Interrogazione n. 441

presentata in data 7 aprile 2022

a iniziativa dei Consiglieri Bora, Mastrovincenzo, Carancini, Biancani, Casini, Cesetti, Mangialardi, Vitri

Attacco ransomware ARPA Marche

a risposta orale

PREMESSO CHE

- l'ARPA Marche, acronimo di Agenzia Regionale per la protezione dell'ambiente per la Regione Marche è un ente della pubblica amministrazione italiana e nasce come ente di diritto pubblico, dotato di autonomia tecnico-giuridica, amministrativa e contabile con sede in Ancona;

- L'ARPA Marche svolge le attività tecnico-scientifiche connesse all'esercizio delle funzioni di interesse regionale di cui all'art. 1 della legge 61/94 ed in particolare fornisce prestazioni e servizi in molteplici campi di azione a supporto di Regione, Enti locali, ASUR, ma anche di imprese e privati cittadini, ai fini della elaborazione di programmi di intervento per la prevenzione, controllo e vigilanza in materia di igiene e salvaguardia dell'ambiente e di verifica della salubrità degli ambienti di vita;

VISTO CHE

- alcuni profili della rete, specializzati in *cyber attack* e sicurezza informatica italiani ed esteri, hanno riportato la notizia che l'Arpa Marche ha subito un attacco informatico con ransomware rivendicato dalla cybergang "Vice Society", la quale è riuscita ad aprire un varco nel sistema informatico dell'Agenzia mettendo alla mercè importanti dati che rientrano nel contesto delle informazioni e dati sensibili;

- il *ransomware* è un programma malevolo eseguito da attaccanti che sono penetrati all'interno di una rete;

- il *ransomware* cifra dati critici dei sistemi sui quali esso è eseguito, rendendone impossibile il recupero senza una chiave di decifratura in possesso solo degli attaccanti;

- il rilascio della predetta chiave di cifratura è spesso subordinata al pagamento di un riscatto (ransom) in criptovalute;

- il ripristino dei dati risulta possibile solo in presenza di un backup dei dati completo e rindondato;

CONSIDERATO CHE

- esistono diversi modi per proteggere dispositivi e dati da attacchi *ransomware* ed evitare di giungere alle estreme conseguenze di un blocco dei sistemi e il pagamento del riscatto;

CONSIDERATO INOLTRE CHE

- la sicurezza informatica è, oggi, una questione molto seria che, se non presa adeguatamente in considerazione, può inevitabilmente compromettere l'attività di un'organizzazione;

- occorre quindi pensare alla *cybersecurity* come ad una parte integrante e soprattutto preventiva di ogni attività aziendale e va quindi intesa come un costo di operatività piuttosto che come spesa accessoria;

Tutto ciò premesso e considerato

SI INTERROGA

La Giunta Regionale e l'Assessore competente per sapere:

- se si è provveduto ad effettuare la segnalazione dell'attacco *ransomware* alla Polizia Postale e in caso affermativo a che punto sono le indagini sull'origine dell'attacco;

- se si è provveduto, inoltre, ad effettuare la segnalazione al Garante della Privacy e, in caso non lo si fosse fatto, per quali motivazioni;

- quali informazioni risultano disponibili relativamente ai dati che sono stati diffusi dalla cybergang "Vice Society" a seguito dell'attacco, se si è provveduto ad informare dell'accaduto tutte le persone che sono state colpite dal *leak* e di cui sono stati eventualmente diffusi i dati sensibili e, in caso non si fosse proceduto in questo senso, per quale motivo;

- che tipo di analisi preventiva è stata eseguita prima che si verificasse il Data Breach, a quando risale l'ultimo *penetration test* effettuato nella rete di Arpa Marche e qualora si vogliano condividere tali risultati si evidenzia che è opportuno inserire *omissis* al fine di non divulgare informazioni sensibili;

- se comminata, l'importo complessivo della multa applicata dal GDPR (*General Data Protection Regulation*);

- quali attività di *remediation* sono state effettuate per accertarsi che gli attaccanti non sono ancora presenti nella rete e per mettere in sicurezza i sistemi di Arpam;

- se e per quali motivi la predetta attività di *remediation* si reputa sufficiente;

- la sequenza di eventi dell'attacco *ransomware* (c.d. *timeline*) contenente anche le azioni di Arpa Marche (ad esempio "scoperto attacco, messa a conoscenza Polizia Postale, informazione agli utenti coinvolti", etc.);

- se e quale attività utile a garantire la sicurezza informatica dell'organizzazione è stata effettuata dai responsabili tecnici e informatici di Arpa Marche e se gli stessi hanno proceduto a far effettuare eventuali ulteriori e necessarie verifiche ad un soggetto terzo al fine di ottenere un quadro più realistico del loro operato.