PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5535 di Venerdì 12 gennaio 2024

Alcune considerazioni sulla sicurezza delle parole chiave

La sicurezza delle parole chiave è un tema fondamentale che deve essere affrontato in ogni progetto di sicurezza informatica. L'esperienza mostra che gli utenti non sono sufficientemente sensibilizzati sui criteri di scelta e conservazione delle password.

Credo che non esista alcun programma di sicurezza informatica, che non preveda un percorso di sensibilizzazione degli utenti sulla scelta e la conservazione di parole chiave. Ad esempio, scegliere parole chiave non banali, non usare la stessa parola chiave in siti diversi, non trascriverla su supporti di vario tipo e via dicendo.

Tuttavia, l'esperienza dimostra come la grande maggioranza degli incidenti e delle violazioni di dati è legata alla sottrazione o alla identificazione di parole chiave. Ecco perché riteniamo opportuno, ancora una volta, ricordare ai nostri lettori i principi fondamentali da rispettare, nella scelta di una parola chiave.

Come scegliere una parola chiave sicura

Prima di tutto, scegliere una parola chiave che sia piuttosto lunga. Una parola chiave di 12 o 15 caratteri, che contiene lettere, numeri e simboli, è indubbiamente più sicura di una parola chiave più corta. Un ulteriore elemento di sicurezza è legato all'utilizzo di lettere maiuscole e minuscole e simboli particolari, che però hanno il difetto che possono essere difficilmente memorizzati ed inducono l'utente a trascrivere da qualche parte la parola chiave.

Gli esperti ricordano ancora una volta che la scelta delle prime parole di una canzone, oppure una frase significativa per l'utente, ma priva di significato per un soggetto terzo, rappresenta uno strumento efficiente ed efficace di impostazione di una parola chiave. L'aggiunta di numeri e l'utilizzo di maiuscole accresce ulteriormente la sicurezza di questa parola.

Usate parole chiavi diverse per accessi a dati particolarmente critici.

Si tratta di un aspetto che occorre insistentemente sottolineare gli utenti, perché è evidente che la violazione di una sola parola chiave può portare a gravi conseguenze, se la stessa viene usata per l'accesso a molti siti.

Utilizzare password manager

Si tratta di applicativi oltremodo efficienti ed efficaci, che aiutano l'utente a ricordare svariate parole chiave, senza obbligarlo a trascriverle. L'esperienza dimostra come l'affidabilità di questi password manager è decisamente assai elevata e costituiscono un prezioso strumento di difesa informatica.

Alcuni di questi applicativi aiutano anche l'utente a scegliere parole chiave tanto facili da ricordare, quanto difficili da individuare.

Ovviamente, occorre sensibilizzare l'utente a scegliere una parola chiave, che permette di accedere all'applicativo di password manager, con caratteristiche di estrema sicurezza.

L'autenticazione a più fattori.

Un elemento che permette di fare un vero balzo in avanti, in termini di sicurezza, è legato all'utilizzo di uno strumento aggiuntivo, rispetto alla parola chiave, per accedere al servizio richiesto.

Esistono numerosi sistemi per creare questa autenticazione a più fattori, basati sul principio: "qualcosa che io posseggo" oppure "qualche cosa che io sono".

È oggi sempre più frequente l'uso di applicativi in cui, quando l'utente richiede di accedere al sistema informatico, deve digitare la propria parola chiave ed inoltre deve digitare un codice, che viene inviato su suo telefono cellulare, mediante SMS.

L'autentica biometrica

Ormai è sempre più diffusa questa forma di identificazione di un utente, che può avvalersi del riconoscimento di un'impronta digitale, oppure del volto, oppure addirittura del modo in cui l'utente appone la propria firma su una tavoletta intelligente. Questo tipo di autentica è soggetto ad alcune limitazioni, legate alla necessità di proteggere i dati personali dell'utente, ma oggi quasi tutte le principali autorità garanti della protezione dati personali, in Europa, stanno allentando in modo significativo i vincoli legati all'utilizzo di queste specifiche applicazioni.

Occhio alle truffe

Vi sono molti modi in cui un malintenzionato può venire a conoscenza delle vostre parole chiave. Tanto per cominciare, è possibile che una vostra parola chiave sia stata catturata, insieme a migliaia di altre, in qualche evento di violazione dei dati, del quale forse non sempre siete a conoscenza.

Inoltre, l'esperienza mostra come l'utilizzo dei social media, gestiti da esperti del settore, può portare a raccogliere una straordinaria quantità di parole chiave, che l'utente è indotto a rivelare, proprio per l'abilità di persuasione del malvivente.

Non dimentichiamo poi che spesso, soprattutto in ambiente familiare, è possibile che le parole chiave vengano condivise e ciò può portare a problemi non trascurabili, se i rapporti familiari, per qualche motivo, vengono ad essere alterati.

Un noto esperto informatico americano, con una frase provocatoria, ma efficace, affermava: "se cambiate la ragazza, cambiate anche la password!"

Al museo delle spie, a Berlino, è presente un dispositivo sul quale i visitatori possono digitare una parola chiave. Il dispositivo reagisce, visualizzando il tempo necessario per la violazione della parola chiave stessa!

Adalberto Biasiotti