Etyczne hakowanie w chmurze

Chmura obliczeniowa zrewolucjonizowała sposób, w jaki firmy i osoby prywatne uzyskują dostęp do danych, przechowują je i przetwarzają, zapewniając dostęp na żądanie do wspólnej puli zasobów obliczeniowych przez Internet. Chociaż korzyści płynące z chmury obliczeniowej, takie jak skalowalność, opłacalność i elastyczność, są oczywiste, bezpieczeństwo danych i aplikacji hostowanych w chmurze jest kwestią priorytetową. Bezpieczeństwo chmury obliczeniowej obejmuje zestaw praktyk, technologii i zasad mających na celu ochronę poufności, integralności i dostępności danych oraz zasobów w środowiskach chmurowych. Bezpieczeństwo w chmurze to wspólna odpowiedzialność dostawców usług chmurowych (CSP) i ich klientów. Dostawcy usług chmurowych odpowiadają za zabezpieczenie infrastruktury bazowej, sieci i sprzętu fizycznego, podczas gdy klienci odpowiadają za ochronę swoich danych, aplikacji, tożsamości i konfiguracji w ramach usługi chmurowej. Wraz ze wzrostem migracji działalności organizacji do chmury, zrozumienie i wdrożenie skutecznych środków bezpieczeństwa staje się kluczowe dla ochrony przed szeregiem potencjalnych zagrożeń, w tym naruszeniami danych, nieautoryzowanym dostępem i zakłóceniami w świadczeniu usług. To etyczny haker rozumie te zagrożenia i wykorzystuje tę wiedzę, aby je łagodzić. Kluczowe elementy bezpieczeństwa chmury obliczeniowej obejmują zarządzanie tożsamością i dostępem, szyfrowanie, bezpieczeństwo sieci, ochronę danych, zarządzanie zgodnością z przepisami i reagowanie na incydenty. Uwzględnienie tych aspektów zapewnia holistyczne podejście do zabezpieczania informacji i zasobów obliczeniowych w chmurze. Wraz z rozwojem technologii ewoluują również wyzwania i rozwiązania w zakresie bezpieczeństwa chmury. Ten dynamiczny krajobraz wymaga ciągłych wysiłków, aby być na bieżąco z pojawiającymi się zagrożeniami, wymogami zgodności i najlepszymi praktykami w zakresie zabezpieczania zasobów w chmurze. W tym kontekście dobrze zaprojektowana i starannie wdrożona strategia bezpieczeństwa chmury jest niezbędna, aby wykorzystać pełny potencjał chmury obliczeniowej, zachowując jednocześnie najwyższe standardy ochrony danych i prywatności. Omówimy następujące tematy:

- Różne rodzaje usług chmurowych i sposób ich działania
- Różne wdrożenia chmurowe i architektura chmury obliczeniowej
- Omówienie różnic między maszynami wirtualnymi, kontenerami i przetwarzaniem bezserwerowym
- Zagrożenia i ataki w chmurze
- Praktyki bezpieczeństwa w chmurze
- Logi w chmurze

Zrozumienie typów usług w chmurze

Chmura obliczeniowa oferuje szereg rodzajów usług, z których każdy zaspokaja różne aspekty infrastruktury IT i potrzeby aplikacji. Trzy główne rodzaje usług w chmurze to infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS) i oprogramowanie jako usługa (SaaS). Aby przybliżyć Ci rozmiar i zakres chmury, wpis na blogu „Cloud Comparison Cheat Sheet" autorstwa Bytebytego omawia niektóre z różnych usług i technologii chmurowych, w tym AWS, AZURE, Google Cloud Platform (GCP) i Oracle Cloud.

Zrozumienie tych typów usług w chmurze i podmiotów je świadczących pomaga organizacjom wybrać odpowiedni model w oparciu o ich specyficzne wymagania. Niezależnie od tego, czy chodzi o zarządzanie infrastrukturą, tworzenie aplikacji, czy dostęp do rozwiązań programowych, chmura obliczeniowa zapewnia elastyczność i skalowalność dzięki zróżnicowanej ofercie usług. Przyjrzyjmy się bliżej, czym są te usługi.

IaaS

IaaS to model chmury obliczeniowej, który zapewnia zwirtualizowane zasoby obliczeniowe przez Internet. W środowisku IaaS użytkownicy mogą uzyskiwać dostęp do podstawowych komponentów infrastruktury obliczeniowej, takich jak maszyny wirtualne, pamięć masowa i sieć, i zarządzać nimi, bez konieczności inwestowania w sprzęt fizyczny ani jego utrzymywania. Jest to model samoobsługowy, który pozwala organizacjom dynamicznie skalować infrastrukturę IT w zależności od zapotrzebowania, oferując elastyczność i efektywność kosztową.

Kluczowe cechy IaaS to:

• Wirtualizacja: IaaS opiera się na technologii wirtualizacji do tworzenia i zarządzania wirtualnymi instancjami zasobów obliczeniowych, umożliwiając efektywne wykorzystanie sprzętu fizycznego.

• Zasoby na żądanie: Użytkownicy mogą udostępniać i usuwać zasoby obliczeniowe w razie potrzeby, płacąc tylko za wykorzystane zasoby. Ta elastyczność pozwala na efektywną alokację zasobów.

• Skalowalność: Platformy IaaS umożliwiają skalowanie zasobów w następujący sposób:

- Pionowo: zwiększając pojemność pojedynczego zasobu

- Poziomo: dodając więcej zasobów

Pozwala to na elastyczność w obsłudze zróżnicowanych obciążeń.

• Samoobsługa: Użytkownicy mają samoobsługowy dostęp do zasobów obliczeniowych za pośrednictwem interfejsów internetowych lub interfejsów API, co umożliwia im zarządzanie infrastrukturą i kontrolowanie jej bez bezpośredniej interwencji człowieka.

• Zarządzana sieć i pamięć masowa: Oferty IaaS obejmują funkcje sieciowe, takie jak zapory sieciowe i moduły równoważenia obciążenia, a także rozwiązania pamięci masowej do przechowywania i pobierania danych.

• Abstrakcja sprzętowa: IaaS oddziela użytkowników od podstawowej infrastruktury fizycznej, pozwalając im skupić się na zarządzaniu i konfigurowaniu zwirtualizowanych zasobów, zamiast zajmować się konserwacją sprzętu.

IaaS jest szczególnie cenny dla firm, które potrzebują skalowalnego i ekonomicznego rozwiązania do hostowania aplikacji, uruchamiania środowisk programistycznych i testowych lub obsługi zmiennych obciążeń. Popularni dostawcy infrastruktury jako usługi (IaaS) to m.in. Amazon Web Services (AWS), Microsoft Azure i Google Cloud Platform (GCP), Oracle, Linode i Rackspace. Oferują oni szeroką gamę usług, które zaspokajają zróżnicowane potrzeby infrastrukturalne.

PaaS

PaaS to model przetwarzania w chmurze, który zapewnia kompleksową platformę do tworzenia, uruchamiania i zarządzania aplikacjami bez konieczności obsługi infrastruktury bazowej. W środowisku PaaS programiści mogą skupić się na pisaniu kodu i budowaniu aplikacji, podczas gdy dostawca usług chmurowych dba o systemy operacyjne, oprogramowanie pośredniczące, środowiska uruchomieniowe i inne narzędzia programistyczne. Kluczowe cechy PaaS to:

• Frameworki programistyczne: Platformy PaaS oferują wstępnie skonfigurowane frameworki programistyczne, biblioteki i narzędzia, które usprawniają proces tworzenia aplikacji.

• Automatyczne wdrażanie: PaaS automatyzuje proces wdrażania, ułatwiając programistom uruchamianie, skalowanie i zarządzanie aplikacjami bez konieczności zajmowania się zawiłościami związanymi z dostarczaniem infrastruktury.

• Skalowalność: Środowiska PaaS zapewniają funkcje skalowalności, umożliwiając płynne skalowanie aplikacji w miarę wahań zapotrzebowania, często poprzez zautomatyzowane mechanizmy skalowania.

• Usługi baz danych i oprogramowania pośredniczącego: PaaS obejmuje zintegrowane usługi dla baz danych, oprogramowania pośredniczącego i innych komponentów, upraszczając tworzenie i integrację tych elementów z aplikacjami.

• Współpraca: PaaS zachęca do współpracy między zespołami programistycznymi, zapewniając współdzielone środowiska programistyczne, kontrolę wersji i narzędzia do współpracy.

• Zarządzanie bezpieczeństwem i zgodnością: Dostawcy PaaS zajmują się środkami bezpieczeństwa i wymaganiami dotyczącymi zgodności dla infrastruktury bazowej, pozwalając programistom skupić się na tworzeniu bezpiecznych aplikacji.

• Efektywność kosztowa: PaaS redukuje koszty związane z infrastrukturą, ponieważ użytkownicy nie muszą inwestować w sprzęt i oprogramowanie ani nimi zarządzać. Użytkownicy zazwyczaj płacą za zasoby i usługi, z których korzystają.

PaaS jest odpowiedni dla programistów, którzy chcą przyspieszyć cykl życia aplikacji, zmniejszyć złożoność operacyjną i wykorzystać platformę, która abstrahuje znaczną część infrastruktury bazowej. Doskonale nadaje się do tworzenia aplikacji internetowych i mobilnych, a także do tworzenia i wdrażania skalowalnych i elastycznych aplikacji chmurowych. Popularne oferty PaaS to Google App Engine, Microsoft Azure App Service i Heroku.

SaaS

SaaS to model przetwarzania w chmurze, który udostępnia aplikacje oprogramowania przez internet w oparciu o subskrypcję. Jest to jedna z najpopularniejszych usług przetwarzania w chmurze. W modelu SaaS użytkownicy mogą uzyskiwać dostęp do aplikacji i korzystać z nich bez konieczności instalowania, zarządzania ani utrzymywania infrastruktury i komponentów oprogramowania. Aplikacje są zazwyczaj hostowane i obsługiwane przez zewnętrznego dostawcę, a użytkownicy uzyskują do nich dostęp za pośrednictwem przeglądarek internetowych lub interfejsów aplikacji. Kluczowe cechy SaaS to:

• Dostępność: Aplikacje SaaS są dostępne przez internet, co pozwala użytkownikom korzystać z nich z dowolnego urządzenia z połączeniem internetowym i kompatybilną przeglądarką internetową.

• Subskrypcja: SaaS jest zazwyczaj oferowane w oparciu o subskrypcję, w ramach której użytkownicy płacą za oprogramowanie w regularnych odstępach czasu, często co miesiąc lub rok.

• Automatyczne aktualizacje: Dostawcy SaaS zarządzają aktualizacjami oprogramowania, zapewniając użytkownikom stały dostęp do najnowszych funkcji, poprawek zabezpieczeń i ulepszeń bez konieczności ręcznej interwencji.

• Skalowalność: Aplikacje SaaS można szybko skalować, dostosowując je do zmieniających się potrzeb użytkowników lub organizacji, dzięki czemu są odpowiednie dla firm różnej wielkości.

• Multi-tenancy: Aplikacje SaaS działają w modelu multi-tenancy, w którym pojedyncza instancja oprogramowania obsługuje wielu użytkowników lub organizacje, jednocześnie zachowując ich dane i konfiguracje w izolacji.

• Zarządzanie bezpieczeństwem: Środki bezpieczeństwa, takie jak szyfrowanie danych, kontrola dostępu i certyfikaty zgodności, są zazwyczaj zarządzane przez dostawcę SaaS, co zwalnia użytkowników z obaw związanych z bezpieczeństwem infrastruktury i warstw aplikacji.

• Efektywność kosztowa: SaaS eliminuje konieczność inwestowania przez użytkowników w sprzęt, licencje na oprogramowanie i konserwację. Oferuje ekonomiczne rozwiązanie z przewidywalnymi cenami subskrypcji.

Popularne przykłady aplikacji SaaS to narzędzia do zarządzania relacjami z klientami (CRM), takie jak Salesforce, platformy współpracy, takie jak Google Workspace i Microsoft 365, WebEx, Zoom oraz różnorodne rozwiązania oprogramowania dla przedsiębiorstw. SaaS stał się powszechnym modelem dostarczania oprogramowania, zapewniając organizacjom elastyczność i wygodę dostępu do aplikacji i korzystania z nich bez złożoności tradycyjnego wdrażania i zarządzania oprogramowaniem. Usługi te są obsługiwane głównie bezpośrednio przez Internet; istnieją jednak inne metody wdrażania usług, które mogą początkowo nie być jasne. Jednym z nich jest model wdrażania w chmurze, który szczegółowo omówimy w następnej sekcji.

Modele wdrażania w chmurze

Modele wdrażania w chmurze odnoszą się do różnych podejść do hostingu i zarządzania aplikacjami, usługami i danymi w środowiskach przetwarzania w chmurze. Istnieją różne modele wdrażania, a każdy z nich oferuje odmienne zalety i kompromisy. Te różnice pozwalają organizacjom dostosować strategię chmurową do konkretnych potrzeb i wymagań. Podstawowe modele wdrażania w chmurze to:

• Chmura publiczna: Usługi i zasoby chmurowe są udostępniane ogółowi społeczeństwa lub dużej grupie branżowej. Usługi te są własnością, są obsługiwane i utrzymywane przez zewnętrznych dostawców usług chmurowych. Użytkownicy korzystają z tej samej infrastruktury, co zapewnia efektywność kosztową, skalowalność i dostępność.

Przypadki użycia: Idealne dla firm każdej wielkości poszukujących skalowalnych i ekonomicznych rozwiązań bez konieczności początkowej inwestycji w infrastrukturę. Powszechnie stosowane do hostingu stron internetowych, tworzenia i testowania oraz aplikacji SaaS.

• Chmura prywatna: Chmura prywatna oznacza wyłączne korzystanie z zasobów chmurowych przez jedną organizację. Infrastruktura może być hostowana lokalnie lub przez zewnętrznego dostawcę i jest dedykowana specyficznym potrzebom organizacji. Chmura prywatna oferuje zwiększoną kontrolę, bezpieczeństwo i możliwość personalizacji.

Przypadki użycia: Odpowiednie dla organizacji o specyficznych wymaganiach w zakresie bezpieczeństwa i zgodności, wrażliwych danych lub tych, które poszukują większej personalizacji i kontroli nad swoją infrastrukturą. Powszechnie stosowane w branżach takich jak finanse, opieka zdrowotna i administracja publiczna.

• Chmura hybrydowa: Chmura hybrydowa to połączenie środowisk chmury publicznej i prywatnej, umożliwiające współdzielenie danych i aplikacji. Model ten zapewnia elastyczność, umożliwiając organizacjom dynamiczne skalowanie zasobów i spełnianie określonych wymagań biznesowych. Ułatwia przenoszenie danych i obciążeń.

Przypadki użycia: Idealne dla organizacji, które muszą znaleźć równowagę między korzyściami skalowalności chmury publicznej a kontrolą i bezpieczeństwem infrastruktury chmury prywatnej. Powszechnie stosowane do tworzenia kopii zapasowych i odzyskiwania danych, przetwarzania impulsowego oraz aplikacji o zróżnicowanym obciążeniu.

• Multi-Cloud: Multi-Cloud obejmuje korzystanie z usług wielu dostawców usług chmurowych, od różnych dostawców chmury publicznej lub kombinacji chmur publicznych i prywatnych. Organizacje mogą wykorzystać mocne strony różnych dostawców dla określonych usług lub aplikacji.

Przypadki użycia: Odpowiednie dla firm, które chcą uniknąć uzależnienia od jednego dostawcy, zwiększyć odporność i zoptymalizować koszty, wybierając najbardziej odpowiednie usługi od różnych dostawców chmury. Używane powszechnie w celu zróżnicowania obciążenia pracą, odzyskiwania danych po awarii i uniknięcia uzależnienia od jednego dostawcy.

• Chmura społecznościowa: Chmura społecznościowa to rodzaj modelu wdrażania chmury obliczeniowej, który jest współdzielony przez kilka organizacji o wspólnych zainteresowaniach, wymaganiach lub obawach. W tym modelu określona społeczność użytkowników, taka jak firmy, agencje rządowe lub instytucje badawcze, wspólnie korzysta z infrastruktury chmurowej i nią zarządza. Chmura społecznościowa zapewnia współdzielone środowisko obliczeniowe, dostosowane do unikalnych potrzeb i wymagań bezpieczeństwa uczestniczących organizacji. Kluczowe cechy chmury społecznościowej to:

- Współdzielona infrastruktura: Wiele organizacji w ramach danej społeczności korzysta z tej samej infrastruktury chmurowej, w tym zasobów obliczeniowych, pamięci masowej i sieci.

- Wspólne problemy: Organizacje w chmurze społecznościowej często mają wspólne interesy, potrzeby zgodności z przepisami lub wymagania branżowe, co sprawia, że współpraca na platformie chmury współdzielonej jest korzystna.

- Dostosowywanie i kontrola: Użytkownicy chmury społecznościowej mają większą kontrolę i możliwości dostosowywania w porównaniu z chmurami publicznymi. Pozwala to organizacjom dostosować środowisko chmurowe do swoich specyficznych potrzeb, jednocześnie współdzieląc infrastrukturę z innymi członkami społeczności.

- Współdzielenie kosztów: Uczestnicy chmury społecznościowej mogą skorzystać z porozumień o współdzieleniu kosztów, co pomaga zmniejszyć ogólne wydatki związane z utrzymaniem i zarządzaniem infrastrukturą.

- Bezpieczeństwo i zgodność: Chmury społecznościowe często rozwiązują specyficzne problemy związane z bezpieczeństwem i zgodnością, z którymi borykają się organizacje uczestniczące w projekcie. Gwarantuje to, że usługi chmurowe spełniają standardy branżowe lub regulacyjne.

Przykładami wdrożeń chmury społecznościowej są wspólne działania w opiece zdrowotnej, gdzie wiele organizacji opieki zdrowotnej współdzieli platformę chmurową w celu bezpiecznego zarządzania i wymiany poufnych danych pacjentów. Model chmury społecznościowej jest szczególnie odpowiedni w scenariuszach, w których grupa organizacji o wspólnych celach może osiągnąć efektywność operacyjną i kosztową, współdzieląc dedykowaną chmurę.

Wybór odpowiedniego modelu wdrożenia zależy od takich czynników, jak wymagania bezpieczeństwa, przepisy dotyczące zgodności, potrzeby skalowalności i względy budżetowe. Organizacje często stosują podejście hybrydowe lub wielochmurowe, aby wykorzystać zalety różnych modeli wdrożenia w zależności od zróżnicowanych potrzeb biznesowych. Oprócz informacji zawartych w niniejszym dokumencie, oficjalna dokumentacja Narodowego Instytutu Standardów i Technologii (NIST) opisuje Architekturę Referencyjną Przetwarzania w Chmurze NIST, opisując inne koncepcyjne komponenty przetwarzania w chmurze. Przyjrzyjmy się informacjom, jakie dostarczają na temat środowisk chmurowych.

Architektura referencyjna chmury obliczeniowej NIST

NIST zapewnia ogólną, koncepcyjną architekturę referencyjną wysokiego poziomu, wykraczającą poza proste definicje. NIST wymienia główne komponenty chmury obliczeniowej i ich role w przetwarzaniu w chmurze, a także ma na celu ułatwienie zrozumienia standardów, zastosowań, potrzeb i cech przetwarzania w chmurze. Architektura chmury obliczeniowej NIST definiuje pięć głównych obszarów w następujący sposób:

• Konsument chmury: Użytkownicy usług dostawcy chmury, niezależnie od tego, czy są to firmy, czy osoby fizyczne.

• Dostawca chmury: Osoba, grupa lub inny podmiot odpowiedzialny za świadczenie usług zainteresowanym stronom.

• Audytor chmury: Osoba lub podmiot zdolny do niezależnej oceny wydajności, bezpieczeństwa i działania systemów informatycznych usług chmurowych i ich wdrożenia.

• Broker chmury: Organizacja kontrolująca sposób użytkowania, realizacji i dostarczania usług chmurowych, a także pośrednicząca w sporach między dostawcami chmury a konsumentami.

• Dostawca chmury: Organizacja łącząca usługi związane z chmurą od dostawców do konsumentów.

NIST definiuje również pięć powodów, dla których organizacje mogą wdrażać usługi chmurowe, i ich korzyści, które obejmują:

• Większa pojemność: Korzystając z chmury obliczeniowej, organizacje nie muszą zajmować się etapami i martwić o pojemność swojej infrastruktury. Platforma dostawcy chmury technicznie ma nieograniczoną pojemność.

• Większa prędkość: W środowiskach chmurowych czas i koszty konfiguracji i wdrażania nowych usług IT są znacznie skrócone. Wynika to głównie z braku konieczności konfigurowania serwerów i infrastruktury, a także koordynacji wdrażania usług.

• Niższe opóźnienia: Klienci mogą korzystać z chmury obliczeniowej do tworzenia aplikacji za pomocą zaledwie kilku kliknięć, wykonując wszystkie swoje zadania szybko i z minimalnym możliwym opóźnieniem.

• Niższe koszty: Główną zaletą chmury obliczeniowej jest jej niski koszt. Nie ma potrzeby zakupu specjalistycznego sprzętu do danego celu. Wirtualizacja chmury ułatwia wirtualizację sieci, centrów danych, zapór sieciowych, aplikacji i innych usług, co zmniejsza potrzebę kosztownego zakupu sprzętu, skomplikowanej konfiguracji i zarządzania oraz bieżącej konserwacji. Należy jednak ściśle monitorować ten proces, ponieważ wydatki mogą szybko wymknąć się spod kontroli. • Większe bezpieczeństwo: Ponieważ przetwarzanie w chmurze wykorzystuje efektywne zarządzanie poprawkami i aktualizacje zabezpieczeń, bezpieczeństwo to kolejny obszar, w którym technologia ta przoduje. Ochronę przed zagrożeniami związanymi z przetwarzaniem w chmurze zapewniają zasoby defensywne, odzyskiwanie po awarii, skalowanie symbiotyczne i inne usługi bezpieczeństwa. Podobnie jak w przypadku niższych kosztów, deweloperzy i operatorzy mogą wprowadzać luki w zabezpieczeniach i luki w zabezpieczeniach, których nie usunie ogólne łatanie. W środowiskach chmurowych należy pamiętać, że im bardziej niezawodnego rejestrowania i telemetrii potrzebujesz, tym wyższe koszty. Ponadto, wyższe poziomy rejestrowania nie działają wstecz, co oznacza, że jeśli wystąpi incydent, a poziom rejestrowania będzie niewystarczający, odpowiedzi na kluczowe pytania związane z tym incydentem mogą nie być możliwe. Kolejnym obszarem, który musimy omówić przed omówieniem zagrożeń i praktyk bezpieczeństwa w chmurze, są wirtualizacja, kontenery i przetwarzanie bezserwerowe, ponieważ te podtematy mogą być mylące dla osób niezaznajomionych z przetwarzaniem w chmurze.

Zrozumienie maszyn wirtualnych/wirtualizacji

W paradygmacie przetwarzania w chmurze maszyny wirtualne (VM) odgrywają kluczową rolę w dostarczaniu użytkownikom skalowalnych i elastycznych zasobów obliczeniowych. Maszyny wirtualne w chmurze działają podobnie do tradycyjnych maszyn wirtualnych, ale są hostowane i zarządzane w środowiskach chmurowych przez dostawców usług w chmurze (CSP). Użytkownicy mogą konfigurować maszyny wirtualne na żądanie, określając wymagane zasoby obliczeniowe, takie jak moc obliczeniowa, pamięć i pamięć masowa, bez konieczności inwestowania w sprzęt fizyczny i jego utrzymywania. Ta elastyczność pozwala organizacjom dynamicznie skalować moc obliczeniową, dostosowując się do zmieniających się obciążeń i wymagań w sposób ekonomiczny. Maszyny wirtualne w chmurze oferują szereg zalet, w tym:

• Szybkie wdrażanie, efektywne wykorzystanie zasobów i możliwość uruchamiania różnych systemów operacyjnych i aplikacji w odizolowanych środowiskach

• Użytkownicy mogą wybierać spośród różnych wstępnie skonfigurowanych obrazów maszyn wirtualnych lub tworzyć obrazy niestandardowe, aby spełnić określone wymagania.

• Dostawcy usług w chmurze często oferują usługi takie jak automatyczne skalowanie, które automatycznie dostosowuje liczbę instancji maszyn wirtualnych w oparciu o wahania obciążenia. Model cenowy „płać za rzeczywiste wykorzystanie" dodatkowo zwiększa efektywność kosztową, pozwalając użytkownikom płacić tylko za wykorzystane zasoby.

Maszyny wirtualne w chmurze stały się integralną częścią oferty IaaS, stanowiąc podstawę do tworzenia i wdrażania aplikacji w chmurze, zapewniając zwiększoną skalowalność, dostępność i łatwość zarządzania. Wdrażanie infrastruktury chmurowej odbywa się zasadniczo w dwóch rodzajach: maszyny wirtualne i kontenery. Przyjrzyjmy się najpierw kontenerom.

Zrozumienie kontenerów

Kontenery w chmurze zrewolucjonizowały sposób tworzenia, wdrażania i zarządzania aplikacjami, zapewniając lekkie, przenośne i skalowalne rozwiązanie. Hermetyzują aplikację i jej zależności, umożliwiając jej spójne działanie w różnych środowiskach, od programowania, przez testowanie, po produkcję. W chmurze konteneryzacja jest powszechnie wspomagana przez narzędzia do orkiestracji, takie jak Kubernetes, które automatyzują wdrażanie, skalowanie i zarządzanie konteneryzowanymi aplikacjami. Platformy chmurowe, takie jak AWS, Azure i Google Cloud, oferują usługi kontenerowe, które upraszczają proces wdrażania i zarządzania konteneryzowanymi obciążeniami, zapewniając użytkownikom infrastrukturę i narzędzia niezbędne do wykorzystania zalet konteneryzacji. Kontenery oferują szereg korzyści w środowiskach chmurowych, w tym:

• Szybsze wdrażanie aplikacji, lepsze wykorzystanie zasobów i zwiększoną wydajność operacyjną

• Umożliwiają płynne przenoszenie aplikacji między różnymi instancjami w chmurze, a nawet między różnymi dostawcami chmury. Ta przenośność zwiększa elastyczność, umożliwiając organizacjom wybór najbardziej odpowiedniego dostawcy chmury lub konfiguracji chmury hybrydowej w oparciu o konkretne wymagania.

• Kontenery przyczyniają się również do skalowalności, ponieważ można je łatwo replikować i organizować w celu obsługi zróżnicowanych obciążeń.

Podsumowując, kontenery w chmurze umożliwiają programistom i zespołom IT wydajniejsze tworzenie i wdrażanie aplikacji, wspierając bardziej zwinne i responsywne podejście do nowoczesnego tworzenia aplikacji i zarządzania infrastrukturą.

Porównanie kontenerów i maszyn wirtualnych

Kontenery często porównuje się z maszynami wirtualnymi; oba te podejścia są popularnymi metodami wdrażania i zarządzania aplikacjami w środowiskach obliczeniowych, jednak różnią się znacznie, oferując odmienne korzyści i funkcje. Poniższa tabela przedstawia porównanie tych dwóch technologii:

Obszar funkcji: Maszyny wirtualne: Kontenery

Architektura: Maszyny wirtualne działają poprzez emulację całego komputera fizycznego,

w tym pełnego systemu operacyjnego (OS), na hiperwizorze. Każda maszyna wirtualna wymaga osobnej instalacji systemu operacyjnego, co przyczynia się do większego obciążenia w zakresie zużycia zasobów: Kontenery współdzielą jądro systemu operacyjnego hosta i izolują aplikacje na poziomie przestrzeni użytkownika. Pakietują aplikacje wraz z ich zależnościami, bibliotekami i środowiskiem

wykonawczym, zapewniając lekki i wydajny sposób uruchamiania aplikacji w odizolowanych środowiskach, bez potrzeby posiadania pełnego stosu systemu operacyjnego dla każdego kontenera.

Efektywność zasobów: Maszyny wirtualne mają większy zasięg zasobów, ponieważ zawierają pełny system operacyjny, co może prowadzić do większego zużycia zasobów i wolniejszego rozruchu. Maszyny wirtualne wymagają również więcej miejsca na dysku ze względu na duplikację obrazów systemu operacyjnego. Kontenery są lżejsze, ponieważ współdzielą jądro systemu operacyjnego hosta i zawierają tylko komponenty specyficzne dla aplikacji. Przekłada się to na krótszy czas uruchamiania, mniejsze zużycie zasobów i większą wydajność zarówno pod względem pamięci masowej, jak i pamięci operacyjnej.

Izolacja: Maszyny wirtualne zapewniają silną izolację, ponieważ każda z nich korzysta z własnego jądra. Dzięki temu maszyny wirtualne są odpowiednim wyborem w scenariuszach, w których wymagany jest wysoki poziom bezpieczeństwa i niezależność między aplikacjami. Kontenery współdzielą jądro systemu operacyjnego hosta, co czyni je lżejszymi, ale może prowadzić do mniej solidnej izolacji w porównaniu z maszynami wirtualnymi. Jednak postęp w technologiach bezpieczeństwa kontenerów, takich jak przestrzenie nazw i grupy cgroups, znacznie poprawił izolację.

Przenośność: Maszyny wirtualne mogą być mniej przenośne ze względu na różnice w bazowych hiperwizorach i konfiguracjach systemu operacyjnego. Migracja maszyn wirtualnych między różnymi środowiskami może wymagać dodatkowych dostosowań konfiguracji. Kontenery są wysoce przenośne, ponieważ hermetyzują aplikację i jej zależności. Ułatwia to przenoszenie kontenerów między różnymi środowiskami, promując spójność w środowisku programistycznym, testowym i produkcyjnym.

Orkiestracja: Orkiestracja maszyn wirtualnych jest zazwyczaj bardziej złożona i wymaga narzędzi specyficznych dla hiperwizorów. Skalowanie maszyn wirtualnych może być wolniejsze w porównaniu z orkiestracją kontenerów. Narzędzia do orkiestracji kontenerów, takie jak Kubernetes, usprawniły wdrażanie, skalowanie i zarządzanie aplikacjami konteneryzowanymi. Oferują zaawansowane funkcje automatycznego skalowania, aktualizacji kroczących i wykrywania usług.

Podczas gdy maszyny wirtualne zapewniają silną izolację i nadają się do obsługi różnych systemów operacyjnych, kontenery oferują lepszą efektywność wykorzystania zasobów, szybsze wdrażanie i zwiększoną przenośność. Wybór między maszynami wirtualnymi a kontenerami zależy od konkretnych przypadków użycia, wymagań oraz kompromisów, jakie organizacja jest gotowa ponieść w zakresie wykorzystania zasobów i izolacji aplikacji. Często stosuje się połączenie obu technologii, aby wykorzystać ich mocne strony w ramach danej infrastruktury IT. Omówmy teraz przetwarzanie bezserwerowe i jego dokładne dopasowanie do architektury chmury obliczeniowej.

Wprowadzenie do przetwarzania bezserwerowego

Przetwarzanie bezserwerowe, często określane jako Funkcja jako Usługa (FaaS), to model przetwarzania w chmurze, który abstrahuje od tradycyjnej infrastruktury serwerowej, pozwalając programistom skupić się wyłącznie na pisaniu kodu bez konieczności zarządzania serwerami bazowymi ani ich udostępniania. W architekturze bezserwerowej aplikacje są podzielone na pojedyncze funkcje, z których każda jest zaprojektowana do wykonywania określonego zadania. Funkcje te są wyzwalane zdarzeniami i wykonywane w bezstanowych kontenerach, które są automatycznie uruchamiane przez dostawcę chmury w odpowiedzi na określone zdarzenia lub żądania. Ten model eliminuje konieczność martwienia się przez programistów o udostępnianie, skalowanie i konserwację serwerów, ponieważ dostawca chmury zajmuje się tymi aspektami operacyjnymi. W środowisku bezserwerowym

programiści przesyłają swoje fragmenty kodu lub funkcje na platformę chmurową, a platforma zajmuje się resztą. Funkcje są wykonywane na żądanie, automatycznie skalując się w zależności od liczby przychodzących zdarzeń lub żądań. Rezultatem jest wysoce skalowalne i ekonomiczne rozwiązanie, w którym organizacje płacą tylko za rzeczywiste zasoby obliczeniowe zużyte podczas wykonywania funkcji. Przetwarzanie bezserwerowe doskonale sprawdza się w architekturach sterowanych zdarzeniami i mikrousługami, umożliwiając deweloperom szybsze i wydajniejsze tworzenie i wdrażanie aplikacji. Promuje model płatności za rzeczywiste wykorzystanie, zmniejsza obciążenie związane z zarządzaniem infrastrukturą i sprzyja bardziej zwinnemu i responsywnemu podejściu do tworzenia aplikacji w chmurze. Popularne platformy bezserwerowe to AWS Lambda, Azure Functions i Google Cloud Functions. Ze względu na swoją unikalność wiążą się one z pewnymi specyficznymi problemami bezpieczeństwa, które albo nie są istotne, albo mogą nie być powszechne wśród specjalistów ds. bezpieczeństwa. Organizacje muszą uwzględnić te problemy, aby zapewnić ochronę swoich aplikacji i danych. Oto lista kluczowych problemów bezpieczeństwa związanych z przetwarzaniem bezserwerowym:

• Nieodpowiednie uwierzytelnianie i autoryzacja: Zapewnienie odpowiednich mechanizmów uwierzytelniania i autoryzacji ma kluczowe znaczenie w środowiskach bezserwerowych. Nieodpowiednie mechanizmy kontroli mogą prowadzić do nieautoryzowanego dostępu do funkcji i danych wrażliwych.

• Bezpieczeństwo i szyfrowanie danych: Zarządzanie bezpieczeństwem danych staje się krytyczne, zwłaszcza gdy dane są przetwarzane przez funkcje bezserwerowe. Wdrożenie odpowiedniego szyfrowania danych w tranzycie i w spoczynku jest niezbędne do ochrony informacji wrażliwych. • Ataki typu „cold start”: Ataki typu „cold start” występują, gdy funkcja bezserwerowa doświadcza opóźnienia podczas inicjalizacji. Przeciwnicy mogą wykorzystać to opóźnienie do przeprowadzenia ataków w fazie inicjalizacji. Firma Microsoft omawia, jak działa „cold start”: https://azure.microsoft.com/en-us/blog/understanding-serverless-cold-start/

• Bezpieczeństwo zależności: Aplikacje bezserwerowe często opierają się na zależnościach i bibliotekach innych firm. Zapewnienie bezpieczeństwa tych zależności ma kluczowe znaczenie dla zapobiegania lukom w zabezpieczeniach, które mogłyby zostać wykorzystane przez atakujących.

• Ograniczona widoczność i monitorowanie: Platformy bezserwerowe mogą oferować ograniczoną widoczność infrastruktury bazowej. Odpowiednie narzędzia i praktyki monitorowania są niezbędne do skutecznego wykrywania i reagowania na incydenty bezpieczeństwa.

• Niezabezpieczone ustawienia wdrożenia: Błędne konfiguracje podczas wdrażania funkcji bezserwerowych mogą ujawnić luki w zabezpieczeniach. Konieczne jest sprawdzenie i zabezpieczenie ustawień wdrożenia, upewniając się, że są one zgodne z najlepszymi praktykami bezpieczeństwa.

• Ataki typu DoS (Domena Odmowy Usługi): Aplikacje bezserwerowe są podatne na ataki DoS, w których atakujący zalewają system żądaniami, powodując nadmierne zużycie zasobów i potencjalnie wpływając na dostępność funkcji.

• Bezpieczeństwo źródeł zdarzeń: Bezpieczeństwo źródeł zdarzeń uruchamiających funkcje bezserwerowe, takich jak interfejsy API czy kolejki komunikatów, ma kluczowe znaczenie. Zapewnienie prawidłowej walidacji i uwierzytelniania tych źródeł zapobiega nieautoryzowanemu wywołaniu.

• Brak kontroli bezpieczeństwa sieci: Funkcje bezserwerowe często korzystają z infrastruktury sieciowej dostawców chmury. Wdrożenie odpowiednich kontroli bezpieczeństwa sieci i izolacji jest

niezbędne, aby zapobiec nieautoryzowanemu dostępowi lub przemieszczaniu się w obrębie środowiska chmurowego.

• Ograniczone możliwości analizy kryminalistycznej: Tradycyjne metody analizy kryminalistycznej mogą być trudne w środowiskach bezserwerowych. Organizacje muszą dostosować swoje mechanizmy reagowania na incydenty i możliwości analizy kryminalistycznej, aby skutecznie badać incydenty bezpieczeństwa.

• Wyzwania związane ze zgodnością: Spełnienie wymogów regulacyjnych i zgodności może być trudne w środowiskach bezserwerowych. Organizacje muszą zapewnić zgodność swoich aplikacji bezserwerowych z przepisami branżowymi.

• Zależności funkcji i ataki typu side-channel: Należy wziąć pod uwagę zależności między funkcjami bezserwerowymi a potencjalnymi atakami typu side-channel. Przeciwnicy mogą wykorzystać te zależności do uzyskania nieautoryzowanego dostępu lub wydobycia poufnych informacji.

• Kontrola kluczy i tokenów: Klucze dostępu, zazwyczaj dostarczane przez dostawców usług chmurowych, przyznają uprawnienia do interakcji z różnymi zasobami chmurowymi. Prawidłowe zarządzanie tymi kluczami, w tym regularna rotacja i ograniczanie dostępu zgodnie z zasadą najmniejszych uprawnień, pomaga zminimalizować potencjalne zagrożenia bezpieczeństwa, takie jak nieautoryzowany dostęp lub naruszenia danych. Ponadto wdrożenie bezpiecznych praktyk obsługi tokenów, takich jak szyfrowanie, wygasanie tokenów i stosowanie bezpiecznych protokołów komunikacyjnych, poprawia ogólny poziom bezpieczeństwa aplikacji bezserwerowych, chroniąc przed typowymi zagrożeniami, takimi jak kradzież tokenów lub manipulacja.

Cloud Security Alliance (CSA), organizacja skupiająca się na bezpieczeństwie w chmurze, dysponuje zasobami i dokumentami na ten temat, w których omawiane są problemy z uwierzytelnianiem, manipulacją bezserwerową logiką biznesową oraz trwałością danych między wykonaniami. Wszystkie te informacje i wiele więcej można znaleźć na stronie internetowej: https://cloudsecurityalliance.org/. Skoro omówiliśmy już usługi, wdrożenia i architekturę, przyjrzyjmy się bliżej rodzajom zagrożeń i ataków występujących w środowiskach chmurowych.

Zagrożenia i ataki w chmurze

Chmura obliczeniowa zapewnia i oferuje liczne produkty i usługi, które można szybko i efektywnie wdrożyć, czasami w ciągu kilku minut. Jednak ta wygoda jest podatna na pewne ryzyka i zagrożenia. Niektóre z nich obejmują między innymi utratę danych, nadużycia usług, niezabezpieczone interfejsy API, luki w zabezpieczeniach dostawców usług i ataki DDoS. Przyjrzyjmy się bliżej i zobaczmy, jak dokładnie wyglądają te zagrożenia.

Utrata/naruszenie danych

Jednym z najpoważniejszych problemów w chmurze obliczeniowej jest możliwość naruszeń danych. W miarę jak organizacje coraz częściej polegają na usługach chmurowych w celu przechowywania poufnych informacji, nieautoryzowany dostęp do tych danych staje się krytycznym zagrożeniem. Typowe przyczyny naruszeń danych w chmurze to słabe uwierzytelnianie, naruszone dane uwierzytelniające i błędne konfiguracje. Jednym z przykładów jest naruszenie bezpieczeństwa danych w firmie Toyota Motor Company w 2023 roku, gdzie dane ponad pół miliona klientów zostały ujawnione z powodu błędnej konfiguracji ich środowiska chmurowego, po wcześniejszym wykryciu wcześniejszej błędnej konfiguracji, która ujawniła ponad dwa miliony kont.

Nadużywanie usług w chmurze

Nadużywanie usług w chmurze w najprostszej formie polega na znalezieniu używanej usługi w chmurze i wykorzystaniu jej w złośliwych celach. Może to przybierać dwie formy:

• Atakujący wykorzystuje lukę w zabezpieczeniach samej usługi, od Dropbox, przez AWS, po Salesforce. Na tym poziomie atakujący wykorzystuje lukę w zabezpieczeniach, która wykracza poza zakres działania użytkowników usługi.

• Atakujący wykorzystuje konkretną instancję usługi w chmurze. Oto kilka przykładów:

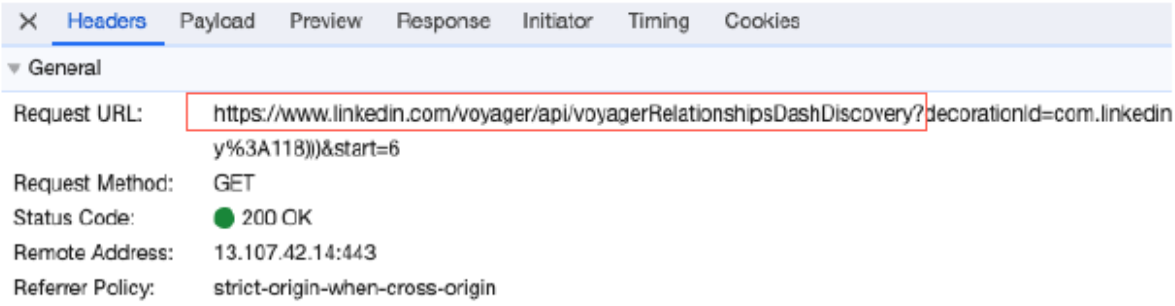
- Organizacja wdrożyła serwer WWW w chmurze i stosowała słabe praktyki kodowania, co spowodowało powstanie luki. Atakujący wykorzystuje to i uzyskuje dostęp do systemu operacyjnego serwera, a następnie do sieci chmurowej klienta.

- Nadużycia usług poczty e-mail Microsoft 365 są powszechnym zjawiskiem. W tym przykładzie użytkownik pada ofiarą ataku phishingowego, w którym jego dane uwierzytelniające zostają naruszone. Atakujący wykorzystuje te dane uwierzytelniające do logowania się do skrzynki pocztowej O365, dzięki czemu może odczytywać i wysyłać wiadomości e-mail w imieniu prawdziwego użytkownika. Mogą również głębiej analizować usługi współdzielone Microsoft, takie jak OneDrive i SharePoint, szukając informacji.

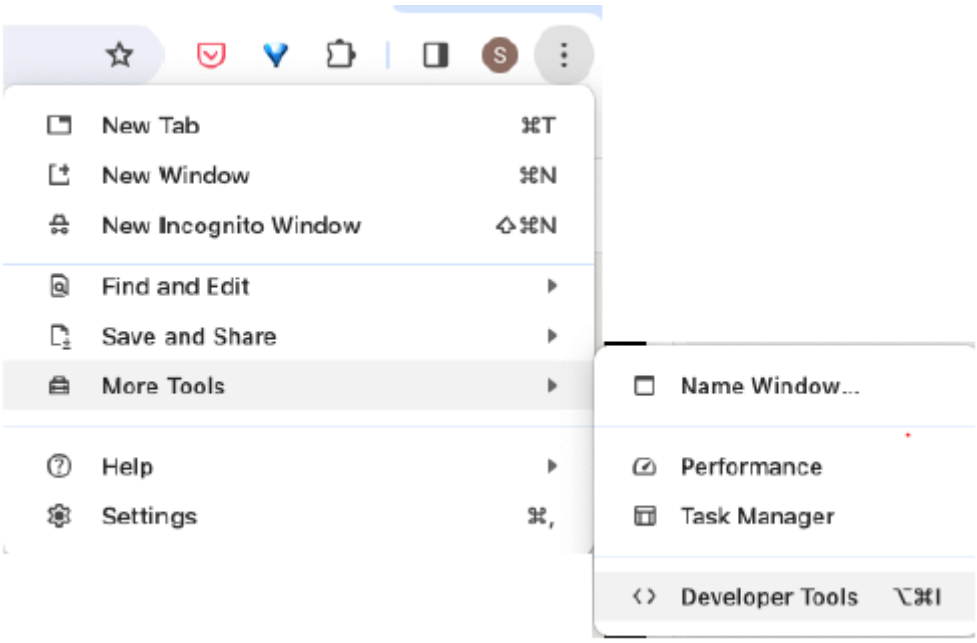
Innym aspektem zagrożeń i ataków w chmurze są niezabezpieczone interfejsy i interfejsy API. Niewłaściwie zabezpieczone interfejsy mogą umożliwić atakującym dostęp do infrastruktury i danych, które nie powinny być dostępne. Przyjrzyjmy się, jak to wygląda.

Niezabezpieczone interfejsy i API

Podczas tworzenia aplikacji i interfejsów użytkownika (UI) w tle wykorzystywane są interfejsy API (Application Programming Interfaces) do odczytu, zapisu i dostępu do danych. To właśnie te interfejsy API, jeśli nie są zabezpieczone, mogą zostać wykorzystane przez atakujących do szkodliwych celów. Można zadać sobie pytanie, jak atakujący znajdują i nadużywają interfejsów API. Istnieje kilka sposobów, od korzystania z narzędzi komercyjnych, takich jak Burp Suite z https://portswigger.net/, który posiada dodatek społecznościowy, po narzędzia programistyczne w przeglądarkach, takich jak Chrome. Poniżej znajduje się przykład wyszukiwania interfejsu API o nazwie voyagerRelationshipsDashDiscovery powiązanego z powiązaniami danej osoby w serwisie LinkedIn:



Aby uzyskać dostęp do narzędzi programistycznych w Chrome, należy poszukać trzech pionowych kropek po prawej stronie okna przeglądarki. Wybierz je, aby wyświetlić menu, a następnie wybierz Więcej narzędzi | Narzędzia programistyczne. Będzie wyglądać podobnie do poniższego zrzutu ekranu:



Po wybraniu otworzy się drugie okno, zapewniające wgląd w przeglądanie, prezentując informacje o sieci, wydajności i pamięci, a także o plikach, do których uzyskiwano dostęp. Zostało ono przeznaczone dla programistów do rozwiązywania problemów i gromadzenia danych o wydajności witryny lub konkretnej strony. Jednak badacze i atakujący wykorzystują je również do gromadzenia podstawowych informacji, które w niektórych przypadkach mogą być wykorzystywane w sposób nadużyciowy. Jednym z przykładów jest wyciek danych z kont LinkedIn w 2021 roku. Wyciek ten dotknął ponad 700 milionów profili LinkedIn. Chociaż wiele danych było już publicznie dostępnych, to istotna była skala, a nie klikanie w profile i ręczne pobieranie informacji. Atakujący wykorzystał interfejs API do uzyskania dostępu do profili na dużą skalę, a następnie pozyskał poszukiwane dane. W tym przykładzie atakujący był w stanie wykorzystać niezabezpieczony interfejs API do celu, do którego nie został on zaprojektowany. Aby uzyskać więcej informacji na temat wycieku, przeczytaj jeden z wielu artykułów, w tym https://www.linkedin.com/pulse/scraped-data-500-million-linkedin-users-being-sold-online-shetty/.

Zabezpieczanie interfejsów API może być trudnym zadaniem, ale można je znacznie zwiększyć dzięki dobremu monitorowaniu i ograniczeniu bezpośredniego dostępu do API.

Niewłaściwe zarządzanie tożsamościami i dostępem

Zarządzanie tożsamościami i dostępem (IAM) odgrywa kluczową rolę w zabezpieczaniu zasobów cyfrowych poprzez zarządzanie i bieżącą kontrolę dostępu użytkowników do systemów i zasobów. Słabości w IAM stanowią poważne zagrożenie dla bezpieczeństwa chmury, podobnie jak bezpieczeństwo kont użytkowników w sieci. IAM jest bramą do sieci chmurowej. Jak można się domyślić, systemy IAM nie są odporne na luki w zabezpieczeniach i ataki. Oto krótki przegląd luk w zabezpieczeniach IAM i typowych ataków:

• Ataki siłowe na hasła: Hakerzy próbują uzyskać nieautoryzowany dostęp, systematycznie wypróbowując wszystkie możliwe kombinacje haseł, aż znajdą właściwą.

• Wypychanie danych uwierzytelniających konta: Atakujący wykorzystują wyciekłe kombinacje nazw użytkowników i haseł z jednej usługi, aby uzyskać nieautoryzowany dostęp do innej, wykorzystując użytkowników, którzy wielokrotnie używają tych samych haseł na wielu platformach.

• Phishing: Cyberprzestępcy nakłaniają użytkowników do ujawnienia swoich danych logowania, podszywając się pod zaufany podmiot za pośrednictwem wiadomości e-mail, fałszywych stron internetowych lub innych oszukańczych metod.

• Zagrożenia wewnętrzne: Złośliwi lub niezadowoleni pracownicy mogą nadużywać swoich praw dostępu, aby naruszyć poufne informacje lub systemy.

• Eskalacja uprawnień: Atakujący próbują uzyskać wyższe uprawnienia dostępu niż pierwotnie przyznane, wykorzystując luki w zabezpieczeniach systemu lub aplikacji.

• Ataki oparte na tokenach: Manipulowanie tokenami uwierzytelniającymi lub ich przechwytywanie może pozwolić atakującym podszywać się pod legalnych użytkowników i uzyskiwać nieautoryzowany dostęp.

• Luki w zabezpieczeniach logowania jednokrotnego (SSO): Luki w implementacji logowania jednokrotnego (SSO) mogą narazić użytkowników na nieautoryzowany dostęp w przypadku naruszenia procesu uwierzytelniania.

• Błędy konfiguracji: Nieprawidłowo skonfigurowane ustawienia IAM mogą prowadzić do niezamierzonego ujawnienia poufnych informacji lub nieautoryzowanego dostępu.

• Integracje z systemami innych firm: Luki w zabezpieczeniach aplikacji innych firm zintegrowanych z systemami IAM mogą umożliwić atakującym przejęcie kontroli nad danymi uwierzytelniającymi użytkowników.

Aby zminimalizować te zagrożenia, organizacje powinny regularnie aktualizować systemy IAM, egzekwować silne zasady dotyczące haseł, wdrażać uwierzytelnianie wieloskładnikowe (MFA), przeprowadzać regularne audyty bezpieczeństwa, edukować użytkowników o zagrożeniach związanych z phishingiem oraz monitorować podejrzane działania, aby szybko wykrywać i reagować na potencjalne incydenty bezpieczeństwa.

Przejęcie kontroli nad usługami (Service Hijacking)

Przejęcie kontroli nad usługami (Service Hijacking) oznacza nieautoryzowane przejęcie lub manipulację różnymi usługami online. W kontekście przetwarzania w chmurze (Cloud Computing) przejęcie kontroli nad usługami (Service Hijacking) może również oznaczać nieautoryzowany dostęp lub kontrolę nad infrastrukturą lub usługami w chmurze, co potencjalnie prowadzi do wycieków danych lub zakłóceń w świadczeniu usług. Ataki te zazwyczaj polegają na manipulacji protokołem, takim jak DNS, poprzez atak bezpośredni. Inny sposób polega mniej na bezpośrednim ataku na protokół, a bardziej na manipulacji protokołem po przechwyceniu pakietów poprzez podsłuchiwanie sieci (Network Sniffing). Podsłuchiwanie sieci (Network Sniffing) polega na pasywnym monitorowaniu i przechwytywaniu pakietów danych przesyłanych przez sieć. Atak ten jest trudniejszy w przypadku technologii chmurowych; przyjrzyjmy się jednak temu procesowi:

1. Polega on na użyciu sniffera pakietów zintegrowanego z transmisją. Strona klienta często, ale nie zawsze, doświadcza tego rodzaju ataku. 2. Następnie sniffer przechwytuje pakiety zawierające dane prywatne, w tym pliki cookie, identyfikatory sesji, hasła i inne dane powiązane z usługami online.

3. Następnie odsyła je z powrotem do atakującego, aby mógł on użyć ich do późniejszego uzyskania dostępu do usługi lub usług. Aby ten typ ataku zakończył się sukcesem, wymagane są następujące elementy:

• Sniffer sieciowy: Atakujący musi mieć możliwość przechwytywania pakietów sieciowych. Atakujący stosują różne techniki, takie jak narzędzia do podsłuchiwania pakietów lub zainfekowane urządzenia sieciowe, aby przechwytywać niezaszyfrowany ruch w środowisku chmurowym. Analizując te przechwycone dane, atakujący mogą potencjalnie wydobyć cenne informacje, w tym dane logowania, klucze API lub poufne dane biznesowe. Narzędziami, które mogą wykonać tę operację, są Wireshark i TCPDump.

• Niezabezpieczony protokół komunikacyjny: Atakujący będą potrzebować jawnego tekstu lub niezabezpieczonych protokołów, aby móc wykorzystać przechwycone pakiety. Jeśli używane są protokoły szyfrowane, dane przechwytywania pakietów będą zawierały jedynie zaszyfrowane transakcje, które nie będą przydatne dla atakującego, ponieważ będą one szyfrowane. Usługi chmurowe często wykorzystują kanały komunikacyjne, takie jak HTTP, FTP lub inne protokoły do przesyłania danych. Jeśli kanały te nie są odpowiednio zabezpieczone szyfrowaniem, stają się podatne na ataki typu sniffing sieciowy. W przypadku braku szyfrowania atakujący mogą podsłuchiwać komunikację między komponentami usług chmurowych, wykorzystując wszelkie niezabezpieczone dane w trakcie transmisji.

W przypadku braku sniffera sieciowego, można również przeprowadzić atak typu Man-in-the-Middle (MitM) w celu przechwycenia aktywności sieciowej. Ataki MitM polegają na tym, że atakujący ustawia się pomiędzy kanałami komunikacyjnymi dwóch stron. W ten sposób może przechwycić i zmodyfikować komunikację, potencjalnie wprowadzając szkodliwą zawartość lub przechwytując poufne informacje w sposób niezauważony. W chmurze ataki MitM mogą prowadzić do nieautoryzowanego dostępu i przejęcia usług.

Przejęcie sesji

Jak już wspomniano, przejęcie sesji często występuje w połączeniu z atakiem MitM. W kontekście przetwarzania w chmurze, przejęcie sesji odnosi się do nieautoryzowanego przechwycenia lub przejęcia aktywnej sesji użytkownika w środowisku przetwarzania w chmurze. Ten rodzaj ataku wykorzystuje luki w zabezpieczeniach procesów uwierzytelniania i zarządzania sesjami, umożliwiając atakującym uzyskanie nieautoryzowanego dostępu do konta użytkownika lub poufnych informacji. Oto krótki przegląd niektórych luk w zabezpieczeniach, które prowadzą do ataków typu „przejęcie sesji" w kontekście przetwarzania w chmurze:

• Pliki cookie sesji: Atakujący często obierają za cel pliki cookie sesji, które przechowują informacje uwierzytelniające użytkownika. Jeśli te pliki cookie zostaną przechwycone, atakujący może je wykorzystać do uzyskania nieautoryzowanego dostępu do sesji użytkownika.

• Niezabezpieczona transmisja: Słabe strony w szyfrowaniu danych podczas transmisji mogą narazić tokeny sesji na przechwycenie. Niezabezpieczone sieci Wi-Fi lub nieprawidłowo skonfigurowane kanały komunikacji zwiększają ryzyko przejęcia sesji.

• Cross-Site Scripting (XSS): Ataki XSS mogą być wykorzystywane do wstrzykiwania złośliwych skryptów do aplikacji internetowych, umożliwiając atakującym kradzież informacji o sesjach innych użytkowników lub manipulowanie ich sesjami.

• Niewystarczające zarządzanie sesjami: Niewłaściwie wdrożone praktyki zarządzania sesjami, takie jak słabe identyfikatory sesji lub nieprawidłowe ustawienia limitu czasu, mogą stwarzać atakującym możliwości przejęcia aktywnych sesji. Konsekwencje przejęcia sesji mogą obejmować nieautoryzowany dostęp do poufnych danych, manipulację ustawieniami użytkownika oraz potencjalne nadużycie jego

uprawnień w środowisku chmurowym. Aby zminimalizować ryzyko przejęcia sesji w chmurze, organizacje powinny podjąć następujące działania:

• Wdrożyć silne szyfrowanie przesyłanych danych

• Egzekwować bezpieczne praktyki zarządzania sesjami

• Regularnie aktualizować i poprawiać oprogramowanie

• Edukować użytkowników w zakresie najlepszych praktyk bezpieczeństwa

• Stosować uwierzytelnianie wieloskładnikowe (MFA), aby dodać dodatkową warstwę ochrony przed nieautoryzowanym dostępem

Ataki na systemy nazw domen (DNS)

Ostatnim obszarem ataków jest system nazw domen (DNS). Tego typu ataki nie są atakami w chmurze, ponieważ mogą wpływać na każdą usługę, która jest ujawniona i dostępna za pośrednictwem Internetu i ma powiązaną z nią nazwę domeny. Niektóre z tych ataków obejmują zatruwanie DNS, typosquatting, przechwytywanie domen i atak typu „Domain Snipping". Przyjrzyjmy się im bliżej:

• Zatruwanie DNS: Zatruwanie DNS, znane również jako podszywanie się pod DNS, to złośliwa technika, w której atakujący manipulują lub uszkadzają DNS w celu przekierowywania prawidłowych rozwiązań nazw domen na złośliwe adresy IP. Wprowadzając fałszywe informacje DNS do systemu, atakujący mogą wprowadzać użytkowników w błąd, kierując ich do niezamierzonych stron internetowych lub usług online. Ta forma cyberataku może mieć poważne konsekwencje, w tym przechwycenie poufnych danych, ataki phishingowe i rozprzestrzenianie złośliwego oprogramowania. Zatruwanie DNS wykorzystuje luki w zabezpieczeniach infrastruktury DNS, często poprzez techniki takie jak zatruwanie pamięci podręcznej lub wstrzykiwanie fałszywych rekordów DNS, zagrażając integralności i wiarygodności procesu rozpoznawania domen. Wdrożenie bezpiecznych konfiguracji DNS, stosowanie protokołów bezpieczeństwa DNS i zachowanie czujności na potencjalne zagrożenia to niezbędne środki minimalizujące ryzyko związane z zatruwaniem DNS.

• Typosquatting: Typosquatting, skrót od typographical squatting, to oszukańcza cybertaktyka, polegająca na tym, że złośliwi aktorzy rejestrują nazwy domen, które są bardzo podobne do legalnych, wprowadzając subtelne błędy ortograficzne, literówki lub wariacje. Celem jest wykorzystanie błędów użytkowników podczas wprowadzania adresów internetowych, co prowadzi do niezamierzonych i często złośliwych witryn. Wykorzystując typowe błędy w pisowni, takie jak zamiana liter lub dodawanie dodatkowych znaków, typosquatterzy mogą nakłonić użytkowników do ujawnienia poufnych informacji, padnięcia ofiarą ataków phishingowych lub nieświadomego pobrania złośliwego oprogramowania. Ta forma podszywania się pod kogoś w sieci podkreśla wagę czujności użytkowników i potrzebę proaktywnego monitorowania i obrony przed takimi oszukańczymi praktykami przez organizacje, aby chronić reputację marki i chronić użytkowników przed potencjalnymi cyberzagrożeniami.

• Przejęcie subdomeny: Przejęcia subdomeny stanowią zagrożenie bezpieczeństwa dla organizacji korzystających z usług w chmurze lub platform hostingowych. Ta luka występuje, gdy subdomena, wcześniej wskazująca na usługę, która została wycofana lub przeniesiona, pozostaje nieodebrana lub nieprawidłowo skonfigurowana. Szkodliwi atakujący mogą wykorzystać to zaniedbanie, rejestrując domenę niedziałającej usługi i potencjalnie uzyskując kontrolę nad subdomeną, przekierowując ruch do złośliwej zawartości lub przeprowadzając ataki phishingowe. Przejęcia subdomeny często wynikają z błędnych konfiguracji lub zaniedbań w praktykach zarządzania domeną, takich jak zaniechanie

usuwania rekordów DNS lub zaniedbanie monitorowania zmian własności domeny. Organizacje powinny wdrożyć solidne zasady zarządzania domenami, aby zminimalizować ryzyko przejęcia subdomeny, regularnie przeprowadzać audyt konfiguracji DNS i niezwłocznie odzyskiwać lub zmieniać przeznaczenie nieużywanych subdomen. Ponadto, korzystanie z narzędzi i usług bezpieczeństwa, które monitorują aktywność domeny i wykrywają nieautoryzowane zmiany, może pomóc w identyfikacji i usuwaniu luk w zabezpieczeniach związanych z przejęciem subdomeny, zanim zostaną one wykorzystane. Podejmując proaktywne działania w odpowiedzi na ten wektor zagrożeń, organizacje mogą chronić swoją obecność w sieci i zabezpieczyć się przed potencjalnymi naruszeniami bezpieczeństwa i szkodami dla reputacji.

• Przejęcie domeny: Przejęcie domeny to złośliwy akt, w którym nieautoryzowane osoby lub podmioty przejmują kontrolę nad zarejestrowaną nazwą domeny bez zgody jej prawowitego właściciela. Zazwyczaj odbywa się to na różne sposoby:

- Wykorzystanie luk w zabezpieczeniach kont rejestratorów domen

- Złamanie danych uwierzytelniających użytkownika

- Manipulacja procesem rejestracji domeny

Po przejęciu domeny atakujący uzyskuje możliwość zmiany ustawień domeny, przekierowywania ruchu, modyfikowania rekordów DNS i potencjalnego wykorzystania domeny do szkodliwych działań, w tym phishingu lub dystrybucji złośliwego oprogramowania. Przejęcie domeny stanowi poważne zagrożenie dla firm i osób prywatnych, ponieważ może prowadzić do zakłóceń w działaniu usług online, utraty reputacji i nieautoryzowanego dostępu do poufnych informacji związanych z przejętą domeną. Ochrona przed przejęciem domeny obejmuje wdrożenie silnych procedur uwierzytelniania u rejestratorów domen, regularne monitorowanie ustawień domeny pod kątem nieautoryzowanych zmian oraz stosowanie skutecznych praktyk cyberbezpieczeństwa w celu zapobiegania nieautoryzowanemu dostępowi do danych uwierzytelniających konta. • Snipping domen: Snipping domen, znany również jako „domain snipping", to kontrowersyjna praktyka w branży nazw domen, polegająca na próbie rejestracji domeny natychmiast po jej wygaśnięciu i udostępnieniu do ponownej rejestracji przez osoby fizyczne lub podmioty. Celem tej strategii jest wykorzystanie okresu karencji między wygaśnięciem domeny a jej udostępnieniem do rejestracji publicznej. Osoby dokonujące snippingu domen używają zautomatyzowanych narzędzi do szybkiej rejestracji niedawno wygasłych domen, licząc na wykorzystanie istniejącego ruchu, linków zwrotnych lub reputacji domeny. Podczas gdy niektórzy uważają snipping domen za legalną strategię biznesową pozyskiwania cennych domen, inni krytykują go jako nieetyczny, zwłaszcza gdy dotyczy on wygasłych domen osób fizycznych lub organizacji, które mogły nieumyślnie pozwolić na wygaśnięcie rejestracji. Proces snippingu domen jest wysoce konkurencyjny, a niektórzy rejestratorzy domen wdrożyli środki mające na celu ograniczenie skuteczności tej praktyki i zapewnienie właścicielom domen uczciwych możliwości odnowienia rejestracji. Teraz, gdy poznaliśmy niektóre zagrożenia i ataki, jakie mogą wystąpić w środowiskach chmurowych, przyjrzyjmy się kilku sposobom ich zabezpieczenia.

Wdrażanie zabezpieczeń w chmurze

Bezpieczeństwo w chmurze to kompleksowy zestaw praktyk, technologii i zasad mających na celu ochronę danych, aplikacji i infrastruktury w środowiskach przetwarzania w chmurze. Ze względu na swoją naturę, bezpieczeństwo w chmurze musi być bardziej kompleksowe niż tradycyjne zabezpieczenia sieci i obejmuje polityki kontroli, implementację zapór sieciowych aplikacji, silniejsze mechanizmy kontroli dostępu, uwierzytelnianie wieloskładnikowe (MFA) oraz bardziej rygorystyczne

mechanizmy kontroli i monitorowania infrastruktury przetwarzania w chmurze. Poniższe sekcje zawierają przegląd zabezpieczeń w chmurze i warstw zabezpieczeń.

Wdrażanie polityk, procedur i świadomości

Wdrażanie polityk i procedur oraz podnoszenie świadomości stanowią fundament bezpieczeństwa infrastruktury chmurowej. Dzieli się on na cztery podstawowe części:

• Model Współodpowiedzialności: Należy jasno zrozumieć bezpieczeństwo i obowiązki dostawcy usług w chmurze (CSP) oraz własne. Wdrożyć środki w celu potwierdzenia i audytu zarówno dostawcy usług w chmurze (CSP), jak i procesów, procedur oraz rezultatów.

• Zgodność z chmurą i ścieżka audytu: Uzupełnia to pierwszą część, ponieważ to logi i dane muszą być przeglądane i monitorowane. Co więcej, to właśnie tutaj identyfikowane są nie tylko luki w zabezpieczeniach, ale także brak wiarygodności otrzymywanych danych.

• Integracja DevSecOps: Dział Rozwoju i Operacji (DevOps) prawdopodobnie charakteryzuje się największą interakcją z infrastrukturą chmurową. To czyni je kluczowym obszarem do integracji bezpieczeństwa z procesami DevOps od samego początku, aby zapewnić bezpieczny cykl życia oprogramowania. Obejmuje to wdrożenie narzędzi do testowania bezpieczeństwa i zautomatyzowanych kontroli bezpieczeństwa oraz zaangażowanie zespołów ds. bezpieczeństwa w proces rozwoju oprogramowania. • Świadomość i szkolenia użytkowników: Użytkownicy zawsze będą najsłabszym ogniwem w procesie kontroli bezpieczeństwa. Promuj kulturę świadomości bezpieczeństwa wśród użytkowników chmury, podkreślając ich rolę w utrzymaniu bezpiecznego środowiska. W tym celu należy regularnie prowadzić szkolenia na temat najlepszych praktyk bezpieczeństwa w chmurze, w tym tego, które usługi są usługami chmurowymi, a które lokalnymi, oraz informować użytkowników o pojawiających się zagrożeniach, takich jak socjotechnika i techniki phishingu.

Zapewnienie bezpieczeństwa obwodowego

Bezpieczeństwo obwodowe w środowiskach chmurowych jest wyjątkowe, ponieważ nie zawsze istnieje wyraźne rozróżnienie między tym, co wewnętrzne, a tym, co internetowe. Mając to na uwadze, bezpieczeństwo obwodowe w chmurze odnosi się do zestawu środków wdrożonych w celu ochrony granic infrastruktury chmurowej, zabezpieczając ją przed nieautoryzowanym dostępem, złośliwymi atakami i innymi zagrożeniami bezpieczeństwa. Tradycyjne bezpieczeństwo obwodowe, które w dużej mierze opiera się na fizycznych zaporach sieciowych i urządzeniach sieciowych, wymaga dostosowania i ulepszenia, aby odpowiadało dynamicznemu i rozproszonemu charakterowi architektur chmurowych. Oto kluczowe metody wdrażania zabezpieczeń obwodowych w środowiskach chmurowych:

• Wirtualne zapory sieciowe i grupy zabezpieczeń sieci (NSG): Zdefiniuj reguły filtrowania ruchu, kontroli dostępu i segmentacji sieci. Wykorzystaj wirtualne zapory sieciowe i grupy zabezpieczeń sieci (NSG) do kontrolowania ruchu przychodzącego i wychodzącego między zasobami w sieci chmurowej.

• Zarządzanie tożsamościami i dostępem (IAM): Ponieważ logowania IAM mogą odbywać się z Internetu, logowania IAM podlegają zarówno zabezpieczeniom obwodowym, jak i samym zabezpieczeniom IAM. Aby wzmocnić bezpieczeństwo IAM, wdróż surowe zasady kontroli dostępu użytkowników do zasobów chmurowych. W tym celu wykorzystaj kontrolę dostępu opartą na rolach (RBAC) i upewnij się, że użytkownicy posiadają minimalne uprawnienia wymagane do wykonywania swoich zadań.

• Zapory sieciowe aplikacji internetowych (WAF): Zapory WAF oferują bardziej kompleksowe mechanizmy wykrywania i logikę dla technologii aplikacji internetowych. Aby chronić aplikacje internetowe przed typowymi atakami i exploitami, należy wdrożyć rozwiązania WAF w celu inspekcji i filtrowania ruchu HTTP między aplikacją internetową a internetem, blokując potencjalne zagrożenia.

• Bezpieczeństwo API: Zabezpiecz interfejsy API, aby zapobiec nieautoryzowanemu dostępowi i ujawnieniu danych. Można to osiągnąć poprzez wdrożenie mechanizmów uwierzytelniania, egzekwowanie prawidłowej autoryzacji i monitorowanie ruchu API pod kątem potencjalnych luk w zabezpieczeniach.

• Ochrona przed atakami DDoS: Ograniczaj skutki ataków DDoS, zapewniając wysoką dostępność i odporność. Wiele usług w chmurze oferuje usługi ochrony przed atakami DDoS, które mogą być wbudowane w usługę lub stanowić produkt dodatkowy.

• Monitorowanie i rejestrowanie sieci: Jak omówiono wcześniej w tym rozdziale, monitoruj ruch sieciowy i inne istotne źródła logów w celu analizy zdarzeń. Korzystaj z natywnych dla chmury narzędzi monitorujących, aby rejestrować i analizować aktywność sieciową, umożliwiając szybkie wykrywanie i reagowanie na incydenty bezpieczeństwa.

• Grupy zabezpieczeń i listy kontroli dostępu do sieci (NACL): Definiuj i egzekwuj reguły grup zabezpieczeń i NACL, aby kontrolować ruch na poziomie podsieci. Konfiguruj grupy zabezpieczeń dla instancji i wykorzystuj NACL do kontrolowania ruchu na poziomie podsieci, zapewniając prawidłową segmentację sieci.

• Model bezpieczeństwa Zero Trust: Przyjmij model Zero Trust, w którym zaufanie nigdy nie jest zakładane, a weryfikacja jest wymagana od każdego, kto próbuje uzyskać dostęp do zasobów. W tym celu wdroż ścisłe mechanizmy uwierzytelniania i autoryzacji, obejmujące ciągłe monitorowanie i zasady dostępu z minimalnymi uprawnieniami.

• Szyfrowanie w ruchu i w spoczynku: Egzekwuj szyfrowanie danych w ruchu i w spoczynku, aby chronić poufne informacje. Można to osiągnąć za pomocą protokołu SSL/TLS do szyfrowania danych w ruchu i wdrażania mechanizmów szyfrowania dostarczanych przez dostawcę chmury dla danych w spoczynku.

• Regularne audyty i oceny bezpieczeństwa: Przeprowadzaj regularne audyty i oceny bezpieczeństwa w celu identyfikacji i wyeliminowania potencjalnych luk w zabezpieczeniach. Procedura zapewniająca skuteczność zabezpieczeń obwodowych obejmuje:

- Przeprowadzanie testów penetracyjnych

- Przeprowadzanie oceny podatności

- Regularne przeglądy bezpieczeństwa.

Środki te pomogą złagodzić wiele, ale nie wszystkie zagrożenia występujące w środowiskach chmurowych.

Bezpieczeństwo aplikacji

Bezpieczeństwo aplikacji w środowiskach chmurowych obejmuje wdrożenie środków chroniących aplikacje hostowane w chmurze przed potencjalnymi zagrożeniami i lukami w zabezpieczeniach. Ponieważ aplikacje są kluczowym elementem każdej infrastruktury chmurowej, ich zabezpieczenie ma kluczowe znaczenie dla ochrony poufnych danych i utrzymania ogólnej integralności systemu. Oto kluczowe aspekty wdrażania bezpieczeństwa aplikacji w środowiskach chmurowych:

• Bezpieczny cykl życia oprogramowania (SDLC): Zintegruj praktyki bezpieczeństwa w całym procesie tworzenia oprogramowania. Jeśli organizacja posiada zespół programistów, wdróż wytyczne dotyczące bezpiecznego kodowania, przeprowadź szkolenia z zakresu bezpieczeństwa dla programistów i wprowadź kontrole bezpieczeństwa na każdym etapie cyklu życia oprogramowania.

• Bezpieczeństwo kontenerów: Zapewnij bezpieczeństwo aplikacji konteneryzowanych i ich środowisk wykonawczych. Wiele aplikacji chmurowych jest wdrażanych w kontenerach lub korzysta z narzędzi do orkiestracji kontenerów, takich jak Kubernetes. Kontenery mają własne najlepsze praktyki dotyczące zabezpieczania obrazów, konfiguracji orkiestratorów i środowisk wykonawczych.

• Przeglądy kodu i analiza statyczna: Regularnie przeglądaj kod aplikacji pod kątem luk w zabezpieczeniach. Jest to zadanie, które należy wykonać, jeśli programiści wdrażają aplikacje. Przeprowadzaj przeglądy kodu i korzystaj z narzędzi do analizy statycznej, aby identyfikować i usuwać luki w zabezpieczeniach w bazie kodu.

• Dynamiczne testowanie bezpieczeństwa aplikacji (DAST): Oceniaj aplikacje pod kątem luk w zabezpieczeniach w czasie rzeczywistym. Aby to zrobić, używaj narzędzi symulujących ataki na działające aplikacje, takich jak Nessus, identyfikując luki i słabości, które mogą nie być widoczne podczas analizy statycznej. Może to być również wykonywane w ramach testów penetracyjnych lub procesu testowania jednostkowego SDLC.

• Uwierzytelnianie i autoryzacja: Wdrażaj silne mechanizmy uwierzytelniania i egzekwuj odpowiednie kontrole autoryzacji. Dotyczy to obszaru lub samej aplikacji, w przeciwieństwie do uwierzytelniania IAM. Wykorzystuj MFA, OAuth, OpenID Connect i RBAC, aby zapewnić dostęp do wrażliwych zasobów tylko autoryzowanym użytkownikom.

• Zarządzanie poprawkami: Regularnie aktualizuj i instaluj poprawki w aplikacjach, aby usuwać znane luki w zabezpieczeniach. Środowiska chmurowe nie różnią się pod względem łatania od tradycyjnych sieci, choć jest to nieco bardziej skomplikowane. Wdrażaj solidny proces zarządzania poprawkami, aby szybko wdrażać aktualizacje zabezpieczeń i poprawki, zmniejszając ryzyko wykorzystania luk.

• Zgodność i kwestie regulacyjne: Upewnij się, że aplikacje są zgodne z odpowiednimi standardami branżowymi i przepisami. Regularnie audytuj i oceniaj aplikacje pod kątem zgodności z przepisami, takimi jak RODO, HIPAA lub standardami branżowymi.

Utrzymanie bezpieczeństwa pamięci masowej i informacji

W chmurze obliczeniowej bezpieczeństwo pamięci masowej i informacji jest kluczowym elementem zapewniającym poufność, integralność i dostępność danych. Rozwiązania pamięci masowej w chmurze, często oferowane przez głównych dostawców usług komunikacyjnych (CSP), oferują organizacjom skalowalne i elastyczne opcje przechowywania i zarządzania danymi. Jednak utrzymanie solidnych środków bezpieczeństwa jest niezbędne, aby zminimalizować ryzyko związane z nieautoryzowanym dostępem, naruszeniami danych i innymi zagrożeniami bezpieczeństwa. Dwa kluczowe elementy arsenału zabezpieczeń w chmurze to:

• System wykrywania włamań (IDS): Systemy te odgrywają kluczową rolę w monitorowaniu aktywności sieci i systemów w celu identyfikacji i reagowania na potencjalne incydenty bezpieczeństwa. Rozwiązania IDS oparte na chmurze analizują ruch sieciowy, logi systemowe i inne źródła danych w celu wykrywania anomalii lub znanych wzorców ataków. Mogą działać w czasie rzeczywistym, zapewniając natychmiastowe alerty lub automatyczne reakcje na potencjalne zagrożenia. Systemy IDS oparte na chmurze są szczególnie cenne w dynamicznym i skalowalnym charakterze środowisk chmurowych, w których tradycyjne zabezpieczenia oparte na ochronie obwodowej mogą być

niewystarczające. Poprzez ciągłe monitorowanie ruchu i aktywności, system IDS pomaga zapewnić wczesne wykrywanie i minimalizowanie naruszeń bezpieczeństwa, chroniąc wrażliwe dane przechowywane w chmurze.

• Zapobieganie utracie danych (DLP): To kolejny kluczowy aspekt zabezpieczania informacji w chmurze. Rozwiązania DLP zostały zaprojektowane w celu zapobiegania nieautoryzowanemu dostępowi, udostępnianiu lub wyciekowi wrażliwych danych. W kontekście chmury, gdzie dostęp do danych może być możliwy z różnych urządzeń i lokalizacji, narzędzia DLP oferują inspekcję treści i egzekwowanie zasad w celu kontrolowania przepływu wrażliwych informacji. Rozwiązania te mogą identyfikować i klasyfikować wrażliwe dane, takie jak dane osobowe (PII), dokumenty finansowe lub własność intelektualna, oraz egzekwować zasady zapobiegające ich nieautoryzowanemu przesyłaniu lub przechowywaniu. DLP w chmurze ma kluczowe znaczenie dla zgodności z przepisami, ochrony przed naruszeniami danych i zapewnienia organizacjom kontroli nad krytycznymi zasobami informacyjnymi podczas ich przechowywania i przetwarzania w środowiskach chmurowych.

Łącząc IDS i DLP, organizacje mogą wdrożyć kompleksową politykę bezpieczeństwa dla swoich pamięci masowych w chmurze, skutecznie przeciwdziałając pojawiającym się zagrożeniom i utrzymując zaufanie użytkowników i interesariuszy. Łącząc te zasady i procedury, organizacje mogą opracować solidną strategię bezpieczeństwa obwodowego, dostosowaną do unikalnych wyzwań i specyfiki środowisk chmurowych. Pomaga to zapewnić integralność, poufność i dostępność zasobów w infrastrukturze chmurowej. Ostatnią kwestią, którą należy omówić przed zakończeniem, jest rejestrowanie bezpieczeństwa w chmurze.

Logi bezpieczeństwa w chmurze

W przypadku korzystania z usług chmurowych kluczowe jest przeglądanie i monitorowanie logów w celu ochrony zasobów cyfrowych w środowisku chmurowym. Obejmuje to systematyczne rejestrowanie, analizę i monitorowanie logów generowanych przez różne usługi chmurowe i komponenty infrastruktury. Logi te rejestrują kompleksowy harmonogram zdarzeń, w tym aktywności użytkowników, modyfikacje zasobów i wywołania API, zapewniając szczegółowy ślad audytu dla celów bezpieczeństwa. Główne cele rejestrowania bezpieczeństwa w chmurze obejmują wykrywanie anomalii, monitorowanie zgodności i reagowanie na incydenty. Przyjrzyjmy się niektórym z jego korzyści:

• Analizując logi, zespoły ds. bezpieczeństwa mogą identyfikować odchylenia od ustalonych norm, zapewniając terminowe wykrywanie potencjalnych zagrożeń i luk w zabezpieczeniach.

• Rejestrowanie bezpieczeństwa w chmurze śledzi zmiany w konfiguracjach, kontroli dostępu i ruchu sieciowym, oferując wgląd w ogólną kondycję i bezpieczeństwo środowiska chmurowego.

• Zintegrowane z systemami zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM), rejestry te umożliwiają scentralizowane monitorowanie, wykrywanie zagrożeń w czasie rzeczywistym i ciągłe doskonalenie poziomu bezpieczeństwa.

• Regularny przegląd i analiza rejestrów bezpieczeństwa w chmurze umożliwiają organizacjom zwiększenie odporności cybernetycznej i skuteczne reagowanie na pojawiające się wyzwania.

Przyjrzyjmy się bliżej rejestrom dostępnym w trzech najpopularniejszych środowiskach: Azure, Amazon Web Services (AWS) i Google Cloud Platform (GCP).

Chmura Azure

Platforma Azure oferuje różnorodne dzienniki generowane przez usługi takie jak Azure Activity Log, Security Center i Azure AD Audit Logs. Możliwości rejestrowania w usłudze Azure są kluczowe dla organizacji poszukujących solidnych praktyk cyberbezpieczeństwa w swoich wdrożeniach w chmurze. Oto kilka kluczowych dzienników i zdarzeń, które należy monitorować w usłudze Azure w celu zwiększenia bezpieczeństwa:

• Azure Activity Log: rejestruje komunikaty operacyjne i monitoruje działania związane z aprowizacją zasobów, przypisaniami ról i zmianami konfiguracji zasobów. Można tu znaleźć podejrzane

próby logowania, modyfikacje zasad zabezpieczeń lub nieoczekiwane zmiany stanów zasobów.

• Alerty Azure Security Center: monitorują alerty bezpieczeństwa generowane przez Azure Security Center, które mogą zawierać informacje o wykrytych zagrożeniach, lukach w zabezpieczeniach i zalecenia dotyczące poprawy bezpieczeństwa, przyczyniając się w ten sposób do proaktywnych środków bezpieczeństwa.

• Azure AD Audit Logs: śledzą zdarzenia w usłudze Azure Active Directory, w tym podejrzane logowania użytkowników, zmiany ról i uprawnień, dostęp do aplikacji oraz wszelkie nietypowe zachowania kont, zwiększając bezpieczeństwo zarządzania tożsamościami i dostępem. W tym miejscu można znaleźć wiele nieudanych prób logowania, zwłaszcza z nietypowych lokalizacji.

• Dzienniki zgodności z zasadami platformy Azure: Monitoruj dzienniki związane ze zgodnością z zasadami platformy Azure, aby upewnić się, że zasoby są zgodne z zasadami bezpieczeństwa. Identyfikuj niezgodne zasoby i naruszenia zasad.

• Analityka usługi Azure Storage: Analizuj dzienniki i dane metryk z kont usługi Azure Storage pod kątem potencjalnych zdarzeń związanych z bezpieczeństwem. Szukaj nieautoryzowanych prób dostępu lub zmian w konfiguracjach magazynu.

• Dzienniki zapory Azure: Monitoruj dzienniki zapory Azure w celu uzyskania informacji o dozwolonym i zabronionym ruchu. Identyfikuj i badaj wszelkie nietypowe wzorce lub zdarzenia bezpieczeństwa.

• Dzienniki z usług takich jak Azure Monitor, Network Security Groups, Key Vault i Azure Sentinel przyczyniają się do holistycznego widoku zdarzeń związanych z bezpieczeństwem, umożliwiając organizacjom monitorowanie anomalii, szybkie reagowanie na incydenty i zachowanie zgodności z zasadami bezpieczeństwa.

Jeśli nie chcesz przeglądać dzienników indywidualnie lub środowisko jest zbyt duże, aby zarządzać nim w tej formie, dzienniki można scentralizować w systemie SIEM. Może to być oddzielny produkt, taki jak Sumo Logic lub Splunk. Jednak Microsoft oferuje również zintegrowane rozwiązanie o nazwie Sentinel One, które przetwarza dzienniki platformy Azure w celu zaawansowanego wykrywania i reagowania na zagrożenia, a także generuje alerty.

AWS

AWS zapewnia kompleksową infrastrukturę rejestrowania zdarzeń z kluczowymi komponentami, takimi jak AWS CloudTrail, Amazon CloudWatch i AWS Config. Integracja tych logów z usługami bezpieczeństwa AWS, takimi jak GuardDuty i Security Hub, zwiększa możliwości skutecznego wykrywania i reagowania na incydenty bezpieczeństwa. Rejestrowanie zdarzeń AWS umożliwia organizacjom proaktywne zarządzanie i zabezpieczanie środowisk chmurowych, zapewniając odporność i zgodność infrastruktury. Przyjrzyjmy się bliżej niektórym z tych logów:

• Logi AWS CloudTrail: Przechwytują wywołania API wykonane na koncie AWS, zapewniając szczegółową historię zmian wprowadzonych w zasobach, ułatwiając audyt i zapewnienie zgodności. Można ich używać do monitorowania nietypowych lub nieautoryzowanych działań API, takich jak tworzenie, modyfikacja lub usuwanie zasobów.

• Logi Amazon CloudWatch: Zbieraj logi z różnych usług, aplikacji i systemów AWS, umożliwiając scentralizowane monitorowanie zdarzeń, błędów i anomalii bezpieczeństwa. Monitoruj zdarzenia, błędy i podejrzane działania związane z bezpieczeństwem w całym środowisku AWS.

• Dzienniki konfiguracji AWS: Śledź zmiany w konfiguracjach zasobów i oceniaj zgodność z regułami AWS Config. Monitoruj zmiany, które mogą mieć wpływ na bezpieczeństwo, takie jak zmiany reguł grup zabezpieczeń lub zasad IAM.

• Dzienniki przepływu w wirtualnej chmurze prywatnej (VPC): Rejestruj informacje o ruchu IP przychodzącym i wychodzącym z interfejsów sieciowych w Twojej sieci VPC, umożliwiając organizacjom identyfikację potencjalnych zagrożeń bezpieczeństwa i nieautoryzowanych działań. Analizuj dzienniki przepływu pod kątem nietypowych wzorców sieciowych, zablokowanego ruchu lub potencjalnych zagrożeń bezpieczeństwa.

• Dzienniki zapory aplikacji internetowych AWS (WAF): Monitoruj dzienniki pod kątem informacji o ruchu aplikacji internetowych i regułach bezpieczeństwa. Identyfikuj i reaguj na potencjalne ataki na aplikacje internetowe.

• Amazon GuardDuty: GuardDuty automatycznie analizuje zdarzenia w CloudTrail, dziennikach przepływu VPC i dziennikach DNS w celu wykrywania zagrożeń. Przejrzyj wyniki GuardDuty pod kątem alertów związanych ze złośliwą aktywnością, zainfekowanymi instancjami lub nieautoryzowanym dostępem.

• Logi AWS Lambda: Jeśli korzystasz z funkcji AWS Lambda, monitoruj logi pod kątem podejrzanej aktywności i błędów. Sprawdź nieautoryzowane wykonania lub nietypowe zachowanie funkcji bezserwerowych.

• Logi dostępu do serwera AWS S3: Włącz rejestrowanie dostępu do kontenerów S3 i monitoruj próby nieautoryzowanego dostępu. Śledź żądania, w tym adres IP osoby żądającej i podjęte działania.

• Logi dostępu AWS CloudFront: Jeśli korzystasz z CloudFront, monitoruj logi dostępu dla swoich dystrybucji. Szukaj nietypowych wzorców, dużej liczby żądań lub zdarzeń związanych z bezpieczeństwem.

• Logi dostępu i uwierzytelniania AWS IAM: Monitoruj logi AWS Identity and Access Management (IAM) pod kątem zmian w politykach IAM, rolach i zdarzeniach uwierzytelniania użytkowników. Wykrywaj i badaj nieautoryzowane próby dostępu lub zmiany uprawnień.

• Logi audytu Amazon RDS: Jeśli korzystasz z Amazon RDS (Relational Database Service), włącz i monitoruj logi audytu bazy danych. Szukaj podejrzanych zapytań do bazy danych lub zmian w konfiguracji bazy danych.

W środowisku AWS GuardDuty może wydawać się systemem SIEM, ale w rzeczywistości monitoruje jedynie logi i generuje alerty. Nie zapewnia jednak możliwości zarządzania zdarzeniami, co wymagałoby osobnej aplikacji.

Google Cloud Platform (GCP)

Logowanie GCP jest fundamentalnym elementem utrzymania bezpieczeństwa i integralności operacyjnej środowisk chmurowych hostowanych w Google Cloud. GCP zapewnia solidną infrastrukturę rejestrowania, koncentrując się na usługach takich jak Cloud Audit Logs, VPC Flow Logs, Cloud Storage Audit Logs i Stackdriver Logging. Rejestrowanie GCP jest integralną częścią organizacji, które dążą do proaktywnego podejścia do bezpieczeństwa, zgodności i doskonałości operacyjnej w swoich wdrożeniach chmurowych. Kompleksowy i zintegrowany charakter rejestrowania GCP zwiększa przejrzystość, umożliwiając organizacjom efektywne zarządzanie infrastrukturą chmurową i jej zabezpieczanie. Oto bardziej szczegółowe podsumowanie logów GCP:

• Cloud Audit Logs: Rejestruje logi wywołań API w różnych usługach GCP. Monitoruje pod kątem podejrzanej aktywności, nieautoryzowanego dostępu lub zmian w zasobach.

• Dzienniki przepływu w chmurze prywatnej wirtualnej (VPC): Zbieraj dzienniki, które rejestrują informacje o przepływie sieci dla instancji maszyn wirtualnych. Analizuj dziennik pod kątem nietypowych wzorców sieciowych, zablokowanego ruchu lub potencjalnych zagrożeń bezpieczeństwa.

• Dzienniki audytu pamięci masowej w chmurze: Monitoruj dzienniki kontenerów pamięci masowej w chmurze w celu wykrywania nieautoryzowanego dostępu lub modyfikacji. Śledź zmiany obiektów, zasad kontenerów i uprawnień dostępu.

• Dzienniki audytu serwera proxy identyfikującego tożsamość w chmurze (IAP): W przypadku korzystania z IAP monitoruj dzienniki pod kątem zdarzeń dostępu i informacji uwierzytelniających. Identyfikuj i badaj wszelkie nietypowe wzorce dostępu.

• Dzienniki audytu usługi DNS w chmurze: Monitoruj dzienniki audytu DNS pod kątem zmian w rekordach DNS. Wykrywaj nieautoryzowane zmiany lub potencjalne ataki oparte na DNS.

• Logi Cloud Armor: Jeśli korzystasz z Cloud Armor, monitoruj logi pod kątem wykrytych zagrożeń bezpieczeństwa i podjętych działań. Identyfikuj ataki DDoS i inne zagrożenia dla aplikacji internetowych oraz reaguj na nie.

• Logi audytu Cloud Functions: Jeśli korzystasz z Cloud Functions, monitoruj logi pod kątem podejrzanych wywołań funkcji lub błędów. Wykrywaj nieautoryzowane wykonania lub nietypowe zachowanie funkcji bezserwerowych.

• Logi audytu Google Kubernetes Engine (GKE): Monitoruj logi klastrów GKE w celu wykrywania zmian w konfiguracjach i aktywności klastra. Identyfikuj nieautoryzowany dostęp lub zmiany w zasobach Kubernetes.

• Logi audytu Cloud IAM: Monitoruj logi pod kątem zmian w zasadach IAM, rolach i uprawnieniach. Wykrywaj i badaj próby nieautoryzowanego dostępu lub zmiany uprawnień.

• Stackdriver Logging: Zbieraj logi z różnych usług i aplikacji GCP za pomocą Stackdriver Logging. Monitoruj zdarzenia, błędy i podejrzane działania związane z bezpieczeństwem.

• Logi audytu Cloud SQL: Jeśli korzystasz z Cloud SQL, włącz i monitoruj logi audytu bazy danych. Szukaj podejrzanych zapytań do bazy danych lub zmian w jej konfiguracji.

Google oferuje Cloud Security Command Center (Cloud SCC). Cloud SCC zapewnia wgląd w bezpieczeństwo i ryzyko w oparciu o wyniki z różnych usług GCP. Cloud SCC można uznać za wersję systemu SIEM firmy Google, ponieważ umożliwia przeglądanie wyników pod kątem alertów związanych z lukami w zabezpieczeniach, potencjalnymi zagrożeniami i błędami konfiguracji, a także alertów dotyczących bezpieczeństwa i ryzyka. Cloud SCC można znaleźć pod adresem

https://cloud.google.com/security/products/security-command-center. Podsumowując, skuteczne monitorowanie logów usług w chmurze jest integralną częścią bezpieczeństwa i integralności środowisk chmurowych. Każdy główny dostawca usług w chmurze, Azure, AWS i GCP, oferuje solidne narzędzia i usługi do tego celu. Azure Monitor, Sentinel One, AWS CloudWatch i pakiet Operations Suite firmy Google Cloud zapewniają kompleksowe rozwiązania do gromadzenia, analizowania i podejmowania działań na podstawie logów generowanych przez różne usługi w chmurze. Jak już wspomniano, solidne rejestrowanie wiąże się z kosztami, które należy zrównoważyć z potrzebami organizacji i dostępnym budżetem. Narzędzia te nie tylko umożliwiają wgląd w czasie rzeczywistym w wydajność i bezpieczeństwo zasobów chmurowych, ale także umożliwiają organizacjom proaktywne identyfikowanie i reagowanie na potencjalne zagrożenia. Ponieważ przetwarzanie w chmurze nadal stanowi fundamentalny element nowoczesnej infrastruktury IT, inwestowanie w dokładne monitorowanie logów w platformach Azure, AWS i GCP staje się niezbędne do zapewnienia odpornego i bezpiecznego środowiska chmurowego. Organizacje muszą dostosować swoje strategie monitorowania logów do specyficznych funkcji i możliwości oferowanych przez każdego dostawcę chmury, aby zmaksymalizować skuteczność swoich zabezpieczeń w dynamicznym krajobrazie przetwarzania w chmurze.

Podsumowanie

Sekcja poświęcona bezpieczeństwu przetwarzania w chmurze omawia kompleksowe ramy i najlepsze praktyki niezbędne do zabezpieczania danych, aplikacji i infrastruktury w środowiskach chmurowych. Podkreśla on potrzebę współpracy między dostawcami usług w chmurze a klientami w celu zapewnienia bezpiecznego ekosystemu chmurowego. Szczegółowo opisuje obowiązki obu stron, podkreślając, że podczas gdy dostawcy zarządzają bezpieczeństwem infrastruktury chmurowej, klienci odpowiadają za ochronę swoich danych i aplikacji. Szczegółowo omawia podstawowe zasady bezpieczeństwa, począwszy od znaczenia szyfrowania w ochronie danych podczas transmisji i przechowywania. Omawia IAM jako fundament kontroli dostępu użytkowników i przestrzegania zasady minimalnych uprawnień. Środki bezpieczeństwa sieci, w tym zapory sieciowe i wirtualne chmury prywatne (VPN), są podkreślane w celu zabezpieczenia kanałów komunikacji w ramach infrastruktury chmurowej. Reagowanie na incydenty i ciągłe monitorowanie są podkreślane jako kluczowe elementy solidnej strategii bezpieczeństwa. Przedstawia znaczenie narzędzi monitorowania w czasie rzeczywistym i praktyk audytowych w celu wykrywania i szybkiego reagowania na incydenty bezpieczeństwa. Podkreśla potrzebę opracowywania i regularnej aktualizacji planów reagowania na incydenty przez organizacje w celu zwiększenia odporności na rozwijające się cyberzagrożenia. Rozdział podkreśla również rolę zgodności, zarządzania i regulacji w bezpieczeństwie chmury. Organizacjom zaleca się dostosowanie działań w zakresie bezpieczeństwa do standardów branżowych i wewnętrznych zasad zarządzania, zapewniając, że wdrożenia chmurowe spełniają wymogi prawne dotyczące miejsca przechowywania danych i jurysdykcji. Bezpieczeństwo aplikacji zajmuje centralne miejsce, omawiając bezpieczne praktyki kodowania, testy penetracyjne i wdrażanie środków, takich jak zapory sieciowe (WAF), w celu ochrony przed typowymi atakami internetowymi. Omówiono również nowe trendy w technologiach kontenerowych i bezserwerowych, kładąc nacisk na zabezpieczanie obrazów kontenerów, konfiguracje orkiestratora oraz wdrażanie najlepszych praktyk w zakresie rozwoju bezserwerowego. W całym rozdziale podkreślono znaczenie szkoleń i podnoszenia świadomości pracowników, uznając, że dobrze poinformowani pracownicy odgrywają kluczową rolę w zapobieganiu incydentom bezpieczeństwa. Rozdział kończy się naciskiem na ciągłe doskonalenie, zalecając regularne wdrażanie praktyk zarządzania poprawkami w celu wyeliminowania znanych luk w zabezpieczeniach i utrzymania odpornej infrastruktury chmurowej.

Ocena

1. Ile jest typów usług chmurowych?

A. 1

B. 2

C. 3

D. 4

2. SaaS to skrót od:

A. Software Archive Analysis Security (Analiza Archiwum Oprogramowania)

B. Service Application Analysis System (System Analizy Aplikacji Usługowych)

C. Security as a Service (Bezpieczeństwo jako Usługa)

D. Software as a Service (Oprogramowanie jako Usługa)

3. Architektura chmury NIST, w której osoba lub podmiot jest w stanie samodzielnie ocenić wydajność, bezpieczeństwo i działanie systemów informatycznych usług chmurowych

A. Broker chmury

B. Audytor chmury

C. Dostawca chmury

D. Operator chmury

4. VM to skrót od

A. Zarządzanie wizualne

B. Zarządzanie wersjami

C. Maszyna Visual Studio

D. Maszyna wirtualna

5. Które z poniższych określeń nie jest sposobem na zabezpieczenie środowisk chmurowych? A. Używaj protokołów takich jak HTTP i FTP

B. Zero Trust

C. Zapór sieciowych aplikacji internetowych

D. Szyfrowania w spoczynku

6. Jednym ze sposobów ochrony poufnych danych przed opuszczeniem chmury jest użycie

A. Monitorowania sieci

B. DLP

C. Ochrony przed atakami DDoS

D. Wirtualnych zapór sieciowych

7. Co odgrywa jedną z najważniejszych ról w zabezpieczaniu zasobów cyfrowych:

A. IaaS

B. Kontenerów

C. API

D. IAM

8. Jedną z cech, które sprawiają, że kontenery są atrakcyjne w użyciu, jest:

A. Są to pełne systemy operacyjne

B. Przenośność

C. Izolacja

D. Oddzielne jądra

9. Architektura bezserwerowa nazywana jest bezserwerową, ponieważ tak naprawdę nie stoi za nią system operacyjny serwera. Prawda czy fałsz? A. Prawda

B. Fałsz

10. Architektura bezserwerowa jest podatna na ataki _____

A. Usługa

B. DoS/DDoS

C. API

D. IAM

Odpowiedzi

1. C

2. D

3. B

4. D

5. A

6. B

7. D

8. B

9. A

10. B