**Zabezpieczenie konta**

#### **Dodanie MFA (Multi-factor authentication) dla użytkownika root**

1. Przejdz do usługi IAM
2. Na pulpicie (IAM Dashboard) zobaczysz sekcję “Security Alerts”. Jeśli znajduje się tam komunikat:
   1. The root user for this account does not have Multi-factor authentication (MFA) enabled.   
      Enable MFA to improve security for this account.

to znaczy, że należy ustawić MFA dla użytkownika root. Kliknij w link enable MFA, a następnie przycisk Activate MFA. Wybierz jedną z opcji i postępuj zgodnie z instrukcją na ekranie. Kolejne kroki dotyczą "Virtual MFA device".

1. Zainstaluj na Twoim urządzeniu aplikację do uwierzytelniania wieloskładnikowego. Może być to np. Authy.
2. Odsłoń QR code na ekranie, a następnie:
   1. wykonaj zrzut ekranu i zachowaj w bezpiecznym miejscu plik i/lub jego wydruk - będzie Ci potrzebny w przypadku utraty urządzenia
   2. używając aplikacji i aparatu zeskanuj QR code
3. Wpisz w pola formularza dwa otrzymane kody MFA
4. Naciśnij przycisk Assign MFA.

Teraz przy logowaniu jako root user konieczne będzie podanie tokena MFA.

#### **Dodanie użytkownika IAM**

Użytkownik root nie służy do codziennej pracy z kontem AWS. Używa się go tylko w wyjątkowych przypadkach. Dlatego tworzymy użytkowników IAM.

Poniżej znajdziesz instrukcję tworzenia użytkownika IAM, który będzie miał pełne uprawnienia do konta.

1. Przejdź do usługi IAM.
2. Z menu po lewej stronie wybierz Users a następnie naciśnij przycisk Add user
3. Podaj nazwę użytkownika (przykładowo: admin-user)
4. Nadaj dostęp. Są 2 rodzaje dostępów: dostęp programistyczny i dostęp do konsoli AWS. Wybierz tylko dostęp do konsoli AWS i naciśnij przycisk Permissions

Pobierz plik CSV z dostępami do konta - znajduje się tam login i hasło dla nowego użytkownika oraz link do logowania z numerem konta AWS.  
  
Zarządzanie użytkownikami jest prostsze jeśli przypiszemy ich do grup i to grupom użytkowników będziemy nadawać uprawnienia.

1. Utwórz grupę Administrators (Naciśnij w tym celu przycisk Create Group i wpisz w pole Group name nazwę grupy).
2. Z listy dostępnych polityk wybierz AdministratorAccess, a następnie naciśnij przycisk Create group
3. Przejdz do kolejnej sekcji naciskając przycisk Next: Tags, a następnie Review

W podsumowaniu zobaczysz, że użytkownik należy do grupy Administrators oraz że ma dodaną politykę IAMUserChangePassword, która pozwala użytkownikowi na zmianę hasła.

1. Naciśnij Create user.
2. Pobierz plik csv z danymi do logowania i/lub wyświetl hasło. Jest to jedyny moment, żeby je zapisać.
3. Zamknij formularz naciskając Close.
4. Zaloguj się do konsoli AWS jako admin-user - tym razem przy logowaniu wybierz typ użytkownika IAM user.

Ale to jeszcze nie koniec. Użytkownik admin-user ma pełne uprawnienia do konta, więc dostęp tego użytkownika również należy zabezpieczyć dodając MFA.

1. Przejdz do sekcji Users i wybierz użytkownika z listy. Przejdz do zakładki `Security credentials.
2. Obok informacji Assigned MFA device znajduje się link Manage. Dodaj MFA w taki sam sposób, jak dla użytkownika root:
   * Zainstaluj na Twoim urządzeniu aplikację do uwierzytelniania wieloskładnikowego. Może być to np. Authy.
   * Odsłoń QR code na ekranie, a następnie:
     + wykonaj zrzut ekranu i zachowaj w bezpiecznym miejscu plik i/lub jego wydruk - będzie Ci potrzebny w przypadku utraty urządzenia
     + używając aplikacji i aparatu zeskanuj QR code.
   * Wpisz w pola formularza dwa otrzymane kody MFA
   * Naciśnij przycisk Assign MFA

Konto użytkownika IAM jest już dodatkowo zabezpieczone.