KLASTER.IT

RYZYKA DOT. KORZYSTANIA Z USŁUG AMERYKAŃSKICH BIGTECH'ÓW

GRZEGORZ KOBER
Dyrektor ds. Rozwoju Biznesu
whitesky.cloud Poland
gkober@whitesky-pl.cloud
609-575-379
www.whitesky.pl

whitesky.cloud Poland

ZAGADNIENIA

W tej prezentacji przedstawimy kluczowe zagrożenia i szanse związane z wykorzystaniem chmury publicznej w Polsce. Pokażemy konkretne przykłady incydentów z ostatnich lat, omówimy zagrożenia dla suwerenności i bezpieczeństwa, a także zaprezentujemy optymalny model rozwiązań jako strategiczne rozwiązanie dla firm dbających o bezpieczeństwo

01 **WPROWADZENIE**

02 **KLUCZOWE INWESTYCJE BIGTECH'ÓW**

03 **HISTORYCZNE INCYDENTY**

04 **RYZYKA DLA POLSKIEGO RYNKU**

05 **ZALETY CHMURY PRYWATNEJ**

06 **OPTYMALNY WYBÓR DLA POLSKICH ORGANIZACJI -DYSKUSJA**

1. WPROWADZENIE

W erze intensywnej cyfryzacji każda firma – niezależnie od wielkości – opiera swoje działanie na danych. **Coraz więcej organizacji przenosi krytyczne systemy do chmury**, widząc w tym szansę na skalowalność, wydajność i elastyczność.

Jednak **równocześnie rośnie skala zagrożeń**: wycieki danych, cyberataki, ataki ransomware, a także ryzyko związane z utratą kontroli nad danymi przechowywanymi poza granicami kraju.

Chmura stała się infrastrukturą o znaczeniu strategicznym.

Globalne koncerny technologiczne (Big Tech) inwestują w Polsce miliardy złotych w centra danych, a jednocześnie zdobywają coraz większy wpływ na sektor publiczny, zdrowie, energetykę czy obronność.

Tu powstawić można pytania nie tylko o technologię – ale też o suwerenność cyfrową, bezpieczeństwo narodowe i konkurencyjność lokalnych firm.

W tej prezentacji pokażemy, realne incydenty jakie wydarzyły się w ostatnich latach, jakie są ich skutki, oraz zachęcimy do reflekcji jak budować strategię chmurową, która łączy elastyczność technologii z pełną kontrolą nad bezpieczeństwem.

2. KLUCZOWE INWESTYCJE BIGTECH'ÓW W POLSCE W 2025 ROKU

GOOGLE

- Memorandum z OChK i PFR z dnia 13.02.2025 (utajnione) - mowa o miliardach PLN inwestycji
- Plan cyfryzacji w sektorach Służba Zdrowia, Energetyka i Cyberbezpieczeństwo.

MICROSOFT

- Ogłoszenie inwestycji w wysokości 3 mld złotych polskich w budowę centrów danych i rozwój sztucznej inteligencji.
- Zakładana współpraca z polskimi Siłami Zbrojnymi w zakresie cyberbezpieczeństwa

3. HISTORYCZNE INCYDENTY

W ostatnich latach świat doświadczył szeregu poważnych incydentów bezpieczeństwa w infrastrukturze chmurowej – również u największych dostawców. W tym fragmencie prezentacji pokazujemy głośne przypadki, które unaoczniły, że nawet najbardziej zaawansowane systemy nie są odporne na błędy, ataki czy luki konfiguracyjne.

Każdy z zaprezentowanych incydentów:

- dotyczy globalnych dostawców (AWS, Microsoft, Alibaba, Oracle),
- został oficjalnie potwierdzony lub udokumentowany,
- wiązał się z wyciekiem danych liczonych w milionach rekordów,
- i pokazał konkretne ryzyka dla firm i instytucji.

Celem tego zestawienia jest rozpoczęcie rozmowy o tym, jakie wnioski powinni wyciągnąć liderzy IT i bezpieczeństwa, planując swoje strategie chmurowe – szczególnie w kontekście ochrony danych wrażliwych i modelu hybrydowego.

01 **WYCIEK DANYC (CHMURA AWS - TWITCH) 2021**

02 **“BLUEBLEED” (MICROSOFT AZURE) - 2022**

03 **ATAK STORM-0558 (AZURE AD / EXCHANGE ONLINE) 2023**

04 **ALIBABA CLOUD -2022**

04 **ATAK NA ORACLE CLOUD – 2025**

Rok	Dostawca	Skala incydentu	Przyczyna	Skutki
2021	AWS (Twitch)	125 GB danych, w tym kod źródłowy i dane streamerów	Błąd konfiguracji serwera	Kara 2 mln TRY (~58 000 USD) nałożona przez turecki organ ochrony danych
2022	Microsoft Azure	2,4 TB danych klientów z 65 000 firm w 111 krajach	Błędna konfiguracja Azure Blob Storage	Ujawnienie danych kontaktowych, e-maili, dokumentów; krytyka za brak zgłoszenia do regulatorów
2023	Microsoft	Dostęp do skrzynek e-mail 22 organizacji, ponad 500 osób	Kradzież klucza podpisującego tokeny przez grupę Storm-0558	Kradzież 60 000 e-maili z Departamentu Stanu USA;
2022	Alibaba Cloud	Wyciek 23 TB danych osobowych 1 mld obywateli Chin	Brak zabezpieczeń w bazie danych policji Szanghaju	Spadek akcji Alibaba o 6%; dochodzenie władz chińskich
2025	Oracle Cloud	6 mln rekordów z SSO i LDAP; 140 000 klientów	Prawdopodobna luka typu zero-day w Oracle Access Manager	Dane wystawione na sprzedaż; Oracle zaprzecza incydentowi, mimo potwierdzeń od klientów

4. RYZYKA DLA RYNKU POLSKIEGO

01

UTRATA SUWERENNOŚCI
– KLUCZOWE SEKTORY (CYBERBEZPIECZEŃSTWO, ZDROWIE, ENERGETYKA) POD KONTROLĄ ZAGRANICZNYCH FIRM I RZĄDÓW.

02

CLOUD ACT
– USA MOŻE UZYSKAĆ DOSTĘP DO DANYCH PRZECHOWYWANYCH W POLSCE (DANE Z CZĘŚCI USŁUG JUŻ SĄ WYSYŁANE DO STANÓW ZJEDNOCZONYCH)

03

ZALEŻNOŚĆ OD OLIGOPOLU BIGTECH
– KRYTYCZNE SYSTEMY POD KONTROLĄ GOOGLE I MICROSOFT.

04

RYZYKO DLA LOKALNYCH FIRM
– BIG TECH OSŁABI POZYCJĘ POLSKICH DOSTAWCÓW CHMURY.

05

RYZYKO DLA BEZPIECZEŃSTWA I CIĄGŁOŚCI USŁUG
– MOŻLIWE ATAKI, WYCIEKI I ZAKŁÓCENIA W DZIAŁANIU SYSTEMÓW, TAKŻE W ODNIESIENIU DO AKTUALNEJ SYTUACJI GEOPOLITYCZNEJ.

5. ZALETY CHMURY PRYWATNEJ

MOŻLIWOŚĆ PERSONALIZACJI I INTEGRACJI

Dostosowanie rozwiązań do specyfiki biznesu – łatwiejsze zarządzanie środowiskami legacy, integracja z własnymi systemami i politykami bezpieczeństwa.

KONTROLA NAD DANYMI

Dane przechowywane i przetwarzane lokalnie lub u zaufanego operatora – pełna kontrola nad lokalizacją, dostępem i zabezpieczeniami.

BRAK VENDOR LOCK-IN

Możliwość budowy infrastruktury z różnych komponentów – elastyczność w integracji infrastrkutury.

ZGODNOŚĆ Z REGULACJAMI

Spełnienie wymagań prawnych i branżowych – zwłaszcza w sektorach wrażliwych: finansowym, medycznym, publicznym.

SUWERENNOŚĆ CYFROWA

Brak zależności od zagranicznych koncernów i regulacji takich jak CLOUD Act – dane pozostają w granicach kraju, pod krajowym nadzorem.

6. OPYMALNY WYBÓR DLA POLSKICH ORGANIZACJI?

ZAPRASZAMY DO DYSKUSJI!

whitesky.cloud
Poland

BEZPIECZNA CHMURA PRYWATNA - DOSTĘPNA NAWET W TWOJEJ SERWEROWNI

WWW.WHITESKY.PL