6 REGOLE FONDAMENTALI PER UNA CORRETTA GESTIONE DELLE PASSWORD

o anche ***Come impostare un'organizzazione più sicura da parte dei reparti IT***

01.

DEFINIRE LE NORME DA SEGUIRE IN UNA FORMA FACILE DA CAPIRE

Documentare le norme di gestione delle password in modo che includano tutte le informazioni importanti, come la lunghezza della password, la complessità e il numero di tentativi di accesso non riusciti.

02.

IMPORRE IL RISPETTO DI TALI NORME A TUTTI I LIVELLI

Tutti i dipendenti devono essere tenuti a seguire la politica aziendale in materia di password. Compresi i proprietari, i dirigenti e i membri del consiglio di amministrazione, senza alcuna eccezione.

03.

BLACKLIST DELLE PASSWORD SBAGLIATE

Creare una "blacklist" delle password più comunemente usate e/o precedentemente compromesse e negare ogni tentativo di utilizzarle.

04.

MEMORIZZAZIONE DELLE PASSWORD UTENTE

Memorizzare le password degli utenti come salted hash e utilizzare un algoritmo di hashing appositamente progettato per la memorizzazione delle password.

05.

NON CAMBIARE LE PASSWORD TROPPO SPESSO

La scadenza periodica della password non è più una pratica di sicurezza consigliata. Il NIST e il National Cyber Security Centre (NCSC) del Regno Unito raccomandano ora di cambiare le password solo nel caso in cui l'abbonato lo richieda o vi siano prove di compromissione. Gli utenti costretti a cambiare troppo spesso la loro password ricorreranno a utilizzare sequenze più semplici e facili da ricordare, o all'adozione di una strategia banale come l'aggiunta di un numero o di una lettera alla fine della password e l'incremento di questa ad ogni cambio. Entrambi gli approcci si traducono in una protezione più debole del sistema aziendale.

06.

APPLICARE LE NORME A TUTTA LA RETE, COMPRESO L'INTERNET DELLE COSE (IOT)

La politica di sicurezza delle password dovrebbe comprendere anche tutte le password che proteggono i dispositivi e i sistemi dell'organizzazione, in particolare i dispositivi IoT, come le telecamere di sicurezza, gli smart hub e i router. Se queste vengono gestite in modo errato o vengono utilizzate con credenziali predefinite, c'è un rischio sempre maggiore che gli aggressori trovino e cerchino di sfruttare questa vulnerabilità.

8 MOSSE PER CREARE PASSWORD FORTI

o anche ***Come istruire i collaboratori della vostra organizzazione***

01.

UNA PASSWORD DEVE ESSERE UNIVOCA

Questo vale per ogni account per evitare di compromettere più risorse, se trapelate. La password non deve essere scritta su note adesive o in un file non criptato salvato su un qualsiasi dispositivo aziendale.

02.

PIÙ LUNGA È LA PASSWORD, MEGLIO È

Il National Institute for Standards and Technology (NIST) degli Stati Uniti raccomanda almeno 8 caratteri, che offrono un ragionevole livello di protezione contro gli attacchi di forza bruta.

03.

INCORAGGIARE L'USO DELLE PASSPHRASE

Una frase con 30 o più caratteri, anche se composta solo da alfabeti, è notevolmente più sicura di una parola di 8 caratteri con sostituzioni comuni (come '3' per la lettera 'e', "!" per "i" o "l", ecc.) Le frasi sono anche intrinsecamente più facili da ricordare, quindi la lunghezza aggiuntiva non è così difficoltosa per l'utente.

04.

ELIMINARE LE REGOLE DI COMPOSIZIONE COMPLESSE

Richiedere agli utenti di includere sia caratteri maiuscoli che minuscoli, almeno un numero e un carattere speciale, raramente incoraggia gli utenti a impostare password più forti, e porta piuttosto a password più deboli e più difficili da ricordare.

05.

NON CONDIVIDERE LE PASSWORD

Non mostrate mai le vostre password ad altri, inclusi colleghi, superiori, familiari o all'HelpDesk, poiché i phisher potrebbero fingere di essere del supporto informatico.

06.

EVITARE CARATTERI RIPETITIVI

"XXXX" non è una buona password. Allo stesso modo, qualsiasi carattere sequenziale (ad esempio 1234'), e modelli riconoscibili come 'qwerty' devono essere vietati.

07.

NON USARE PAROLE COMUNI DEL DIZIONARIO

Queste parole possono essere forzate in un attacco di brute force di dizionario. Questo include le lingue straniere, o termini specifici di diversi settori.

08.

NON UTILIZZARE MAI INFORMAZIONI PERSONALI

Questi possono essere indovinati dagli aggressori sulla base delle informazioni acquisite dai social media. Sono inclusi i secondi nomi, le date di nascita, gli indirizzi, le scuole, il nome del coniuge o del figlio.