Opis sytuacji:

Cześć Drogi Architekcie!

Witam Cię ponownie, ale tym razem w kolejnej przygodzie, jaką jest tożsamość w Chmurach. Jeśli nadal uważasz, że nie wiesz o niej zbyt wiele to proponuję jeszcze raz przejść przez wszystkie filmy oraz linki do tych lekcji. Wiem, że linków sporo, dlatego zachęcam do analizy i wniknięcia w szczegóły.

Pamiętasz, kiedy planowałeś swoją migrację do Chmury?

Kiedy miałeś napisać plan migracji i zdecydować jak podejść do takiego wyzwania w dużej firmie o ogromnej skali przetwarzania?

W tym tygodniu nadal jesteś architektem, który migruje całe środowisko swojej firmy do Chmury.

W trakcie migracji jedne z aplikacji migrowałeś do usług IaaS drugie do PaaS. Możliwości zapewne jest wiele ale czas połączyć wiedzą o aplikacjach z wiedzą o tożsamości a to wszystko polane sosem hybrydowości.

Zadanie

Napisz proszę jakbyś podszedł do architektury zarządzania tożsamością w Azure?

A tak konkretnie:

1. Jakie usługi wykorzystasz i dlaczego? Jakich nie wykorzystasz i gdzie? Bądź pragmatyczny.
2. Jakie polityki logowania (jak MFA czy inne) możesz użyć by cały proces uczynić bezpieczniejszym? Zobacz, co faktycznie jest dostępne, oceń pod kątem przydatności i wygody korzystania.
3. Jakich usług bezpieczeństwa chciałbyś włączyć i w jakim zakresie by to wszystko działało w dobrze znany sposób?
4. Jakie aspekty, związane z tożsamością i w jaki sposób będzie monitorował?

Na koniec - jeśli Ci się uda - policz, ile to wszystko będzie Cię kosztowało :)

Nie pracujemy w aptece, przyjmij jakieś założenia i policz zgrubne kwoty.

#TYDZIEN10.1

To zacznę od założeń na jakich będę bazował i które wydają mi się istotne:

- migracja będzie stopniowa, także przez pewien okres czasu muszę mieć 2 DC

- firma dla której robimy migracje to jakiś duży biznes e-commerce

1. Jakie usługi wykorzystasz i dlaczego? Jakich nie wykorzystasz i gdzie? Bądź pragmatyczny.

Wykorzystam:

- Azure Active Directory & AD Connect – z racji na to, że podczas migracji będziemy mieć 2 DC, a chcemy aby nasi pracownicy mogli się uwierzytelniać z usługami chmurowymi, potrzebować będziemy Azure AD wraz z AD Connectem na potrzeby synchronizacji usług AD.

- Azure AD Connect Health – na pewno na początku i w trakcie migracji, aby zwiększyć możliwości monitorowania i wglądu w on-premowe jednostki które będą miały dostęp do Office 365, czy uwierzytelniały z AAD. Jest to rekomendowane w dokumentacji.

- App Registration – nie wiem na ile to osobna usługa a na ile część AAD, ale na pewno wykorzystam ją w celach uwierzytelniania różnych aplikacji działających w obrębie moich systemów

- Azure Key Vault – jeden z elementów migracji NIE lift-and-shift, na pewno będę chciał użyć tej usługi do przechowywania kluczy, haseł i certyfikatów używanych przez migrowane systemy

- Azure AD B2C – z racji na to że mamy wielu klientów B2C dobrze będzie mieć usługę która pozwoli np. na korzystanie z naszego sklepu klientom za pomocą ich np. kont Facebookowych

- Azure AD PIM – zdecydowanie tak, nie jestem w tej dziedzinie ekspertem, ale zawsze wydawało mi się że posiadanie takiej wiedzy i możliwości dla administratora to coś co musi być. Więc jeżeli nie bawimy się w organizacje a jesteśmy poważną firmą, używam!

- Azure AD Application Proxy – w trakcie migracji systemów on-prem które wymagają uwierzytelniania na tradycyjnych dla on-prem zasadach

Nie wykorzystam:

- Azure AD DS – z tego co rozumiem, jest to swego rodzaju alternatywa dla klasycznego Windows AD, więc o ile zakładam że na czas migracji utrzymuje AD w on-prem DC, to nie korzystam z tej usługi. Rozważyłbym dopiero w momencie, gdy będę chciał wyłączyć on-premowe DC. Bardzo proszę o feedback czy dobrze kombinuję 😊

1. Jakie polityki logowania (jak MFA czy inne) możesz użyć by cały proces uczynić bezpieczniejszym? Zobacz, co faktycznie jest dostępne, oceń pod kątem przydatności i wygody korzystania.

- MFA – użycie tego wydaje mi się trochę skomplikowane, ze względu na różne wersje (<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-whichversion>) mam wrażenie, że potrzebuję obu: np. chce mieć synchronizację z AAD dla hashy haseł, no ale tez na 100% będę miał jeszcze w trakcie migracji jakieś apki wystawione przez IIS. Także po migracji opcja „MFA in the cloud”, ale w trakcie chyba żadna. Póki co nie uwzględniam tego w obliczeniach

- Password protection – wygląda bardzo fajnie, minus taki że wspieranie tego dla Windows Server AD jest obecnie w preview. Na pewno zdecydowałbym się na zastosowanie chmurowe, jest to jeden z ficzerów AAD.

1. Jakich usług bezpieczeństwa chciałbyś włączyć i w jakim zakresie by to wszystko działało w dobrze znany sposób?

- Azure Security Center – tak naprawdę to chyba głównie ze względu na to, że taka migracja to duży krok dla organizacji i zawsze lepiej się dodatkowo zabezpieczyć niż nie. Możemy coś przeoczyć lub przytrafi nam się jakiś inny losowy / niechciany wypadek, któremu możemy w ten sposób zaradzić (lub zwiększyć prawdopodobieństwo że podejmiemy kroki).

- Key Vault – nie chcę przechowywać kluczy, haseł i certyfikatów w miejscach do których sam dodatkowo muszę zatroszczyć się o wszystkie aspekty bezpieczeństwa, a Key Vault jest zintegrowany chyba z każdą usługą z której do tej pory korzystałem i dobrze się sprawdza

- ASG – migrujemy, więc pewnie na początku będzie bardzo dużo VM-ek, a to bardzo przystępny sposób na blokowanie i zezwalanie na ruch pomiędzy kolejnymi tierami aplikacji

- enkrypcja – nie chcę tutaj jakoś wchodzić w szczegóły, bo opcji jest wiele, ale będę się starał znaleźć jakiś złoty środek (żeby nie szyfrować po kilka razy na każdym z kroków)

- Azure DdoS Protection – nie wiem, trochę za drogo jak na to na ile sam znam temat 😊 póki co nie inwestuję, ale na pewno poruszyłbym temat z trochę bardziej zorientowanym gronie, czy jest to faktycznie warte swojej ceny

1. Jakie aspekty, związane z tożsamością i w jaki sposób będzie monitorował?

- Azure Monitor (AD activity logs)

Wycena:

Wyceniałem troche na oko, szczególnie Key Vault :)