Jak odnieść sukces w procesie transformacji cyfrowej - sześć newralgicznych punktów

OVHcloud

vmware®

Chmura obliczeniowa mocno zakorzeniła się w sektorze IT. W związku z transformacją cyfrową we wszystkich branżach firmy coraz częściej wybierają strategię multicloud, aby lepiej dostosować się do nowych wymagań rynku. Kluczowym elementem tego podejścia jest chmura prywatna, która jest uważana za bezpieczniejszą niż chmura publiczna .

Choć firmowa chmura prywatna zapewnia większą kontrolę nad środowiskiem fizycznym i ogromne możliwości adaptacji, jej budowa wiąże się z kilkoma problemami.

Incydenty bezpieczeństwa

Naruszenia ochrony danych, łamanie mechanizmów uwierzytelnienia, hakowanie interfejsów i API - nie ma tygodnia, abyśmy nie słyszeli o incydentach bezpieczeństwa. Wieści te nie pomagają rozwiać obaw związanych z bezpieczeństwem chmury obliczeniowej.

W związk z tym wiele firm utwierdza się w przekonaniu, że ich dane są najbezpieczniejsze w ich własnych środowisku chmurowym. Tymczasem w rzeczywistości środowiska hostowane w chmurze są równie bezpieczne jak te hostowane lokalnie, a nawet bezpieczniejsze. Są one projektowane i utrzymywane przez ekspertów, którzy rozumieją wyzwania związane z bezpieczeństwem chmury i doskonale wiedzą, jak zapobiegać zagrożeniom.

Ataki DDoS

Ataki typu Distributed Denial of Service (DDoS) są poważnym problemem dla wszystkich firm działających w obszarze rozwiązań cyfrowych. Z biegiem lat metody cyberprzestępców stają się coraz bardziej wyrafinowane, a wraz z nowymi technologiami, takimi jak Internet Rzeczy (IoT), pojawiają się nowe zagrożenia.

Atak DDoS przeciąża serwer WWW, a jeśli się powiedzie, sprawia, że strona internetowa staje się niedostępna przez wiele godzin, a nawet dni. Może to spowodować utratę przychodów i zaufania klientów. Ochrona Anty-DDoS nie jest już więc dla firm jedynie dodatkiem, ale stała się podstawowym systemem bezpieczeństwa. Należy jednak pamiętać, że ochrona wdrożona w infrastrukturze lokalnej nigdy nie dorówna skuteczności systemów do zwalczania ataków stosowanych przez dostawców usług cloud.

[1] *Źródło: Infobrief IDC, czerwiec 2019.*

"Jako dostawca chmury, neutralizujemy ponad 2000 ataków DDoS każdego dnia. Nasz system Anty-DDoS domyślnie chroni wszystkich klientów. Wynika to z bardzo prostej przyczyny: jeśli atak DDoS nie zostanie zmitygowany, zakres szkód może znacznie wykroczyć poza pierwotny cel. Dzieje się tak dlatego, że atak obejmuje również wszystkie sąsiadujące ze sobą w szafie serwery. VAC (kombinacja technologii opracowanych przez OVHcloud w celu neutralizowania ataków DDoS) aktywuje się po wykryciu ataku. Jednak w przypadku klientów, którzy mają specyficzne potrzeby w zakresie bezpieczeństwa, zapewniamy stałe filtrowanie ruchu, innymi słowy, VAC jest włączony na stałe".

Jakub Słociński, Network Innovation Manager w OVHcloud

System zabezpieczeń fizycznych i redundancja

W większości przypadków właściciele zewnętrznych centrów danych nie zapewniają firmom takich samych zabezpieczeń fizycznych, co może stanowić ryzyko dla danych. Tymczasem renomowane centrum danych działa jak forteca. Dostęp do niego jest ściśle monitorowany i jest on ogrodzony drutem kolczastym. Systemy monitoringu wizyjnego i detekcji ruchu są na stałe włączone, podobnie jak systemy wykrywania i gaszenia pożaru.

Aktualnie wysoka dostępność i niezawodność są kluczowymi elementami wielu usług IT. Osiągnięcie tego samego poziomu redundancji dla lokalnej chmury prywatnej byłoby niezwykle trudnym zadaniem. Podwójne zasilanie elektryczne, generatory prądu, urządzenia UPS i redundantne łącza sieciowe zwiększają koszty utrzymania i wymagają wysokiego poziomu wiedzy specjalistycznej w firmie.

Wyzwania dotyczące zgodności

Standard PCI DSS określa ponad 250 punktów kontrolnych oraz środków ochrony, które należy wdrożyć, aby bezpiecznie przetwarzać dane kart płatniczych. Chmura prywatna zapewnia większą kontrolę nad bezpieczeństwem, ale nie ułatwia zachowania zgodności z przepisami.

Gwarancja zgodności powinna zawsze znajdować się na pierwszym miejscu, zwłaszcza gdy mamy do czynienia z wieloma rodzajami danych, takich jak dane kart płatniczych, wrażliwe analizy biznesowe czy dane klientów. Uzyskanie zgodności jest procesem czasochłonnym i kosztownym, często wymagającym zatrudnienia przez firmę eksperta znającego odpowiednie przepisy. Ponadto zespół IT musi stale monitorować systemy, opracowywać przejrzyste procedury dotyczące incydentów bezpieczeństwa oraz stosować szyfrowanie danych.

Problemy związane z wydajnością

W dynamicznym środowisku chmurowym trudno przewidzieć, jak zmiany wprowadzone na poziomie infrastrukturalnym wpłyną na funkcjonowanie aplikacji, ponieważ nawet prosta aktualizacja oprogramowania może zaburzyć równowagę zamkniętego ekosystemu.

Aby mieć pewność, że w pełni wykorzystujesz infrastrukturę, wprowadź ciągły proces sprawdzania wydajności chmury. W przypadku każdego nowego wdrożenia i kluczowej zmiany należy przeprowadzić test wydajności, najlepiej zautomatyzowany, który pomoże ujawnić potencjalne problemy na wczesnym etapie projektu. Stosowanie takiego procesu chroni firmę przed niepotrzebnymi kosztami i pozwala zachować ścisłą kontrolę nad relacją ceny do wydajności.

Overbooking zasobów

Niezależnie od tego, czy budujesz prywatną chmurę w oparciu o OpenStack czy VMware, zawsze stajesz przed tym samym wyzwaniem: jak osiągnąć zwinność i skalowalność, zarządzając wewnętrzną infrastrukturą? W przypadku utrzymywania własnej infrastruktury zwiększenie wydajności wymaga użycia większej ilości sprzętu. Zespoły IT nie są w stanie precyzyjnie przewidzieć potrzebnej wydajności, dlatego często zamawiają zasoby z nadwyżką, aby mieć pewność, że w razie potrzeby dysponują odpowiednią ich ilością. Efektem takiego działania są jednak wysokie koszty inwestycyjne i niski potencjał skalowalności.

Trwają dyskusje, czy infrastruktura lokalna naprawdę może stać się „chmurą”, ponieważ definicja chmury podkreśla elastyczność i skalowalność bez konieczności inwestowania w dodatkowy sprzęt. Choć wiele osób uznaje, że chmura prywatna oznacza po prostu infrastrukturę lokalną, nie do końca jest to zgodne z rzeczywistością. Chmura prywatna to infrastruktura wykorzystywana wyłącznie przez jeden podmiot. Jej zasoby nie są współdzielone, lecz odizolowane i dedykowane. Warunek ten spełnia hostowana chmura prywatna, która zapewnia środki niezbędne do uzyskania zwinności i zwiększenia wydajności operacyjnej, przy jednoczesnym ograniczeniu typowych zagrożeń związanych z chmurami korporacyjnymi. W środowisku hostowanej chmury prywatnej część kontroli i odpowiedzialności za bezpieczeństwo jest przekazywana zaufanemu dostawcy usług. W związku z powyższym wybór odpowiedniego dostawcy, który posiada udokumentowane doświadczenie w zakresie bezpieczeństwa, ma kluczowe znaczenie dla sprostania tym wyzwaniom.

OVHcloud jest globalnym i wiodącym w Europie dostawcą chmury, zarządzającym 400 000 serwerów w 32 własnych centrach danych na czterech kontynentach. Od dwudziestu lat Grupa wykorzystuje zintegrowany model, który zapewnia jej pełną kontrolę nad łańcuchem wartości: począwszy od projektowania własnych serwerów, poprzez zarządzanie należącymi do niej centrami danych, po budowanie i utrzymywanie własnej globalnej sieci światłowodowej. To unikatowe podejście umożliwia OVHcloud wspieranie, w sposób niezależny, wszystkich potrzeb 1,6 miliona klientów z ponad 140 krajów. OVHcloud oferuje klientom rozwiązania najnowszej generacji, łączące wysoką wydajność, przewidywalną cenę i pełną kontrolę nad danymi, wspierając w ten sposób ich nieograniczony rozwój.