Le aziende sanitarie sono pronte?

La cyber security oggi è considerata un aspetto rilevante delle organizzazioni sanitarie. Una ricerca fotografa lo stato dell'arte e mostra qual è il livello di attenzione delle Aziende sul tema

di PAOLO PETRALIA

Le Aziende sanitarie stanno vivendo un profondo cambiamento operazionale, legato da un lato alle applicazioni della Salute digitale, ossia l'insieme di tecnologie utilizzate per curare i pazienti, ma anche per condividere informazioni sullo stato di salute dei cittadini; e dall'altro all'implementazione di sistemi di Cyber security, per garantire la sicurezza delle informazioni e nel contempo far fronte agli attacchi hacker sempre più frequenti. Al fine di capire lo stato dell'arte in merito, e poi di fornire alle Aziende associate indicazioni metodologiche, organizzative e formative riguardo al percorso di innovazione digitale, di implementazione e di miglioramento delle sperimentazioni digitali e della gestione della cyber security, la Federazione Italiana delle Aziende Sanitarie e Ospedaliere (Fiaso), il Cergas Bocconi e la rivista Mecosan hanno realizzato nei mesi scorsi una ricerca, pubblicata open source del numero 125 di Mecosan.

La survey è stata somministrata alle Aziende associate a Fiaso su base volontaria con l'ausilio di una piattaforma Google, nella prima decade di settembre 2022. Dopo due sezioni di inquadramento e sul livello di digitalizzazione dell'azienda, la terza ed ultima parte della survey sviluppa gli item riguardanti la Cyber security, con particolare riferimento ai sistemi in grado di proteggere le reti e i programmi informatici dagli attacchi digitali e dal rischio di violazione, trasformazione e diffusione di dati e informazioni sensibili.

Come detto, il questionario ha sviluppato alcuni aspetti in grado di far comprendere qual è l'attenzione delle Aziende associate alla Fiaso sul tema della Cyber security.

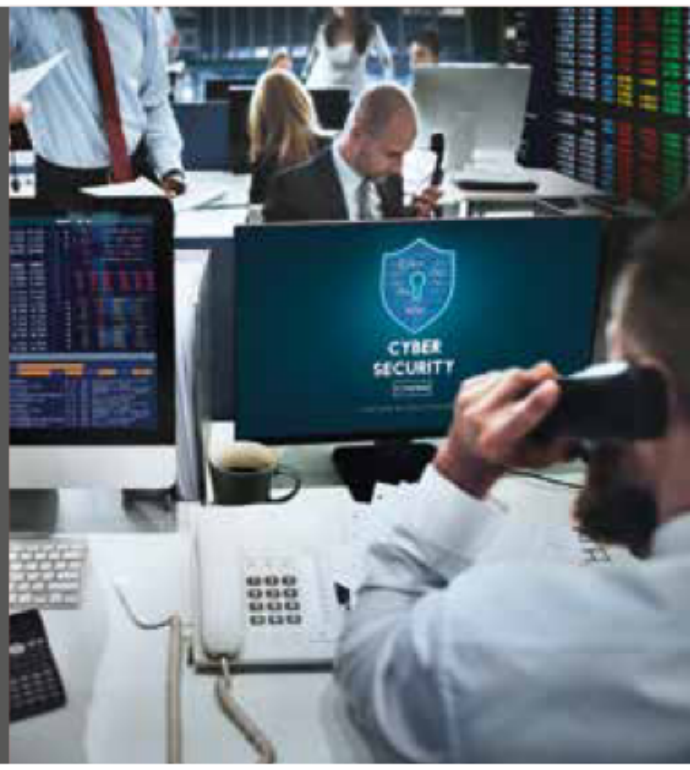
La prima domanda, a risposta multipla, riguarda gli eventi correlati alla Cyber security nell'ultimo triennio, a partire dal 2019. **In ordine di importanza, i fenomeni più rilevati sono stati nel 57% dei casi il phishing e nel 13% l'attacco hacker con blocco dei sistemi informativi.** Al momento della compilazione dei questionari il 17 % delle Aziende non aveva ancora registrato alcun evento correlato alla

za Firewall, un software per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi. Si tratta di una barriera tra le reti interne ed esterne. L'altro 50% utilizza ulteriori software come Sonde Deep Inspector, Oda (Oracle Database Appliance), Siem log management, Authenticator Token 2FA. **Sugli aspetti software sono state individuate, invece, diverse tipologie di intervento,** come aggiornamenti per compatibilità Gdpr, aggiornamenti antivirus client e server, messa in produzione dell'applicativo One Identity Password Manager per la gestione delle credenziali aziendali. **Un altro aspetto considerato dalla survey riguarda la formazione sul tema della Cyber security.** Tutte le Aziende hanno sviluppato nell'ultimo triennio interventi che spaziano da forme più blande, come l'invio di circolari informative sui rischi e le misure preventive da adottare, a momenti più corposi ed importanti, come la formazione specifica per personale Ict, la formazione globale per tutto il personale (awareness), percorsi di aderenza al framework nazionale Cyber security. Se la Cyber security oggi è considerata un aspetto rile-

Alla survey hanno aderito 51 Aziende sanitarie (Asl, Aziende Ospedaliere, Irccs) distribuite sul territorio nazionale. Nello specifico, 30 sono situate al Nord Italia, 14 al Sud e 7 al Centro.
In totale, nelle Aziende che hanno partecipato all'indagine operano 204.902 dipendenti, 99.408 dei quali al Nord, 22.664 al Centro, 82.830 al Sud.
Un altro aspetto preso in considerazione riguarda il valore della produzione delle Aziende nel 2021. In totale questo dato ammonta nel 2021 a 26.276.981.942 euro, 14.896.612.442 euro dei quali delle Aziende localizzate al Nord, 3.857.388.272 euro delle Aziende al Centro, 7.522.981.227 euro delle Aziende al Sud.

Cyber security.
Le successive due domande riguardavano "i più significativi interventi infrastrutturali (dispositivi hardware) e le procedure software nel campo della cyber security". **Sugli aspetti hardware, circa il 50% delle Aziende utiliz-**

Una domanda della ricerca ha voluto indagare il grado di sensibilità dei vari professionisti ai temi della Cyber security. I professionisti interessati sono stati il top e il middle management, il personale amministrativo e quello sanitario. **In media, 10 tra tutti i professionisti coinvolti hanno una bassa sensibilità al tema, 18 un'alta sensibilità, e 23 una sensibilità intermedia.** Specificatamente, il 71% dei top manager ed il 53% dei middle manager hanno un'alta sensibilità sui temi della Cyber security. Una situazione diversa si presenta, invece, per il personale amministrativo e sanitario, che presentano rispettivamente per il 59% e il 55% sensibilità media al tema, per il 29% e il 35% una bassa sensibilità e solo per il 12% e il 10% un'alta sensibilità.



"IL 71% DEI TOP MANAGER ED IL 53% DEI MIDDLE MANAGER HANNO UN'ALTA SENSIBILITÀ SUI TEMI DELLA CYBER SECURITY"

Ransomware e violazione dei dati

Il ransomware è emerso come una delle principali minacce nel settore sanitario (54% degli incidenti). Si ritiene che questa tendenza continui. Solo il 27% delle organizzazioni intervistate nel settore sanitario dispone di un programma di difesa dai ransomware dedicato. Spinti dal profitto finanziario, i criminali informatici estorcono denaro sia alle organizzazioni sanitarie che ai pazienti, minacciando di divulgare dati, personali o di natura sensibile. I dati dei pazienti, comprese le cartelle cliniche elettroniche, sono stati le risorse più prese di mira (30%). In modo allarmante, quasi la metà di tutti gli incidenti (46%) mirava a rubare o divulgare dati delle organizzazioni sanitarie.

Fonte: Enisa Threat Landscape: Health Sector (gennaio 2021 a marzo 2023)-pubblicato luglio 2023.

"IL 61% DELLE AZIENDE SANITARIE NON HA LA FIGURA DEL CHIEF INFORMATION SECURITY OFFICER"

vante delle organizzazioni sanitarie, è interessante verificare se al loro interno sia prevista la figura del Chief Information Security Officer. Dall'analisi dei dati risulta che il 61% delle Aziende non ha questa figura, mentre il 39% ha istituito il Chief Information Security Officer formalmente, se pur con soluzioni differenti quali: Coordinatore dell'attività per la sicurezza informatica interna, Responsabile della Cyber sicurezza, Operatore sistemista formato su Cyber security, Responsabile della Sicurezza delle informazioni, Responsabile della sicurezza dei dati, Data protection officer aziendale con supporto consulenziale e figure professionali necessarie (esempio Ict), Cabina di regia privacy con figura con competenza informatica, Direttore Uoc Sistemi informativi.

Alle Aziende che hanno partecipato alla survey è stato chiesto quali fossero gli interventi di cyber security realizzati. Il 68% delle Aziende ha adottato interventi misti, ossia in parte sviluppati all'interno delle organizzazioni, in parte all'esterno con l'ausilio di figure specialistiche, il 16% ha sviluppato interventi solo interni attraverso l'utilizzo dei propri servizi informativi, mentre nessuna Azienda ha coinvolto agenzie pubbliche specializzate in materia.

Anche per la domanda "Si ritiene che le competenze in materia di cyber security possedute siano adeguate ad affrontare i rischi di incidenti informatici e di violazione dei dati personali?" è stata utilizzata come metodo di valutazione la scala Likert. In questo caso i professionisti coinvolti oltre ai top e middle manager, personale amministrativo e sanitario sono stati anche il personale Ict interno e i fornitori di strumenti e servizi. Il top management con il 51%, il middle management con il 53%, il personale amministrativo con il 67% e quello sanitario con il 57% hanno una media adeguatezza di competenze in materia di Cyber security, mentre il 65% del personale Ict interno e il 59% dei fornitori di strumenti e servizi Ict presentano un alto livello di competenze.

Infine, l'ultima domanda del questionario ha posto l'attenzione sulla vulnerabilità (punti di debolezza) degli strumenti informatici e delle modalità con cui sono utilizzati.

Si evince che il 38% delle Aziende avvia analisi sulla vulnerabilità e sull'utilizzo degli strumenti informatici solo occasionalmente, il 35% ogni anno, il 20% ogni sei mesi e solo il 7% ogni tre mesi.