PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4109 di giovedì 26 ottobre 2017

Guida sull'identità digitale e sulla scelta delle parole chiave

Un manuale che aiuta sia il responsabile della sicurezza informatica, sia gli operatori sul campo nella scelta del più diffuso strumento di autentica informatica, vale a dire la parola chiave.

Il continuo furto di parole chiave e di codici di autentica informatica rappresenta uno tra i maggiori problemi che devono fronteggiare non solo i responsabili della sicurezza informatica, ma anche gli operatori, i cui dati identificativi vengono sottratti. La gestione delle parole chiave, che sono una manifestazione di identità digitale, è molto complessa, perché aumentano sempre più le identità digitali che vengono utilizzate, ad esempio per i servizi di posta elettronica, per l'accesso ai dati bancari, per l'accesso a pezzi musicali disponibili on-line e via dicendo.

Il fatto che manchi un contatto fisico diretto fra chi dichiara di essere un determinato soggetto e chi deve accettare questa dichiarazione di identità crea dei problemi, che non sono facili da superare.

La disponibilità di queste linee guida permette di offrire delle procedure che mitigano le vulnerabilità presenti in tutti i servizi on-line, cercando di offrire procedure differenziate in funzione del rischio che viene attribuito ad una possibile frode, legata alla identità digitale.

Come regola generale, l'autentica digitale stabilisce che un soggetto, che cerca di accedere ad un servizio digitale, ha a disposizione uno o più elementi di autentica, associati con la sua identità digitale. Il fatto che la connessione possa avvenire su una rete aperta consente ai malviventi di perpetrare diversi tipi di attacco e attuare diverse modalità di sostituzione di persona, ad esempio con l'ormai famoso attacco *man in the middle.*

Questo documento è stato sviluppato dalla NIST ed è stato messo a disposizione soprattutto di enti federali americani, che possono far riferimento a queste linee guida per la valutazione di rischio e l'attuazione di misure di sicurezza per i propri servizi digitali.

Queste linee guida permettono di mettere sotto controllo gli impatti negativi connessi a un errore di autentica, separando gli elementi individuali di garanzia di identità in parti discrete e separate.

In realtà il documento che presentiamo ai lettori è composto da ben quattro diversi documenti, di cui quello che presentiamo è solo il primo. D'altro canto, ci si rende conto facilmente che l'impegno richiesto per leggere, meditare ed applicare anche solo il primo di questi documenti, che fa riferimento ai processi di garanzia di identità, rappresenta un impegno non indifferente e quindi è bene cominciare ad affrontare il tema un poco alla volta.

Un elemento che mi ha colpito, leggendo questo manuale, è la sua impostazione pratica, tipicamente anglosassone, che fa riferimento a fatti concreti e chiaramente individuati, rispetto a proclamazioni perfette, da un punto di vista assoluto, ma spesso poco realizzabili in pratica. Ecco un esempio.

Tra le varie opzioni che vengono messe a disposizione di chi deve verificare un'identità digitale, spesso vi è anche la proposizione di una domanda, la cui risposta dovrebbe essere nota soltanto a chi dichiara di avere quella specifica identità digitale.

Una proposta perfetta e complicata è quella di chiedere di digitare la intera data di nascita, mentre una proposta meno perfetta, ma assai più pratica e rapida, è quella di dichiarare se chi richiede l'accesso è più vecchio o più giovane, rispetto ad una certa età.

Il bello di questo documento sta nel suo approccio tanto semplice quanto allargato, tanto è vero che lo sviluppo e l'uso delle linee guida offerte può essere applicabile non solo all'interno del governo federale, ma anche a transazioni di commercio elettronico.

Gli altri tre documenti, che compongono la serie completa, fanno riferimento a procedure sempre più approfondite di verifica dell'identità digitale, come ad esempio i processi di autentica e la gestione delle procedure di autentica e di gestione del ciclo di vita.

Un altro aspetto che mi ha colpito e mi induce ancora una volta a raccomandare ai lettori la lettura di questo documento, è legata alla affermazione che molte dichiarazioni, che il responsabile della sicurezza informatica accetta a valore facciale, senza troppe discussioni, vengono invece contestate, proponendo soluzioni altrettanto efficaci e più semplici.

Una delle affermazioni che viene contestata riguarda il fatto che le parole chiave debbano essere sostituite con una certa frequenza e che maggiore è la frequenza, maggiore è la sicurezza della parola chiave.

L'esperienza ha dimostrato che questo fatto non corrisponde alla realtà e che sia molto meglio scegliere una parola chiave tanto facile da ricordare, quanto difficile da indovinare, senza cambiarla troppo spesso, perché la modifica comporta la nascita di nuovi problemi, che possono inficiare il livello iniziale di sicurezza della parola chiave.

In conclusione, una Bibbia sulle parole chiave, che dovrebbe essere presente nella biblioteca informatica di qualsiasi responsabile della sicurezza ITC!

Adalberto Biasiotti

scarica il documento (formato pdf. 2.1 MB)

www.puntosicuro.it