Linee guida sull'uso delle password

L'uso di passworde il metodo più semplice e diffuso per accedere agli account sia su stazioni di lavoro sia in Internet: appare evidente che la scelta della password è estremamente importante per la sicurezza dei propri dati e dell'intera rete del Ministero della Giustizia. Vengono quindi elencate in questa sezione una serie di norme che dovrebbero essere rispettate e che l'Amministratore di sistema dovrebbe imporre per scegliere una password quanto più sicura possibile e garantire che questa non venga violata facilmente, a norma dell'articolo 25 del DM 24/5/2001.

Imporre il cambiamento delle password con frequenza:

mensile, per gli account a rischio, di sistema o con elevati privilegi (inclusi amministratori, manutentori, ecc.)

bimestrale per gli account utenti

annuale per le password di accensione delle postazioni di lavoro.

Le policy di autenticazione dovranno rispettare le seguenti modalità:

dovrà essere tenuto uno storico di almeno 5 password;

nel caso di digitazione errata della password, l'account verrà bloccato dopo 5 accessi errati e potrà essere sbloccato solo ed esclusivamente dall'amministratore di rete;

le password degli account appena creati o le password resettate a causa di blocco dell'account o a causa di perdita della password dovranno essere cambiate al primo logon da parte dell'utente;

Al proposito si noti che l'articolo 25 comma 3 del DM 24/5/2001 richiede che tutte le password siano rinnovate almeno una volta all'anno.

Imporre che tutte le password rispettino i seguenti requisiti:

devono essere composte da almeno dieci caratteri

devono contenere almeno tre tipi diversi di caratteri inclusi tra quelli maiuscoli, minuscoli, cifre e simboli di interpunzione

non devono essere parole presenti in dizionari delle lingue più diffuse

non devono essere basate su parole dialettali o gergali

non devono essere basate su informazioni personali come data di nascita, numeri di telefono, indirizzi

non devono essere basate su informazioni personali di familiari, amici, colleghi, attori, personaggi famosi, ecc.

termini tecnici o informatici, comandi, siti, società, ecc.

non devono essere del tipo aaabbb, 123456, fedcba, o simili

non devono essere password dei tipi elencati in precedenza scritte al contrario

non devono essere basate su password analoghe alle precedenti con l'aggiunta di cifre iniziali o finali.

Alcuni di questi vincoli possono essere imposti in modo automatico tramite opportuni programmi, mentre altri vincoli possono essere rispettati solo dietro espressa volontà dell'utente che deve quindi essere adeguatamente informato sui propri obblighi. Ne consegue

che il Servizio di Assistenza tecnica unificata, in accordo con l'Amministratore di sistema e con l'autorizzazione scritta del Capo dell'Ufficio, per le aree di propria competenza, deve:

sottoporre le password a controlli che verifichino debolezze come ripetizioni, sequenze note, parole comuni sia al momento della definizione di un account e in caso di cambiamento sia periodicamente

eseguire periodicamente programmi (crack, sniffer etc) per evidenziare le debolezze delle password imponendo agli utenti di cambiarle nel caso vengano individuate. È consigliabile sfruttare i tempi in cui le apparecchiature sono inattive o sottoposte a basso carico di lavoro per lanciare appositi programmi di controllo

bloccare gli account, di rete e dei software che lo permettano, in caso di tre immissioni errate consecutive della password. In questo caso, poiché un malintenzionato potrebbe sbagliare deliberatamente la password di un utente per bloccargli l'account, è indispensabile che esista una procedura (ad esempio un help desk) che permetta all'utente legittimo di riabilitare l'account. In generale, per impedire questo tipo di attacchi e simultaneamente impedire tentativi miranti ad indovinare la password, è meglio imporre un ritardo (fisso o – meglio – crescente) tra due successivi tentativi di immissione della password quando si riscontrano tentativi errati

sensibilizzare gli utenti e – se possibile – verificare che vi sia utilizzo di password diverse per servizi e account a livelli di sicurezza diversa (es. posta elettronica gratuita su Internet ed accesso ai DB interni)

non memorizzare nei log le password utilizzate nei tentativi falliti di accesso agli account perché, dato che la maggior parte degli errori di immissione delle password sono fatte dagli utenti stessi e differiscono dalla password corretta di pochi caratteri, riuscire a leggere i log permetterebbe di accedere a molti account. Deve però essere memorizzato nei log il fatto che vi è un tentativo errato di immissione di password ed eventualmente il numero di tentativi sbagliati

impostare i sistemi in modo tale da segnalare all'utente al momento dell'immissione avvertimenti che richiamino l'attenzione sull'importanza di non far leggere la propria password

impostare i sistemi in modo tale da visualizzare al momento del login l'ora ed il giorno dell'ultimo accesso e chiusura, facendo in modo che tali informazioni vengano lette e verificate dagli utenti, segnalando ad un apposito servizio di sicurezza eventuali incongruenze (ad esempio, ultimo login alle 3:15 AM)

disabilitare gli account che non vengono utilizzati da più di tre mesi

impostare, dove possibile, sistemi di autenticazione che non richiedano il transito delle password in chiaro sulla rete (art. 19 comma 4 DM 24/5/2001)

L'Amministratore di sistema ed il Responsabile della sicurezza dell'Ufficio devono inoltre sensibilizzare gli utenti affinché:

non rivelino le password a nessuno, inclusi amici e familiari

non condividano le password con altri colleghi o assistenti

non inviino le password tramite e-mail o altri metodi di comunicazione elettronica, né tramite telefono

non scrivano le password su carta e non memorizzino le password su file o altri sistemi (palmari o agende elettroniche) senza cifratura

non scrivano la propria password su questionari o presunti moduli di sicurezza

non parlino della propria password o rivelino indizi su essa

non utilizzino sistemi informatici che permettono di memorizzare le password o gestire un database di password

segnalino tutti i sospetti di compromissione o le richieste di informazioni sulle password (es. ultimo login non corrispondente ad orario di ufficio)

non riutilizzino in nessun caso le password.