

ATTACCO HACKER ASL L'AQUILA: "QUANDO SI TORNERA' ALLA NORMALITA'?", INTERPELLANZA CENTROSINISTRA-M5S

20 Maggio 2023



L'AQUILA - "Il disagio conseguente all'attacco degli hacker al sistema della Asl 1 si allarga a macchia d'olio, coinvolgendo la privacy dei pazienti, con malattie, prestazioni e cure personali messe alla berlina e l'affidabilità di una gestione della rete che ha rivelato tutta la sua incredibile vulnerabilità. Interpelliamo l'esecutivo per fare luce sullo stato dell'arte, perché a giorni dai fatti siamo incredibilmente ancora in alto mare sulle cause e, soprattutto, mancano informazioni sulla vicenda e su quanto tempo ci vorrà per ripristinare un minimo di normalità, dando ai cittadini e alle prestazioni richieste certezza e salvaguardia".

Così, in una nota, il capogruppo Pd, Silvio Paolucci e il consigliere regionale del M5S Giorgio Fedele, firmatari di un'interpellanza sullo stato dei sistemi informatici a seguito dell'attacco hacker di oltre due settimane fa.

Nell'interpellanza, sottoscritta anche dai consiglieri regionali Pierpaolo Pietrucci, Americo Di Benedetto, di Legnini Presidente, Marianna Scoccia, del Gruppo misto, e da tutti i consiglieri regionali del Movimento 5 Stelle, chiedono anche una relazione dettagliata delle iniziative messe in campo a sostegno dell'azienda per fronteggiare e superare l'attuale situazione di emergenza.

"Non solo, servono risposte a una serie di problemi concreti che la Regione non ha dato - aggiungono - ad esempio se si intende avviare un'indagine interna per verificare le eventuali carenze dei sistemi informatici, questo per adottare protocolli funzionali e innalzare i livelli di sicurezza anche nelle altre Aziende sanitarie abruzzesi, alcune delle quali stanno vivendo importanti disagi a causa dell'accaduto".

"Chiediamo, inoltre, se esiste un fornitore unico della Regione Abruzzo e delle Aziende sanitarie abruzzesi dei servizi di Cyber Security, nonché se alla data dell'attacco ransomware erano operative tutte le basilari schermature capaci di effettuare stress test e identificare eventuali falle e vulnerabilità nel sistema, in modo da difenderlo in caso di attacchi. Sono tanti i dettagli tecnici che restano ignoti, non ultimo capire la 'porta' da cui il ransomware sia entrato in contatto con il sistema informatico aziendale, nonché se i dati erano presenti su un server interno aziendale o su un Cloud e, di conseguenza, quali altre tipologie di dati siano stati hackerati o a rischio".

“Certo stupisce la grave assenza di precauzioni che questa situazione ha rivelato: il sistema è risultato più che vulnerabile e non c'erano protocolli per gestire l'emergenza in caso di attacco. Per questo chiediamo anche di sapere se è stato disposto un controllo del 'vulnerability assessment', cioè la verifica della vulnerabilità di tutto il potenziale digitale della sanità regionale, questo per capire l'effettiva capacità di resilienza cibernetica dello stesso, specie con riferimento alla strumentazione che assicura funzioni cliniche che sono state ad oggi compromesse, riportando prestazioni e servizi indietro di vent'anni e confinando alla carta qualunque tipo di attività connessa con il diritto alla salute nell'ambito sotto attacco”.

“Informazioni tecniche e oggettive che sono dovute alla comunità, che mai è stata esposta a un rischio simile, ma anche necessarie a capire quando il lavoro di operatori e medici, che stanno gestendo direttamente e in ogni modo possibile i disagi e le legittime reazioni dell'utenza, potrà tornare all'epoca contemporanea”, concludono.