

Nová smernica o heslách spoločnosti Arbonia

Vážené spolupracovníčky, vážení spolupracovníci,

Silné heslo je prvou líniou obrany našich systémov a údajov.

Hlavným cieľom útočníkov je okrem iného krádež prístupových údajov k používateľským účtom s cieľom získať prvotný prístup do našich sietí, serverov a IT systémov a v najhoršom prípade nepozorovane vykonávať činnosti, ako je napr. krádež údajov, špionáž alebo inštalácia škodlivého softvéru. Z tohto dôvodu predstavujú slabé alebo kompromitované heslá, ako aj nesprávna manipulácia s nimi, značné riziko. S cieľom lepšie splniť naše bezpečnostné požiadavky a lepšie vás chrániť pred týmito hrozbami bola pre spoločnosť Arbonia definovaná nová smernica o heslách.

Zmena smernice o heslách

Kompletnú stratégiu hesiel nájdete prehľadne uvedenú nižšie. Zmena sa týka najmä minimálnej dĺžky hesla, maximálnej platnosti hesla a jeho zložitosti.



Minimálna dĺžka hesla sa zvýši zo súčasných 8 na 12 znakov, aby bolo ťažšie prelomiť heslo, ale zároveň sa predĺži platnosť hesla na minimálne 360 dní. Ak použijete dlhšie heslo (≥ 16 znakov), platnosť hesla sa predĺži na 540 dní. Vo všetkých prípadoch je potrebné zabezpečiť vysokú úroveň zložitosti (= silné heslo) nových hesiel. To sa dosiahne kombináciou veľkých/malých písmen/číslic 0 až 9/interpunkčných alebo špeciálnych znakov.



Okrem toho sa automaticky zabráni používaniu hesiel, ktoré už boli kompromitované a sú voľne dostupné na internete, ako aj slov z čiernej listiny (napr. názvov spoločností).



Ak sa heslo objaví v databáze kompromitovaných hesiel počas svojej platnosti, automaticky sa zobrazí výzva na zmenu hesla.

Nová smernica o heslách sa automaticky aktivuje pri najbližšej zmene hesla systému Windows alebo na žiadosť lokálneho oddelenia IT. Pripomenutie dostanete 14 dní pred uplynutím platnosti hesla. **Smernica sa však vzťahuje na všetky systémy IKT spoločnosti Arbonia, t. j. aj na iné systémy ako Windows.** Vy ako majiteľ účtu ste v každom prípade zodpovedný za dodržiavanie smernice o heslách, aj keď to nie je možné technicky vynútiť.

Vytvorenie silného hesla

Existuje niekoľko techník na vytvorenie a zapamätanie si silného hesla. Silné heslo môžete vytvoriť napríklad na základe vety alebo nahradením definovaných reťazcov:

- Vyberte si vetu, ktorú si dobre pamätáte, a pretvorte ju na heslo. Napr.: *«Nie je až také zložité vybrať si silné heslo.»* Použite prvé písmená alebo niekoľko písmen jednotlivých slov a heslo doplňte o čísla a špeciálne znaky. Napr.: *«Njatz,vs1Sh.»*
- Vyberte si slovo, ktoré si dobre pamätáte, napr. „Popoludnie“ a definujte špeciálny reťazec, napr. *«1\$1»*. Teraz nahraďte definované časti/písmená slova špeciálnym reťazcom, aby ste vytvorili silné heslo. Napr. *«P1\$1p1\$1ludnie»*

Ďakujeme za oboznámenie sa s informáciou a zostávame s pozdravom
Tím Arbonia Security



Stratégia vytvárania hesiel

História hesiel (počet posledných hesiel, ktoré nesmiete znova použiť)	5	Počet neúspešných pokusov o prihlásenie, kým sa účet zablokuje	6
Minimálna dĺžka hesla	12 znakov	Trvanie blokovania účtu	Do odblokovania administrátorom
Maximálna platnosť hesla	360 dní (12 – 15 znakov), príp. 540 dní (≥ 16 znakov)	Trvanie do vynulovania počítadla neúspešných pokusov o prihlásenie	≥ 60 minút
Zložitosť	<ul style="list-style-type: none"> ➤ Veľké písmená ➤ Malé písmená ➤ Čísla od 0 po 9 ➤ Interpunkčné znamienka alebo špeciálne znaky 	Špeciálne (heslá systému Windows – interné a automaticky vytvárané v spoločnosti Arbonia)	Heslo nesmie obsahovať žiadne čísla na prvej a poslednej pozícii a žiadne 3 po sebe idúce rovnaké znaky



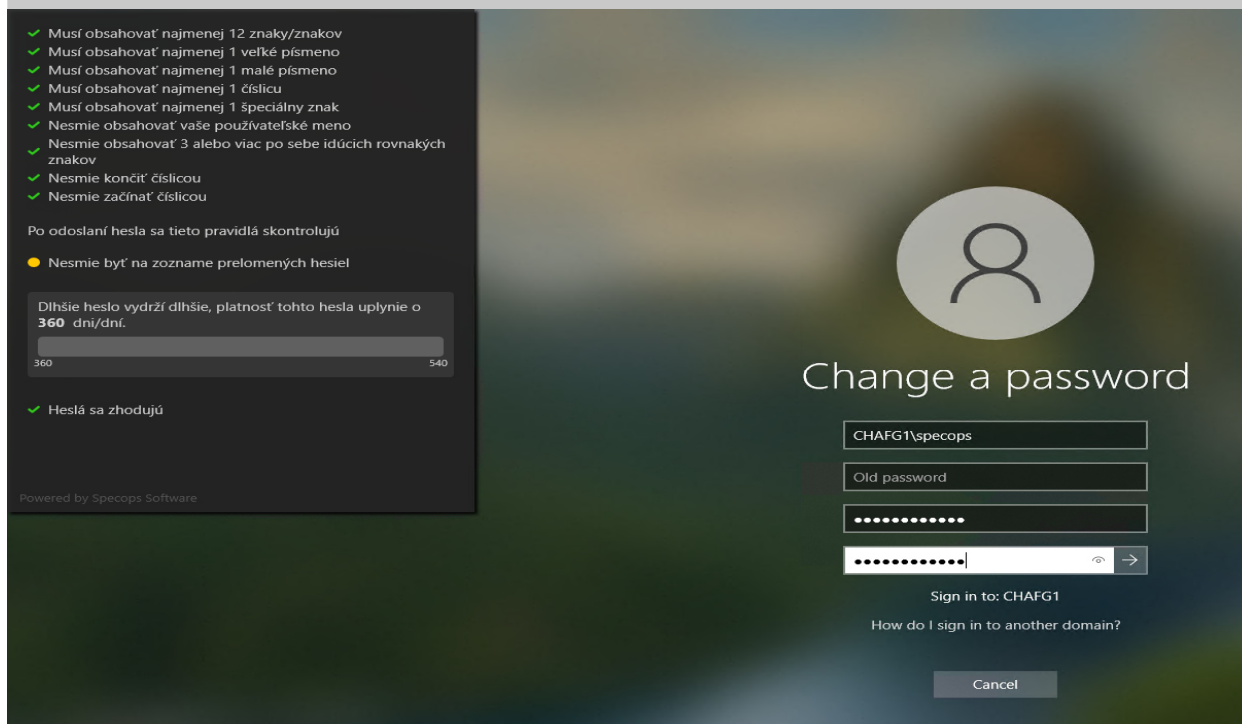
Nepoužívajte heslá, ktoré sú uvedené ako príklady v tomto dokumente. Tieto vzorové heslá sú teraz «kompromitované» a zaradené na čiernu listinu.



Okrem tohto informačného listu si prečítajte aj platnú smernicu o heslách (IS-ISP-GROUP-001-PASSWORD-POLICY) na adrese <https://security.arbonia.com>



Pri zmene hesla systému Windows sa priamo zobrazia požiadavky, ktoré je potrebné splniť.



The screenshot shows the Windows 'Change a password' dialog box. On the left, a list of requirements is displayed with green checkmarks:

- Musí obsahovať najmenej 12 znaky/znakov
- Musí obsahovať najmenej 1 veľké písmeno
- Musí obsahovať najmenej 1 malé písmeno
- Musí obsahovať najmenej 1 číslicu
- Musí obsahovať najmenej 1 špeciálny znak
- Nesmie obsahovať vaše používateľské meno
- Nesmie obsahovať 3 alebo viac po sebe idúcich rovnakých znakov
- Nesmie končiť číslicou
- Nesmie začínať číslicou

Below the list, it states: 'Po odoslaní hesla sa tieto pravidlá skontrolujú'. A yellow dot indicates a requirement: 'Nesmie byť na zozname prelomených hesiel'. A progress bar shows 'Dlhšie heslo vydrží dlhšie, platnosť tohto hesla uplynie o 360 dní/dní.' with a range from 360 to 540 days. At the bottom, it says 'Heslá sa zhodujú' with a green checkmark and 'Powered by Specops Software'.

On the right, the 'Change a password' dialog box is shown with input fields for 'CHAFG1\specops', 'Old password', and a new password field with a strength indicator. Below the fields, it says 'Sign in to: CHAFG1' and 'How do I sign in to another domain?' with a 'Cancel' button.