CONSIGLIO REGIONALE DEL PIEMONTE

ORDINE DEL GIORNO n. 878

Oggetto: Potenziamento delle funzioni di cybersicurezza

Il Consiglio regionale

premesso che:

- l'informatizzazione dei sistemi e dei documenti è un processo da tempo iniziato, giunto a uno stadio avanzato e da considerarsi irreversibile;
- la quasi totalità dei documenti e delle procedure delle Istituzioni sono oramai in formato digitale;
- la Regione Piemonte non fa, in questo senso, eccezione;
- la sicurezza informatica ("information security" e "cybersecurity") è l'insieme dei mezzi, delle tecnologie e delle procedure tese alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici.

rilevato che:

- sempre più frequenti sono i casi di attacchi informatici ai sistemi delle Istituzioni;
- ampia copertura mediatica hanno ricevuto i recenti casi di attacchi hacker ad ATC, al Comune di Torino e alla Regione Lazio.

rilevato, altresì che:

- lo scorso 19 agosto l'Asl Città di Torino è stata oggetto di un attacco hacker che ha reso necessario, come da linee guida sugli attacchi informatici, il blocco di tutti i sistemi informatici aziendali, per effettuare le verifiche ed i monitoraggi indispensabili, mettere in sicurezza i dati e ripristinare gli applicativi aziendali cautelativamente bloccati;
- secondo quanto ipotizzato e successivamente confermato dai responsabili della rete informatica dell'azienda, gli hacker avrebbero utilizzato un attacco ransomware, probabilmente a partire da una mail di phishing recapitata ad una mail aziendale e trattata impropriamente.

considerato che:

- attacchi di questo genere possono causare un danno gravissimo alle Istituzioni che ne sono colpite e dunque, per diretta e immediata conseguenza, anche alla cittadinanza;
- il Governo stesso ha recentemente creato un'Agenzia per la cybersicurezza nazionale.

tenuto conto che:

- per garantire e prevenire eventuali situazioni di attacco, è molto importante porre attenzione alla gestione dei messaggi e degli allegati di posta elettronica, soprattutto se di dubbia provenienza;

- è fondamentale definire una strategia anti-hacker accompagnata da un percorso di aggiornamento e consapevolezza degli utenti: tale percorso non deve limitarsi alla sola formazione, ma deve fornire all'utente gli strumenti di conoscenza per una corretta valutazione del rischio, permettendogli di reagire in modo corretto alle situazioni potenzialmente pericolose

impegna il Presidente e la Giunta Regionale

a valutare il potenziamento delle funzioni di cybersicurezza.

---==oOo==---

Testo del documento votato con modifiche e approvato all'unanimità nell'adunanza consiliare del 16 novembre 2022