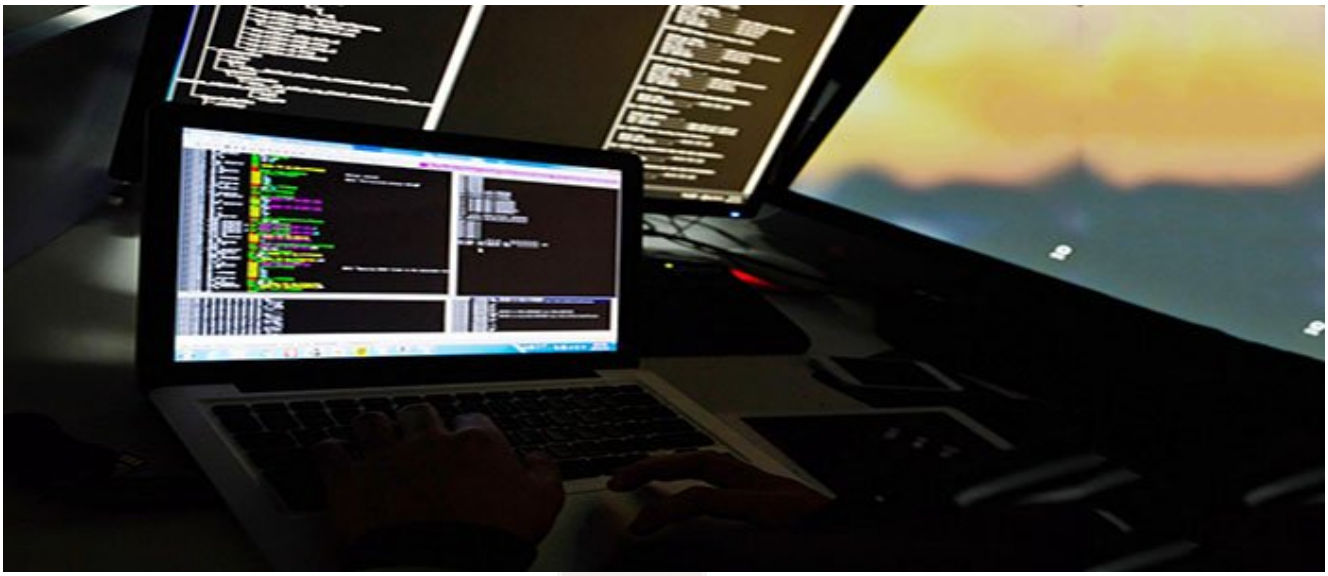
Referendum: hacker, voto non sicuro; i dati erano accessibili

Data: Invalid Date | Autore: Redazione



MILANO, 20 OTTOBRE -Il voto elettronico scelto dalla Regione Lombardia per il referendum sull'autonomia di domenica prossima potrebbe non essere sicuro. Ad AGI risulta che alcuni server per mesi non avrebbero avuto protezioni sufficienti da intrusioni esterne. Al momento non sarebbe possibile escludere che qualcuno, in questo periodo, sia entrato nei database con l'intento di studiare parti del software per la gestione del voto, e cercare eventuali vulnerabilita'. Per manomettere il risultato della consultazione. Dalla Regione rassicurano sulla solidita' del sistema. Ma andiamo con ordine. [MORE]

La denuncia arriva da Matteo Flora, hacker e imprenditore, che ripercorre le fasi della sua ricerca. E' partito da una frase del presidente della Lombardia Roberto Maroni: "I tablet con cui si votera' per il referendum in Lombardia e' a prova di hacker". E ha fatto il suo personale fact checking sulle property online di SmartMatic, la societa' venezuelana che ha vinto l'appalto della Regione per la gestione della votazione sui tablet.

L'hacker, esperto di analisi di fonti aperte in rete, sostiene che la societa' avrebbe omesso "i piu' basilari protocolli di sicurezza" su alcune alcune cartelle contenenti dati sensibili, tra cui certificati e pezzi di codice per la configurazione delle macchine. Questi dati, sempre secondo Flora, sarebbero stati per mesi "accessibili a chiunque", lasciando aperta la possibilita' di "scaricare ampie porzioni di codice" del software della SmartMatic che dovrebbe gestire il voto referendario: SmartMatic Election 360.

Non solo. Se e' vero che questi dati sono stati alla merce' di potenziali 'criminali informatici' o magari di istituzioni interessate a manomettere l'esito referendario in Lombardia, questi avrebbero avuto tutto il tempo di scaricarli e studiare le macchine per prepararsi alle elezioni con dei software in grado di manipolarne i risultati. In una serie di documenti che AGI ha avuto moto di consultare, Flora

mostra con ogni evidenza quelli che definisce "grossolani errori di configurazione dei server" che hanno lasciato disponibili i contenuti del server, compresi i parte codici del software per la gestione del voto elettronico.

I dati sono contenuti in una cartella "Italy/RefLombardia2017". Errori gravi e "non certamente volontari", dice Flora, ma la sensibilita' dei dati lasciati senza protezione potrebbe essere confermata dal fatto che la Regione a poche ore dalla segnalazione arrivata dall'hacker (tramite una mail al Cert-Pa, la struttura dell'Agenzia per l'Italia Digitale della Presidenza del Consiglio dedicata alla sicurezza informatica) ha rimosso i contenuti 'scoperti' segnalati, circa una 25 indirizzi url.

SmartMatic minimizza e fa quadrato intorno al suo sistema di votazione: "Tutti i sistemi di sicurezza che garantiscono l'integrita' del voto durante il referendum rimangono intatti, il sistema e' sicuro" spiega un portavoce. "Non ci sono stati attacchi hacker al sistema di votazione elettronica. Questa persona (Flora, ndr) ha semplicemente avuto accesso a una repository pubblica con dati non confidenziali e non sensibili". SmartMatic sostiene che i dati a cui Flora ha avuto accesso sono quelli di "applicazioni che consentono operazioni per il coordinamento della logistica".

Una versione sostenuta anche da alcuni tecnici della Regione contattati da Agi che, pur non smentendo il problema, ribadiscono che il voto di domenica ora e' sicuro e che non risultano dati rubati nel momento in cui gli indirizzi erano senza protezione. Alcuni sostengono pero' che il voto referendario non sara' gestito dalla suite SmartMatic Election 360, ma un altro programma dell'azienda.

Se questa indiscrezione fosse confermata, lascerebbe sul campo due ipotesi: o le cartelle di SmartMatic Election 360 servivano solo per 'simulare' il voto, oppure che, per evitare problemi, le istituzioni, scoperto il problema, abbiano chiesto alla societa' di usare un software diverso. Va detto inoltre che al momento non c'e' prova che altri soggetti abbiano scaricato i dati, ma e' un'ipotesi che non puo' essere del tutto esclusa.