

5 základných pravidiel pre dobrú bezpečnostnú politiku hesiel

1

Definujte politiku hesiel v zrozumiteľnej forme. Zaveďte pravidlá tak, aby obsahovali všetky dôležité informácie:

- dĺžka hesla
- zložitosť hesla (malé a VEĽKÉ písmená, čísla, znaky)

Zabezpečte dodržiavanie zavedených pravidiel. Politiku hesiel musia dodržiavať všetci. Zamestnanci, majitelia, vrcholový manažment aj členovia správnej rady.

2

3

Vytvorte čiernu listinu hesiel (blacklist)

Blacklist je zoznam hesiel, ktoré sa používajú najčastejšie (napríklad 1234, heslo, admin,...). Na blacklist dajte aj heslá, ktoré boli prelomené.

Pokusy o vytvorenie týchto hesiel by mali byť zamietnuté.

Nevyžadujte príliš časté zmeny hesiel

Dôvod je ten, že používatelia ktorí sú nútení k častým zmenám hesiel volia jednoduchšie zapamätateľné heslá a každou zmenou hesla len pridajú číslo a toto číslo navyšujú.

Výsledok je slabšia ochrana zabezpečenia.

4

5

Aplikujte politiku hesiel na všetky zariadenia

Bezpečnostná politika hesiel by sa mala uplatňovať nie len na používateľov, ale aj na všetky zariadenia vo firemnej infraštruktúre, napríklad: IoT zariadenia, routrov, hubov, kamier atď.