il Giornale

26-OTT-2021

GUERRA AGLI HACKER

Quello della sanità è anche un problema di cybersecurity

Protezione dei dati e continuità operativa le priorità per il settore farmaceutico. L'azione di Dompé

L'IMPEGNO

Non lasciare mai il paziente senza il farmaco: ecco la sfida più importante

Riccardo Cervelli

Secondo gli istituti che raccolgono e analizzano gli incidenti di *cybersecurity* nel mondo, la sanità è tra i 10 settori industriali più colpiti dagli *hacker* e tra i primi bersagli dello spionaggio informatico. Ne parliamo con Daniele Rizzo, CIO e Head of Global ICT & Digital Transformation di Dompé farmaceutici, un'azienda globale, con la produzione in Italia, il mercato principale negli Usa e consegne anche in Cina e in altri 80 Paesi.

Quali sono i maggiori rischi che un'azienda farmaceutica può correre? «Il primo pensiero - risponde - va sempre alla questione dei dati personali e alla *privacy* dei pazienti, ma in realtà i dati sanitari di cui disponiamo, seppure delicati come tipologia, riguardano i relativamente pochi pazienti che partecipano agli studi clinici, e peraltro non li custodiamo nemmeno di prima mano. La più grande minaccia nel nostro settore è un attacco informatico chiamato *ransomware*, un vero crimine assimilabile al ricatto con il blocco o peggio il sabotaggio dell'attività produttiva e della filiera, con il rischio di minare la continuità operativa. Compromettere l'infrastruttura informatica è come togliere la rete elettrica: il livello di automazione di un'azienda come la nostra è tale da non consentire di restare fermi per più di un certo tempo».

Un altro esempio di attività di un'azienda farmaceutica in cui il rischio di attacchi informatici deve essere prevenuto è quello della fornitura diretta di farmaci. «Parto da un esempio pratico», spiega Rizzo. «Tra i nostri prodotti c'è un collirio per una malattia rara che viene spedito con dosi bisettimanali in tutto il mondo, a partire dal nostro stabilimento a L'Aquila. Durante la fase più acuta della pandemia di Covid-19, la sfida che abbiamo affrontato con successo è stata quella di non lasciare i pazienti senza il farmaco. In fondo, che il nemico sia il Covid-19 o un *ransomware*, l'obiettivo è sempre quello di riuscire a portare il farmaco al paziente».

Oggi fare sicurezza non è più solo proteggere con pochi *software* e *hardware* le reti e i computer da attacchi esterni. Richiede analisi di rischio in molte aree, cultura della sicurezza diffusa, capacità di integrare la *cybersecurity* direttamente nei processi, nei prodotti e nei servizi a partire dalla progettazione. «Oggi la sicurezza - sottolinea Rizzo - è un aspetto complementare alla trasformazione digitale. Trattando dati importanti, privati e sensibili, le capacità legate alla sicurezza informatica sono un argomento necessario per operare nel dominio della salute. Se non si ha sufficiente sicurezza – e cultura della sicurezza – non si può nemmeno pensare di entrare in ambiti così delicati. Da quando sono arrivato in Dompé ho voluto creare dei momenti di condivisione e di consapevolezza legati alla *security* per approfondire di cosa si tratta e discutere gli eventuali rischi che corriamo se non si affronta tutta una serie di situazioni assicurandoci un adeguato livello di protezione, informatico e non solo. Ma la *security* è anche un'opportunità, uno strumento per sviluppare applicazioni che altrimenti non potrebbero esistere». In altre parole, la sicurezza tutela sia i risultati raggiunti sia la capacità di innovazione per vincere nuove sfide nel mondo della salute.

NEL MIRINO È stato accertato che la sanità è tra i dieci settori industriali più colpiti dagli hacker e tra i primi bersagli dello spionaggio informatico