Nota sull'attacco hacker del 25 agosto

Tecnici al lavoro, attivate procedure di emergenza

Si comunica che, in data 25 agosto 2024 alle ore 23:42, il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), ha provveduto a segnalare un data leak, cioè la divulgazione non autorizzata di dati, del contenuto di un database associato al CNR. Da un'analisi effettuata si è evidenziato che il data leak è avvenuto tramite un accesso non autorizzato al componente PhpMyAdmin utilizzato per la gestione del database relativo all'applicazione denominata Arch-Motro, che gestisce gli elenchi di versamento della documentazione non più di uso corrente destinata all'Archivio di Deposito dell'Ente. Sulla base della segnalazione, i dati sarebbero stati pubblicati su un forum underground (BreachForums) e resi accessibili attraverso un link specifico.

Il CNR, a partire dalla mattina del 26 agosto, ha attivato tutte le adeguate azioni da parte delle strutture interne competenti al fine effettuare le opportune verifiche circa lo stato delle informazioni pubblicate e al contempo attuare le relative misure per mettere in sicurezza i sistemi interessati e quelli correlati.

La verifica dei contenuti esposti ha evidenziato che si tratta di una copia del database applicativo del servizio Arch-Motro, riportante i dati registrati dall'applicazione. Si conferma che il CNR non è stato oggetto di alcun criptaggio dati, né c'è stata alcuna interruzione dei servizi. Inoltre, l'esfiltrazione dati non è avvenuta a seguito di alcun attacco ransomware e, ad oggi, non risulta nessuna richiesta di riscatto.

Si sottolinea che i dati oggetto della violazione sono esclusivamente quelli ricavabili dagli elenchi di versamento del materiale documentario cartaceo destinato all'Archivio di Deposito dell'Ente. Si tratta, tecnicamente, di metadati descrittivi che indentificano i faldoni conservati nell'Archivio di Deposito e non dei dati relativi ai documenti in essi contenuti. Essi, in alcuni casi, possono riportare denominazioni parlanti e quindi lasciare dedurre alcuni dati personali; tuttavia, non si tratta né di documentazione, né di dati contenuti nei procedimenti.

I dati personali riconducibili agli interessati sono limitati alle descrizioni usate per individuare i contenuti dei faldoni e a garantire il corretto alloggiamento degli stessi, non contengono, quindi, dati relativi ai procedimenti. Le categorie di interessati identificate dall'analisi dei dati esfiltrati sono: personale con rapporto di lavoro strutturato e non strutturato, soggetti che hanno avuto con l'Ente contenziosi cessati da almeno 10 anni, soggetti che hanno partecipato a procedure interne o esterne per la selezione di personale concluse da almeno 10 anni, fornitori. Si darà tempestiva comunicazione di eventuali ulteriori categorie che dovessero risultare da successivi approfondimenti .

Si precisa che nel database sottratto non sono presenti dati, riferimenti, atti e progettualità, inerenti ad affari o pratiche in corso di trattazione o svolgimento, né dati o informazioni sensibili riferibili a progetti, proprietà intellettuale e/o ai nominativi del personale CNR su di essi impiegato inerente ad affari o pratiche in corso di trattazione o svolgimento, così come non sono presenti informazioni relative a interessi strategici, politici e organizzativi dell'Ente.

Alla luce dell’istruttoria condotta dai responsabili interni, nell’immediato sono state adottate misure tecniche quali: disabilitazione dell'accesso tramite Internet all'applicativo, limitazione dell'accesso all'applicativo dalle sole reti interne CNR dell’area romana o tramite VPN, disattivazione del componente PhpMyAdmin e cambio delle password applicative di accesso al database.

Erano, invece, già in corso misure tecniche e organizzative come: la sostituzione dell'applicativo nel perimetro delle misure di trasformazione digitale programmate dall'Ente e l’emanazione - a maggio 2024 - del “Regolamento di organizzazione dell’Archivio di Deposito dell’Amministrazione Centrale del Consiglio Nazionale delle Ricerche e degli Archivi Intermedi delle strutture della Rete Scientifica del CNR (Circolare CNR n. 20/2024).

La presente nota viene pubblicata dopo aver ottemperato alle prescrizioni normative agli organi competenti. A tal riguardo il CNR garantisce la prosecuzione dell’analisi, anche attraverso tecniche di digital forensics, al fine di effettuare il monitoraggio proattivo di simili situazioni sul resto dell'infrastruttura e consentire gli eventuali successivi adempimenti previsti dalla normativa.

Il CNR già dal 2022, con l’avvio della digitalizzazione delle attività dell’Ente, ha migliorato la postura di sicurezza concentrandosi sui sistemi più vulnerabili, riducendo significativamente i fattori di rischio seguendo il percorso indicato dalle linee guida Agid. Negli ultimi due anni questi sforzi hanno consentito di rinnovare i servizi di collaborazione digitale, sostituire il sistema di protocollo, della conservazione documentale e attivare il nuovo catalogo dei prodotti della ricerca.

Per ogni chiarimento o ulteriore informazione in relazione alla violazione in oggetto ed eventuali questioni relative ai profili privacy: violazione.archmotro@cnr.it