ARBONIA
IT SECURITY

Nowe wytyczne dotyczące haseł Grupy Arbonia

Szanowni Pracownicy

Silne hasło to pierwsza linia obrony naszych systemów i danych.

Głównym celem atakujących jest m. in. kradzież danych dostępowych z konta użytkownika w celu uzyskania wstępnego dostępu do naszych sieci, serwerów i systemów informatycznych, a w najgorszym przypadku, bez zauważenia, do wykonywania czynności takich jak kradzież danych, szpiegostwo lub instalowanie złośliwego oprogramowania. Z tego powodu słabe lub skompromitowane hasła oraz ich niewłaściwe użycie stanowią znaczne ryzyko. Aby jeszcze lepiej spełniać nasze wymagania w zakresie bezpieczeństwa i lepiej Państwa chronić przed tymi zagrożeniami, zdefiniowano nowe wytyczne dotyczące haseł dla Grupy Arbonia.

Zmiana wytycznych dotyczących haseł

Poniżej znajduje się pełna strategia dotycząca haseł. Zmiana dotyczy głównie minimalnej długości hasła, maksymalnej ważności hasła i złożoności.

Minimalna długość hasła została zwiększona z 8 do 12 znaków, aby utrudnić złamanie hasła, ale jednocześnie ważność hasła zostanie wydłużona do co najmniej 360 dni. W przypadku używania dłuższego hasła (≥ 16 znaków), ważność hasła zostaje przedłużona do 540 dni. We wszystkich przypadkach należy zapewnić wysoki poziom złożoności (= silne hasło) dla nowych haseł. Osiąga się to poprzez kombinację wielkich / małych liter / cyfr 0–9 / znaków interpunkcyjnych lub znaków specjalnych.

Użycie już skompromitowanych haseł, które są swobodnie dostępne w Internecie, oraz słów z czarnej listy (np. nazwy firm) jest automatycznie blokowane.

Jeśli hasło pojawi się w bazie danych ze skompromitowanymi hasłami, gdy będzie ono nadal ważne, zostaną Państwo automatycznie poproszeni o zmianę hasła.

Nowe wytyczne dotyczące haseł zostaną aktywowane automatycznie przy następnej zmianie hasła systemu Windows lub na żądanie lokalnego działu IT. Na 14 dni przed wygaśnięciem hasła otrzymają Państwo powiadomienie. **Wytyczne dotyczą jednak wszystkich systemów teleinformatycznych Grupy Arbonia, czyli również systemów innych niż Windows. Jako właściciel konta są Państwo odpowiedzialni za przestrzeganie wytycznych dotyczących haseł w każdym przypadku, nawet jeśli nie są one technicznie egzekwowane.**

Tworzenie silnego hasła

Istnieje kilka technik tworzenia i zapamiętywania silnego hasła. Hasło można utworzyć na przykład na podstawie zdania lub zastępując zdefiniowane ciągi znaków:

- Prosimy wybrać zdanie, które łatwo Państwo zapamiętają i przekształcić je w hasło. Np.: „*To wcale nie jest takie trudne, aby wybrać jedno silne hasło.*" Należy użyć pierwszych liter lub kilku liter poszczególnych słów oraz wzbogacać hasło o cyfry i znaki specjalne. Np.: *„Twnjtt,aw1sh."*
- Należy wybrać słowo, które łatwo Państwo zapamiętają np. „Teleskop" i zdefiniować specjalny ciąg znaków np. „*1$1*". Teraz należy zastąpić zdefiniowane części/litery słowa wybranym ciągiem znaków, aby uzyskać silne hasło. Np.: „*T1$1l1$1skop*"

Dziękujemy za zapoznanie się z powyższymi informacjami i pozdrawiamy serdecznie
Zespoł Arbonia Security

ARBONIA
IT SECURITY

Strategia dotycząca haseł			
Historia haseł (liczba ostatnich haseł, których nie można ponownie użyć)	5	**Liczba nieudanych prób logowania nim dojdzie do zablokowania konta**	6
Minimalna długość hasła	12 znaków	**Czas trwania blokady konta**	Dopóki administrator nie odblokuje
Maksymalna ważność hasła	360 dni (12–15 znaków) lub 540 dni (≥16 znaków)	**Czas do zresetowania licznika nieudanych prób logowania**	≥ 60 minut
Złożoność	➢ Wielkie litery ➢ Małe litery ➢ Cyfry 0–9 ➢ Znaki interpunkcyjne lub znaki specjalne	**Informacje specjalne (hasła Windows – wewnętrznie i automatycznie egzekwowane przez firmę Arbonia)**	Hasło nie może zawierać cyfr na pierwszej lub ostatniej pozycji ani 3 kolejnych identycznych znaków

Nie należy używać żadnych haseł podanych jako przykłady w tym dokumencie. Te przykładowe hasła są teraz „skompromitowane" i znajdują się na czarnej liście.

Oprócz tego pisma informacyjnego należy również zwrócić uwagę na obowiązujące wytyczne dotyczące haseł (IS-ISP-GROUP-001-PASSWORD-POLICY) pod adresem https://security.arbonia.com

Po zmianie hasła systemu Windows zostaną wyświetlone wymagania, które należy spełnić.