***Kontakt dla prasy:***

*Agnieszka Juraszczyk*

*+48 883 357 638*

*E-mail:* [*agnieszka.juraszczyk@capgemini.com*](file:///C%3A%5CUsers%5Cakmiecik%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CEP33X1N0%5Cagnieszka.juraszczyk%40capgemini.com)

***Kontakt dla prasy:***

*Aleksandra Witkowska*

*+48 693 407 831*

*E-mail:* *aleksandra.witkowska@linkleaders.pl*

**10 kluczowych czynników dla udanej transformacji chmurowej**

**Transformacja cyfrowa przedsiębiorstw i migracja do chmury to zmiany, które radykalnie poprawiają sprawność, wydajność i bezpieczeństwo firm. Jednak bez jasnych celów biznesowych i planu, taka zmiana może być dużym wyzwaniem. Aby uniknąć problemów i dobrze go przeprowadzić, eksperci przygotowali listę 10 kluczowych czynników, które umożliwią sprawną cyfrową transformację.**

Transformacja do chmury nie jest już hipotetyczną koncepcją ani marketingowym hasłem. Dziś organizacje mają realną szansę na zdecydowaną poprawę sprawności, innowacyjności, efektywności kosztowej i odporności poprzez przejście na oparty na chmurze, cyfrowy model operacyjny. Jakie czynniki mają wpływ na pomyślną implementację rozwiązań chmurowych?

**Planowanie migracji i modernizacji aplikacji**

Przeniesienie aplikacji do chmury jest jednym z kluczowych czynników napędzających transformację – zapewnia zupełnie nowy poziom elastyczności, wydajności i oszczędności w porównaniu z modelami lokalnymi. Migracja setek, a czasem tysięcy aplikacji do chmury, przy użyciu metod dostosowanych do celów biznesowych, składa się z dwóch powiązanych ze sobą kroków. Pierwszy z nich to ocena portfela aplikacji, a drugi – rzeczywista transformacja.

* Ten pierwszy krok ocenia naszą obecną sytuację. Ocena portfela aplikacji pozwala obrać docelowe rozwiązania oraz najlepsze ścieżki migracji. Na podstawie analizy i pełnej znajomości naszego portfela aplikacji oraz wszystkich elementów przyszłego rozwiązania (w tym modelu migracji, rodzaju rozwiązania dostawcy chmury IaaS, PaaS, SaaS itp.), poznajemy docelowy koszt jaki wiąże się z przeprowadzeniem tej zmiany, TCO (ang. *total cost of ownership,* całkowity koszt posiadania) – komentuje **Artur Kmiecik, Head of Cloud and Data Services CIS** **w Capgemini Polska.**

**Wykonywanie migracji i modernizacji aplikacji**

Drugim, powiązanym procesem jest wykonanie planu zbudowanego podczas analizy portfela w chmurze. Transformacja chmury aplikacji składa się z trzech etapów: przygotowania, planowania i samej transformacji. Wybór metodologii będzie oddziaływał na wymagany czas i działania, które należy wykonać na każdym etapie, a docelowo będzie miał wpływ na wyniki. Faza ta jest w pełni zautomatyzowana i zapewnia wykonanie wdrożenia, testowania i synchronizacji. Kompletnym wdrożeniem zarządzają narzędzia do implementacji i konfiguracji infrastruktury. Następnie przeprowadza się testy. Istnieją dwa etapy testowania: automatyczny test infrastruktury oraz test akceptacji wykonywany przez użytkowników aplikacji. Pierwszy etap oparty na automatyzacji wpływa na oszczędność czasu i minimalizuje ryzyko wystąpienia błędów. Ostatnim krokiem jest synchronizacja – aktualizuje aplikację docelową, przesyłając ostatnie dane operacyjne zarejestrowane w aplikacji źródłowej, aby zminimalizować przerwy w świadczeniu usług. Wreszcie po zakończeniu aktualizacji następuje przejście do nowego systemu dla wszystkich użytkowników, co kończy migrację.

**Bezpieczeństwo i zgodność w chmurze**

Modele chmury publicznej wykorzystują zabezpieczenia oparte na współodpowiedzialności, dlatego ważne jest wbudowanie zabezpieczeń w celu ochrony przed lukami i wykorzystanie chmury do usprawnienia procesów zapewniania zgodności. Organizacje muszą wziąć pod uwagę planowanie ochrony w chmurze w zakresie zarządzania tożsamością i dostępem, ochrony danych, bezpieczeństwa aplikacji i infrastruktury. Firmy muszą wdrażać strategie zarządzania dostępem, aby mieć pewność, że potencjalne problemy informatyczne organizacji nie zostaną powielone w chmurze (zarządzanie tożsamością, zapewnienie bezpieczeństwa danych i nadzór nad nimi są zawsze obowiązkiem właściciela danych i nie są udostępniane ani zlecane na zewnątrz).

* Obowiązki te muszą być jasno określone w umowach o świadczeniu usług i dostosowane do nadrzędnego modelu zapewniania bezpieczeństwa organizacji. Zawsze rekomenduje przestrzeganie standardów i certyfikatów bezpieczeństwa w chmurze, takich jak certyfikaty ISO/IEC 27001, 27017/18 i innych, zgodnych z najnowszymi warunkami rynkowymi oraz naszymi wymaganiami organizacji – dodaje **Artur Kmiecik, Head of Cloud and Data Services CIS** **w Capgemini Polska.**

**Zapewnienie jakości (QA)**

Zapewnienie jakościowej transformacji musi uwzględniać rozmaite scenariusze, takie jak narażenie na ryzyko i skrócenie czasu wprowadzania na rynek. Organizacje „przechodzące na chmurę” mogą przyjąć model DevSecOps oraz praktyki ciągłego testowania i monitorowania jakości. Automatyzacja jest tu istotnym elementem. Aby skorzystać ze sztucznej inteligencji, eksperci ds. jakości będą potrzebować wiedzy i szkolenia w zakresie danych i modelowania statystycznego, natomiast narzędzia QA powinny umożliwiać walidację interfejsu użytkownika, wzorców i wizualizacji, a zespoły powinny obejmować zarówno ekspertów QA, jak i zespoły biznesowe.

**Testy**

Testowanie jest podstawą silnego, elastycznego planu rozwoju oprogramowania, który wspiera potrzeby i oczekiwania biznesowe. Organizacje muszą jednak przejść tu od tradycyjnego do bardziej nowoczesnego podejścia. Zapewni to efektywny i wydajny program, który z kolei wpłynie na bezproblemową obsługę klienta i pozwoli lepiej zarządzać ryzykiem. Na rynku istnieją platformy zapewniające holistyczne rozwiązania skoncentrowane na doświadczeniu klienta, które umożliwiają organizacjom przejście od tradycyjnych metod do nowoczesnej inżynierii jakości. Firmy powinny również rozważyć przyspieszenie inwestycji w umiejętności i ciągłe testowanie rozwiązań w swoich zespołach Agile i DevOps. Aby to osiągnąć, muszą wyposażyć międzyfunkcyjne zespoły Agile w wystarczającą wiedzę oraz umożliwić automatyzację QA i dostarczanie środowiska testowego. Skuteczne i wydajne zarządzanie środowiskami testowymi z ustrukturyzowaną automatyzacją może przynieść organizacji znaczące korzyści i oszczędności.

**DevSecOps**

DevSecOps łączy zespoły ds. rozwoju, bezpieczeństwa i operacji i przyspiesza czas wprowadzania produktów na rynek, stosując technologie umożliwiające ciągły rozwój rozwiązań. Kluczowe zalecenia dotyczące efektywnej realizacji działań w chmurze obejmują koncentrację na stałym doskonaleniu środowiska projektów i platform. Skonfigurowane potoki Blueprint i DevSecOps należy opracować wstępnie na różnych platformach. Wymaga to zdobywania wiedzy w zakresie dostosowywania, instalacji i integracji rozwiązań i narzędzi CI/CD, jakości, zarządzania, komunikacji i orkiestracji środowisk oraz wdrażania akceleratorów w celu optymalizacji środowiska pracy DevSecOps (RPA, QA, dashboardy, Cognitive QA, automatyzacja testów, integracja z chatbotami itp.).

**Ekonomia chmury i FinOps**

Zrozumienie ekonomii adopcji chmury ma kluczowe znaczenie dla biznesowego uzasadnienia transformacji, a jeszcze bardziej krytyczne dla fazy realizacji. Jednak zarządzanie kosztami w chmurze i osiąganie celów redukcji kosztów to wyzwanie, które wiele organizacji uważa za trudne do osiągnięcia. W rzeczywistości ekonomia chmury powinna być integralną częścią wszystkich działań transformacyjnych. W fazie realizacji musi dotyczyć zarządzania FinOps, usług dostawców chmury oraz analizy i optymalizacji kosztów.

* Podejście do zarządzania kosztami powinno obejmować coś więcej niż posiadanie dźwigni do uruchomienia działań kontrolnych lub optymalizacyjnych. Ważne jest, aby stworzyć podstawy zarządzania FinOps usprawniające działalność organizacji. To wymaga połączenia profili technicznych i biznesowych oraz umiejętności identyfikowania obszarów do optymalizacji i podejmowania decyzji zapewniających osiągnięcie celów ekonomicznych. Istotne jest dostosowanie do procesów biznesowych w celu zachowania elastyczności oferowanej przez rozwiązania chmurowe przy jednoczesnym zapewnieniu spójności w korzystaniu z usług i ich wpływu ekonomicznego – komentuje **Artur Kmiecik, Head of Cloud and Data Services CIS** **w Capgemini Polska.**

**Zarządzanie**

Wdrożenie chmury to złożony proces, co wynika m.in. z mnogości dostawców i usług, wyzwań związanych z bezpieczeństwem, czy czynników zewnętrznych, takich jak obowiązujące regulacje. Aby sprostać tym wyzwaniom, kluczowy jest odpowiedni model zarządzania. Brak nadzoru może generować dodatkowe koszty i odstępstwa od dobrych praktyk zarządzania chmurą, a działania naprawcze mogą być żmudne i kosztowne. Zarządzanie musi koncentrować się na wszystkich aspektach migracji i powinno obejmować wszystkich interesariuszy oraz zapewniać wsparcie wykonawcze dla przyjęcia chmury. Mechanizm zarządzania musi obejmować system oceny i kontroli, który pomoże sprawnie przeprowadzić cały proces oraz skoncentrować się na mierzeniu efektywności i biznesowej wartości dodanej, a także definiować procesy pomiaru korzyści w chmurze.

**Zautomatyzowane operacje IT**

W pełni zautomatyzowane operacje IT oparte na chmurze, to kierunek, do jakiego dąży branża IT, by wspierać organizacje na drodze cyfrowej. Model produktowy jest skoncentrowany na wynikach, a wskaźniki KPI są zawsze powiązane z wynikami biznesowymi. Zespół produktowy powinien składać się z osób o różnych umiejętnościach i ściśle współpracować we wszystkich aspektach rozwoju, aby zapewnić optymalne wyniki, od dostarczania po prowadzenie zespołu SCRUM do rozwoju, przez potok CI/CD i ostatecznie – wydanie produktu. Jest to model, w którym wszyscy dzielą odpowiedzialność za maksymalizację szybkości i zwinności.

**Zrównoważony rozwój**

Odpowiedzialność za zmiany klimatyczne i redukcję emisji dwutlenku oraz zrównoważony rozwój to kluczowe czynniki w realizacji odpowiedzialnej transformacji w chmurze. Taka transformacja powinna być zaplanowana z wyprzedzeniem, a w całym procesie należy pamiętać o działaniach takich, jak wyznaczenie osób odpowiedzialnych za zarządzanie energią. Te osoby powinny stale kwestionować planowanie wszystkich jednostek operacyjnych, zaszczepiając nastawienie polegające na monitorowaniu zużycia energii i próbach optymalizacji. Obejmuje to wewnętrzne i zewnętrzne zużycie energii dla wszystkich części ogólnej konfiguracji IT i stanu docelowego.

Capgemini rekomenduje organizacjom mierzenie i monitorowanie zużycia energii przez aplikacje oraz stałą ocenę wpływu działów IT na środowisko. Firmy powinny mieć wgląd w redukcję emisji CO2 poprzez strategie transformacji, takie jak konsolidacja, migracja do chmury i/lub wycofywanie aplikacji. Stawianie na „zielone rozwiązania” wszędzie tam, gdzie to możliwe, pozwoli na wdrożenie zrównoważonej transformacji cyfrowej – a tylko taka dziś powinna mieć miejsce.

**O Capgemini**

Capgemini to światowy lider w dziedzinie doradztwa w zakresie transformacji i zarządzania biznesem poprzez wykorzystanie mocy technologii. Celem Grupy jest dążenie do odpowiedzialnej społecznie, zintegrowanej i zrównoważonej przyszłości, w której potencjał ludzki jest wspierany nowymi technologiami. Capgemini jest odpowiedzialną i wielokulturową organizacją, liczącą ponad 300 000 pracowników zatrudnionych w prawie 50 krajach. Dzięki silnemu 50-letniemu dziedzictwu i szerokiej wiedzy branżowej cieszy się zaufaniem swoich klientów, a także jest zdolna kompleksowo zaspokoić ich potrzeby biznesowe: od strategii i projektowania rozwiązań po działania operacyjne napędzane przez dynamicznie rozwijający się i innowacyjny świat technologii chmury, danych, sztucznej inteligencji, łączności, oprogramowania, inżynierii cyfrowej i platform. W 2020 roku Grupa odnotowała globalne przychody w wysokości 16 miliardów euro.

Get The Future You Want | [www.capgemini.com](http://www.capgemini.com#_blank)