Migracja do Microsoft 365 i Azure – różnice, zagrożenia oraz zabezpieczenia (portal rekrutacyjny)

Opracowanie zgodne z metodyką podmiotów publicznych

Dominik Rolek

1. Wstęp....1
2. Zarządzanie zmianą....1
2.1 Cel....1
2.2 Zarządzanie zmianą wg normy ISO 27002....1
2.3 Scenariusz zmiany dla badanego podmiotu....2
2. Różnice on-prem vs chmura (Microsoft 365/ Azure)....2
2.1 Cel....2
2.2 Kluczowe pojęcia....2
2.3 Porównanie on-prem i chmury....3
3. Zagrożenia i szanse specyficzne dla chmury....4
3.1 Cel....4
3.2 Wykaz szans i zagrożeń....4
4. Zagrożenia procesu migracji....5
4.1 Cel....5
4.3 Wykaz zagrożeń....5
5. Zabezpieczenia dla bezpiecznej migracji....6

1. Wstęp

Firma informatyczna świadczy usługi pośrednictwa pracy i utrzymuje dziś infrastrukturę on-premises we własnej serwerowni, posiadając własny zespół IT. Środowisko biurowe jest oparte o Windows oraz usługi Exchange/SharePoint/Office, a serwery działają na Linux. Firma planuje przeniesienie usług biurowych do Microsoft 365 oraz migrację serwerów do Microsoft Azure. Celem jest przeprowadzenie migracji bez pogorszenia poufności, integralności i dostępności informacji Poniżej omówiono różnice on-prem vs chmura, specyficzne zagrożenia i szanse chmury, ryzyka migracji oraz wymagane zabezpieczenia.

2. Zarządzanie zmianą

2.1 Cel

Zapewnić, że wszystkie zmiany związane z migracją do Microsoft 365 i Azure są planowane, oceniane pod kątem ryzyka, testowane, zatwierdzane, wdrażane w sposób kontrolowany oraz możliwe do odtworzenia/wycofania, tak aby nie pogorszyć P/I/D oraz nie pozostawić „tymczasowych” luk po migracji.

2.2 Zarządzanie zmianą wg normy ISO 27002

Zarządzanie zmianą powinno być realizowane jako formalny, udokumentowany i egzekwowany proces, który chroni bezpieczeństwo informacji podczas wdrażania nowych rozwiązań i modyfikacji istniejących systemów. ISO/IEC 27002:2022 wskazuje, że zmiany w systemach i urządzeniach przetwarzających informacje muszą podlegać procedurom zarządzania zmianą, aby zachować bezpieczeństwo informacji.

W praktyce (wg ISO/IEC 27002:2022, kontrola 8.32) proces zarządzania zmianą powinien obejmować co najmniej:

- planowanie zmiany oraz ocenę wpływu i zależności,
- autoryzację (zatwierdzenie) zmiany,
- komunikację zmiany do właściwych stron zainteresowanych,
- testy i akceptację wyników testów przed wdrożeniem,
- kontrolowane wdrożenie wraz z planem wdrożenia i planem awaryjnym (w tym możliwość wycofania),
- prowadzenie rejestru zmian (ślad audytowy),
- aktualizację dokumentacji operacyjnej i procedur,
- aktualizację elementów powiązanych, np. karty stosowania, SZBI

2.3 Scenariusz zmiany dla badanego podmiotu

- Zgłoszenie i zakres zmiany (M365 + Azure) oraz wskazanie właścicieli zmian, ryzka.
- Spis elementów do migracji i powiązań (systemy/usługi, dane, konta techniczne).
- Ocena wpływu na P/I/D oraz identyfikacja ryzyk migracyjnych.
- Plan migracji (etapy, okna serwisowe, kryteria postępu) + plan zabezpieczeń.
- Testy i pilotaż oraz poprawki po wynikach testów.
- Zatwierdzenie i wdrożenie produkcyjne etapami z możliwością wycofania (rollback).
- Weryfikacja po wdrożeniu (dostępy, uprawnienia, logi, dostępność) i usunięcie wyjątków tymczasowych.
- Zamknięcie zmiany (aktualizacja dokumentacji i przekazanie do utrzymania).

3. Różnice on-prem vs chmura (Microsoft 365/ Azure)

3.1 Cel

- Pokazać najważniejsze różnice między modelem on-prem a chmurowym dla tej firmy.
- Wskazać, co się zmienia w odpowiedzialnościach i w sposobie zabezpieczania (mniej „murów", więcej tożsamości i konfiguracji).
- Dać podstawę do dalszych punktów: szanse/zagrożenia i ryzyka migracji.

3.2 Kluczowe pojęcia

- **On-prem** – infrastruktura utrzymywana we własnej serwerowni; organizacja odpowiada za całość (sprzęt, sieć, systemy, aplikacje, dane).
- **Chmura (Microsoft 365/Azure)** – usługi dostawcy dostępne przez internet; część odpowiedzialności przechodzi na dostawcę, ale organizacja nadal odpowiada za konfigurację, dostęp i dane.

Identyfikator	Obszar	On-prem	Chmura (Microsoft 365 / Azure)	P/I/D (wpływ główny)
O-1	Odpowiedzialność	Organizacja odpowiada za pełne bezpieczeństwo na wszystkich warstwach: fizycznej (serwerownia), infrastruktury i sieci, systemów, aplikacji oraz danych (dostęp, kopie, monitorowanie). Poziom bezpieczeństwa zależy bezpośrednio od procesów i kompetencji zespołu IT (aktualizacje, konfiguracje, kontrola zmian).	Model współodpowiedzialności: dostawca zabezpiecza „chmurę", organizacja odpowiada za dostęp, konfigurację i dane.	P/I/D
O-2	Granica zaufania i kontrola dostępu	Kontrola dostępu często oparta o sieć (wewnątrz sieci/VPN).	Kontrola dostępu oparta o tożsamość i polityki (logowanie, warunki dostępu, uprawnienia) niezależnie od lokalizacji.	P/I/D
O-3	Uprawnienia administracyjne	Trudność w kontroli rozproszonej administracji.	Uprawnienia oparte o role i możliwość ograniczania/rozliczania administracji.	P/I/D
O-4	Ekspozycja usług i konfiguracja	Ekspozycja zwykle ograniczona do kilku punktów wejścia.	W chmurze łatwiej o niezamierzoną ekspozycję zasobów lub danych na zewnątrz, dlatego konfiguracja jest krytyczna.	P/I/D
O-5	Monitoring i logi	Logi lokalne, często rozproszone.	Wiele źródeł logów (M365/Azure) — trzeba je włączyć, zebrać i ustawić alerty.	P/I/D

3. Zagrożenia i szanse specyficzne dla chmury

3.1 Cel

Wskazać szanse i zagrożenia charakterystyczne dla chmury (M365/Azure), które wpływają na P/I/D.

3.2 Wykaz szans i zagrożeń

ID	Kategoria	Opis	P/I/D
S-1	Szansa	Wyższa odporność na awarie lokalne – infrastruktura oparta o wiele ośrodków przetwarzania danych zmniejsza wpływ awarii pojedynczej serwerowni/siedziby na działanie usług.	P/I/D
S-2	Szansa	Lepsze możliwości odtworzenia i ciągłości działania – łatwiej zaplanować i uruchomić rozwiązania zapewniające ciągłość w przypadku awarii lub przeciążenia (organizacyjnie i technicznie).	P/I/D
S-3	Szansa	Standaryzacja bezpieczeństwa i procesów – łatwiej wprowadzić jednolite zasady konfiguracji, uprawnień i monitoringu dla całego środowiska, zamiast utrzymywać wiele lokalnych wyjątków.	P/I/D
Z-1	Zagrożenie	Błędna konfiguracja może szybko spowodować ujawnienie danych lub nieautoryzowany dostęp (np. niezamierzone wystawienie zasobu lub zbyt szerokie udostępnienia).	P/I/D
Z-2	Zagrożenie	Przejęcie kont (np. phishing) daje bezpośredni dostęp do usług i danych, szczególnie przy braku silnych zasad logowania i kontroli dostępu.	P/I/D
Z-3	Zagrożenie	Zależność od dostawcy usług – awarie lub ograniczenia po stronie dostawcy mogą wpływać na dostępność; organizacja ma ograniczony wpływ na usunięcie przyczyny.	P/I/D

4. Zagrożenia procesu migracji

4.1 Cel

Wskazać typowe zagrożenia występujące w trakcie migracji do Microsoft 365 i Azure, które mogą wpłynąć na poufność, integralność i dostępność informacji oraz ciągłość działania usług.

4.3 Wykaz zagrożeń

Identyfikator	Nazwa	Opis	P/I/D
M-1	Przenoszenie danych	Ryzyko wycieku danych podczas przenoszenia (eksporty, kopie, pliki tymczasowe) oraz w trakcie prac migracyjnych.	P/I/D
M-2	Konfiguracja i uprawnienia	Ryzyko błędnego ustawienia uprawnień po migracji (zbyt szeroki dostęp), prowadzącego do ujawnienia danych lub nieuprawnionej modyfikacji.	P/I/D
M-3	Zmiany tymczasowe	Ryzyko, że „tymczasowe" obejścia bezpieczeństwa na czas migracji (otwarte dostępy/wyłączenie kontroli) pozostaną i staną się trwałą podatnością.	P/I/D
M-4	Logowanie i administracja	Ryzyko przejęcia kont (w tym kont uprzywilejowanych) wskutek zbyt słabych zasad logowania lub błędnej konfiguracji dostępu administracyjnego.	P/I/D
M-5	Monitoring i wykrywanie	Brak logowania i monitoringu od początku migracji ogranicza wykrycie incydentów w najbardziej ryzykownym okresie.	P/I/D

5. Zabezpieczenia dla bezpiecznej migracji

Identyfikator	Zabezpieczenie (ISO/IEC 27002:2022)	Jak to zastosować w tej migracji	Neutralizowane zagrożenia	PID

O-1	**8.32 Zarządzanie zmianą**	Każdą zmianę migracyjną (konfiguracje, przełączenia, wyjątki) prowadzić formalnie: plan => test => zatwierdzenie => wdrożenie kontrolowane => możliwość wycofania, rejestr zmian i usuwanie wyjątków tymczasowych.	M-1, M-2M-3, M-4, M-5	P/I/D
O-2	5.8 Bezpieczeństwo informacji w zarządzaniu projektami	Włączyć bezpieczeństwo do planu migracji: przeglądy ryzyk przed falami, odpowiedzialności, wymagania minimalne dla konfiguracji i logów.	M-3, M-5	P/I/D
O-3	8.9 Zarządzanie konfiguracją	Ustalić konfigurację bazową (baseline) dla M365/Azure i kontrolować odchylenia (publiczne zasoby, zbyt szerokie uprawnienia, błędne udostępnienia).	M-1, M-2, M-3	P/I/D
O-4	5.14 Transfer informacji + 8.24 Wykorzystanie kryptografii	Bezpieczny transfer danych migracyjnych: kontrolowane kanały, autoryzacja, szyfrowanie w transmisji i ochrona kluczy/sekretów.	M-1	P/I/D
O-5	5.15 Kontrola dostępu + 8.5 Bezpieczne uwierzytelnianie + 8.16 Monitorowanie	Wymuszenie silnego logowania (np. MFA), ograniczenie uprawnień, logowanie działań adminów i logowań oraz alerty na anomalie od początku migracji.	M-2, M-4, M-5	P/I/D