Digeat N.1 - 19 Marzo 2024

La modifica periodica delle password: come affrontare professionalmente un argomento tecnico

Di Cesare Gallotti Stefano Ramacciotti

Abstract

Croce e delizia di chi si occupa di cybersecurity, la gestione delle password è un elemento cruciale per proteggere dati sensibili e informazioni personali. Si tratta di un argomento tecnico che è entrato a far parte della nostra quotidianità, assumendo spesso un ruolo cruciale per l'accesso ai servizi essenziali che ci riguardano. Ancora, il "cambio" della password, per quanto possa apparire un momento routinario, è in realtà argomento dibattuto che merita ancor oggi qualche commento dal punto di vista professionale, considerando che proprio i professionisti della sicurezza sono chiamati a decidere quali meccanismi mettere in atto, districandosi tra varie fonti autorevoli talvolta in disaccordo tra loro.

Indice

Croce e delizia di chi si occupa di cybersecurity è la gestione delle password come elemento cruciale per proteggere dati sensibili e informazioni personali.

Nemmeno troppo recentemente, e cioè nel 2017, l'ente di standardizzazione americano, il NIST, ente di sicuro riferimento per il mondo occidentale e uno dei più influenti al mondo, emetteva un suo "diktat" con il quale rivoluzionava l'opinione ormai diffusa e apparentemente ineluttabile per cui è necessario cambiare periodicamente ogni password. Infatti, con la sua Special Publication **NIST SP 800-63B asserisce che non vi sia più la necessità di cambiare periodicamente la password.** Il cambio della password è ritenuto invece necessario quando si ha notizia di una sua compromissione. Questa presa di posizione, nonostante sia stata recepita anche dalla ISO/IEC 27002:2022, rappresenta un argomento dibattuto che ancora oggi merita di essere commentato. Infatti non tutti i *think tank* concordano, tanto che il considerando 49 della recente NIS 2, che dovrà essere recepita entro il 18.10.2024, riporta il cambio delle password come misura di "***cyber hygiene***", e anche la PCI DSS V 4.0 del 2022 ne prevede il cambio ogni 90 giorni.

Cosa dice il NIST

Il NIST, al paragrafo 9 della Sezione 5.1.1.2 della SP 800-63B, si limita a dire "*I software di verifica dell'identità non dovrebbero richiedere che i segreti memorizzati [N.d.R. ossia le password, altri codici o frasi segreti] siano cambiati arbitrariamente (ad esempio, periodicamente). Tuttavia, questi software devono imporre un cambio se ci sono prove di compromissione dell'autenticatore*".

L'Ente, quindi, suggerisce ("*dovrebbero*") di non cambiare le password periodicamente, mentre invece obbliga ("*devono*") a modificarle quando c'è un **sospetto di compromissione.**

Per capire questa presa di posizione si rinvia alla spiegazione contenuta nelle FAQ "Linee guida sull'identità digitale" alla risposta "A-B05":*"Gli utenti tendono a scegliere segreti memorizzati più deboli quando sanno che dovranno cambiarli nel prossimo futuro. Quando avviene tale cambio, spesso selezionano un segreto simile al loro vecchio segreto memorizzato applicando una serie di trasformazioni comuni, come aumentare un numero nella password. Questa pratica fornisce una falsa sensazione di sicurezza se uno dei segreti precedenti è stato compromesso, poiché gli attaccanti possono applicare queste stesse trasformazioni comuni. Tuttavia, se ci sono prove che il segreto memorizzato è stato compromesso, ad esempio attraverso una violazione del database di password hash del software di gestione delle identità o attraverso un'attività fraudolenta osservata, agli utenti dovrebbe essere richiesto di cambiare i loro segreti memorizzati. Tuttavia, questo cambio basato sugli eventi dovrebbe verificarsi raramente, in modo che siano meno motivati a scegliere un segreto debole sapendo che sarà utilizzato solo per un periodo limitato di tempo."*

Il NIST riporta che alcune ricerche avvalorano questa presa di posizione, ma non le cita. Roger Grimes, in un suo articolo su LinkedIn, dichiara: *"Non fanno semplicemente raccomandazioni a caso basate su sensazioni istintive. Ma, per essere onesti, non ho mai visto i dati alla base di questa decisione, e non li hanno mai resi pubblici per quanto ne so. Ho cercato di ottenerli diverse volte, inviando email a vari membri del team che conosco nel comitato sulla politica delle password del NIST. Non ho mai ricevuto una risposta cortese, figuriamoci una spiegazione riassuntiva o i dati effettivi."*

La modifica periodica delle password: riflessioni alla luce delle raccomandazioni del NIST

Esaminiamo i pro e i contro alla luce di tali indicazioni.

I PRO alla modifica periodica delle password	I CONTRO alla modifica periodica delle password
1. **Riduzione del rischio di accessi non autorizzati**: cambiare regolarmente le password può contribuire a ridurre il rischio di accessi non autorizzati a causa di attacchi a forza bruta online ma, soprattutto, offline a seguito di un dump del file delle password. Anche se una password dovesse essere compromessa, la finestra di opportunità per un attaccante sarebbe limitata, poiché la password verrebbe presto modificata.	1. **Complessità e difficoltà per gli utenti**: chiedere agli utenti di cambiare frequentemente le password può portare a complicazioni. Gli utenti potrebbero optare per password più deboli o scrivere le nuove password in luoghi facilmente accessibili, riducendo così la sicurezza complessiva.
2. **Sensibilizzazione sulla sicurezza**: la pratica di cambiare le password può contribuire a mantenere elevati livelli di consapevolezza della sicurezza tra gli utenti, sottolineando l'importanza di mantenere password robuste e proteggere l'accesso ai propri account, fondamentale in un contesto digitale sempre più complesso.	2. **Interruzione delle attività**: la modifica periodica delle password può causare interruzioni nella produttività, specialmente in ambienti aziendali quando l'utente non è in grado di portare a termine la procedura di cambio. Questo si traduce in un aggravio per gli amministratori di sistema costretti a ripristinare le password manualmente.

I PRO alla modifica periodica delle password	I CONTRO alla modifica periodica delle password
3. **Conformità alle politiche di sicurezza**: in molti settori, la modifica periodica delle password è richiesta dalle politiche di sicurezza e dalle normative di conformità. Mantenere questa pratica può contribuire a rispettare normative e requisiti di conformità.	3. **Rischio di password prevedibili**: in risposta alla frequente necessità di cambiare le password, gli utenti potrebbero scegliere sequenze facili da ricordare o fare piccole modifiche alle password esistenti. Ciò aumenta il rischio che le password diventino prevedibili e, di conseguenza, più vulnerabili agli attacchi.
4. **Evitare lo scavenging**: qualora una password fosse individuata o decifrata e l'attaccante avesse accesso ai file protetti con la vecchia password, dopo che è stata modificata potrà acquisire unicamente ciò che era stato protetto con la vecchia password (backup, documenti cifrati con quella password, ecc.) per il limitato periodo in cui era valida.	4. **Maggiore attenzione alla robustezza delle password**: il non dover più cambiare la password frequentemente permette di scegliere password più lunghe e complesse.
5. **Resilienza**: nel caso in cui il sistema usato (come dimostrano i molti siti da cui sono reperite, estrapolate e pubblicate le password degli utenti) non applichi tutte le regole di controllo della robustezza delle password, il loro cambio riduce gli impatti degli attacchi.	

Cosa dice la teoria

Da tempo veniva insegnato che, analogamente alle chiavi di cifratura, le password, per essere buone, dovevano possedere alcune caratteristiche, come riporta anche la NIST.SP.800-63B "*Appendix A — Strength of Memorized Secrets*", ovvero:

1. essere **lunghe,** perché più sono lunghe più tempo occorre al tool di cracking per decifrarle (anche se la lunghezza non è aumentata nel tempo con la legge di Moore per le varie tecniche che si sono fatte strada, tra cui il *salting* che rende più difficile l'attacco da parte di attaccanti che utilizzano tabelle di hash precalcolate (*rainbow tables*) o attacchi di forza bruta);
2. di elevata **complessità** per poterne aumentare l'entropia come accade con le chiavi crittografiche $H = log_2 N^L = L\, log_2 N = L \frac{\log N}{\log 2}$ dove **N** = numero caratteri alfabeto e **L** = Lunghezza password, che fa passare l'entropia da 4,7 bit per le 26 lettere dell'alfabeto a 6,6 per l'ASCII di 94 caratteri per il numero di lettere della password);
3. scelta opportuna dei cosiddetti parametri segreti (**Randomly-Chosen Secrets**) per evitare che algoritmi banali ne minino la robustezza.

La NIST. SP. 800-63B fa anche altre affermazioni che sembrano in contraddizione soprattutto con il punto 2 di cui sopra, visto che richiedono di ridurre la complessità, ad esempio:

- *"Non dovrebbero essere imposti ulteriori requisiti di complessità per i segreti memorizzati."* (5.1.1.1 – Memorized Secret Verifiers)*;*
- oppure ***"****Il software di verifica dell'identità non dovrebbe imporre altre regole di composizione (ad esempio, richiedere combinazioni di diversi tipi di caratteri o vietare caratteri ripetuti consecutivamente) per i segreti memorizzati****."*** (5.1.1.2 – Memorized Secret Verifiers)*.*

Mentre, in un altro passaggio delle medesime FAQ, il NIST promuove nuovamente criteri di complessità:

"Una maggiore sicurezza è principalmente ottenuta attraverso la capacità della maggior parte delle applicazioni di gestione delle password di generare password uniche, lunghe, complesse e che possano essere cambiate facilmente".

Si denota una **certa confusione** e occorre pertanto **leggere questi documenti con attenzione critica**.

Le ricerche

> Un articolo che potrebbe aver ispirato l'orientamento del NIST è del celeberrimo Prof. Eugene Howard *"Spaf"* Spafford, che nel 2006 affermava: "*Ora, guardando indietro su tutto ciò, il cambio periodico delle password riduce davvero solo le minacce poste dal tirare a indovinare e dai tentativi di decifrazione deboli. […]. Il tirare a indovinare può essere contrastato imponendo una buona selezione delle password, ma questo aumenta poi la probabilità di perdita a causa dell'oblio da parte degli utenti. L'unica minaccia rimasta è che i cambi periodici possono annullare i tentativi di decifrazione, in media.*"

Come riportato nell'articolo di Dan Goddin, "*Frequent password changes are the enemy of security, FTC technologist says*" nel 2010 è stato pubblicato uno studio dell'Università North Carolina a Chapel Hill dove è riportato che i ricercatori ottennero gli hash crittografici di 10.000 account scaduti di dipendenti, docenti e studenti dell'università, tutti tenuti a cambiare le loro password ogni tre mesi. Avendo ricevuto gli hash delle ultime password utilizzate da ognuno, ebbero modo di verificare come le password fossero state mediamente cambiate nel tempo e verificarono empiricamente come gli utenti, nel cambio trimestrale delle password, adottassero metodi facilmente indovinabili.

Più recentemente sono stati pubblicati due interessanti lavori:

- "*Measuring Real-World Accuracies and Biases in Modeling Password Guessability*" a cura dell'Università Carnegie Mellon e l'Università di Maryland, che approfondisce il tema degli algoritmi per l'individuazione delle password;
- "*Quantifying the Security Advantage of Password Expiration Policies*" a cura della Scuola di Computer Science dell'Università di Carleton, Ottawa, Canada.

Il secondo lavoro conclude: "*Tuttavia, [il cambio della password] fornisce un aiuto limitato contro numerosi altri attacchi, tra cui quelli che, al primo accesso, procurano immediatamente i file di destinazione, stabiliscono una backdoor, o installano keylogger o altri malware persistenti per rendere inefficaci i successivi cambiamenti di password*". Qui, di nuovo, non dice che il cambio della password non serve ma che fornisce solo un aiuto limitato.

Il ruolo dei professionisti di sicurezza

I professionisti di sicurezza sono chiamati a decidere quali meccanismi mettere in atto, districandosi tra varie fonti autorevoli talvolta in disaccordo tra loro.

> **Le scelte non riguardano solo la tecnologia, ma anche l'organizzazione e il rispetto della normativa vigente**. Per questo sono coinvolti i tecnici dei sistemi informatici, gli specialisti privacy, i referenti legali e i responsabili dell'organizzazione. Ciascuno di essi deve capire le questioni tecniche, quanto è richiesto dalla normativa (e dalle decisioni prese in fase di giudizio, se disponibili), gli impatti

> sull’organizzazione.

Per questo tutti sono chiamati a confrontarsi sia all’interno dell’organizzazione, sia nell’ambito di gruppi di professionisti di una specifica disciplina e multidisciplinari. Sono molte le associazioni italiane e internazionali attive e molte di esse si confrontano attivamente allo scopo di esaminare a fondo ogni questione, da punti di vista differenti, alla ricerca di soluzioni il più possibile condivise.

Questo stesso articolo è stato scritto a 4 mani: Stefano Ramacciotti, autore principale, con competenze più tecniche, e Cesare Gallotti, con competenze più di carattere organizzativo. Gli autori si sono trovati a discutere delle diverse soluzioni, partendo da posizioni diametralmente opposte, per poi trovare un punto di incontro condiviso, raccomandando di cambiare le password dei servizi più critici almeno due volte all’anno e degli altri almeno una volta all’anno.

Da questo si conclude che anche la capacità di confronto è una delle caratteristiche necessarie per i professionisti della sicurezza. Una capacità che parte dalla consapevolezza di non essere padroni della verità e dell’unica interpretazione possibile, ma che altri, pur con competenze specialistiche diverse (per esempio, chi si occupa di gestione organizzativa, i tecnici e i legali), è doveroso che intervengano, ognuno per la parte di competenza, e partecipino sinergicamente per la soluzione delle questioni che necessariamente riguardano tematiche diverse.

Conclusioni

In conclusione, la **modifica periodica delle password presenta pro e contro, e la sua efficacia dipende da vari fattori, inclusi il contesto operativo e la sensibilità delle informazioni gestite**.

Ovviamente, trovare un equilibrio tra sicurezza e praticità diventa essenziale per garantire un adeguato livello di protezione senza compromettere la *user experience*, soprattutto se è usato un buon password manager, con incluso un generatore di password, con cui è banale cambiare le password anche spessissimo (vedere anche https://doi.org/10.1016/j.jksuci.2019.06.006).

Non potendo essere certi né dell’ipotesi di cambiare le password né di quella di modificarle periodicamente, in mancanza di ulteriori ricerche sull’argomento, è opinione di chi scrive che non occorra modificare le password con elevata frequenza ma che è comunque meglio cambiarle periodicamente. Pertanto, il **suggerimento è di cambiarle almeno una volta all’anno.** Password per controllare gli accessi a informazioni più sensibili potrebbero essere invece modificate con una maggiore frequenza, almeno una volta ogni sei mesi.

Il 2 maggio prossimo, come ogni primo giovedì di ogni anno è il World Password Day. Perché non approfittiamo dell’occasione per modificare le nostre password?