PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4305 di Lunedì 10 settembre 2018

Alcune leggende metropolitane sulla sicurezza delle parole chiave

L'utilizzo di una parola chiave rappresenta ancora oggi uno dei più diffusi sistemi di autenticazione per l'accesso ad un sistema informatico: vediamo alcuni errati convincimenti, diffusi anche tra i responsabili della sicurezza informatica.

Anche se l'utilizzo di una complessa parola chiave è una buona idea, questo approccio è efficace solamente contro un attacco con la tecnica del dizionario o di forza bruta, vale a dire tecniche che oggi vengono utilizzate solo in casi delimitati.

È infatti ormai dimostrato che una parola chiave complessa offre protezione zero nel caso il data base di un sistema informatico, che archivia le parole chiave degli utenti, venga compromesso. La parola chiave diventa immediatamente di pubblico dominio ed i criminali la aggiungono alla lista di parole chiave, già in loro possesso, per cercare di assumere l'identità del soggetto, la cui parola chiave è stata violata.

Questa parola chiave può essere utilizzata su migliaia di siti Web e milioni di tentativi possono essere fatti nel giro di alcuni minuti. Poiché molti utenti utilizzano la stessa parola chiave per accedere a numerosi siti, la probabilità che l'attacco vada a buon fine è molto elevata.

Secondo le ultime statistiche, ad oggi sono circa 5 miliardi i profili di accesso che sono stati violati e le relative parole chiave sono diventate di pubblico dominio.

La realtà è che l'utilizzo delle sole parole chiave non è sufficiente per proteggere un profilo di accesso, e anche l'utilizzo di parole chiave complesse poche garanzie offre circa il livello di protezione dagli attacchi.

Il problema è particolarmente sentito nell'accesso ai siti Web, che raramente offrono una autentica a due livelli, ad esempio abbinando l'utilizzo della parola chiave ad un codice che viene inviato per SMS.

Ciò premesso, una valida parola chiave deve essere generata utilizzando delle regole semplici, perché sia facile da ricordare. Un consiglio assai valido riguarda la memorizzazione dei versi di una poesia. La parola chiave è costituita dalle prime lettere delle prime parole della poesia. Tornerò su questo argomento in chiusura dell'articolo.

Anche l'utilizzo di due parole chiave, il cui abbinamento abbia un senso solo per l'utente che le ha scelte, può costituire un valido approccio. Se poi una di queste parole viene convertita in numeri equivalenti, tanto di guadagnato.

Un altro aspetto da tenere sotto controllo, in fase di cambio della parola chiave, è legato alla modifica sostanziale della parola chiave e non solo alla modifica dell'ultimo numero, ad esempio, abbinato alla parola chiave stessa.

Mi rendo conto che può essere un problema l'abbinare la semplicità di scelta, per facilitare la memorizzazione, con la relativa complessità, per rendere più difficoltoso un attacco sistematico.

Un altro aspetto che negli ultimi tempi si è messo in particolare evidenza riguarda il fatto che si sta cominciando a diffondere il convincimento che la frequente sostituzione della parola chiave non sia una buona politica di sicurezza. Mi rendo conto che per molti lettori questa affermazione sembra quasi blasfema, ma la realtà mostra che una frequente cambio della parola chiave induce l'utente a riutilizzare la stessa parola chiave con minime modifiche.

Niente meno che il General Communication Headquarter-GCHQ- vale a dire il centro nazionale di intelligence informatica del Regno Unito, ha abbandonato l'idea di cambiare le parole chiave ogni tre mesi, come fatto per decenni in precedenza.

È ben vero che oggi è possibile installare degli applicativi che fanno una valutazione della parola chiave, confrontandola con quelle precedentemente utilizzate ed accertandosi che non sia stato cambiato soltanto un numero od una lettera, ma non tutti i responsabili della sicurezza informatica utilizzano questo efficiente ed efficace approccio.

Anche l'utilizzo di generatori casuali di parole chiave, che sembra molto attraente, deve essere attivato con prudenza. Molti generatori sono in grado di produrre parole chiave, secondo preferenze indicate dall'utente, che aiutano indubbiamente nella memorizzazione della parola chiave, generata casualmente.

Ciò non toglie che ormai sia sempre più diffuso il convincimento che la parola chiave non sia più sufficiente ed occorra utilizzare tecniche più evolute, anche senza arrivare ad una delle tecniche più pratiche e raffinate, come appunto il riconoscimento biometrico.

Ecco perché si raccomanda di studiare attentamente la possibilità di attuare tecniche chiamate 2FA- autenticazione a due fattori, oppure MFA - autenticazione a più fattori.

Infine, vorrei chiudere questo appunto facendo presente che, anche se è vero che spesso la violazione di una parola chiave è dovuta ad un comportamento incauto dell'utente o ad una infelice scelta, è compito e responsabilità di ogni soggetto, coinvolto nella sicurezza del sistema informativo, sensibilizzare in vari modi tutti gli utenti coinvolti.

Oggi sono disponibili degli applicativi che permettono di effettuare una rapida valutazione del livello di sicurezza di una parola chiave e questi applicativi dovrebbero essere sempre a disposizione degli utenti.

È importante che, in fase di sensibilizzazione, si spieghi all'utente coinvolto quali possano essere le gravi conseguenze di una violazione di una parola chiave e di un accesso illecito a dati di interesse aziendale o addirittura a dati personali.

In questo senso, il nuovo regolamento generale 679/2016 rappresenta un prezioso elemento di sensibilizzazione degli utenti.

Altri accorgimenti che l'esperienza ha dimostrato essere utili fanno sì che la scadenza di una parola chiave, con conseguente obbligo di modifica, non venga mai presentata di venerdì all'utente coinvolto. L'esperienza ha mostrato infatti che una parola chiave, cambiata il venerdì, a un'elevata probabilità di essere dimenticata, quando si arriva nuovamente in ufficio il lunedì mattina. L'accumulo degli impegni e le distrazioni del sabato e domenica contribuiscono in modo determinante a far dimenticare la parola scelta. È questa un'esperienza vissuta da una banca svizzera, di dimensioni mondiali, che ha tassativamente proibito ai propri dipendenti di cambiare la parola chiave di venerdì, perché il lunedì spesso il responsabile della sicurezza era bersagliato da numerose richieste, provenienti da varie parti del mondo, che chiedevano attivare la procedura di reset della parola chiave!

In sintesi, il consiglio che mi sento di dare quello di rivedere attentamente le politiche esistenti in azienda, in tema di scelta iniziale e manutenzione delle parole chiave, per vedere se tali politiche corrispondono ad approcci ormai superati dall'esperienza e abbisognano di una cura di ringiovanimento.

Raccomando quindi di pensare a una frase, alle parole di una canzone, al titolo di un film, ad un detto memorabile, facilmente memorizzato. Si costruisce la parola chiave, prendendo la prima e l'ultima lettera di ogni parola e aggiungendo infine un paio di non lettere. Aggiungete il numero di parole presenti nella frase ed avrete costruito una parola chiave facile da ricordare, per voi, ma difficile da individuare con tecniche brutali di attacco!

Adalberto Biasiotti