IL TORMENTONE DELLE PASSWORD E DELLA LORO GESTIONE

QUANTO LUNGHE?
QUANTO COMPLESSE?
QUANTO REALMENTE SICURE?

Marco Bozzetti, OAI founder

Negli attuali sistemi informatici e per gli accessi ai siti web, le password sono un elemento preponderante per l'identificazione ed autenticazione di un utente. Un mondo sempre più digitale ci costringe a usare, e quindi a gestire, innumerevoli password: centinaia e centinaia di identificativi d'utente (u-id) e di password (pwd) che dobbiamo governare e gestire.
Tra i principali problemi che l'utente deve conoscere e saper gestire, per proteggere la sua identità digitale, spiccano la scelta delle u-id e pwd più sicure, e la gestione sicura ed efficace di tutti gli u-id e pwd in uso.
Gli u-id sono alcune volte imposti dai siti stessi, si pensi ad esempio all'home banking dove normalmente l'u-id è un codice cliente fornito dalla banca, oppure, come nel caso dei social network, sono lasciati all'utente che spesso usa il proprio indirizzo di posta elettronica, o semplici combinazioni del suo nome e cognome, e così via. E, come è 'fisiologico', lo stesso u-id viene ripetuto, se possibile, per i diversi siti web, almeno a parità di criticità: conoscendo l'identità della persona, individuare il suo u-id è così molto facile.
Per quanto riguarda le pwd, i criteri di scelta, a parte alcune imposizioni e regole, tipicamente in ambito bancario e finanziario, sono simili a quelli dell'u-id, e il più delle volte si basano su facili combinazioni di dati personali, del proprio lavoro, della propria famiglia e della cerchia di conoscenze e amicizie, di località conosciute (visitate di recente), di frasi famose o spiritose, e così via. Tutte informazioni che troppo spesso sono fornite direttamente dall'utente sui social network.

Attenzione ai criteri di scelta

La regola di base per la creazione di una pwd, così come di un u-id, è che deve essere facile da ricordare per il suo proprietario, ma difficile da scoprire. È evidente che la criticità di un u-id e relativa pwd è ben diversa per l'accesso all'home banking rispetto all'accesso ad un social network: ma si deve ben tener in conto che gli attaccanti tendono ad individuare u-id e pwd dai sistemi a bassa sicurezza, che non si considerano critici.
Conoscendo, o immaginando l'u-id, esistono innumerevole strumenti software, anche gratuitamente scaricabili da Internet, che tentano tutte le combinazioni di un insieme di caratteri fino a trovare la pwd corretta: è il così detto attacco "bruto" (in inglese brut force o deep-crack).
I tipici attacchi per scoprire le pwd includono (ma non si limitano), oltre al già citato "brute-force", il "phishing" con la posta elettronica, il "keylogging" con la trasmissione in remoto dei caratteri digitati dalla tastiera, l'accesso fraudolento ai file/banche

dati dei server contenenti gli account, l'accesso fraudolento agli applicativi per la gestione in locale, tipicamente sul PC dell'attaccato, degli account e delle pwd in uso, la scoperta degli account e delle pwd con tecniche anche semplici di social engineering tipo "shoulder sniffing", ossia osservare alle spalle della persona quali codici inserisce sulla tastiera. Altri software, anche gratuiti, tipo Cain&Abel, consentono poi di intercettare, "sniffare", sulla rete, senza che l'utente se ne accorga, tutti i dati inoltrati in rete dal PC attaccato, individuato dal suo indirizzo IP o MAC.

Pagine e pagine di policy aziendali e un'infinità di articoli sulla sicurezza informatica evidenziano come l'efficacia della pwd risieda nella sua lunghezza e complessità. I tipici suggerimenti o norme per la creazione di pwd includono la minima lunghezza di otto caratteri con uso di lettere, numeri, caratteri speciali, minuscole e maiuscole, l'uso di pwd diverse per accedere a diversi servizi, la modifica della pwd almeno ogni tre mesi senza recuperare quelle precedentemente usate. Si dovrebbe poi evitare l'uso di informazioni personali e dei propri famigliari.
Ma quanto devono essere 'forti' per essere ragionevolmente sicure?
L'autenticazione 'forte' richiede tecniche crittografiche ed il certificato digitale: ma le pwd?
Le indicazioni sopra esposte per creare una pwd sono sicuramente valide e rendono più difficile la loro scoperta con un 'attacco brutale'.
Ma una pwd complessa, ad esempio di 25 o più caratteri diversi, serve d'avvero ? Sicuramente serve, ma serve assai di più che sia difficile da immaginare, e quindi scoprire: e non è la stessa cosa.
La lunghezza di una pwd in effetti non ha più l'importanza che aveva una volta con le attuali tecniche in uso, come ad esempio il controllo del numero di tentativi in un dato arco temporale.
Più che creare e gestire pwd complesse dobbiamo imparare ad inventare pwd difficili da scoprire. Occorre bilanciare complessità con gestibilità: non è importante ottimizzare una pwd, ma crearne una che, nel suo contesto, sia sufficientemente e ragionevolmente sicura.
Personalmente ritengo che una buona pwd dovrebbe essere di almeno 10 caratteri, e piuttosto che incrementare la lunghezza della pwd sia meglio usare u-id non banali e non facilmente riconducibili a dati personali, ovviamente se si ha la libertà di poterli definire liberamente.

Anche gli archivi vanno protetti

Al di là della lunghezza e della complessità di una pwd e di un u-id, è essenziale poi proteggere adeguatamente dove vengono archiviati gli account, che contengono sia u-id che pwd che possono essere anche centinaia: praticamente impossibile rammentarle tutte, quindi occorre registrarle da qualche parte. Al di là del quadernetto sul quale trascriverle (ma dove poi nasconderlo?), esistono programmi anche open-source che consentono la gestione dei vari account personali, criptandoli sull'hard-disk del PC e/o su storage removibili, tipicamente le chiavette USB. Ma possono essere usati anche strumenti di informatica individuale, quali fogli elettronici e trattamento testi: basta che questi documenti siano criptati. In tutti questi casi occorre proteggere la pwd di accesso al programma o per la crittazione: è bene che sia "forte" e ...che venga tenuta a mente. Suggerisco , e non è un'esagerazione, di inserirla stampata assieme alle istruzioni su come usarla (quale PC, quale programma, ecc.) in un documento cartaceo da riporre in busta chiusa e da conservare in un luogo sicuro, ad esempio nella cassaforte in casa o in banca. È poi conveniente memorizzare l'elenco degli account su storage removibili, le tipiche chiavette USB: sempre criptando il tutto.
Ma per la protezione dei propri account, ed in particolare delle pwd, occorre stare molto attenti nel loro uso in Internet, ed in particolare sulle reti WiFi. Se ne trovano molte libere, non protette da pwd. Attenzione!! Potrebbe essere quella di un attaccante che l'ha sprotetta appositamente per far abboccare le sue vittime, allettate dalla connessione gratuita, soprattutto nelle località di vacanza.
È molto meglio cercare, se disponibili, hot spot pubblici che consentano sì la navigazione gratuita, ma fornendo una chiave di protezione WPA (WiFi Protected Access): così facendo, tutto il traffico viene criptato e risulterà incomprensibile.

Marco Bozzetti
marco.bozzetti@malaboadvisoring.it