6 ZÁKLADNÝCH PRAVIDIEL PRE DOBRÚ BEZPEČNOSTNÚ POLITIKU HESIEL

Ako majú IT oddelenia postupovať pre zvýšenie firemnej bezpečnosti?

01.

DEFINUJTE POLITIKU HESIEL V ZROZUMITEĽNEJ FORME

Zdokumentujte politiku hesiel tak, aby obsahovala všetky dôležité informácie – napríklad požadovanú dĺžku a zložitosť hesiel, ako aj prípustný počet neúspešných pokusov o prihlásenie.

02.

ZABEZPEČTE DODRŽIAVANIE POLITIKY NA VŠETKÝCH ÚROVNIACH

Bezpečnostnú politiku hesiel by mali dodržiavať všetci zamestnanci. Platí to bez výnimiek aj pre majiteľov, vrcholový manažment a členov správnej rady.

03.

SLABÉ HESLÁ DAJTE NA BLACKLIST

Vytvorte „blacklist" najbežnejších hesiel alebo už raz prelomených hesiel a zabezpečte, aby boli pokusy o použitie takýchto hesiel zamietnuté.

04.

CHRÁŇTE UKLADANÉ POUŽÍVATEĽSKÉ HESLÁ

Heslá používateľov ukladajte ako hash reťazce aj s pridávaním náhodných hodnôt („salt") a používajte hash algoritmus špecificky navrhnutý na ukladanie hesiel.

05.

NEVYŽADUJTE PRÍLIŠ ČASTÉ ZMENY HESIEL

Pravidelne nechávať platnosť hesiel vypršať a následne vyžadovať ich zmenu už viac nie je odporúčaným postupom. Národný inštitút pre štandardy a technológie (NIST) Spojených štátov a Národné centrum kybernetickej bezpečnosti (NCSC) Spojeného kráľovstva odporúčajú meniť heslá len v prípade, že to vyžaduje sám používateľ alebo je bezpečnosť hesla preukázateľne ohrozená. Používatelia, ktorí sú nútení meniť svoje heslá príliš často, volia jednoduchšie a ľahšie zapamätateľné heslá, prípadne používajú obvyklú stratégiu pridania čísla alebo písmena na koniec hesla a s každou nútenou zmenou hesla toto číslo či písmeno len navýšia. Výsledkom oboch týchto postupov je slabšia ochrana firemných systémov.

06.

APLIKUJTE POLITIKU NA CELÚ SIEŤ VRÁTANE IOT

Bezpečnostná politika hesiel by sa mala uplatňovať na všetky heslá, ktoré chránia zariadenia a systémy organizácie, teda aj na IoT zariadenia, akými sú bezpečnostné kamery, smart hub a routery. Ak nie sú tieto zariadenia dobre spravované alebo sa pri nich používajú predvolené prístupové údaje, zvyšuje sa riziko, že útočníci takúto bezpečnostnú zraniteľnosť nájdu a pokúsia sa ju zneužiť.