PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 8 - numero 1549 di venerdì 15 settembre 2006

Tante password, poca sicurezza

Una indagine statunitense mette in luce ansie e comportamenti scorretti nella gestione delle password. Cosa fare e cosa non fare.

"Ansia da password" e comportamenti scorretti nella loro gestione costituiscono un rischio per la sicurezza informatica delle aziende e possono comportare la violazione delle leggi in materia di protezione e sicurezza dei dati.
Lo afferma la seconda indagine annuale realizzata da RSA Security su un campione di 1300 rappresentanti aziendali - provenienti da Nord America, Europa, America Latina e Asia-Pacifico - coinvolti nella problematica della gestione delle password per la loro azienda.

Si consideri ad esempio che un intervistato su 4 ha ammesso di essere a conoscenza di violazioni della sicurezza collegabili alla compromissione di password. Tra gli esempi di violazioni citati vi sono ex dipendenti che hanno acceduto al loro vecchio account aziendale usando le loro password, oppure casi di lavoratori temporanei che hanno indovinato la password dei loro ex referenti (introducendosi da remoto nel sistema aziendale), ma anche dipendenti che hanno acceduto agli archivi delle Risorse Umane per alterare le informazioni su colleghi.

"Le aziende investono sempre più tempo e denaro per proteggere le informazioni sensibili, ma le password continuano a rimanere l'anello debole della catena della sicurezza e ciò è dovuto soprattutto al gran numero di esse che viene normalmente utilizzato da un singolo utente", ha commentato John Worrall della RSA Security.

Nelle interviste sono state inserite domande sulla compliance (conformità alle normative di legge e di settore in materia di sicurezza di dati e informazioni) e sulla sicurezza IT in generale.
La maggior parte (59%) delle aziende intervistate ritiene che una corretta gestione delle password sia "estremamente importante" ai fini della compliance. Più convinti dell'importanza gli americani (66% del campione USA), lievemente meno gli europei (48%).
Riguardo alla sicurezza informatica, l'indagine di RSA Security ha rilevato che le aziende sono preoccupate dell'impatto negativo che una cattiva gestione delle password può avere sulla sicurezza IT: il 41% si dice "fortemente preoccupato", il 44% "moderatamente preoccupato".

Le password servono, inoltre devono essere cambiate frequentemente. Ma il 57% degli intervistati ha dichiarato che la propria azienda non richiede frequenti cambi di password o non attua stringenti politiche in merito per non creare difficoltà ai propri dipendenti.

Tuttavia gli utenti sovraccaricati di diverse password necessarie per accedere alle applicazioni di lavoro, ai siti web e ai portali, possono adottare comportamenti a rischio.
Ad esempio il 66% degli intervistati coinvolti nei temi di gestione delle password in azienda sa di dipendenti che annotano le password su carta, eppure solo il 13% degli utenti finali ammette di farlo; il 58% sa di dipendenti che conservano le password in file, anche qui il 24% ammette di farlo.
Il 50% sa di colleghi che archiviano le password in palmari o dispositivi mobili. Il 40% ha visto più volte in azienda post-it con password annotate appiccicati allo schermo dei computer.

RSA Security ha fornito allora alcuni **consigli** per gestire in sicurezza le password:
-Creare password di minimo 8 caratteri

-Includere diversi tipi di caratteri: maiuscole e minuscole, numeri, simboli, ecc. Più ce n'è, più si rende difficile la vita a chi tenta di indovinare la password
-Usare password diverse per le diverse applicazioni
-Cambiare le password almeno ogni 3 mesi
-Non usare informazioni personali quali nome, data di nascita, anniversari, nome dei figli o del cane. Sono le prime cose a cui pensano i cacciatori di password.
-Evitare di usare parole d'uso comune, anche non italiane. Anche se scritte all'incontrario possono essere rischiose.
-Non riutilizzare la stessa password prima che siano trascorsi 9 mesi dall'ultima volta che è stata usata.
-Evitare di usare lo steso carattere per più di 3 volte o 3 volte di seguito
-Non confidare a nessuno le proprie password.

Seguendo questi consigli si creano password sicure...ma come **ricordarle** senza ricorrere a file e post-it? Per generare le password, RSA consiglia ad esempio di utilizzare se possibile una frase anziché una parola, magari usando solo l'iniziale di ogni parola che la compone. Es. "ho accompagnato Marco a scuola alle 9" può essere reso con "hAm@S@9".

---

www.puntosicuro.it