CONSIGLIO REGIONALE DEL VENETO

UNDICESIMA LEGISLATURA

MOZIONE N. 522

ATTACCO HACKER ALL'AOUI DI VERONA: LA GIUNTA PROMUOVA UNA REVISIONE DEI SISTEMI DI SICUREZZA E ISTITUISCA UN FONDO PER IL RISARCIMENTO DEGLI UTENTI COLPITI

presentata il 4 marzo 2024 dalla Consigliera Bigon

Il Consiglio regionale del Veneto

PREMESSO CHE:

- il giorno 23 ottobre 2023 l'Azienda Ospedaliera Universitaria Integrata (AOUI) di Verona è stata vittima, a partire dalle prime ore del mattino, di un attacco hacker che ne ha compromesso il funzionamento del sistema informativo e che ha portato all'estrazione di oltre 900 mila files, pari a 612 gigabyte;
- il gruppo hacker Rhysida, autore dell'attacco, ha chiesto un riscatto per la restituzione dei files sottratti minacciando, a un eventuale rifiuto, di venderli nella rete Onion al miglior offerente, al prezzo di 10 Bitcoin corrispondenti a circa 350 mila euro. A seguito del rifiuto dell'AOUI di Verona, infatti, è seguita la pubblicazione dei dati estratti;

RILEVATO CHE:

- dall'analisi svolta dall'AOUI di Verona è emerso che sono stati esfiltrati poco più del 2% dei dati dell'archivio aziendale e che, in particolare, si tratta di dati che erano archiviati sulle cartelle di rete aziendali, senza il coinvolgimento degli applicativi utilizzati per la gestione corrente delle informazioni personali che riguardano gli utenti dell'Azienda, compresi il dossier sanitario elettronico, il fascicolo sanitario elettronico o le cartelle cliniche elettroniche dei pazienti;
- nello specifico, risultano violate le seguenti categorie di dati: anagrafici, di contatto, di pagamento, relativi a condanne penali e reati, relativi a documenti di identificazione e riconoscimento, relativi alla salute e quelli genetici;

EVIDENZIATO CHE:

- le informazioni esfiltrate, secondo l'analisi dei tecnici dell'AOUI di Verona, risultano parziali, spesso raggruppate in database riferiti a un elevato numero di

persone e, il più delle volte, identificate in maniera incompleta o comunque difficilmente ricostruibile in assenza di ulteriori elementi conoscitivi;

- l'AOUI di Verona ha predisposto una strategia di confronto con gli utenti più "critici", ovvero coloro che hanno subito la sottrazione di dati altamente sensibili. Allo scopo, infatti, sono stati loro inviati degli SMS corredati dei riferimenti e delle informazioni utili a comprendere quanto accaduto, nonché dei contatti dedicati;

RILEVATO altresì che già il giorno 3 dicembre 2021 l'Azienda ULSS 6 Euganea è stata oggetto di un attacco informatico che ha portato alla sottrazione di dati sensibili di numerosi utenti, diffusi in rete nel corso del mese successivo;

CONSIDERATO CHE:

- nonostante la parzialità dei dati esfiltrati e la difficoltà del concreto verificarsi di un nocumento giuridicamente rilevante in capo ai soggetti coinvolti, è impossibile non rilevare le ripercussioni psicologiche e di perdita di fiducia sulla sicurezza dei database ospedalieri da parte degli utenti;
- il precedente dell'attacco informatico subito dall'Azienda ULSS 6 Euganea avrebbe dovuto portare a maggiori approfondimenti sui presidi dei database contenenti dati sensibili e quanto accaduto all'AOUI di Verona rende ancora più urgente una revisione dei sistemi di sicurezza;

impegna la Giunta regionale

- a valutare l'opportunità di accantonare le risorse necessarie alla costituzione di un fondo per il risarcimento degli utenti dell'AOUI di Verona che hanno subito un danno dalla sottrazione di dati sensibili da parte del gruppo hacker Rhysida;
- a predisporre un piano di investimenti per aumentare la sicurezza dei database informatici delle Aziende Ospedaliere e delle ULSS del Veneto, nonché per garantirne il costante monitoraggio e aggiornamento ai più alti standard di *cybersecurity*.