1. Atak typu Man-in-the-Middle (MitM)

Opis:
Atakujący przechwytuje ruch sieciowy między użytkownikiem a dostawcą chmury, mogąc w ten sposób kraść dane logowania, zmieniać przesyłane informacje lub przechwytywać wrażliwe dane.

Przeciwdziałanie:

- Wymuszanie szyfrowania transmisji danych za pomocą protokołów TLS/SSL.
- Korzystanie z VPN i bezpiecznych połączeń sieciowych.
- Implementacja mechanizmów wykrywania anomalii w ruchu sieciowym.
- Uwierzytelnianie wzajemne klient-serwer.

2. Atak na konto użytkownika (Credential Theft)

Opis:
Hakerzy wykorzystują wykradzione lub wyłudzone dane logowania (np. poprzez phishing), aby uzyskać dostęp do zasobów chmurowych.

Przeciwdziałanie:

- Wdrożenie uwierzytelniania wieloskładnikowego (MFA).
- Regularna rotacja i monitorowanie poświadczeń użytkowników.
- Ograniczenie dostępu do zasobów na zasadzie minimalnych uprawnień (principle of least privilege).
- Wykorzystanie narzędzi do wykrywania anomalii w logowaniach i alertowania o podejrzanych działaniach.

3. Atak DDoS na usługi chmurowe

Opis:
Atakujący generują ogromny wolumen ruchu, aby przeciążyć infrastrukturę dostawcy chmury i uniemożliwić dostęp do usług.

Przeciwdziałanie:

- Wykorzystanie systemów ochrony przed DDoS, np. AWS Shield, Cloudflare DDoS Protection.
- Skalowanie zasobów w celu absorpcji ataku.
- Konfiguracja firewalli i mechanizmów ograniczających podejrzany ruch.
- Użycie mechanizmów rate-limiting oraz filtracji ruchu.

4. Atak poprzez błędy w konfiguracji usług chmurowych

Opis:
Niepoprawna konfiguracja zasobów (np. publiczny dostęp do baz danych, brak szyfrowania) może umożliwić nieautoryzowany dostęp do wrażliwych informacji.

Przeciwdziałanie:

- Regularne audyty bezpieczeństwa i przegląd konfiguracji.
- Automatyczne skanowanie błędów konfiguracji za pomocą narzędzi takich jak AWS Config, Microsoft Defender for Cloud.
- Zasada minimalnych uprawnień (least privilege).
- Monitorowanie logów i alertowanie o zmianach w konfiguracji.

5. Wstrzyknięcie złośliwego kodu poprzez luki w aplikacjach webowych (np. SQL Injection, XSS)

Opis:
Atakujący wykorzystują podatności w aplikacjach działających w chmurze, wstrzykując złośliwe zapytania do baz danych lub skrypty mogące kraść dane użytkowników.

Przeciwdziałanie:

- Wdrożenie firewalli aplikacyjnych (WAF).
- Regularne testowanie bezpieczeństwa aplikacji (pentesty, SAST/DAST).
- Walidacja i filtrowanie danych wejściowych.
- Stosowanie mechanizmów typu prepared statements oraz CSP (Content Security Policy).

Źródła:

https://pl.wikipedia.org/wiki/Atak_man_in_the_middle

https://www.techtarget.com/searchsecurity/definition/credential-theft

https://pl.wikipedia.org/wiki/DDoS

https://nflo.pl/baza-wiedzy/atak-cybernetyczny-kompendium/

https://pl.wikipedia.org/wiki/SQL_injection

https://chatgpt.com/