

HACKER ASL L'AQUILA: "SPIATI IN 10MILA". VERDETTO GARANTE, RISCHIO STANGATA RISARCIMENTI

16 Aprile 2025



L'AQUILA – Una “mancata adozione di misure adeguate a rilevare tempestivamente la violazione dei dati personali” di 10.631 persone tra pazienti, dipendenti e consulenti.

A due anni dal grave attacco hacker arrivano le avvisaglie dal Garante per la protezione dei dati personali che ha adottato un provvedimento di ammonizione nei confronti della Asl 1 Avezzano Sulmona L'Aquila, accertando “l'illiceità del trattamento” dei dati con il rischio di dover pagare danni enormi.

Un'azione omissiva certificata, riporta *Il Centro*, che può sfociare in una vagonata di azioni risarcitorie di fronte a tribunali o giudici di pace nei confronti dell'azienda sanitaria della provincia dell'Aquila.

Il provvedimento del Garante per la protezione dei dati personali, dipartimento Sanità e ricerca, riguarda una paziente aquilana, assistita dall'avvocato Berardino Terra, e porta la data del 13 febbraio. Giorno in cui si è riunita la commissione del Garante presieduta dal giurista Pasquale Stanzione.

La Asl 1 d'Abruzzo ha subito un attacco ransomware (dall'inglese ransom, riscatto) in data 3 maggio 2023 che ha determinato significativi problemi di funzionalità dei sistemi informatici e l'esfiltrazione di dati personali. Gli hacker, come accertato nei giorni seguenti, appartenevano al gruppo filorusso Monti che utilizza un sofisticato sistema progettato per crittografare i dati e richiedere il pagamento in bitcoin per gli strumenti di decrittazione.

La stessa azienda sanitaria, ricorda *Il Centro*, ha dichiarato che sono stati oggetto di violazione 3.814 tra dipendenti e consulenti: dati anagrafici, dati di accesso e di identificazione, dati di pagamento, dati relativi a documenti di identificazione e riconoscimento, dati che rivelano l'appartenenza sindacale. Per quanto riguarda assistiti, pazienti (anche minori), persone vulnerabili (vittime di violenza o abusi, rifugiati, richiedenti asilo) sono stati catturati i dati di 6.817 persone. Dati che in questo caso hanno riguardato anagrafe, condanne penali, reati, misure di sicurezza, origine razziale o etnica, dati relativi alla vita sessuale o all'orientamento sessuali, dati relativi alla salute (esempio scheda paziente, diario clinico, terapie, diagnosi,

lettera di dimissione).

L'azienda ha presentato una corposa documentazione difensiva: massimo impegno profuso per evitare attacchi da parte di criminali informatici, l'implementazione di misure adeguate alla prevenzione, la complessità dell'attacco subito, la minimizzazione dei danni, la collaborazione con la polizia.

Secondo quanto emerso, però, i criminali informatici hanno "effettuato una serie di operazioni propedeutiche all'attacco". Misure "non conformi" secondo il Garante. Inoltre, risulta una "mancata adozione di misure adeguate a garantire la sicurezza delle reti e di misure organizzative per assicurare la consapevolezza e l'accesso degli incaricati ai sistemi".

Il Garante ricorda quindi il ruolo rivestito dall'azienda che "richiede un elevato grado di responsabilizzazione al fine di garantire la fiducia nei suoi confronti da parte degli assistiti, soddisfacendo, in particolare, le legittime aspettative di trasparenza e sicurezza del trattamento".