Israelitico: di avere piena visibilità sui flussi informativi, di monitorare il corretto funzionamento delle postazioni di lavoro, degli elettromedicali e dei dispositivi wearable dei pazienti e di avere a disposizione un servizio di tipo SOC e SIEM che si avvale di operatori specializzati nel funzionamento e nella reattività dei processi sanitari per identificarne eventuali anomalie ed agire in tempi rapidi. L'interoperabilità con i sistemi ERP, di ausilio anche all'Ingegneria Clinica, e con le altre soluzioni poste a difesa cyber del network ospedaliero si è rivelata fondamentale per l'implementazione di un sistema di monitoraggio e protezione: proattivo, innovativo e all'avanguardia.

La soluzione di *Claroty* ha, inoltre, permesso al nosocomio ebraico di gestire in modo centralizzato, con cruscotti facili ed intuitivi, le attività e i volumi di produzione dei device medicali collegati alla rete consentendo di cambiare totalmente la modalità di interazione con le macchine e di semplificare la gestione dell'operatività dei sistemi e degli end-point. Attraverso una dashboard completamente user friendly, infatti, ogni operatore è in grado di monitorare, in real-time, tutti i sistemi e i processi di competenza, come: il rilevamento di eventuali anomalie nelle strumentazioni, il monitoraggio del loro livello di produttività sulla base degli obiettivi predisposti ed il loro ciclo di vita per preventivare aggiornamenti straordinari. In questo modo, il *Servizio ClinicalSOC di Mead* interviene tempestivamente non solo per prevenire e/o arginare eventuali problematiche ma, anche, per mappare e programmare le manutenzioni degli apparecchi elettromedicali avvisando preventivamente il tecnico addetto.

Ad un mese dall'implementazione, Israelitico ha già riscontrato dei risultati più che positivi. Questi dati hanno permesso di pensare ad un'evoluzione futura della soluzione di sicurezza, in un'ottica di "Health Global Solution" ovvero di disporre, grazie al progetto HGS, di una ulteriore protezione delle cinque sedi del gruppo ospedaliero. Infatti, la piattaforma *Medigate di Claroty* inserita nel framework HGS fornisce la possibilità di innestare nuovi algoritmi e nuovi appliance per il monitoraggio dei flussi informativi anche provenienti: dagli ambienti, dalle sale di attesa, dai varchi di accesso e dai processori dei server oltre a quelli dei medicali e dei dispositivi indossati dai pazienti allettati. Un nuovo concetto di sicurezza, appunto, 'GLOBALE'. Ad esempio, sarà possibile monitorare, grazie a mappe di calore elaborate in real-time, il livello di criticità, di sovraffollamento o esagitazione presenti nelle sale d'attesa oppure intercettare, nei dialoghi tra l'operatore del call center e l'utente, parole chiave che manifestino chiaramente delle minacce.

L'obiettivo finale di *Claroty* e *Mead* è costruire una soluzione unica, un framework centralizzato di monitoraggio e di conseguente protezione di altissimo profilo che, adiuvata da algoritmi di machine learning ed intelligenza artificiale, permetta non soltanto di analizzare i dati in modo preciso e puntuale ma di innescare automatismi per l'attivazione di azioni di remedation automatiche e semiautomatiche a supporto dei tecnici specializzati.

"La grande esposizione delle strutture sanitarie ai rischi cyber e a quelli legati alla sicurezza in generale ci ha spinto verso questa soluzione e ci ha mosso ad avviare, d'intesa con altre strutture, un progetto evolutivo alimentato da un concetto di sicurezza che definiamo a 'geometria variabile'. Avevamo bisogno di una soluzione che ci permettesse di migliorare la nostra capacità di reazione in caso di attacco: un framework grazie al quale essere sempre pronti a raccogliere sul campo le mutevoli informazioni che manifestano possibili vulnerabilità. Non sempre, infatti, si ha la possibilità di conoscere il problema in tempo e di reagire in maniera immediata alle nuove e sofisticate minacce introdotte dai criminali (anche per una mancanza di competenze mirate). Sappiamo, infatti, che una corretta protezione cyber si fonda su tre capacità di management: bisogna essere predittivi, preventivi e proattivi.

***Claroty* e *Mead* ci hanno permesso, non solo di includere questi tre elementi in un'unica soluzione ma, anche, di ampliare ulteriormente la visione della sicurezza lavorando sul concetto di ciclicità. È fondamentale esaminare ciò che è successo, decodificare gli eventi, effettuare l'analisi della situazione e della vulnerabilità riscontrate e misurare sempre l'efficacia dell'azione intrapresa: HGS**

si pone questo obiettivo. Solo in questo modo è possibile migliorare la difesa, diminuire i tempi di reazione e aumentare la capacità di resilienza della propria infrastruttura IT al fine di garantire la continuità dei servizi in risposta agli eventi avversi", ha spiegato **Riccardo Fragomeni**.

"La fiducia accordataci dall'Ospedale Israelitico è stata per noi un'ulteriore conferma della qualità e dei vantaggi che le nostre soluzioni possono offrire alle infrastrutture critiche, in particolare nell'Healthcare. L'evoluzione dell'Extended Internet of Things (XIoT) ha ampliato notevolmente l'efficienza e i vantaggi in termini di prestazioni delle aziende del settore sanitario, ma ha inevitabilmente portato alla luce nuovi rischi informatici che devono necessariamente essere arginati. Le aziende sanitarie sono pertanto chiamate a mettere in campo azioni mirate

per proteggere i propri sistemi e salvaguardare la salute dei propri pazienti da eventuali minacce esterne. Questo è ciò che stiamo facendo con L'Ospedale Israelitico di Roma, con un occhio già proteso verso gli sviluppi futuri che aiuteranno la struttura a espandere e migliorare ulteriormente la messa in sicurezza di tutti i propri sistemi e apparati", ha dichiarato **Alessandro Battella, Channel Manager Italia, Malta, Grecia e Cipro di *Claroty*.**

"Siamo orgogliosi di potere mettere al servizio dell'Ospedale Israelitico le nostre competenze attraverso ClinicalSOC. La protezione delle infrastrutture elettromedicali è un tema estremamente importante e delicato. Garantire la resilienza e la disponibilità delle prestazioni sanitarie è il nostro obiettivo primario: ci appassiona e ci responsabilizza", ha dichiarato **Fabio Tolomelli, Marketing Director di Mead**.

Claroty
Claroty è specializzata in soluzioni di sicurezza volte a proteggere i sistemi cyber-fisici in ambienti industriali (OT), sanitari (IoMT) e aziendali (IoT): il cosiddetto Extended Internet of Things (XIoT). La piattaforma unificata dell'azienda si integra con l'infrastruttura esistente dei clienti per fornire una gamma completa di controlli per la visibilità, la gestione dei rischi e delle vulnerabilità, il rilevamento delle minacce e un accesso sicuro da remoto. Supportate dalle più grandi società di investimento e provider di automazione industriale del mondo, le soluzioni *Claroty* vengono distribuite da centinaia di organizzazioni in migliaia di siti in tutto il mondo. La società ha sede a New York e filiali in Europa, Asia-Pacifico e America Latina. Per maggiori informazioni: www.claroty.com

Mead
Mead, con oltre 28 anni di esperienza, 4 sedi (RE, ME, VE e Roma) ed un organico composto da più di 150 addetti (dei quali oltre il 70% tecnici pluri-certificati) si pone come Partner strategico di sicurezza a 360 gradi. La proposta si sviluppa attraverso un approccio consulenziale che parte da una prima fase di analisi del rischio per proseguire, poi, nella progettazione e realizzazione di una adeguata infrastruttura ICT osservando tutte le normative internazionali e rimanendo fedele al principio di security by design includendo anche l'hardening della infrastruttura preesistente.
Mead ha progettato, ingegnerizzato e certificato alcuni servizi distintivi indirizzati a mercati verticali, sia pubblici che privati: **Cyber Security Control Room, IndustrialSOC® e ClinicalSOC®.**
Per saperne di più: www.meadinformatica.it

MEAD INFORMATICA s.r.l.

Sede legale ed amministrativa:
Via G. Ferraris, 2 | 42122 REGGIO EMILIA
Tel +39 0522 265800 | **Fax** +39 0522 393306
info@meadinformatica.it
P.IVA 01604010353

Sede operativa
Via delle Industrie, 19/d | 30175 MARGHERA
Tel +39 041 5997411 | **Fax** +39 041 5997444

Sede operativa
Centro Direzionale Colleoni, Palazzo Liocorno A/2
Via Paracelso, 4 | 20864 Agrate Brianza (MB)
Tel +39 039 9899011 | **Fax** +39 039 9899020

Sede operativa
ROMA