Podręcznik zabezpieczeń platform chmurowych

Spis treści

Najważniejsze wnioski

1

W sytuacji idealnej dostawca chmury powinien umożliwiać integrację systemu zarządzania tożsamością przedsiębiorstwa Klienta ze swoją platformą, a w każdym przypadku oferować godne zaufania rozwiązanie do zarządzania tożsamością, z którego Klient będzie mógł korzystać stosownie do własnych wymagań.

2

Po czym poznać platformę chmurową, której można zaufać? Otóż należy sprawdzić, czy jest ona wyposażona w dobrze zintegrowane firewalle, grupy bezpieczeństwa, opcje mikrosegmentacji oparte na obciążeniach i zaufane hosty obliczeniowe.

3

Dostawca chmury powinien oferować rozwiązania, w przypadku których pracownicy używają własnych kluczy (BYOK), co pozwoli przedsiębiorstwu Klienta na wyłączne zarządzanie kluczami obejmujące wszystkie pamięci masowe na dane, a także usługi.

4

W przypadku kontenerów najlepszą procedurą zabezpieczeń jest ich skanowanie pod kątem słabych punktów zabezpieczeń zarówno przed wdrożeniem, jak i w trakcie działania.

5

Zabezpieczenie platformy chmurowej musi umożliwiać efektywną kontrolę dostępu, działanie na poziomie obciążeń, szczegółowe śledzenie aktywności oraz integrację z systemami lokalnymi.

Nowa koncepcja zabezpieczeń aplikacji chmurowych

Coraz więcej firm przenosi swoje zasoby cyfrowe do modelu chmurowego na potrzeby tworzenia aplikacji i zarządzania obciążeniami. Migracja ta powoduje jednak, że efektywność tradycyjnych modeli zabezpieczeń na brzegu sieci szybko spada. Zabezpieczenia brzegowe, choć wciąż są niezbędne, już nie wystarczają. Dane i aplikacje w chmurze znajdują się poza tradycyjnymi granicami przedsiębiorstwa, dlatego wymagają nowych typów zabezpieczeń.

Przedsiębiorstwa przechodzące do modelu chmurowego lub planujące wdrożenia aplikacji w chmurze hybrydowej muszą uzupełnić tradycyjne zabezpieczenia brzegowe technologiami, które chronią obciążenia w chmurze. Należy zatem sprawdzić, w jaki sposób dostawca chmury chroni środowiska informatyczne firmy Klienta od poziomu infrastruktury w górę. Zaufanie do zabezpieczeń platformy stało się głównym kryterium wyboru takiego dostawcy.

Czynniki wpływające na bezpieczeństwo chmury

Ochrona danych i zachowanie zgodności z przepisami należą do głównych czynników wpływających na bezpieczeństwo chmury, choć jednocześnie stanowią bariery utrudniające migrację do niej. Czynniki te odnoszą się do wszystkich aspektów programowania i eksploatacji systemów. W przypadku aplikacji w chmurze dane mogą być rozproszone między różnymi składnicami obiektów, usługami przetwarzania danych i chmurami, co stwarza wiele frontów potencjalnych ataków. Ataki są inicjowane nie tylko z zewnątrz, a ich sprawcami są nie tylko cybergangi stosujące wyrafinowane metody. Jak wynika z niedawno przeprowadzonych badań, 53% respondentów stwierdziło u siebie ataki wewnętrzne w ciągu poprzednich 12 miesięcy.[1]

Pięć podstawowych aspektów bezpieczeństwa w chmurze

Przedsiębiorstwa, które potrzebują specjalnych zabezpieczeń w związku z używaniem platform chmurowych, oczekują od dostawców, aby byli zaufanymi partnerami technologicznymi. W związku z tym dostawcę chmury należy ocenić na podstawie następujących pięciu aspektów bezpieczeństwa, które mają związek z konkretnymi wymaganiami firmy:

1. **Zarządzanie tożsamością i dostępem:** Uwierzytelnianie, sprawdzanie tożsamości i kontrola dostępu
2. **Bezpieczeństwo sieci:** Ochrona, izolacja i segmentacja
3. **Ochrona danych:** Szyfrowanie danych i zarządzanie kluczami
4. **Bezpieczeństwo aplikacji i metodyka DevSecOps:** Testy bezpieczeństwa i ochrona kontenerów
5. **Widoczność i analiza danych:** Monitorowanie i analizowanie dzienników, przepływów i zdarzeń w celu wykrycia wzorców

Weryfikacja tożsamości i zarządzanie dostępem na platformie chmurowej

Każda interakcja z platformą chmurową zaczyna się od weryfikacji tożsamości oraz określenia, kto lub co bierze udział w interakcji (administrator, użytkownik, a nawet usługa). W środowisku opartym na interfejsach API usługi przyjmują własną tożsamość, więc możliwość bezpiecznego i dokładnego wywołania interfejsu API do usługi na podstawie tej tożsamości jest niezbędna do efektywnego uruchamiania aplikacji chmurowych.

Warto poszukać dostawców, którzy oferują spójną metodę uwierzytelniania i potwierdzania tożsamości podczas uzyskiwania dostępu do interfejsu API oraz obsługi zgłoszeń serwisowych. Potrzebne są również identyfikacja i uwierzytelnianie użytkowników końcowych uzyskujących dostęp do aplikacji w chmurze. Przykładowo platforma IBM Cloud wykorzystuje usługę App ID, aby umożliwić programistom integrowanie procesu uwierzytelniania z ich aplikacjami mobilnymi i WWW.

Silne uwierzytelnianie sprawia, że nieuprawnieni użytkownicy nie uzyskają dostępu do systemów chmurowych. Zarządzanie tożsamością i dostępem (ang. identity and access management – IAM) na platformie jest bardzo ważne. Dlatego przedsiębiorstwa mające już systemy IAM powinny szukać dostawców, którzy oferują ich integrację. Integracja taka często jest oparta na technologii federacji tożsamości, która łączy identyfikator i atrybuty określonej osoby w wielu systemach.

Dlaczego należy uwierzytelniać zgłoszenia serwisowe?

W architekturach opartych na mikrousługach interfejsy API umożliwiają komunikację i udostępnianie danych między aplikacjami. Uruchomiona aplikacja wykorzystuje interfejsy API do wywoływania usług potrzebnych do wykonania różnych operacji (na przykład aplikacja Klienta może wywołać usługę dotyczącą składnicy obiektów dla danych). Realizując żądanie, sama usługa obiektowej pamięci masowej może wywołać usługę zarządzania kluczami, aby pozyskać klucze szyfrowania potrzebne do odszyfrowania danych. W ramach obsługi użytkownika aplikacja może wykorzystać interfejsy API na potrzeby pozyskania danych identyfikacyjnych użytkownika, przesyłania zawartości między aplikacjami (np. z określonej aplikacji do Twittera) oraz ustalania lokalizacji użytkownika w celu obsługi specyficznych dla niej danych. **Wszystkie te punkty integracji stwarzają wyzwania dotyczące bezpieczeństwa.**

Dostawca chmury powinien oferować spójną metodę uwierzytelniania tożsamości użytkowników i usług, które wymagają dostępu do interfejsu API lub do określonej usługi. Oczywiście w ramach uwierzytelniania wszystkie sesje i transakcje związane z żądaniem dostępu powinny być zapisywane w dzienniku na potrzeby audytu. **Interfejsy API i usługi często stanowią cenną własność intelektualną, w związku z czym Klient nie chce, aby każdy mógł z nich korzystać.**

Warto poprosić potencjalnego dostawcę chmury o udowodnienie, że jego architektura i systemy IAM obejmują wszystkie podstawowe elementy. Przykładowo na platformie IBM Cloud zarządzanie tożsamością i dostępem jest oparte na kilku podstawowych funkcjach (patrz rys. 1):

Tożsamość

- Każdy użytkownik ma unikalny identyfikator
- Usługi i aplikacje są oznaczone za pomocą identyfikatorów usług
- Zasoby są identyfikowane i obsługiwane za pomocą nazwy zasobu chmurowego (ang. cloud resource name – CRN)
- Po uwierzytelnieniu użytkowników i usług wydawane są tokeny określające ich tożsamość

Zarządzanie dostępem

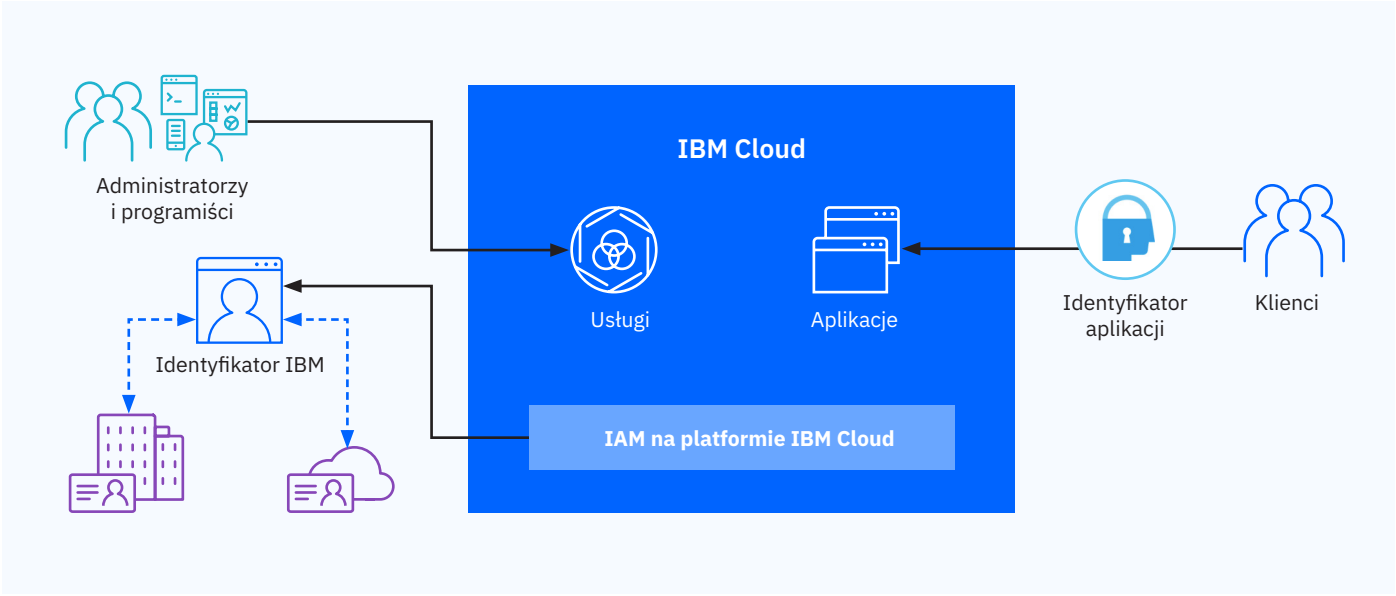
- Gdy użytkownicy i usługi próbują uzyskać dostęp do zasobów, system IAM określa, czy taki dostęp i inne działania są dozwolone
- Działania, zasoby i role są określane przez usługi
- Administratorzy określają strategie, które przypisują użytkownikom role i zezwolenia dotyczące różnych zasobów
- Ochrona rozszerza się na interfejsy API, funkcje chmury i zasoby zaplecza udostępniane w chmurze

Podczas oceny zabezpieczeń oferowanych przez dostawcę chmury należy sprawdzić, czy istnieje lista kontroli dostępu z nazwami wspólnych zasobów, która pozwoli ograniczyć liczbę użytkowników nie tylko do określonych zasobów, lecz również operacji wykonywanych przy ich użyciu. Zapewnia to ochronę danych przed dostępem ze strony nieautoryzowanych użytkowników wewnętrznych i zewnętrznych.

Rozszerzenie usług dostawcy tożsamości w przedsiębiorstwie (ang. Enterprise Identity Provider – Enterprise IdP) na chmurę jest szczególnie użyteczne w przypadku tworzenia aplikacji chmurowych na bazie istniejących aplikacji korporacyjnych, które wykorzystują usługę Enterprise IdP. Użytkownicy Klienta mogą łatwo logować się zarówno w aplikacjach chmurowych, jak i bazowych bez konieczności używania wielu systemów lub identyfikatorów. Uproszczenie systemów i procesów to cel, do którego zawsze warto dążyć.

Najważniejsze wnioski

W sytuacji idealnej dostawca chmury powinien umożliwiać integrację systemu zarządzania tożsamością przedsiębiorstwa Klienta ze swoją platformą, a w każdym przypadku oferować godne zaufania rozwiązanie do zarządzania tożsamością, z którego Klient będzie mógł korzystać stosownie do własnych wymagań.



Rysunek 1. Odseparowanie elementów klastra zarządzanych przez dostawcę i przez klienta.

Nowa definicja izolacji i ochrony sieci

Wielu dostawców chmur wykorzystuje segmentację sieci, aby ograniczyć dostęp do znajdujących się w niej urządzeń i serwerów. Dostawcy tworzą również wirtualne odizolowane sieci na bazie infrastruktury fizycznej i automatycznie ograniczają użytkownikom lub usługom dostęp do nich. Te i inne podstawowe technologie zabezpieczeń sieci są niezbędne w każdej platformie chmurowej, której można zaufać.

Dostawcy sieci oferują technologie zabezpieczające, od firewalli aplikacji WWW po wirtualne sieci prywatne i rozwiązania ograniczające skutki ataków typu „odmowa usługi", jako usługi w zakresie bezpieczeństwa sieci sterowanej programowo z opłatą za używanie. Należy uwzględnić następujące technologie jako najważniejsze zabezpieczenia sieci w erze przetwarzania w chmurze.

Grupy bezpieczeństwa i firewalle

Klienci korzystający z platform chmurowych często wdrażają firewalle sieciowe w celu zabezpieczenia brzegu sieci (dostępu do wirtualnej chmury prywatnej / dostępu do sieci na poziomie podsieci) oraz tworzą grupy bezpieczeństwa sieci, aby zabezpieczyć dostęp na poziomie instancji. Grupy bezpieczeństwa stanowią dobrą pierwszą linię ochrony, która umożliwia przypisanie uprawnień dostępu do zasobów chmury. Klient może wykorzystać te grupy, aby w łatwy sposób dodawać zabezpieczenia sieci na poziomie instancji w celu zarządzania ruchem przychodzącym i wychodzącym w sieciach publicznych i prywatnych.

Wielu Klientów wymaga kontroli brzegu sieci w celu zapewnienia ochrony sieci i podsieci. Łatwe we wdrażaniu firewalle nadają się do tego znakomicie. Celem firewalli jest ochrona serwerów przed niepożądanym ruchem danych oraz ograniczenie obszaru narażonego na ataki. Dostawcy chmur powinni oferować firewalle zarówno wirtualne, jak i sprzętowe, które umożliwiają konfigurowanie reguł opartych na uprawnieniach dla całej sieci lub podsieci.

Sieci VPN zapewniają oczywiście bezpieczne połączenia od poziomu chmury po zasoby lokalne. Są one niezbędne w przypadku korzystania z chmury hybrydowej.

Mikrosegmentacja

Tworzenie aplikacji w chmurze w formie zestawu małych usług jest bezpieczniejsze, ponieważ usługi takie można od siebie odizolować za pomocą segmentów sieci. Platforma chmurowa powinna umożliwiać stosowanie mikrosegmentacji poprzez automatyzację konfiguracji sieci i udostępnianie sieci. **Aplikacje kontenerowe oparte na modelu mikrousług szybko stają się standardem izolacji obciążeń na coraz większą skalę.**

Najważniejsze wnioski

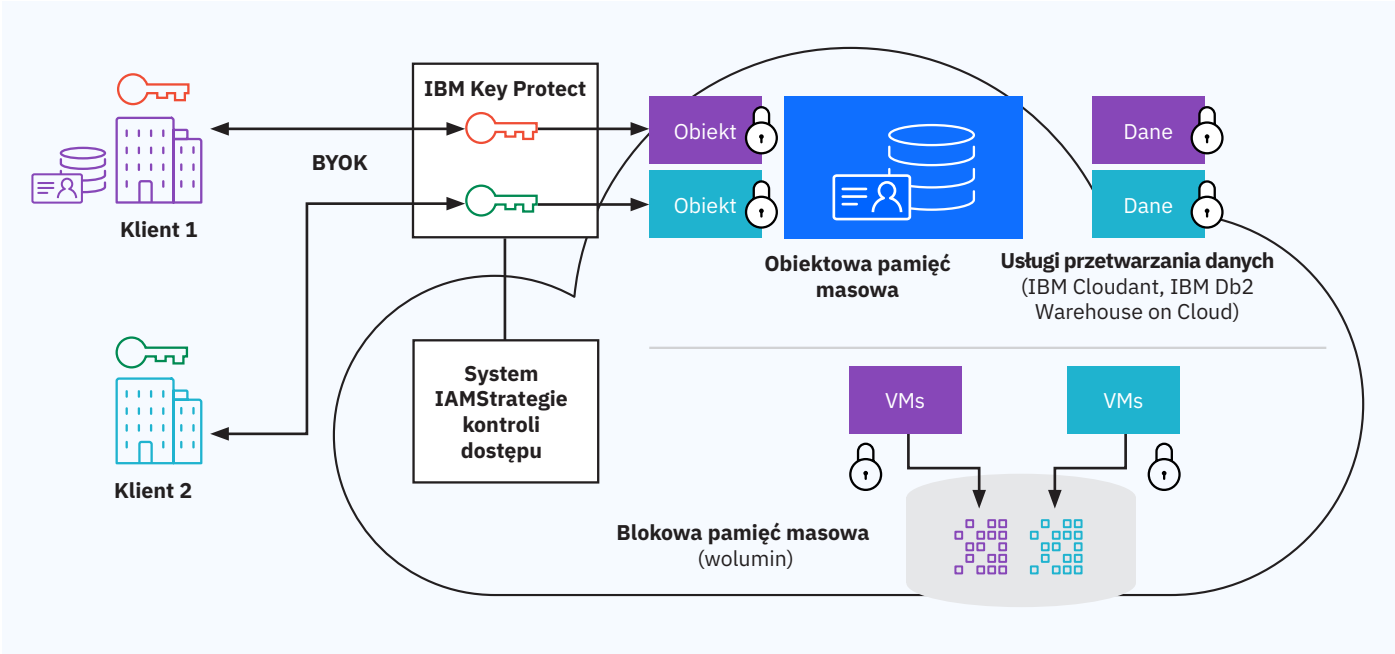
Po czym poznać platformę chmurową, której można zaufać? Otóż należy sprawdzić, czy jest ona wyposażona w dobrze zintegrowane firewalle, grupy bezpieczeństwa, opcje mikrosegmentacji oparte na obciążeniach i zaufane hosty obliczeniowe.

Ochrona danych za pomocą szyfrowania i zarządzania kluczami

Niezawodna ochrona danych jest podstawą bezpieczeństwa w każdym przedsiębiorstwie cyfrowym, zwłaszcza w ściśle regulowanych sektorach, takich jak usługi finansowe i służba zdrowia.

Dane powiązane z aplikacjami w chmurze mogą być rozproszone między wieloma składnicami obiektów, usługami przetwarzania danych i chmurami. Tradycyjne aplikacje mogą mieć własne bazy danych, maszyny wirtualne i dane wrażliwe ulokowane w plikach. W takich przypadkach szyfrowanie danych wrażliwych zarówno podczas ich przechowywania, jak i przesyłania ma znaczenie newralgiczne.

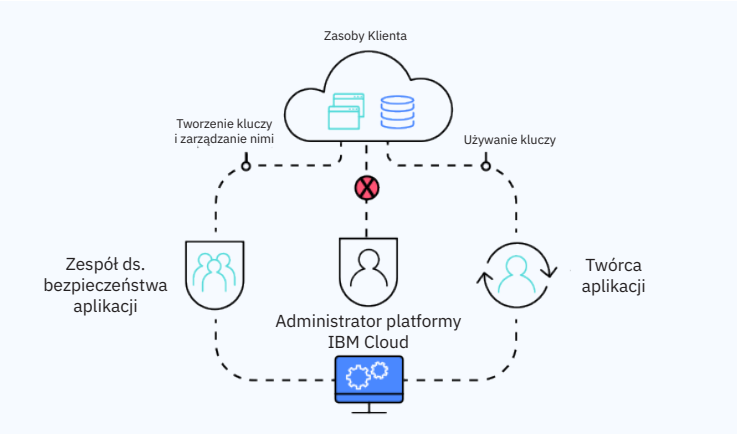
Przedsiębiorstwa słusznie obawiają się, że operatorzy chmur lub inni nieautoryzowani użytkownicy mogą uzyskać dostęp do ich danych bez ich wiedzy. W związku z tym oczekują pełnej widoczności w tym zakresie. **Wymagają więc takich zabezpieczeń, jak kontrola dostępu do danych za pomocą szyfrowania oraz kontrola dostępu do kluczy szyfrowania.** Model, w którym pracownicy używają własnych kluczy (ang. bring-your-own-keys, BYOK), jest obecnie niezbędnym elementem zabezpieczeń chmury. Umożliwia on zarządzanie kluczami szyfrowania z centralnego punktu i sprawia, że klucze główne nigdy nie opuszczają granic systemu zarządzania kluczami. Pozwala również na kontrolowanie wszystkich głównych działań z zakresu zarządzania cyklem życia (patrz rys. 2).



Rysunek 2. Architektura rozwiązania BYOK.

Przechowywanie przez pracowników własnych kluczy (ang. keep your own key, KYOK)

IBM jako jedyny dostawca oferuje rozwiązanie, które pozwala Klientowi być jedynym podmiotem sprawującym nadzór nad swoim kluczem szyfrowania. Takie rozwiązanie zabezpieczające dane pozostaje w 100% prywatne, mimo że jest zainstalowane w chmurze publicznej. Jako jedyna w branży usługa oparta na sprzęcie z certyfikatem FIPS 140-2 na poziomie 4, IBM Cloud Hyper Protect Crypto Services umożliwia zarządzanie kluczami i moduł bezpieczeństwa sprzętu w chmurze (HSM).



Zaufane hosty obliczeniowe

Ważny jest sprzęt: nikt nie chce wdrażać cennych danych i aplikacji na niezaufanym hoście. Dostawcy platform chmurowych, którzy oferują sprzęt z protokołami typu pomiar-weryfikacja-uruchomienie, zapewniają bardzo bezpieczne hosty dla aplikacji wdrożonych w systemie orkiestracji kontenerów.

Intel Trusted Execution Technology (Intel TXT) i Trusted Platform Module (TPM) to przykłady technologii na poziomie hosta, które zabezpieczają platformy chmurowe. Intel TXT chroni przed atakami opartymi na oprogramowaniu, mającymi na celu kradzież informacji wrażliwych poprzez uszkodzenie systemu lub kodu BIOS, lub poprzez zmianę konfiguracji platformy. Intel TPM to sprzętowe urządzenie zabezpieczające, które pomaga w ochronie procesu uruchamiania systemu i zapewnia, że nikt nie naruszy bezpieczeństwa tego procesu i systemu przed udostępnieniem mechanizmu kontrolnego systemu operacyjnego.

Bezpieczeństwo danych przechowywanych i przesyłanych

Wbudowane szyfrowanie oraz używanie przez pracowników własnych kluczy (BYOK) umożliwia zachowanie kontroli nad danymi zarówno w środowiskach lokalnych, jak i w chmurze. To znakomity sposób kontrolowania dostępu do danych w aplikacjach chmurowych. W tym modelu system zarządzania kluczami Klienta generuje klucz lokalnie i przekazuje go do usługi zarządzania kluczami dostawcy. Model ten obejmuje szyfrowanie danych podczas ich przechowywania w różnych typach pamięci, takich jak pamięć blokowa, obiektowa i usługi przetwarzania danych.

W przypadku przesyłania danych bezpieczeństwo komunikacji i transferu jest oparte na protokole TLS/SSL (Transport Layer Security/Secure Sockets Layer). Ponadto szyfrowanie TLS/SSL umożliwia wykazanie zgodności z przepisami oraz zapewnienie bezpieczeństwa i nadzoru bez konieczności stosowania kontroli administracyjnej nad systemem szyfrowania lub infrastrukturą. Aby platforma chmurowa była godna zaufania, musi również udostępniać funkcje zarządzania certyfikatami SSL.

Spełnienie wymagań w zakresie audytu i zgodności z przepisami

Klient może mieć własne klucze szyfrowania i przechowywać je w chmurze bez dostępu dla dostawcy usług. Zapewnia to widoczność informacji wymaganych podczas audytów zgodności z przepisami przeprowadzanych przez dyrektorów ds. bezpieczeństwa informacji oraz umożliwia kontrolę nad tymi informacjami.

Najważniejsze wnioski

Dostawca chmury powinien oferować rozwiązania, w przypadku których pracownicy używają własnych kluczy (BYOK), co pozwoli przedsiębiorstwu Klienta na zarządzanie kluczami obejmujące wszystkie pamięci masowe na dane, a także usługi.

Automatyzacja bezpieczeństwa na potrzeby metodyki DevOps

Zespoły pracujące w środowisku DevOps, które tworzą usługi chmurowe i pracują z technologiami kontenerów, potrzebują rozwiązań umożliwiających integrację mechanizmów zabezpieczeń z coraz bardziej zautomatyzowanym potokiem. Dzięki serwisom wspierającym otwartą wymianę, takim jak Docker Hub, programiści mogą łatwo przyspieszyć przygotowanie obrazów, po prostu pobierając potrzebne elementy. Ten elastyczny model wymaga jednak rutynowej kontroli wszystkich umieszczonych w rejestrze obrazów kontenerów przed ich wdrożeniem.

Automatyczny system skanowania pomaga w zapewnieniu bezpieczeństwa, ponieważ umożliwia wyszukiwanie słabych punktów zabezpieczeń w obrazach przed ich uruchomieniem. Warto zapytać dostawcę platformy, czy pozwala ona firmie na tworzenie reguł (np. „nie wdrażaj obrazów, które mają słabe punkty zabezpieczeń” lub „ostrzeż mnie przed wprowadzeniem takich obrazów do produkcji”) w ramach zabezpieczeń potoku DevOps.

Na przykład usługa IBM Cloud Container Service udostępnia system Vulnerability Advisor (VA), który umożliwia skanowanie kontenerów zarówno w trybie statycznym, jak i dynamicznym. VA kontroluje każdą warstwę każdego obrazu w prywatnym rejestrze chmury klienta w celu wykrycia słabych punktów zabezpieczeń lub szkodliwego oprogramowania przed wdrożeniem obrazu. Ponieważ proste skanowanie obrazów rejestru może nie wykryć takich problemów, jak przeniesienie obrazu statycznego do wdrożonych kontenerów, VA przeprowadza również skanowanie uruchomionych kontenerów pod kątem ewentualnych nieprawidłowości i przedstawia rekomendacje w formie warstwowych alertów.

Najważniejsze wnioski

W przypadku kontenerów najlepszą procedurą zabezpieczeń jest ich skanowanie pod kątem słabych punktów zabezpieczeń zarówno przed wdrożeniem, jak i w trakcie działania.

Oto inne funkcje systemu VA, które pomagają w automatyzacji zabezpieczeń w potoku DevOps:

- **Ustawienia dotyczące naruszania reguł:** Za pomocą systemu VA administratorzy mogą tworzyć reguły wdrażania obrazów oparte o trzy typy sytuacji awaryjnych dotyczących obrazu: zainstalowane pakiety ze znanymi słabymi punktami zabezpieczeń; aktywowane zdalne logowanie; aktywowane zdalne logowanie dla użytkowników, którzy łatwo odgadli hasła.
- **Sprawdzone procedury:** VA sprawdza obecnie 26 reguł opartych na normie ISO 27000, w tym takie ustawienia, jak minimalny wiek i długość hasła.
- **Wykrywanie błędów w konfiguracji zabezpieczeń:** VA oznakowuje każdy błąd konfiguracji, tworzy jego opis i rekomenduje działania w celu jego usunięcia.
- **Integracja z rozwiązaniem IBM X-Force:** VA pobiera dane dotyczące bezpieczeństwa z pięciu źródeł zewnętrznych i ocenia każdy słaby punkt zabezpieczeń według takich kryteriów, jak wektor ataku i stopień jego złożoności oraz dostępność znanej poprawki. System ocen (poziom krytyczny, wysoki, średni lub niski) pomaga administratorom w szybkim określeniu wagi każdego słabego punktu zabezpieczeń oraz ustaleniu priorytetów działań naprawczych.

Jeśli chodzi o działania naprawcze, to system VA nie przerywa działania obrazów w celu wdrażania poprawek. IBM naprawia natomiast wzorcowy obraz w rejestrze i wdraża nowy obraz w kontenerze. Dzięki takiemu podejściu wszystkie przyszłe instancje tego obrazu będą już miały wdrożoną tę poprawkę. Maszyny VM można wciąż obsługiwać w sposób tradycyjny, wykorzystując usługę zabezpieczenia punktu końcowego w celu wdrażania poprawek w maszynach VM oraz usuwania słabych punktów zabezpieczeń w systemie Linux.

Technologia Kubernetes

Jeśli zespoły pracujące w środowisku DevOps używają popularnego oprogramowania do orkiestracji kontenerów Kubernetes, należy upewnić się, czy mogą one nadal używać preferowanych przez siebie narzędzi. Warto również sprawdzić, czy platforma łatwo udostępnia nowe klastry Kubernetes i zarządza już istniejącymi.

Dostawcę platformy chmurowej należy zapytać, czy w ramach swojego systemu Kubernetes obsługuje rozwiązania Calico i Istio – dwa główne komponenty systemu Kubernetes, które pomagają w zabezpieczeniu aplikacji i obciążeń. Calico upraszcza zarządzanie adresami IP przypisanymi do obciążeń w węźle obliczeniowym oraz programuje listy kontroli dostępu w każdym takim węźle obliczeniowym na potrzeby wdrożenia strategii bezpieczeństwa. Wykorzystując definicje reguł skonfigurowane i wdrożone za pośrednictwem etykiet konfiguracji, Istio umożliwia opartą na certyfikatach kontrolę komunikacji między mikrousługami w ramach zasobnika lub klastra Kubernetes.

Tworzenie bezpiecznego i odpornego systemu z wykorzystaniem inteligentnego monitorowania

Podczas migracji do chmury dyrektorzy ds. bezpieczeństwa informacji obawiają się zmniejszenia widoczności i utraty kontroli. W przypadku usunięcia określonego klucza cała chmura przedsiębiorstwa może przestać działać, a zmiana konfiguracji może niespodziewanie przerwać zwrotne połączenie z zasobami lokalnymi lub centrum operacji bezpieczeństwa (ang. security operations center – SOC). Inżynierowie ds. operacyjnych potrzebują więc pełnej widoczności obciążeń chmurowych, interfejsów API, mikrousług itd., i powinni tego wymagać od platformy.

Dostęp do zapisów kontrolnych i dzienników kontroli

Każde uzyskanie dostępu do systemu przez dowolnego użytkownika lub administratora, zarówno po stronie dostawcy chmury, jak i przedsiębiorstwa, powinno być automatycznie rejestrowane. Wbudowane chmurowe urządzenie do śledzenia działań może tworzyć zapisy każdego dostępu do platformy i usług, w tym dostępu poprzez interfejs API, strony WWW i urządzenia mobilne. Przedsiębiorstwo powinno mieć możliwość korzystania z takich dzienników oraz integrowania ich ze swoim centrum SOC.

Analiza danych dotyczących bezpieczeństwa w przedsiębiorstwie

Należy sprawdzić, czy na platformie dostępna jest opcja integrowania wszystkich dzienników i zdarzeń z lokalnym systemem zarządzania informacjami i zdarzeniami dotyczącymi bezpieczeństwa (SIEM) w przedsiębiorstwie (rysunek 3). Niektórzy dostawcy usług w chmurze oferują również monitorowanie bezpieczeństwa z zarządzaniem incydentami i ich raportowaniem, analizą alertów dotyczących bezpieczeństwa w czasie rzeczywistym oraz zintegrowanym widokiem wszystkich wdrożeń hybrydowych.

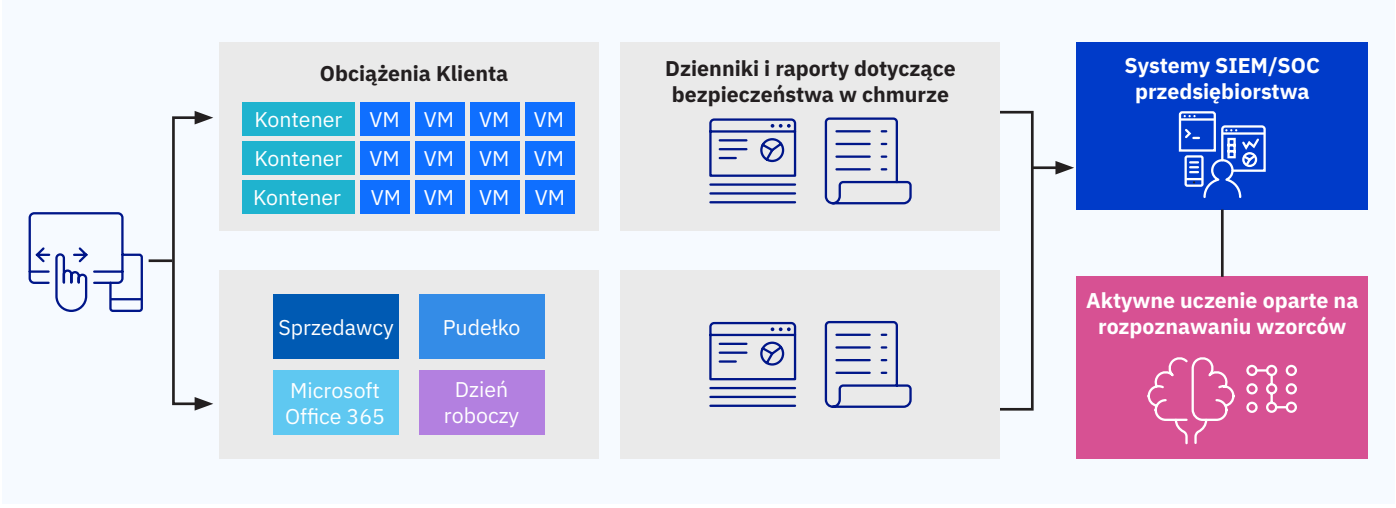
Na przykład IBM QRadar to kompleksowy system SIEM obejmujący rozwiązania do analizy danych dotyczących bezpieczeństwa, który przedsiębiorstwo może rozszerzać w miarę potrzeb. Jego funkcje uczenia maszynowego uczą się na podstawie wzorców zagrożeń w sposób, który pozwala tworzyć odporny system oparty na zabezpieczeniach predykcyjnych.

Zarządzane zabezpieczenia połączone z wiedzą specjalistyczną

Jeśli firma nie dysponuje dużą wiedzą specjalistyczną w zakresie bezpieczeństwa, powinna poszukać dostawcy, który może zarządzać zabezpieczeniami w jej imieniu. Niektórzy dostawcy oferują monitorowanie incydentów dotyczących bezpieczeństwa, analizę danych o zagrożeniach dla różnych branż oraz korelowanie informacji w celu podjęcia odpowiednich działań. Warto też zapytać o konsolę, na której zintegrowane są zarówno wewnętrzne, jak i zarządzane z zewnątrz usługi zabezpieczeń.

Najważniejsze wnioski

Zabezpieczenie platformy chmurowej musi umożliwiać efektywną kontrolę dostępu, działanie na poziomie obciążeń, szczegółowe śledzenie aktywności oraz integrację z systemami lokalnymi.



Rysunek 3. Integracja widoczności chmury z systemem SIEM/SOC przedsiębiorstwa.

Bezpieczeństwo jako czynnik pomagający firmie w osiąganiu sukcesów

Technologia przetwarzania w chmurze odgrywa coraz większą rolę w prowadzeniu cyfrowego przedsiębiorstwa. Dlatego warto poszukać dostawcy, który oferuje odpowiedni zestaw funkcji i mechanizmów kontrolnych oraz zapewnia ochronę danych, aplikacji i infrastruktury będącej podstawą aplikacji obsługi klienta. Rozwiązanie zabezpieczające platformę powinno obejmować pięć głównych obszarów bezpieczeństwa chmury: tożsamość i dostęp, bezpieczeństwo sieci, ochronę danych, bezpieczeństwo aplikacji oraz widoczność i analizę danych. Chodzi o to, aby firma mogła przeznaczać mniej czasu i energii na zajmowanie się technologiami, a więcej na swoją zasadniczą działalność.

Dobrze zabezpieczona chmura zapewnia duże korzyści biznesowe i informatyczne, takie jak:

- **Szybsze osiąganie wymiernych rezultatów:** Zabezpieczenia są już zainstalowane i skonfigurowane, więc zespoły mogą łatwo udostępniać zasoby, szybko tworzyć prototypy rozwiązań do obsługi klienta, oceniać rezultaty, a w razie potrzeby powtarzać procesy.
- **Mniejsze wydatki kapitałowe:** Używając usług zabezpieczających w chmurze, można wyeliminować wiele kosztów początkowych dotyczących np. zakupu serwerów, licencji na oprogramowanie i urządzeń.
- **Niższe koszty administracyjne:** Dostawca zaufanej platformy chmurowej, który oferuje odpowiednie zabezpieczenia, bierze na siebie większą część obciążeń administracyjnych, co obniża koszty przedsiębiorstwa związane z tworzeniem raportów i konserwacją zasobów.

Więcej informacji

Więcej informacji o pięciu głównych obszarach bezpieczeństwa chmury oraz powiązanych z nimi technologiach i usługach IBM można znaleźć tutaj:

Bądź na bieżąco

Blog na temat platformy IBM Cloud

Obserwuj

@IBMcloud
Facebook

Skontaktuj się z nami

LinkedIn
YouTube

IBM Polska Sp. z o.o.
ul. Krakowiaków 32
02-255 Warszawa

Strona WWW IBM znajduje się pod adresem:
ibm.com

[1] Raport Insider Threat 2018 opublikowany w listopadzie 2017 r.: http://crowdresearchpartners.com/portfolio/insider-threat-report