PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5774 di Venerdì 24 gennaio 2025

Cybersicurezza: Linee guida conservazione delle password

Un documento pubblicato dall'agenzia per la cybersicurezza nazionale (ACN) presenta un aspetto fondamentale nell'ambito della sicurezza informatica e della protezione dei dati personali: la conservazione delle password.

L'agenzia per la cybersicurezza nazionale ACN ha pubblicato un documento dedicato alle modalità di conservazione sicura delle password, per aggiornare gli esperti di sicurezza informatica su tecniche di attacco e tecniche di difesa. E' importante che i gestori di sistemi e servizi prevedano misure tecniche per proteggere gli archivi delle password in caso di attacchi e data breach.

Linee guida funzioni criptografiche ? conservazione delle password

Un pregio non indifferente di queste linee guida è legato al fatto che il testo è stato elaborato d'intesa con il Garante per la protezione dei dati personali, perché è ben noto che la adozione di password rappresenta il più comune e diffuso strumento di blocco dell'accesso a dati personali, presenti su un computer.

Anche in questo caso, la ACN si preoccupa di mettere in evidenza il fatto che la rapida evoluzione degli strumenti di attacco può rendere necessario un frequente aggiornamento di questo documento.

D'altro canto, nessuno può dubitare del fatto che la gestione delle password sia un aspetto fondamentale di una strategia di sicurezza informatica, sia a livello di scelta delle password, sia a livello di loro conservazione sicura. Qualora la password sia conservata in un archivio digitale, diventa altrettanto fondamentale proteggere questo archivio con robuste funzioni criptografiche, chiamate "password hashing".

Una funzione di hashing prende come input una stringa di bit di lunghezza arbitraria e restituisce una stringa di bit di lunghezza fissa, detta "digest". La proprietà di questo sistema di calcolo è di essere non invertibile, il che significa che, anche se si è in possesso del digest, diventa estremamente difficile ricostruire la password, sulla base della quale il digest è stato calcolato.

Il documento passa successivamente ad illustrare quali sono le tecniche di attacco utilizzate dai malviventi, che portano al temibile scenario, chiamato " data breach", vale a dire la cattura delle password.

Il malvivente può utilizzare l'attacco per forza bruta, vale a dire calcolando l'hashing di password casuali, fino a trovare una corrispondenza, oppure può effettuare un attacco basato sul dizionario. Quest'ultimo attacco spesso dà risultati positivi, quando l'utente sceglie come password una parola di senso compiuto, reperibile sul dizionario.

L'attacco diventa ancora più efficiente ed efficace, quando il malvivente ha già compilato le cosiddette tabelle arcobaleno, ovvero tabelle precompilate, che contengono i digest di un numero elevato di password. Confrontando direttamente questi digest con quelli presenti nell'archivio, il recupero di una parola chiave è banale e rapidissimo.

Il documento prosegue illustrando varie tecniche di protezione degli archivi, ove sono presenti le password, illustrandone i punti forti ed i punti deboli. Al proposito, il documento ricorda come nel 2013 venne lanciato un bando per la creazione di nuovi algoritmi di password hashing, che ha portato, al termine della gara, a selezionare come vincitore l'algoritmo Argon2.

Come accennato in precedenza, il manuale quindi non prende in considerazione suggerimenti su come scegliere parole chiave, da offrire al personale che ha accesso a sistemi informativi, ma prende in considerazione le modalità di conservazione sicura.

Quanto prima sarà reso disponibile un nuovo documento, indirizzato agli utenti di base, che potranno così selezionare parole chiave, che renderanno sempre più difficile la violazione degli archivi, ove esse sono conservate, da parte di malviventi purtroppo sempre più attrezzati.

Agenzia per la Cybersicurezza Nazionale - Garante per la protezione dei Dati Personali - Linee guida Funzioni crittografiche - Conservazione delle Password

Adalberto Biasiotti

www.puntosicuro.it