L'allarme

Da Gentiloni a Mattarella le password dei politici nell'archivio degli hacker

Pubblicate le credenziali di 450 milioni di indirizzi e-mail La Polizia: "Vecchie di anni, rischi per chi non le cambia"

ARTURO DI CORINTO
FABIO TONACCI

ROMA. Sarà pure un archivio vecchio di qualche anno, come si affretta in serata a specificare la Polizia Postale, ma le password, nella maggior parte dei casi, sono vere. L'immenso database riporta gli indirizzi mail istituzionali di centinaia di politici italiani: deputati, senatori, membri di governo, ministeriali. Qualche nome? Paolo Gentiloni, Angelino Alfano, Silvio Berlusconi, Giorgia Meloni, Daniela Santanché, Roberto Maroni, Nicola Latorre e perfino il capo dello stato Sergio Mattarella, con la posta elettronica di quando era deputato.

Si chiama Anti Public e potrebbe essere il data leak di email più grande della storia. Coinvolge istituzioni di tutto il mondo, dalla Casa Bianca al Parlamento Europeo, da Europol a Eurojust. L'archivio di 17 giga, contenente 450 milioni di email e relative password (alcune delle quali valide anche per i social network), si trova su una piattaforma cloud russa ed è stato scoperto dagli analisti di Var Group, azienda di sicurezza informatica con partner in Italia.

Dalle verifiche che è stato possibile fare è risultato che alcune email appartengono a deputati e senatori che non siedono più sugli scranni del parlamento da almeno una legislatura ma che possono continuare a usare le vecchie mailbox per lavorare. Alcune hanno come password i nomi dei figli o la città di provenienza. Qualcuna è vecchia di anni, molte sono codici alfanumerici senza un significato particolare.

> Nell'elenco anche Alfano e Berlusconi. La traccia che porta a una piattaforma russa

Gli analisti della Polizia postale e dei servizi interni di intelligence stanno studiando l'elenco. «Si tratterebbe di una raccolta di informazioni datate, frutto di attacchi informatici già oggetto in passato di divulgazione, non privi di errori». Il problema, però, rimane, perché per alcuni anni le credenziali private di politici e uomini di Stato sono state molto probabilmente utilizzate da hacker per spionaggio, ricatti o altro.

Ma come è potuto succedere? La notizia del leak gira tra gli esperti di cybersecurity dal dicembre scorso, ma solo oggi è stato possibile renderla pubblica dopo che gli esperti hanno avvisato il ministero dell'Interno. È ancora possibile accedere all'archivio, cliccando su un link della piattaforma cloud di mail.ru, un provider russo di servizi Internet. E se oggi è ancora accessibile, può voler dire due cose: «O è stato già acquistato e usato, chissà con quali profitti per i criminali che l'hanno creato — sostiene Pierluigi Pagani, capo tecnologo della Cse CybSec e consulente del nostro governo — oppure potrebbe essere il risultato di una faida tra gruppi criminali. Ritengo sia più probabile la prima».

Secondo i ricercatori di D3Lab, gli hacker sono riusciti a mettere insieme un database così vasto sfruttando tre sistemi: rastrellando il risultato di furti fatti con campagne massicce di phishing; attaccando attraverso reti di computer di utenti ignari controllati via software; infilandosi nelle falle dei server di servizi internet molto popolari per telefonare online, leggere la posta, acquistare libri e scarpe.

Per evitare problemi la polizia postale consiglia comunque di «effettuare il periodico cambio della password, utilizzando una combinazione di numeri, lettere maiuscole, minuscole e caratteri speciali».