

I PROFILI DI RESPONSABILITÀ CYBER IN SANITÀ

di ERNESTO MACRÌ – consulente legale di Sham – gruppo Relyens e avvocato del libero foro di Roma, esperto di responsabilità civile e diritto assicurativo

I NUOVI RISCHI INFORMATICI E IL RUOLO DELLE ASSICURAZIONI. UN'ANTEPRIMA DEL WHITEPAPER “CAPIRE IL RISCHIO CYBER: IL NUOVO ORIZZONTE IN SANITÀ” DI PROSSIMA USCITA, FRUTTO DELLA PRIMA SURVEY DEDICATA AL RILEVAMENTO DELLA PERCEZIONE DEL RISCHIO CYBER DA PARTE DELLA SANITÀ ITALIANA, CONDOTTA DA SHAM – GRUPPO RELYENS IN COLLABORAZIONE CON L'UNIVERSITÀ DI TORINO

Uno dei settori specifici che, negli ultimi decenni, più di altri ha subito notevoli trasformazioni è senza alcun dubbio quello sanitario, che ha registrato un progressivo utilizzo di nuove tecnologie e una crescente attenzione da parte dei *tech giant*. Le previsioni relative al solo mercato globale dell'intelligenza artificiale nel settore sanitario indicano che il relativo giro d'affari è cresciuto con un *compounded average growth rate* (Cagr) del 43,5% nel 2018 per raggiungere i 27,6 miliardi di dollari entro il 2025 (fonte Prnewswire.com). Cresce, però, anche l'interesse del cybercrime. Come dichiarato il 4 maggio 2020 a Repubblica dall'esperto di sicurezza informatica Eugene Kaspersky, solo tra gennaio e febbraio 2020 gli attacchi informatici nei confronti di ospedali e strutture sanitarie sono aumentati del 50%.

LE PRINCIPALI MINACCE PER LA SANITÀ

Le principali minacce in ambito sanitario riguardano la divulgazione di informazioni protette, il furto di ricerche e il blocco dei sistemi informatici con conseguenti danni, anche catastrofali, a terzi. In questa ultima ipotesi l'estorsione prevede, nella maggior parte dei casi, il pagamento del riscatto tramite valuta digitale.

NUOVI PROFILI DI RESPONSABILITÀ

I profili di responsabilità sono principalmente collegati ai rischi tecnologici connessi al cosiddetto *Internet delle*

cose (IoT), tra i quali c'è sicuramente il rischio informatico di hackeraggio, ma non solo. Il rischio di malfunzionamento interessa dai produttori delle componenti hardware ai progettisti software, dai servizi di *data analytics* ai provider di rete e di connessione. Sempre più si profila all'orizzonte, inoltre, un'interessante questione: la responsabilità di macchine AI che modificano il loro comportamento sulla base dell'esperienza.

COME CAMBIA LO SCENARIO ASSICURATIVO IN QUESTO CONTESTO

Nel corso degli ultimi anni è cresciuta in maniera esponenziale la domanda di coperture assicurative strutturate in modo da affrontare i costi relativi a questi nuovi rischi. Il mercato assicurativo non si limita solo alla copertura della violazione dei dati, ma offre una vasta gamma di prodotti in grado di fornire una garanzia nei confronti delle diverse sfaccettature del rischio informatico. Tuttavia, e in conclusione, è importante considerare che in sanità diventa necessario, accanto all'assicurazione informatica, un cambio di paradigma: il diretto coinvolgimento del risk management nella declinazione del problema della cybersecurity. ❶