# Modelowe (fikcyjne) przedsiębiorstwo

# Scenariusz bazowy (firma LambaTECH)

## Stan przed lockdownem:

Sieć sklepów stacjonarnych (1000 w Europie) zarządzanych oprogramowaniem sprzedażowo-magazynowym z hostingu (dwie lokalizacje – prod/non-prod i DR), połączenia liniami dedykowanymi, ostatnio zmigrowane na Internet z VPN-em L2L.
Infrastruktura użytkowników i sprzętu w sklepach, tak jak i w centrali (biuro 200 pracowników) zarządzana centralnie z serwerowni (głownie usługi sieciowe i bezpieczeństwa) w biurze i hostingu (usługi biurowe i biznesowe). Krocząca wirtualizacja wszystkich zasobów i usług IT w celu optymalizacji kosztów hostingu (jak na razie zwirtualizowane systemy biznesowe).
System sprzedażowo-magazynowy pisany przez zespół wewnętrznych deweloperów (10 osób) pracujących w centrali, centralne repo kodu (lokalny GIT) i środowiska rozwojowe są w hostingu. Developerzy rozwijają kod na lokalnych maszynach i robią update to repo w hostingu. Pracują w quasi-agile z ambicjami DevOps (zespół się przeszkolił 2 lata temu z AGILE i ustabilizował proces przed pandemią), pipeline nie jest stabilny, są problemy z powtarzalnością procesu i jakością kodu, zgodnie z wynikami audytu firmy zewnętrznej.
System obsługi klienta, karty lojalnościowej, mailingu promocji itp. jest aplikacją webową w architekturze (front/web w DMZ, serwer app w LAN hosting, baza danych w LAN biznes prod hosting synchronizowana z bazą klientów systemu sprzedażowego w LAN hosting. Baza sekretów klientów jest szyfrowana z solą, uwierzytelnienie loginem i hasłem lub przez sieci społecznościowe. Aplikacja ma również moduł dla pracowników firmy (sklepy i biuro) w formie korporacyjnego intranetu z modułem bloga, systemem ticketowym i czatem, baza danych tego modułu jest zlokalizowana w LAN, użytkownicy w hostingu. Pracownicy firmy logują się domenowo. Oba moduły dostępne są w Internecie (serwery web są w DMZ hostingu).
Aplikacja do obsługi klienta jest pisana przez zewnętrzny software house, który ma dostęp do środowisk przez VPN. Dostęp jest ograniczony do zarzadzania kopią repozytorium kodu, CI/CD pipeline, dostęp do produkcji wyłącznie w zakresie konstrukcji CI/CD pipeline. Infrastruktura deweloperów i użytkowników w pełni zarządzana przez software house, tak samo jak zasoby ludzkie, trening, itp.
Standardowe strefy bezpieczeństwa rozciągnięte na całą infrastrukturę (biuro, hosting): DMZ, LAN biznes prod, LAN biznes non-prod, LAN użytkownicy, LAN infra. NGF w formie appliance obecny w hostingu, jako wirtualki w sklepach i biurze, Load balancer i proxy w hostingu, Lokalna infrastruktura DNS, brak 802.1x uwierzytelnienie sieciowe windowsowe, – środowisko serwerowe głownie na starych windowsach (blisko EOL), rezerwacja IP dla serwerów i infrastruktury sieciowej, użytkownicy przez DHCP. VPN terminowany w DMZ. Standardowo TLS 1.2 dla wszystkiego co poza LAN. Szyfrowanie wyłącznie infrastruktury w sklepach i hostingu na poziomie Full Disc Encryption (dla wirtualizacji szyfrowane wyłącznie dane w macierzy, VM-ki nie szyfrowane – standardowe ustawienie).
System backupu jest centralny, w hostingu, z lokalnym obrazem na 24h (max 72h) i backupem zewnętrznym wysyłanym do bunkra danych (dostawca zewnętrzny) jako backup przyrostowy co 24h, nocą).
Środowisko DR jest kompletne i w trybie warm-up (w przypadku awarii jest uruchamiane, sieciowo ruch jest przepinany na usługi w DR, bazy danych replikowane co 1h są podpinane pod aplikacje).
Jedynie operacje IT (głownie admini systemowi, sieciowi i bezpieczeństwa) mają dostęp zdalny do infrastruktury w biurze i hostingu przez korporacyjny VPN z uwierzytelnieniem w domenie i 2FA (tokeny software od RSA lub SymantecVIP), tylko Ci użytkownicy posiadają laptopy służbowe.
Kadra zarządcza ma dostęp do Office365: OneDrive, Excel, Office, Word, Teams, synchronizacja z lokalnego AD do Azure AD w jednym kierunku. Uwierzytelnienie domenowe, uwierzytelnienie warunkowe wyłączone, z uwagi na częste podróże kadry i problemy ze zmiennym IP/geolokalizacja (jest akceptacja ryzyka ze strony MB).

# Scenariusz bazowy (firma LambaTECH)

## W związku z lockdawnem organizacja:

Zamyka stacjonarne sklepy i wysyła pracowników do domu ze sklepów i biura, zostawia tylko 2+2 osoby do obsługi biurowej serwerowni i powierzchni biurowej w trybie zmianowym.
Rozszerza umowę z Microsoftem na uslugi Office365 (E3) dla wszystkich pracowników.
Wykupuje 2 subskrypcje Azure (prod i non-prod) oraz angażuje lokalną firmę konsultingową na migracje usług publicznych z hostingu do Azure w modelu “lift and shift”. Migracja ma zakończyć się audytem bezpieczeństwa realizowanym przez audyt wewnętrzny.
Podpisuje nową umowę z software housem na sklep internetowy z serwisem aukcyjnym oraz pełną obsługą klienta (integracja funkcjonalności wcześniejszego serwisu obsługi klienta, wraz z migracją danych)
Podejmuje decyzje o przeniesieniu wszystkich operacji do Azure w modelu:

- Pracownicy sklepów wspierają sklep internetowy łącząc się bezpośrednio do nowej aplikacji sklepu, do backendu używając integracji z Azure AD.
- Pracownicy biura pracują na wirtualnych desktopach w Azure i Office365.
- Cała komunikacja wewnętrzna odbywa się wyłącznie przez MS Teams i outlooka.
- Administratorzy i wsparcie operacji pracują zdalnie na służbowych laptopach używając wcześniejszego VPN-a z software tokenem i uwierzytelnieniem domenowym.
- Wszyscy pracownicy firmy zostają skierowani na szkolenie z obsługi MS Teams-a i Office365 w trybie zdalnym przez Teamsa. Administratorzy Azure dostają vouchery na egzaminy Microsoftu (szkolenia są za darmo).

Gdzie to możliwe, rozwiązania chmurowe mają zastąpić wcześniejsze modele, jeśli nie są dostępne w Azure, to dopuszczone są inne usługi chmurowe. I tak, GIT jest zastąpiony Githubem, wewnętrzne systemy rozwiązaniami in-housowymi. Marketing silnie inwestuje w rebranding marki i modelu inwestując w integrację z SocialSelling.

Po trzech miesiącach intensywnych prac migracyjnych firma funkcjonuje w modelu:

- Powstała platforma sklepu internetowego z interaktywnym wsparciem klienta i serwisem aukcyjnym umożliwiającym transakcje z użyciem kart płatniczych, bramek płatności, oraz krypto walut.
- Całość platformy jest hostowana w Azure region EU, w ramach dwóch subskrypcji prod i non-prod, kazda w jednej strefie dostępności (AZ).
- Zgodnie ze strategia lift&shift bazy danych maja 24-78 snapshoty jak poprzednio, tylko ze w Azure, we właściwej strefie (AZ).
- Dostawca zewnętrzny i jego rozwiązanie jest nadal używane dla backupu, tym razem zdalnie, udostępniając bezpieczny buckety w AWS dla przyrostowych backupów z Azure

Marketing zbudował silna markę przy współpracy z zewnętrzną agencją reklamową tworząc system SocialSelling (użycie sieci społecznościowych do reklamy i sprzedaży produktów) zintegrowanej z platformą.
System SocialSelling jest dostarczony przez zewnętrznego dostawce z chmury Google, interfejsu je się przez API.
Azure AD jest głównym systemem zarzadzania tożsamością dla pracowników, wdrożenie MFA i warunkowego dostępu zakończyło się przerwą usług na dobę z uwagi na masowe lockdowny i problemy ze zmiennym IP pracowników pracujących z domu (głownie admini, którzy raz występowali jako IP domowy, raz IP biura z powodu VPN-a).
CI/CD pipeline jest w chmurowo “natywne” będąc zbudowane z chmurowych produktów i usług w implementacji Azure lub przez API/webHook do innych subskrypcji w Azure lub innych chmurach.
Narzędzia bezpieczeństwa są również chmurowe, z dużym naciskiem na użycie rozwiązań Microsoftu w zakresie Azure (Guard, WAF).
Management zadowolony ze współpracy z Software Housem rozszerzył umowę o aplikację mobilną dla platformy sklepu i aukcji, która obecnie jest w fazie beta testów dla zaproszonych klientów.
Baza zarejestrowanych klientów aktywnych od uruchomienia serwisu w dniu 1 Czerwca 2021 to ok. 500 000 użytkowników (po migracji danych ze starego sklepu i platformy wsparcia klienta).
Firma jest notowana na giełdzie i ostatnie kursy pokazały znaczny wzrost akcji o ponad 5%.

Wynik audytu wewnętrznego dla nowego modelu nie daje jednoznacznej odpowiedzi koncentrując się na aspektach umowy z dostawcami firm trzecich i problemami w zakresie:
A) bezpośredniego zastosowania w nowym modelu procedur dla starych polityk bezpieczeństwa;
B) testem zaimplementowanych kontroli w nowym modelu operacyjnym (niejasna interpretacja w środowisku chmurowym, za krótki okres testu kontroli).

FIRMA FIKCYJNA