PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4738 di Lunedì 13 luglio 2020

Un'importante aggiornamento sull'utilizzo dell'uso delle parole chiave

Ancora oggi, le parole chiave sono lo strumento più diffuso di controllo dell'accesso al sistema informativo. I dubbi, che già da tempo esistevano, in merito alla efficienza ed efficacia di questo sistema di controllo dell'accesso, continuano a crescere.

La parola chiave è stata per lungo tempo utilizzata come il sistema più diffuso di autentica dell'utente, ma già da lungo tempo sono apparsi dubbi sull'efficienza ed efficacia di questo sistema.

In realtà, il rapporto sulle violazioni dei dati avvenuti nel 2019, a cura di Verizon, ha confermato che l'80% delle violazioni erano legate a credenziali rubate o riutilizzate.

Ecco il motivo per cui è importante che una azienda si attivi tempestivamente per migliorare il livello di sicurezza di questa tecnica di autentica dell'utente.

Le parole chiave sono soggette a numerosi tipo di attacchi, tra i quali quelli chiamati in inglese *brute force* sono i più diffusi. Questi attacchi effettuano combinazioni automatiche di parole chiave composte da lettere e numeri ed altri contrassegni, per confezionare innumerevoli parole chiave. Una possibile difesa contro questo attacco è quello di bloccare l'accesso dopo tre tentativi di autentica abortiti.

Ancora più diffusa è la tecnica di attacco che inganna l'utente coinvolto, inducendolo a mettere a disposizione le proprie credenziali di accesso. Gli specialisti di queste tecniche di attacco, mediante ingegneria sociale, diventano sempre più bravi e riescono sempre meglio ad ingannare gli utenti.

D'altro canto, un utente medio può essere obbligato a ricordare una ventina di credenziali di accesso e non vi è da stupirsi per il fatto che l'utente le scriva in qualche ubicazione, che egli ritiene sicura, ma che sicura non è.

Un'altra debolezza degli utenti riguarda il fatto che la stessa parola chiave viene utilizzata per accedere a diversi applicativi e quindi la violazione di questa parola chiave fa crollare il sistema di difesa.

Aggiungete a questo fatto la considerazione che molti applicativi impongono la sostituzione della parola chiave ogni qualche mese, aggravando ancora di più il carico di responsabilità sull'utente.

I gestori dei sistemi informativi hanno cercato di aumentare il livello di protezione nella custodia delle parole chiave, custodendole in archivi protetti da applicativi crittografici, ma oggi questo tipo di protezione non sembra sufficientemente garantistico. Ormai tutti i responsabili della sicurezza informatica sono convinti che, in attesa di sistemi più efficaci, l'unico approccio che permetta di accrescere il livello di sicurezza delle parole chiave è quello di allungarne il numero dei caratteri.

Ormai quasi tutti i principali siti richiedono che una parola chiave sia lunga almeno 6-8 caratteri, mescolando numeri, lettere maiuscole e minuscole e caratteri vari. Questa situazione però rende più difficile per l'utente ricordare la parola chiave in questione. Ecco la ragione per la quale ormai da tempo gli esperti suggeriscono agli utenti di passare dalle parole chiave alle frasi chiave.

Con frase chiave si intende un testo, anche piuttosto lungo, che per l'utente è facile da ricordare, perché legato a qualche sua esperienza personale, ma che può essere estremamente difficile da individuare, soprattutto utilizzando tecniche automatiche di costruzione della parola chiave.

Naturalmente la frase chiave non va trascritta in chiaro, ma va alterata con semplici accorgimenti, che non compromettono la facilità di ricostruirla, da parte dell'utente. Ad esempio, la frase "il mio secondo figlio frequenta la classe 4A delle elementari", può trasformarsi in "2figlio4Ascuola".

L'adozione di queste misure comporta l'avvio di un processo di educazione degli utenti, che in genere ricevono molto bene questo tipo di formazione, perché aumenta il loro livello di sicurezza e non aumenta il loro stress, nel ricordare le parole chiave.

Ovviamente, chi sa guardare lontano fin da adesso dovrà cominciare a pensare a tecniche più avanzate, come ad esempio le tecniche biometriche, o quelle a doppia tecnologia o a due fattori.

Nel frattempo, la soluzione proposta è efficiente, efficace e di immediata attuazione.

Adalberto Biasiotti