DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Conservazione delle password: linee guida e misure di protezione

11 Luglio 2024

Pietro Boccaccini, Director, Deloitte Legal
Alessandro Amoroso, Senior Associate, Deloitte Legal

Pietro Boccaccini, Director, Deloitte Legal

Alessandro Amoroso, Senior Associate, Deloitte Legal

Studio Legale Associato

Deloitte Legal

Sommario: 1.Introduzione; 2. Le principali indicazioni contenute nelle Linee guida; 2.1 L'hashing, il salting, il peppering e l'adeguatezza delle funzioni crittografiche; 2.2 Conservazione e cancellazione delle password; 3. Rischi connessi a un data breach; 4. Misure di gestione del rischio cyber; 5. La responsabilità del data processor; 6. Conclusioni.

1. Introduzione

Nell'attuale contesto fortemente digitalizzato le password sono uno strumento fondamentale per proteggere la sicurezza delle persone e delle aziende.

L'accesso alla maggior parte dei sistemi e servizi informatici richiede il superamento di procedure di autenticazione che spesso coinvolgono l'uso di una password o di una parola chiave, come una domanda segreta.

Gli archivi in cui sono conservate le password sempre più frequentemente finiscono nelle mani di soggetti malintenzionati e, talvolta, vengono anche pubblicati nel dark web e utilizzati per condurre attacchi definiti di *compromised credentials*. Circa il 31% di tutti gli attacchi a livello internazionale è legato alla compromissione delle credenziali.

L'adeguata protezione delle password è quindi diventata una misura necessaria non solo per la sicurezza dei sistemi e servizi informatici ma anche – allargando la prospettiva – per salvaguardare l'interesse generale, evitando la propagazione di attacchi malevoli.

L'esigenza di individuare misure tecniche idonee per proteggere efficacemente le password degli utenti conservate nell'ambito dei sistemi di autenticazione informatica, o di altri sistemi, hanno condotto alcune Autorità ad adottare linee guida relative alle misure di sicurezza da applicare per la conservazione delle password.

Il framework legale applicabile in materia è in evoluzione, il tema delle password deve quindi essere visto anche in un'ottica di compliance alla normativa sulla protezione dei dati personali e a quella in materia di cybersicurezza.

vedi l'articolo online

2. Le principali indicazioni contenute nelle Linee guida

L'Agenzia per la Cybersicurezza Nazionale (ACN) e il Garante per la protezione dei dati personali nel dicembre 2023 hanno pubblicato le *Linee guida funzioni crittografiche - la conservazione delle password* ("**Linee guida**").

Queste Linee guida hanno un ambito d'applicazione molto ampio, dovendosi ritenere valide in relazione a tutti i casi in cui le password riguardino numerosi utenti, permettano l'accesso a banche dati di particolare rilevanza o dimensioni, siano utilizzate da utenti che trattano dati appartenenti a categorie particolari.

Le raccomandazioni fornite da ACN e Garante includono anche le seguenti.

2.1 L'hashing, il salting, il peppering e l'adeguatezza delle funzioni crittografiche

Mediante la funzione di hash crittografica, l'input della password (di lunghezza arbitraria) anziché essere salvato in chiaro è trasformato in una stringa di bit di lunghezza fissa (detto digest). Mentre un determinato input darà sempre un certo digest, la caratteristica della funzione di hashing è quella di essere solo *one-way* e pertanto non invertibile.

Il solo hashing, tuttavia, in caso di data breach espone ad alcuni rischi, tra cui i seguenti.

a. Attacchi di tipo forza bruta (*brute force*): una volta ottenuta la lista di coppie utente-digest, l'attaccante potrebbe ricercare l'hash di password casuali fino ad individuare una corrispondenza. Al riguardo, una tipologia di attacchi sempre più frequente è il cd. reverse brute force o password spraying, in cui gli attaccanti utilizzano sempre la stessa password, modificando gli username (in modo da aggirare i limiti sul numero massimo di tentativi per ogni utente).

b. Attacchi al dizionario (*dictionary attacks*): l'attaccante potrebbe cercare una corrispondenza con gli hash delle password più comuni.

Al fine di scoraggiare attacchi *brute force*, occorre utilizzare algoritmi di hashing che abbiano un funzionamento tale da rallentare le capacità offensive dell'attaccante.

Quanto invece all'impedire attacchi al dizionario – in particolare tramite "tabelle dati" (*look up tables*) e "tabelle arcobaleno" (*rainbow tables*) – è consigliato utilizzare algoritmi di password hashing che prevedono l'aggiunta di un salt ad ogni password, cioè una stringa di bit casuali che viene concatenata alla password prima del calcolo del digest e poi salvata in chiaro insieme al digest della password dell'utente. L'aggiunta del salting permette di ottenere, tra l'altro: (i) che il digest di due password uguali non sia lo stesso (con il solo hashing, dalla comparazione dei digest sarebbero facilmente individuabili gli utenti con la stessa password); (ii) che anche le password più comuni vengano modificate nel digest.

Infine, per un ulteriore livello di sicurezza, è possibile aggiungere anche un pò di "pepe". A differenza del salt, il pepper può essere composto dalla stessa stringa per tutte le password nell'archivio, ma deve essere tenuto segreto e separato.

L'elemento principale per la sicurezza della conservazione delle password resta in ogni caso la complessità della funzione crittografica di hashing. Le Linee guida forniscono indicazioni dettagliate sulle funzioni crittografiche considerate al momento più sicure, individuando i parametri raccomandati per gli algoritmi.

Le Linee Guida, infine, riconoscono l'importanza di un approccio sistemico alla sicurezza delle password e, pertanto, non solo l'adozione di meccanismi di hashing avanzati, ma anche l'implementazione di politiche aziendali adeguate, la formazione di tutto il personale ed una gestione attenta delle chiavi di cifratura.

2.2 Conservazione e cancellazione delle password

Le FAQ collegate alle Linee guida approfondiscono anche il tema della conservazione delle password, che può essere necessaria: (i) per consentire la verifica dell'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online; oppure (ii) per garantire la sicurezza delle procedure di autenticazione informatica, ad esempio per impedire il riuso da parte dell'utente delle precedenti password (c.d. password history) o per assicurare il ripristino del sistema di autenticazione informatica in caso di incidente (copie di backup).

Le FAQ specificano che le password devono essere tempestivamente cancellate nel caso di cessazione

vedi l'articolo online

o dismissione dei sistemi informatici o servizi online oppure nel caso di disattivazione o revoca delle credenziali di autenticazione di un utente, che non ha più necessità di accedere a un sistema informatico o un servizio online o che non ha più i requisiti che ne hanno determinato l'abilitazione.

3. Rischi connessi a un data breach

L'utilizzo di hashing con una funzione crittografica conforme allo stato dell'arte, del salting e eventualmente del peppering, costituiscono misure tecniche fondamentali per attenuare gli effetti negativi di un data breach. Come indicato anche nelle "*Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali*" dell'EDPB, se sono state adottate tecniche crittografiche conformi allo stato dell'arte per proteggere le password degli utenti e non sono state coinvolte anche altre tipologie di dati personali (e.g. dati personali di categorie particolari), la violazione potrebbe non presentare rischi per i diritti e le libertà degli interessati, permettendo di non avere l'obbligo di effettuare la notifica della violazione all'Autorità competente in materia di protezione dei dati personali, che comunque rimarrebbe una buona pratica e un adempimento fortemente consigliabile in tali circostanze.

Naturalmente, la valutazione dei rischi in relazione all'eventuale violazione di credenziali deve tenere conto non solo dei rischi connessi all'utilizzo di tali credenziali sui sistemi cui sono collegate, ma anche di quelli collegati all'utilizzo delle stesse per l'accesso ad altri servizi online, anche erogati da soggetti diversi dal titolare che ha subìto la violazione, in considerazione dell'uso da parte degli interessati di identiche o simili credenziali (ad esempio, cambiando un numero o una lettera) per usufruire di più servizi. Si tratta dei cc.dd. attacchi di credential stuffing, volti a verificare la validità di credenziali di autenticazione acquisite nell'ambito di altri attacchi informatici. Al riguardo, nel provvedimento del 10 marzo 2022 [9780717], il Garante ha sottolineato come la comunicazione agli interessati costituisca non solo un adempimento generalmente obbligatorio ma anche come essa stessa sia un fattore importante di mitigazione dei rischi in presenza di un'esfiltrazione di credenziali di autenticazione. I rischi saranno naturalmente maggiori nel caso di violazione delle credenziali per un single sign-on, in quanto la compromissione delle credenziali potrà riguardare tutti i servizi cui l'interessato ha dato accesso al single point.

I rischi di una possibile violazione, inoltre, sono più alti laddove gli attacchi riguardino determinati settori come il settore bancario, che costituisce da sempre un obiettivo primario per i criminali informatici (cfr. Garante, provvedimento dell'8 febbraio 2024 [9991020]).

4. Misure di gestione del rischio cyber

È opportuno evidenziare che l'adozione delle misure necessarie per il rispetto delle Linee guida e delle best practice in materia di conservazione delle password è un rilevante tassello della struttura per la cybersicurezza – che si compone di una serie di procedure, processi, documenti legali e tecnici, monitoraggi e interventi operativi – la cui definizione è richiesta:

- sia dalla Legge 90/2024 di recentissima approvazione ("Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" - pubblicata nella Gazzetta Ufficiale n. 153 del 2 luglio 2024);
- che dal framework introdotto dalla direttiva 2022/2555 (NIS2), che impone a tutti i soggetti essenziali e importanti di adottare misure tecniche, operative e organizzative di gestione del rischio cyber.

Anche i presidi di sicurezza che devono essere adottati da ogni organizzazione, pubblica o privata, per la tutela dei dati personali in base al Regolamento 2016/679 (GDPR) devono includere misure stringenti per una adeguata protezione delle password.

Appare quindi complesso e variegato il set di norme che assumono rilevanza in questo contesto e che impongono un approccio alla sicurezza integrato: legale, organizzativo e tecnico.

Il report denominato "Operational Summary" recentemente pubblicato dall'ACN ha messo in evidenza – fotografando la situazione delle minacce cyber in Italia a maggio 2024 – come le tecniche impiegate (e.g. phishing, spear phishing, smishing) per cercare di acquisire informazioni riservate di persone o organizzazioni come password, numeri di carta di credito o dati bancari siano sempre più diffuse e tocchino in modo trasversale le PA e tutti i settori del privato, dai trasporti, alle telecomunicazioni, ai servizi bancari e finanziari, al sanitario, ecc.

Approntare un sistema strutturato di difesa da queste minacce, peraltro in costante evoluzione, risulta

quindi fondamentale non solo per assolvere agli obblighi normativi esistenti e a quelli di imminente introduzione ma anche, e soprattutto, per garantire la sicurezza dell'organizzazione, dei suoi asset e delle persone, che possono subire gravi pregiudizi in conseguenza della violazione dei propri dati.

5. La responsabilità del data processor

La compromissione delle credenziali può avere un impatto su molteplici organizzazioni nel caso di un attacco alla supply chain, per esempio nel caso di attacco a un soggetto nominato responsabile del trattamento ai sensi dell'articolo 28 del GDPR.

In tal caso, il responsabile potrebbe assumere responsabilità nei rapporti interni con il titolare del trattamento (in quanto verso l'interessato il titolare e il responsabile rispondono solidalmente) per i danni direttamente derivanti dall'inadeguatezza delle proprie misure di sicurezza per non aver adempiuto agli obblighi previsti per i responsabili del trattamento o aver agito in modo difforme o contrario alle istruzioni del titolare, salvo ove dimostri che l'evento dannoso non gli è in alcun modo imputabile. Ciò non significa, tuttavia, che il titolare del trattamento potrebbe facilmente "scaricare" la responsabilità per l'eventuale inadeguatezza delle misure di sicurezza solo sul responsabile del trattamento. Come anche indicato dal Garante nel provvedimento del 17 settembre 2020 [9461168] in ragione della "responsabilità generale" del titolare del trattamento, questo risponde della violazione ove non abbia impartito al responsabile del trattamento le necessarie istruzioni o non abbia svolto attività di vigilanza o revisione in merito alla sicurezza dei dati trattati per proprio conto, indipendentemente dal fatto che l'outsourcer abbia un ruolo predominante nella concreta gestione del contesto del trattamento.

Qualsivoglia nesso causale, inoltre, si interromperebbe nel caso in cui il responsabile informi il titolare della violazione e l'attaccante utilizzi le informazioni raccolte durante tale attacco per un successivo attacco. In tale caso, infatti, verrebbe meno il rapporto di cd. "sequenza costante" da un evento originario, poiché il fatto del terzo costituirebbe elemento idoneo a determinare l'evento, a prescindere dalla condotta precedente del responsabile del trattamento, non avendo il titolare adottato misure adeguate a ridurre e mitigare il rischio.

6. Conclusioni

Il futuro è passwordless. L'utilizzo di device esterni di cui il solo utente ha il possesso o l'utilizzo di informazioni biometriche permettono di sostituire le credenziali con le cd. passkeys. Allo stato attuale, però, le password continuano ad essere il principale e più diffuso strumento di identificazione digitale, per cui la protezione delle stesse è un elemento cruciale, per tutte le organizzazioni, a tutela degli interessi propri e altrui.

Lo scenario attuale, peraltro, è contraddistinto, da un lato, da un aumento esponenziale delle minacce ai sistemi informatici per via di attacchi sempre più insidiosi e, dall'altro, da un framework normativo in materia di cybersicurezza complesso e in evoluzione, che impone sia alle PA che alle imprese di ragionare molto attentamente sui propri presidi in materia di security, strutturando procedure adeguate, implementando processi efficaci e disciplinando in modo opportuno i rapporti con i fornitori, anche in un'ottica di attribuzione specifica dei compiti legati al mantenimento di un alto livello di sicurezza (inclusa la protezione delle password) e di allocazione delle responsabilità in caso di inadempimenti e incidenti.

L'approccio da tenere per una corretta gestione dei rischi cyber - che coinvolgono in modo sostanziale anche le password e la loro protezione - è necessariamente integrato, venendo in rilievo temi di governance e aspetti tecnici, organizzativi e legali.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it