INTERPELLANZA
Stato dei sistemi informatici della ASL 1 in seguito all'attacco hacker

***

PREMESSO che lo scorso 3 maggio si è verificato un attacco ai sistemi informatici della Azienda sanitaria locale n. 1 della Regione Abruzzo, rivendicato dal *cd. Gruppo Monti*;

DATO ATTO che tale attacco informatico ha paralizzato il sistema informatico della ASL 1 Abruzzo, con gravi ripercussioni sui servizi erogati agli utenti/pazienti afferenti alle strutture pubbliche e private nel territorio provinciale aquilano;

DATO ATTO che, nei giorni scorsi, è stato reso pubblico un significativo quantitativo di dati dai *database* della ASL, contenenti milioni di informazioni sensibili, tra cui referti medici e patologie, pregiudicando la *privacy* degli interessati e mettendo a serio rischio il regolare svolgimento delle terapie;

PRESO ATTO dall'edizione delle 14:00 del TgR Abruzzo del 14.5.2023, che anche la copia dei *backup* dei dati della ASL 1 Abruzzo sarebbe stata violata, causando l'impossibilità di procedere ad un rapido ripristino dei dati, capace di consentire la normale prosecuzione dei servizi sanitari nella provincia de L'Aquila;

VISTO che tale vicenda sta provocando disservizi generalizzati, tanto al settore pubblico quanto a quello privato, come – solo a titolo esemplificativo – il rinvio di prestazioni sanitarie, con evidenti profili di rischio per la salute dei pazienti;

EVIDENZIATO il clima di inevitabile confusione nel quale gli operatori sanitari sono costretti a svolgere le proprie attività, al di fuori di ogni ordinaria procedura, non avendo a disposizione pressoché alcuno strumento informatico operativo;

CONSIDERATO che tutti i procedimenti e le prestazioni in corso non sono catalogati e archiviati nei sistemi informatici e, dunque, restano collazionati in resoconti cartacei che, usciti dall'emergenza, dovranno essere oggetto di un notevole carico di lavoro e impiego di risorse per essere reinseriti nei sistemi digitali;

ATTESO che, oltre ai danni subiti nell'immediato, i pazienti della ASL 1 Abruzzo potranno essere esposti - loro malgrado - ad eventuali e ulteriori ricatti subiti da coloro i quali sono entrati in possesso con le informazioni illecitamente pubblicate sul *Dark Web* dagli Hacker;

tutto ciò premesso
i sottoscritti Consiglieri della Regione Abruzzo
INTERPELLANO

il Presidente della Giunta Regionale, Sen. Marco Marsilio,
ovvero l'Assessore competente per conoscere:

1. le informazioni in possesso sul merito della vicenda;
2. i tempi stimati entro i quali l'azienda possa tornare a fornire ordinariamente i servizi all'utenza a salvaguardia della sicurezza e della salute pubblica;
3. le iniziative messe in campo a sostegno dell'azienda per fronteggiare e superare l'attuale situazione di emergenza;
4. se intende avviare un'indagine interna per verificare le eventuali carenze dei sistemi informatici, al fine di adottare protocolli funzionali ad innalzare i livelli di sicurezza nelle altre Aziende sanitarie abruzzesi;

5. se esiste un fornitore unico della Regione Abruzzo e delle Aziende sanitarie abruzzesi che fornisce servizi di Cyber Security;
6. se, alla data dell'attacco *ransomware,* erano operativi nella ASL 1 Abruzzo:
    a. un servizio di Security Operations Center (SOC), centro da cui vengono forniti servizi finalizzati alla sicurezza dei sistemi informativi;
    b. un servizio di Security Information and Event Management;
    c. i cosiddetti *Red Team* per effettuare stress test ed identificare eventuali falle e vulnerabilità nel sistema e *Blue Team* per la difesa di quest'ultimo in caso di attacchi;
    d. gli *Endpoint Protection* (EDP) e gli *Extended detection and response* (XDR) sulle postazioni aziendali e se gli stessi erogatori di tali servizi presso l'Azienda rispettano le disposizioni di cui al D.L. 14/2022 – Disposizioni urgenti sulla crisi in Ucraina (cd. "Decreto Kaspersky");
7. se è stata fatta una *detection,* indagando come il *ransomware* sia entrato in contatto con il sistema informatico aziendale, ovvero da quale "porta" sia entrato;
8. se i dati oggetto dell'attacco *ransomware* erano presenti su un server interno aziendale o su un *Cloud;*
    a. in caso di presenza su *Cloud,* di conoscere dove il fornitore ha allocato i dati (ad es. territorio extra UE o UE) e se aveva completato il processo di migrazione e di qualificazione dei dati (es. ordinari, critici, strategici) e quali tra queste tipologie di dati sono stati hackerati;
9. se è stato disposto un *vulnerability assessment* generale su tutto il potenziale digitale della sanità regionale, volto ad accertare l'effettiva capacità di resilienza cibernetica dello stesso, con particolare riferimento ai dispositivi medici/elettromedicali connessi che assicurano funzioni cliniche.

Silvio Paolucci

Pierpaolo Pietrucci

Americo Di Benedetto

Marianna Scoccia

Giorgio Fedele

Barbara Stella

Domenico Pettinari

Francesco Taglieri Sclocchi

Pietro Smargiassi