CONSIGLIO REGIONALE DEL VENETO

UNDICESIMA LEGISLATURA

INTERROGAZIONE A RISPOSTA IMMEDIATA N. 239

ENNESIMA FALLA NEI SISTEMI INFORMATICI VENETI. QUALE È IL LIVELLO DI CYBER SICUREZZA DELLA REGIONE DEL VENETO?

presentata il 10 febbraio 2022 dai Consiglieri Camani, Bigon, Montanariello, Giacomo Possamai, Zottis e Zanoni

Premesso che:

- il 6 febbraio 2022 i quotidiani locali il Mattino di Padova, la Nuova Venezia e la Tribuna di Treviso hanno pubblicato due articoli in cui si dimostra come dall'esterno fosse possibile accedere facilmente all'archivio delle Ulss del Veneto in cui sono registrati i dati sensibili dei cittadini;
- in particolare sembra fosse agevole accedere a un notevole numero di documenti, inclusi i dati relativi ai certificati di negativizzazione e alle comunicazioni di sorveglianza sanitaria inviate dalle Ulss del Veneto ai cittadini che hanno contratto il Covid.

Rilevato che:

- quanto riportato dalla stampa suscita forti dubbi sul sistema di sicurezza informatica delle aziende sanitarie del Veneto e sulla protezione dei dati sensibili, anagrafici e sanitari, dei cittadini;
- sebbene il Presidente Zaia abbia dichiarato pubblicamente che non si sarebbe trattato di un attacco hacker ma di un bug della rete, il fatto sembra confermare una evidente vulnerabilità dei siti regionali.

Considerato che già nel dicembre scorso un gruppo di pirati informatici aveva hackerato il sistema informatico dell'Ulss 6 Euganea, paralizzando l'attività sanitaria della provincia padovana; in conseguenza di ciò furono resi pubblici circa 9 mila dati sensibili, tra cui cartelle sanitarie, esiti di tamponi, diagnosi e buste paga.

Ritenuto che:

- quanto avvenuto recentemente, su cui non è ancora stata fatta chiarezza, avrebbe dovuto spingere la Regione a verificare senza indugio i livelli di sicurezza dei propri sistemi informatici e a migliorare eventuali meccanismi di disaster recovery;

- in ragione della delicatezza dei dati trattati, non è accettabile che lo stato di emergenza collegato alla pandemia venga addotto come giustificazione per spiegare le evidenti falle del sistema.

Tutto ciò premesso, i sottoscritti consiglieri

interrogano il Presidente della Giunta regionale

per sapere quali sono le responsabilità coinvolte nei gravi fatti esposti in premessa e quali contromisure sono state messe in campo per evitare che queste circostanze si ripetano.

Proposta n. 806 / 2022

PUNTO 29 DELL'ODG DELLA SEDUTA DEL 20/05/2022

ESTRATTO DEL VERBALE

DELIBERAZIONE DELLA GIUNTA REGIONALE n. 82 / IIM del 20/05/2022

OGGETTO:
Risposta all'interrogazione a risposta immediata n. 239 del 10 Febbraio 2022 presentata dai Consiglieri Vanessa CAMANI, Anna Maria BIGON, Jonatan MONTANARIELLO, Giacomo POSSAMAI, Francesca ZOTTIS e Andrea ZANONI avente per oggetto "ENNESIMA FALLA NEI SISTEMI INFORMATICI VENETI. QUALE È IL LIVELLO DI CYBER SICUREZZA DELLA REGIONE DEL VENETO?".

ea1ae768

COMPONENTI DELLA GIUNTA REGIONALE

Presidente	Luca Zaia	Assente
Vicepresidente	Elisa De Berti	Presente
Assessori	Gianpaolo E. Bottacin	Presente
	Francesco Calzavara	Presente
	Federico Caner	Presente
	Cristiano Corazzari	Assente
	Elena Donazzan	Assente
	Manuela Lanzarin	Presente
	Roberto Marcato	Presente
Segretario verbalizzante	Lorenzo Traina	

RELATORE ED EVENTUALI CONCERTI

FRANCESCO CALZAVARA

STRUTTURA PROPONENTE

AREA RISORSE FINANZIARIE, STRUMENTALI, ICT ED ENTI LOCALI

APPROVAZIONE

Sottoposto a votazione, il provvedimento è approvato con voti unanimi e palesi.

OGGETTO: Risposta all'interrogazione a risposta immediata n. 239 del 10 Febbraio 2022 presentata dai Consiglieri Vanessa CAMANI, Anna Maria BIGON, Jonatan MONTANARIELLO, Giacomo POSSAMAI, Francesca ZOTTIS e Andrea ZANONI avente per oggetto "ENNESIMA FALLA NEI SISTEMI INFORMATICI VENETI. QUALE È IL LIVELLO DI CYBER SICUREZZA DELLA REGIONE DEL VENETO?".

Il relatore propone alla Giunta di adottare la seguente risposta:

Come riferito dal Direttore Generale di Azienda Zero, nel "*Portale Sorveglianza Covid*" (https://sorveglianzacovid.azero.veneto.it), in data 21/01/2022 all'interno del modulo "*Portale Web Cittadino*" alla sezione "*Certificati*", è stata introdotta la possibilità di recuperare in maniera autonoma da parte dei cittadini i certificati di isolamento e di negativizzazione (qualora prodotti).
Nei giorni 6 e 7 febbraio u.s., sulla stampa locale sono stati pubblicati 2 articoli in cui veniva messa in evidenza l'erronea possibilità da parte di un cittadino, manipolando intenzionalmente i parametri contenuti nell'URL di collegamento, di recuperare i certificati di isolamento e di negativizzazione afferenti ad altri cittadini.
Già in data 6 febbraio, alle ore 7.54 il problema di sicurezza veniva prontamente segnalato da Azienda Zero alla Ditta fornitrice del software la quale già alle ore 9.32 interveniva inibendo la pubblicazione dei suddetti certificati.
Da un'analisi approfondita è emerso che il problema ha coinvolto soltanto i due certificati di isolamento e di negativizzazione e non i restanti presenti nella sezione "*Certificati*" (es. certificato vaccinale certificato vaccinale COVID) e l'accesso ad ulteriori dati contenuti all'interno dell'intero sistema gestionale SIAVr non era consentito.
Non sono state altresì estratte informazioni infrastrutturali dell'applicativo stesso o di altre componenti regionali così come non sono state rilevate intrusioni all'interno della rete informatica di Regione del Veneto.
L'analisi dei log conservati dalla piattaforma SIAVr, ha consentito di individuare i soggetti che hanno effettuato accessi impropri e per i quali sono state predisposte le dovute segnalazioni agli organi giudiziali.
Azienda Zero, in qualità di Responsabile del trattamento dei dati nominata dalle varie Aziende ULSS, si è fatta portavoce all'interno del sistema Sanitario regionale nel diffondere tali informazioni ai referenti dei sistemi informativi e privacy e ai loro DPO e nel supportare le varie Aziende nella eventualità di segnalazioni all'Autorità Garante per la protezione dei dati personali.
Quali contromisure da mettere in campo, con nota prot. 58.275 del 9.02.2022 viene istituita una task force di esperti di sicurezza informatica al fine di individuare le carenze delle varie Aziende Sanitarie.
Conseguentemente è stata effettuata una ricognizione sui livelli di sicurezza della Aziende Sanitarie, ed è stato predisposto il documento *"Proposta di intervento per la Sicurezza ICT della Sanità della Regione del Veneto"*, prot. 170.650 del 13/04/22 con cui venivano individuate le azioni da intraprendere a sostegno e protezione della Sanità Veneta e l'istituzione di una struttura organizzativa quale organo di gestione e controllo di tutti gli aspetti relativi alla Cyber Security.
Si evidenzia che ulteriori dettagli tecnici sono a disposizione presso la Direzione ICT e Agenda Digitale dove è reperibile la documentazione e il personale tecnico per eventuali ulteriori chiarimenti.

LA GIUNTA REGIONALE

UDITO il relatore, il quale dà atto che la struttura competente ha attestato, con i visti rilasciati a corredo del presente atto, l'avvenuta regolare istruttoria della pratica, anche in ordine alla compatibilità con la vigente legislazione statale e regionale, e che successivamente alla definizione di detta istruttoria non sono pervenute osservazioni in grado di pregiudicare l'approvazione del presente atto;

2c5cd9ca

DELIBERA

1. di approvare, nel testo riportato in premessa, la risposta all'atto ispettivo richiamato in oggetto;
2. di incaricare dell'esecuzione del presente atto la Segreteria della Giunta - Direzione Attività Istituzionali della Giunta Regionale e Rapporti Stato/Regioni.

IL VERBALIZZANTE
Segretario della Giunta Regionale
f.to - Dott. Lorenzo Traina -