Attacco di hacker russi alla Pubblica amministrazione, scongiurato lo stop degli stipendi

Colpito il sistema di servizi a 1.300 enti tra cui Comuni, Anac e Csm

ROMA, 19 dicembre 2023, 10:59

di Lorenzo Attianese e Massimo Nesticò

https://www.ansa.it/sito/notizie/cronaca/2023/12/18/massiccio-attacco-di-hacker-russi-alla-pubblica-amministrazione-chiesto-il-riscatto_649585ff-1f0d-4f3b-98e3-486f02531ad3.html

Scongiurato il blocco degli stipendi di dicembre e delle tredicesime per i dipendenti degli enti locali colpiti dal massiccio attacco degli hacker russi di Lockbit all'azienda Walpole la cui infrastruttura cloud è utilizzata da Pa Digitale, società che fornisce servizi a circa 1.300 enti della pubblica amministrazione.

Lo comunica l'Agenzia . per la cybersicurezza nazionale, informando che a dieci giorni dall'offensiva l'attività svolta per contenere i danni "ha consentito il ripristino di tutti i servizi impattati, nonché il recupero dei dati oggetto dell'attacco per più di 700 dei soggetti pubblici nazionali e locali", legati alla catena di approvvigionamento di Pa Digitale".

Per le restanti amministrazioni, aggiunge, "resta l'esigenza di recuperare i dati risalenti ai 3 giorni precedenti l'attacco, avvenuto l'8 dicembre". L'offensiva aveva criptato e reso inaccessibili diversi database. La rivendicazione di Lockbit è giunta con la richiesta di riscatto in criptovaluta da parte dei criminali informatici. Ma il ministro della Pa, Paolo Zangrillo, assicura: "Stiamo verificando, al momento non mi risultano problemi. Finora non ho ricevuto feedback di emergenza su questo fronte ma adesso approfondirò la questione".
Indaga la Polizia postale, mentre anche il Garante della privacy è stato avvisato. Il ransomware - un virus che prende in ostaggio i dispositivi - era stato lanciato lo scorso 8 dicembre contro una serie di server a Milano e Roma di Westpole, l'azienda di sviluppo la cui infrastruttura cloud è utilizzata da Pa Digitale: si tratta della società privata del gruppo Buffetti, che eroga prestazioni a centinaia realtà della pubblica amministrazione, tra cui rendicontazione di buste paga e fatturazione elettronica. Uno dei sistemi colpiti è Urbi, il software cloud di servizi di gestione digitali (demografici, anagrafici, pagamento di stipendi ai dipendenti comunali) di cui si avvalgono circa cinquecento Comuni, alcune Province, diverse Unioni di Comuni e Comunità montane ed enti tra cui l'Agenzia per l'Italia digitale, il Consiglio superiore della magistratura e l'Autorità nazionale anticorruzione. Per una buona metà dei servizi è stata avviata la procedura di ripristino attraverso backup, ma l'altra metà potrebbe essere difficilmente recuperabile. Potrebbe quindi essere necessario, ad esempio, rifare i conti per quanto riguarda gli stipendi, cosa che potrebbe far slittare il pagamento da dicembre a gennaio in alcuni casi. Disagi e rallentamenti a cui per fortuna non sarebbero seguiti furti digitali, almeno per il momento.

"Riteniamo poco probabile l'esfiltrazione dei dati da parte dell'attaccante, evidentemente interessato al blocco dell'infrastruttura, non al contenuto dei dati, di tipo indifferenziato, presenti sui nostri repository e all'interno delle circa 1.500 macchine virtuali", aveva specificato qualche giorno fa Westpole Spa in una mail a Pa digitale. Lockbit è uno dei gruppi cybercriminali più attivi che già in passato ha attaccato vari enti in Italia.

"La loro finalità tipica è l'estorsione, l'elemento che fa un po' specie è - a

quanto risulta finora - l'assenza di esfiltrazione, che in genere precede la minaccia della loro pubblicazione: è possibile che l'infrastruttura attaccata non lo abbia permesso anche grazie alle contromisure di sicurezza in essere - ha commentato Matteo Macina della Cyber Security Italy Foundation - . Dall'esterno non è possibile conoscere i tempi di risoluzione del problema con certezza , che potrebbe essere risolto a breve oppure in tanti giorni, soprattutto nel caso in cui i dati non siano disponibili nel backup, ad esempio nel caso di registrazioni elettroniche non salvate che potrebbe essere necessario riprocessare manualmente ".