VADEMECUM DEL COMMERCIALISTA DIGITALE

Guida alla sicurezza informatica degli studi

Ver. 1.0 23 ottobre 2017

Sommario

Introduzione

E' innegabile ormai che ogni giorno, anche il meno tecnologico di noi, ha a che fare con un computer, uno smartphone o con qualche congegno elettronico che comunica con altri dispositivi all'interno di una rete. Questo vale sia nella quotidianità della nostra vita privata, sia, soprattutto, nel campo lavorativo.
La tecnologia e internet sono ormai alla portata di tutti, sia economicamente che dal punto di vista dell'utilizzo. Le grandi società che progettano software e dispositivi collaborano sempre di più con antropologi sociologi e altre figure professionali con conoscenze specialistiche al fine di rendere più a misura umana strumenti dotati di un grande livello di complessità. Avere accesso alle mail, usare le app o il software gestionale che abbiamo nei nostri uffici è diventato davvero molto semplice, non serve di certo essere ingegneri informatici.
Tale semplicità, tuttavia, se da una parte ha davvero reso facile per tutti accedere alla tecnologia, dall'altra presenta delle **insidie** che, se non vengono **percepite** e **controllate**, possono causarci parecchi problemi: dal perdere qualche foto delle vacanze al mare fino ad arrivare a veri e propri furti di identità.
Nei paragrafi che seguiranno cerchiamo di spiegare quali sono quei piccoli accorgimenti che, se applicati, possono farci stare molto più tranquilli nell'utilizzo quotidiano dei nostri strumenti informatici. Probabilmente un sistema sicuro al 100% non esiste; ne sono la prova i vari attacchi informatici subiti dalle grandi società del web, nonostante abbiano investito milioni in sicurezza. Tuttavia tra l'essere completamente in balia degli eventi ed avere un buon piano di sicurezza che ci protegga nell'utilizzo normale dei nostri sistemi informatici

c'è una bella differenza, per non parlare dell'essere costretti a ingegnarsi per tentare di recuperare i **dati perduti**.

1 – La gestione delle password

La password è la prima cosa che ci viene chiesta (o almeno dovrebbe esserlo) quando accendiamo il nostro computer. Per molti potrebbe essere considerata una seccatura dover inserire ad ogni accesso la password, e spesso sentiamo commenti del tipo: "ma chi vuoi che guardi il mio pc", oppure: "non ho nulla da nascondere o da farmi rubare" o ancora: "se metto una password poi me la dimentico".
In realtà la corretta gestione delle password è di fondamentale importanza per disporre di un livello minimo di sicurezza. Se ci fermiamo un attimo a pensarci ci sono molte cose che un malintenzionato potrebbe fare a nostro danno venendo in possesso di una nostra password: leggere le nostre email, accedere ai nostri social, connett nostro gestionale ecc. Senza contare che l'utilizzo accurato di pa li intermediari E*ntratel*, in quanto tuisce uno dei punt personali e del codice priva che oggetto d Regionale delle Entrate.
La regola basilare quindi ord vanno s essere efficace, deve ess aratteristiche riconoscibile. Per conosce à è bene cercare er usano per indovinare nza scendere tro ssiamo riassumerli ai due seguen

1. l'attacco basato su
2. l'attacco basato s

La prima metodologia, c scia immaginare, consiste in un attacco basato sulla ricerca della pass di parole definito a priori. Solitamente viene utilizzato un file di testo e ci sono milioni di parole in ogni lingua, con tutte le loro possibili vari a che se utilizziamo come password una singola parola, in qualsiasi lingua facilmente individuata nel giro di pochi minuti.
La seconda metodologia è grado di individuare qualsiasi tipo di password, perché prova tutte le p zioni di un determinato insieme di caratteri disponibili. L'aspetto negat po di attacco è la grandissima quantità di tempo necessaria per portarlo a co r esempio, su una password di 8 caratteri, scelti tra le 26 lettere dell'alfabeto ing ci cifre e sedici simboli disponibili, sono oltre 52^8 possibili combinazioni; ciò sign che ammontano a 53.459.728.531.456 i tentativi per trovare la giusta combinazione. Anche con un hardware molto potente in grado di elaborare

circa 850.000 prove al secondo occorrerebbe un tempo totale di calcolo di quasi 2 anni. Se la lunghezza della password salisse da 8 a 9 caratteri il tempo necessario per decifrarla aumenterebbe a quasi 104 anni.

Alla luce di quanto detto sui metodi per individuare le password, vien da pensare che basterebbe utilizzare una password di almeno 9 caratteri, con maiuscole, numeri e caratteri speciali per essere tranquilli. In pratica non è così, poiché, oltre alla lunghezza, bisogna anche considerare la "**forza**" di una pa **intuibilità** della stessa. Esistono infatti i "*patterns*" che or le password implementano di default. I *patterns* r i usati dagli utenti per inventare o rende modelli tipici nella scelta della pas l'anno (*Pizza1* o *Pizza2017)* o *rzziP1).* Questi esempi, an quisito della "forza". In e parole di dizionari si provano le varie nizio/fine parola, password *Pizzaazz*

La stess no nostre informazi domestici. Queste no e ecc. Se ci pensiamo è i anche da un grandissimo assword tipo *NomeCognomean*

Molto spesso vedia *nf@asYV74_Xur*" che, per lunghezza e casuali cordare. In questi casi si ricorre a metodi più o meno a mento che ne compromettono la validità: ad esempio scriverla su un **post-it** attaccato al monitor o vicino alla tastiera, o in un file di testo in *.txt* o *.doc* sul desktop dal quale fare un *copia-incolla* nel momento del login.

Come si crea allora una password forte? Un metodo semplice per creare password sicure e nello stesso tempo facili da ricordare è quello di utilizzare le cosiddette "*passphrase*", frase che ci ricordiamo bene e dalla quale estrarre la password. Ad esempio: "mi sono sposato con Anna il 14 giugno!" La password potrebbe diventare *MsscAi14g!* utilizzando solamente le lettere iniziali di ogni parola, aggiungendo qualche maiuscola e la ! finale. Si crea, in questo modo, una password complessa, **facile da ricordare ma difficile per un software da indovinare**.

Un'altra criticità relativa alla password, che molto spesso non consideriamo, è quella di utilizzarne una sola, per quanto complessa, per tutti i nostri account, che siano quello della