Egregio Signor
Claudio Soini
Presidente del Consiglio provinciale

Interrogazione a risposta scritta n. 2215

Oggetto: Criticità cybersicurezza sanità trentina: isolamento RSA e inadempienze NIS2 (Network and Information Security 2 - Direttiva sulla sicurezza delle reti e dei sistemi informativi)

Già all'indomani dell'approvazione in Consiglio provinciale del disegno di legge fortemente voluto e promosso dall'assessore Spinelli avente al centro la struttura strategica di Trentino Digitale in merito a sicurezza, salvaguardia dei dati e gestione innovativa la realtà ci restituisce l'ennesimo, impietoso schiaffo. In queste stesse ore, infatti, ci ritroviamo ad affrontare l'ennesimo grave attacco hacker che ha travolto le strutture sanitarie del nostro territorio, tra cui le RSA di Rovereto (Vannetti).
Segnalo infatti con forte preoccupazione quanto emerso sulla stampa locale in merito alla gestione della cybersicurezza nella sanità provinciale. A seguito degli attacchi hacker che hanno colpito le RSA di Predazzo e Rovereto, l'ASUIT e Trentino Digitale sono state costrette a isolare d'urgenza la rete delle strutture residenziali per anziani, interrompendo servizi essenziali come la consultazione delle cartelle cliniche elettroniche, i teleconsulti e l'accettazione dei prelievi.

Se da un lato la disconnessione della rete rappresenta una misura di contenimento necessaria a proteggere l'infrastruttura centrale, dall'altro l'episodio evidenzia una gestione reattiva che arriva purtroppo a danno già avvenuto. Nello specifico, emergono tre rilevanti criticità:
Ritardo nell'adeguamento alle prescrizioni NIS2 (D.Lgs. 138/2024)

Come tutti gli "addetti ai lavori" sanno, entro la fine di ottobre (cioè domani) scade il termine tassativo fissato dell'Agenzia per la Cybersicurezza Nazionale (ACN) per l'attuazione di tutte le misure di sicurezza informatica imposte dalla normativa.
L'isolamento drastico delle strutture a fronte di questi gravissimi incidenti dimostra che

ASUIT, pur rientrando tra i soggetti "essenziali" del settore sanitario, non è riuscita ad adeguarsi per tempo a tutti i requisiti di prevenzione richiesti dalla normativa come la segmentazione avanzata dei nodi e la protezione della catena di interconnessione trovandosi costretta a bloccare l'operatività anziché contenere in modo mirato la minaccia. Tale aspetto evidenzia in maniera inequivocabile l'inerzia di ASUIT in relazione agli adempimenti di sicurezza informatica.

Rischio sanzionatorio e responsabilità della dirigenza

Il mancato o parziale completamento del percorso di conformità nei termini imposti da ACN (cioè domani) espone ASUIT a conseguenze sanzionatorie particolarmente severe. L'art. 38 del D.Lgs. 138/2024 prevede infatti sanzioni amministrative fino a 10 milioni di euro (o al 2% del fatturato annuo), a cui si sommano i rischi di sanzioni GDPR per la compromissione di dati sanitari sensibili e la responsabilità diretta degli organi direttivi (art. 23) per l'approvazione e la vigilanza sulle misure di sicurezza;

Vulnerabilità delle RSA e impatto sulla continuità assistenziale

Le RSA continuano a rappresentare uno degli anelli deboli della rete sociosanitaria, assieme ad ASUIT (i cui disservizi sono ormai tristemente noti). Scegliere la disconnessione totale come principale strumento di difesa evidenzia in maniera inequivocabile l'assenza di adeguate misure preventive sull'operatività quotidiana del personale sanitario e sui servizi erogati agli ospiti anziani.
Sulla base di questi elementi, i quesiti da chiarire urgentemente sono molteplici e urgentissimi.

Tutto ciò premesso si interroga la Giunta provinciale per sapere

1. Se ASUIT e Trentino Digitale hanno completato l'implementazione delle Misure di Sicurezza Minime previste dall'ACN per i soggetti essenziali in vista della scadenza di fine ottobre, ovvero di domani? In caso contrario, quali e quante misure risultano ancora inattuate e chi ne è responsabile? In caso di grave incidente, a fronte del grave stato di inadempienza normativa alle misure minime di sicurezza, chi ne risponde?
2. Se la Giunta Provinciale è consapevole dei rischi finanziari e normativi (sanzioni ACN fino a 10 milioni di euro e sanzioni GDPR) derivanti dal mancato o tardivo adeguamento delle infrastrutture e delle interconnessioni con le strutture periferiche quali le RSA?
3. Quali verifiche di sicurezza informatica sono state condotte sulla rete delle RSA e quali supporti tecnici ed economici specifici sono stati messi a disposizione

dall'ASUIT prima dell'ondata di attacchi per garantire standard di protezione omogenei

4. Con quali tempi e modalità si intende ripristinare la piena operatività dei servizi sospesi (teleconsulti, cartelle cliniche, referti) senza esporre ulteriormente i dati sanitari dei cittadini o dover ricorrere sistematicamente all'isolamento delle strutture?

Paola Demagri

Documento firmato digitalmente: se trasmesso in forma cartacea costituisce copia dell'originale, predisposto e conservato presso questa amministrazione in conformità alle linee guida AGID (artt. 3 bis e 71 d.lgs. 82/2005).

30 ottobre 2026