

Nová směrnice skupiny Arbonia k heslům

Vážené zaměstnankyně, vážení zaměstnanci!

Silné heslo je první obrannou linií našich systémů a dat.

Hlavním cílem útočníků je mimo jiné krádež přístupových údajů o uživatelském účtu za účelem získání iniciálního přístupu k našim sítím, serverům a systémům IT a v nejhorším případě za účelem nepozorovaného provádění činností, jako např. krádeže dat, špionáže nebo instalace škodlivého softwaru. Z tohoto důvodu představují slabá hesla nebo kompromitovaná hesla, jakož i neodborné zacházení s hesly, značné riziko. Aby bylo ještě více vyhověno našim bezpečnostním požadavkům a abyste byli před těmito hrozbami ještě lépe chráněni, byla pro skupinu Arbonia definována nová směrnice k heslům.

Změna směrnice k heslům

Kompletní strategie hesel je přehledně představena níže. Změna se týká hlavně minimální délky hesla, maximální doby platnosti hesla a komplexnosti.



Minimální délka hesla se nyní zvyšuje z 8 na 12 znaků, aby se ztížilo prolomení hesla, současně se však prodlužuje doba platnosti hesla na minimálně 360 dní. Pokud použijete delší heslo (≥ 16 znaků), jeho doba platnosti se prodlouží na 540 dní. Ve všech případech musí být pro nová hesla zajištěna vysoká komplexnost (= silné heslo). Toho se dosáhne kombinací velkých / malých písmen / číslic 0–9 / interpunkčních znamének nebo zvláštních znaků.



Dále je automaticky zamezeno použití již kompromitovaných a na internetu volně přístupných hesel a slov ze seznamu blokových slov (např. názvu firmy).



Pokud se heslo během své platnosti vyskytne v databázi s kompromitovanými hesly, budete automaticky vyzváni k jeho změně.

Nová směrnice k heslům bude automaticky aktivována při Vaší příští změně hesla pro Windows nebo po vyžádání z Vaší strany u lokálního oddělení IT. Vždy 14 dní před uplynutím hesla Vám to bude připomenuto. Směrnice však platí pro všechny systémy ICT skupiny Arbonia, to znamená také pro jiné operační systémy než systémy Windows. Jako vlastníci účtu jste v každém případě odpovědní za dodržování směrnice k heslům, i když to od Vás není technicky vymáháno.

Vytvoření silného hesla

Pro vytvoření silného hesla a jeho zapamatování existují různé techniky. Silné heslo vytvoříte např. na základě věty nebo nahrazením definovaných posloupností znaků:

- Zvolte větu, kterou si můžete dobře zapamatovat a převedte ji do hesla. Např.: *"Dosáhnout toho, aby bylo zvoleno silné heslo, není vůbec tak obtížné."* Použijte počáteční písmena nebo více písmen jednotlivých slov a přidejte k heslu číslice a zvláštní znaky. Např.: *"Dt,abz1sh,nvto."*
- Zvolte slovo, které si můžete dobře zapamatovat, např. "Dopoledne" a definujte speciální posloupnost znaků, např. *"1\$1"*. Nyní nahradte definované části / písmena slova svou zvolenou speciální posloupností znaků za účelem získání silného hesla. Např.: *"D1\$1p1\$1ledne"*

Děkujeme Vám za to, že jste informace vzali na vědomí a zůstáváme s přátelským pozdravem
Arbonia Security Team



Strategie hesel

Historie hesel (počet posledních hesel, která nesmějí být opětovně použita)	5	Počet chybných pokusů o přihlášení až do zablokování účtu	6
Minimální délka hesla	12 znaků	Doba trvání zablokování účtu	Až do odblokování administrátorem
Maximální doba platnosti hesla	360 dní (12–15 znaků), příp. 540 dní (≥16 znaků)	Doba, než bude vynulován čítač chybných pokusů o přihlášení	≥ 60 minut
Komplexnost	<ul style="list-style-type: none"> ➤ Velká písmena ➤ Malá písmena ➤ číslice 0–9 ➤ Interpunkční znaménka nebo zvláštní znaky 	Specifika (hesla pro Windows – prosazována v Arbonia interně a automaticky)	Heslo nesmí obsahovat číslice na prvním a posledním místě a 3 po sobě následující identické znaky



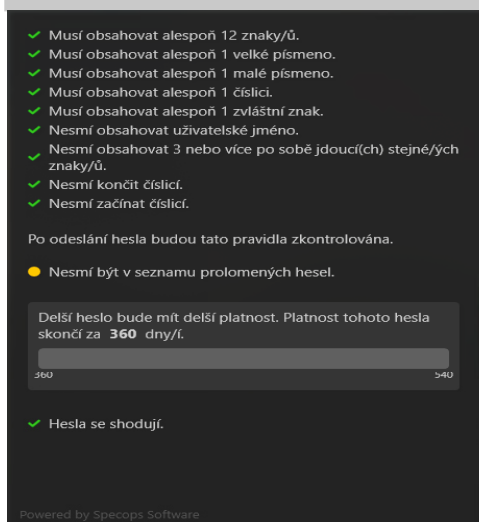
Nepoužívejte hesla, která jsou uvedena jako příklad v tomto dokumentu. Tato jako příklad uvedená hesla jsou nyní "kompromitovaná" a jsou obsažena v seznamu blokových slov.



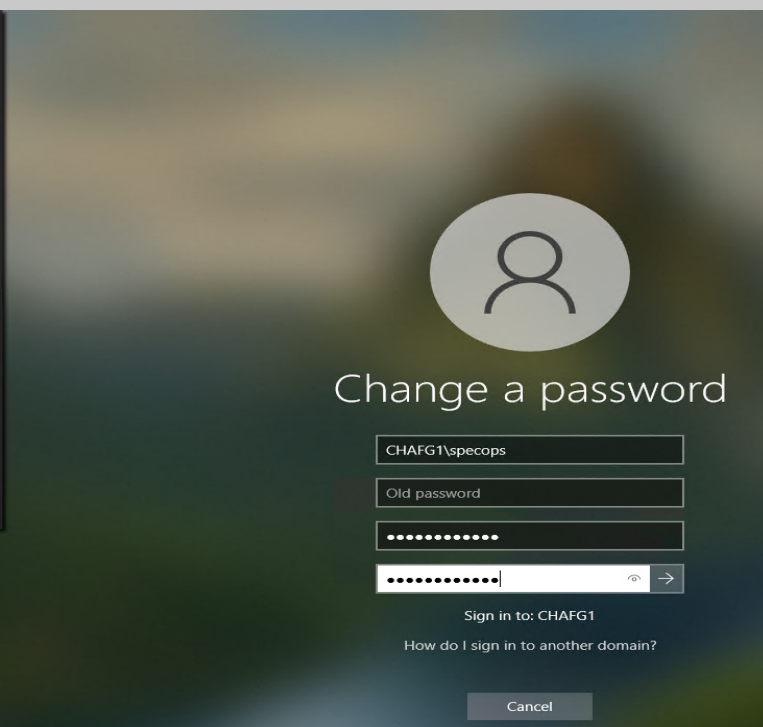
Dodatečně k tomuto informačnímu dopisu věnujte pozornost i platné směrnici k heslům (IS-ISP-GROUP-001-PASSWORD-POLICY) na adrese <https://security.arbonia.com>



Při změně Vašeho hesla pro Windows se Vám přímo zobrazí požadavky, které musejí být splněny.



✓ Musí obsahovat alespoň 12 znaky/ů.
 ✓ Musí obsahovat alespoň 1 velké písmeno.
 ✓ Musí obsahovat alespoň 1 malé písmeno.
 ✓ Musí obsahovat alespoň 1 číslici.
 ✓ Musí obsahovat alespoň 1 zvláštní znak.
 ✓ Nesmí obsahovat uživatelské jméno.
 ✓ Nesmí obsahovat 3 nebo více po sobě jdoucích stejné/ých znaky/ů.
 ✓ Nesmí končit číslicí.
 ✓ Nesmí začínat číslicí.
 Po odeslání hesla budou tato pravidla zkontrolována.
 ● Nesmí být v seznamu prolomených hesel.
 Delší heslo bude mít delší platnost. Platnost tohoto hesla skončí za **360** dny/l.
 ✓ Hesla se shodují.
 Powered by Specops Software



Change a password
 CHAFG1\specops
 Old password
 Sign in to: CHAFG1
 How do I sign in to another domain?
 Cancel