Zgodność usług AWS w odniesieniu do postanowień GDPR (RODO)

Październik 2019

Uwagi

Odpowiedzialność za dokonanie własnej, niezależnej oceny informacji zawartych w niniejszym dokumencie spoczywa na klientach. Niniejszy dokument: (a) służy wyłącznie do celów informacyjnych, (b) przedstawia aktualne oferty produktowe AWS oraz praktyki spółki, które mogą ulec zmianie bez wcześniejszego powiadomienia, oraz (c) nie ustanawia żadnych zobowiązań ani gwarancji ze strony AWS, jej oddziałów, dostawców lub licencjodawców. Produkty lub usługi AWS są dostarczane "w stanie, w jakim się znajdują", bez gwarancji, oświadczeń czy jakiegokolwiek rodzaju warunków, wyraźnych lub dorozumianych. Odpowiedzialność i zobowiązania AWS w stosunku do klientów są regulowane przez umowy AWS, a niniejszy dokument nie jest częścią, ani nie zmienia żadnej umowy pomiędzy AWS a klientami.

Spis treści

Streszczenie

Niniejszy dokument zawiera informacje na temat usług i zasobów, które Amazon Web Services (AWS) oferuje klientom, aby pomóc im w dostosowaniu się do wymogów ogólnego rozporządzenia o ochronie danych (RODO, ang. GDPR), które mogą mieć zastosowanie do ich działalności. Należą do nich: przestrzeganie norm bezpieczeństwa IT, atestacja katalogu AWS Cloud Computing Compliance Controls Catalog (C5, katalog kontroli zgodności obliczeń w chmurze), przestrzeganie kodeksu postępowania Cloud Infrastructure Services Providers in Europe (CISPE, Dostawców usług infrastruktury chmurowej w Europie), mechanizmy kontroli dostępu do danych, narzędzia do monitorowania i logowania, szyfrowanie i zarządzanie kluczami.

Przegląd ogólnego rozporządzenia o ochronie danych

General Data Protection Regulation (GDPR, Ogólne rozporządzenie o ochronie danych, RODO) jest europejskim prawem ochrony prywatności [1] (rozporządzenie Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. [2]), które weszło w życie 25 maja 2018 r. GDPR zastępuje unijną dyrektywę o ochronie danych osobowych (Dyrektywa 95/46/WE) i ma na celu harmonizację przepisów o ochronie danych w całej Unii Europejskiej (UE) poprzez zastosowanie jednego prawa o ochronie danych, które jest wiążące dla każdego państwa członkowskiego UE.

GDPR ma zastosowanie do wszelkiego rodzaju przetwarzania *danych osobowych* przez organizacje mające siedzibę w UE lub organizacje przetwarzające dane osobowe mieszkańców UE oferujące towary lub usługi osobom fizycznym w UE lub monitorujące zachowania mieszkańców UE w UE. Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Zmiany wprowadzone przez GDPR w stosunku do organizacji działających w UE

GDPR stara się zapewnić spójność między państwami członkowskimi UE w zakresie bezpiecznego przetwarzania, wykorzystywania i wymiany danych osobowych. Organizacje muszą wykazać bezpieczeństwo przetwarzanych przez siebie danych i ich zgodność z GDPR w sposób ciągły, wdrażając i regularnie weryfikując środki techniczne i organizacyjne, jak również politykę zgodności mającą zastosowanie do przetwarzania danych osobowych. Za naruszenie GDPR organy nadzoru UE mogą nakładać grzywny w wysokości do 20 mln EUR lub 4% rocznych obrotów światowych, w zależności od tego, która z tych kwot jest wyższa.

Przygotowanie AWS do GDPR

Eksperci ds. zgodności z przepisami i bezpieczeństwa AWS współpracują z klientami na całym świecie, aby odpowiedzieć na ich pytania i pomóc im wykonywać zadania w chmurze zgodnie z GDPR. Zespoły te weryfikują również obowiązki AWS w odniesieniu do wymogów GDPR.

Możemy zapewnić, że wszystkie usługi AWS mogą być wykorzystywane zgodnie z wymogami GDPR.

AWS Data Processing Addendum (DPA, Uzupełnienie dotyczące przetwarzania danych AWS)

AWS oferuje zgodne z GDPR uzupełnienie dotyczące przetwarzania danych (GDPR DPA), które umożliwia klientom wywiązywanie się ze zobowiązań umownych w ramach GDPR. GDPR DPA AWS jest zawarte w Warunkach świadczenia usług AWS i stosuje się automatycznie do wszystkich klientów na całym świecie, którzy wymagają zgodności z GDPR.

Rola AWS zgodnie z zapisami GDPR

Zgodnie z zapisami GDPR AWS może być zarówno podmiotem przetwarzającym dane, jak i ich administratorem.

AWS jako podmiot przetwarzający dane

Gdy klienci i dostawcy rozwiązań AWS korzystają z usług AWS w celu przetwarzania danych osobowych w swoich treściach, AWS pełni rolę podmiotu przetwarzającego dane. Do przetwarzania danych osobowych klienci i dostawcy rozwiązań AWS mogą korzystać z funkcji kontrolnych dostępnych w usługach AWS, w tym kontroli konfiguracji zabezpieczeń. W takich okolicznościach klient lub dostawcy rozwiązań AWS mogą pełnić rolę administratora lub podmiotu przetwarzającego dane, a AWS – podmiotu przetwarzającego dane lub podwykonawcę podmiotu przetwarzającego dane. Uzupełnienie dotyczące przetwarzania danych zgodnie z wymogami GDPR AWS (DPA) zawiera obowiązki AWS jako podmiotu przetwarzającego dane.

AWS jako administrator danych

Kiedy AWS gromadzi dane osobowe oraz określa cele i sposoby ich przetwarzania, działa jako administrator danych. Na przykład AWS przechowuje informacje o koncie jako administrator danych do celów rejestracji konta, administracji, dostępu do usług, kontaktu z klientem i pomocy technicznej.

Zgodnie z art. 32 administratorzy i podmioty przetwarzające dane są zobowiązani do „wdrożenia odpowiednich środków technicznych i organizacyjnych”, które uwzględniają „stan wiedzy i koszty wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania,

jak również ryzyko różnego prawdopodobieństwa i dotkliwości w odniesieniu do praw i wolności osób fizycznych". GDPR zawiera konkretne sugestie, jakiego rodzaju działania w zakresie bezpieczeństwa mogą być wymagane, np.:

- Pseudonimizacja i szyfrowanie danych osobowych.
- Zdolność do zapewnienia ciągłej poufności, integralności, dostępności i niezawodności systemów i usług przetwarzania danych.
- Możliwość przywrócenia w odpowiednim czasie dostępności i dostępu do danych osobowych w przypadku wystąpienia awarii fizycznej lub technicznej.
- Proces regularnego testowania, szacowania i oceny skuteczności środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania danych.

Model współdzielonej odpowiedzialności za bezpieczeństwo

Za bezpieczeństwo i zgodność z przepisami odpowiada wspólnie AWS i klient. Kiedy klienci przenoszą swoje systemy komputerowe i dane do chmury, obowiązki w zakresie bezpieczeństwa są dzielone pomiędzy klienta i dostawcę usług w chmurze. Kiedy klienci przenoszą się do chmury AWS Cloud, AWS jest odpowiedzialne za zabezpieczenie podstawowej infrastruktury, która obsługuje chmurę, a klienci są odpowiedzialni za wszystko, co umieścili w chmurze lub połączyli z chmurą. To zróżnicowanie odpowiedzialności jest powszechnie nazywane *bezpieczeństwem chmury* w przeciwieństwie do *bezpieczeństwa w chmurze.*

Ten współdzielony model może pomóc zmniejszyć koszty operacyjne klientów i zapewnić im niezbędną elastyczność i kontrolę nad wdrażaniem infrastruktury w chmurze AWS Cloud. AWS obsługuje, kontroluje i zarządza elementami infrastruktury, począwszy od systemu operacyjnego hosta i warstwy wirtualizacji, a skończywszy na fizycznym zabezpieczeniu obiektów, w których działa usługa. Klienci przejmują odpowiedzialność za system operacyjny klienta i zarządzanie nim (w tym aktualizacje i poprawki bezpieczeństwa), inne powiązane oprogramowanie użytkowe oraz konfigurację zapory sieciowej grupy zabezpieczeń dostarczonej przez AWS. Więcej informacji znajduje się na stronie Model współdzielonej odpowiedzialności za bezpieczeństwo.

Ramy ścisłej zgodności i normy bezpieczeństwa

Zgodnie z zapisami GDPR odpowiednie środki techniczne i organizacyjne mogą wymagać uwzględnienia „zdolności do zapewnienia ciągłej poufności, integralności, dostępności i niezawodności systemów i usług przetwarzania danych”, jak również niezawodnych procesów przywracania, testowania i ogólnego zarządzania ryzykiem.

Program zgodności AWS

Program AWS Compliance umożliwia klientom zapoznanie się z mocnymi mechanizmami kontrolnymi stosowanymi w AWS w celu utrzymania bezpieczeństwa i ochrony danych w chmurze AWS Cloud. Po wbudowaniu systemów w chmurę AWS Cloud odpowiedzialność za zgodność jest dzielona. Dzięki połączeniu zorientowanych na zarządzanie, przyjaznych dla audytora funkcji usług z obowiązującymi standardami zgodności lub audytu, mechanizmy zapewniające zgodność AWS Compliance, takie jak AWS Config, AWS CloudTrail, AWS Identity i Access Management, Amazon GuardDuty i AWS Security Hub opierają się na tradycyjnych programach, które pomagają klientom tworzyć i działać w środowisku kontrolowanym pod względem bezpieczeństwa. Infrastruktura IT, którą AWS zapewnia swoim klientom, jest projektowana i zarządzana zgodnie z najlepszymi praktykami w zakresie bezpieczeństwa i wieloma standardami bezpieczeństwa IT, np.:

- SOC 1/SSAE 16/ISAE 3402 (dawniej SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP i FedRAMP
- DoD SRG
- PCI DSS Poziom 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Tier 3

Ponadto elastyczność i kontrola, jakie zapewnia platforma AWS, umożliwia klientom wdrażanie rozwiązań, które spełniają kilka branżowych standardów[3].

AWS dostarcza klientom szereg informacji na temat swojego środowiska kontroli IT za pośrednictwem białych ksiąg, raportów, certyfikatów, akredytacji i innych poświadczeń od stron trzecich. Więcej informacji znajdziesz na stronie Amazon Web Services: Biała księga Risk and Compliance.

Cloud Computing Compliance Controls Catalog

Cloud Computing Compliance Controls Catalog (C5) to wspierany przez rząd niemiecki system atestacji, który został wprowadzony w Niemczech przez Federalny Urząd Bezpieczeństwa Teleinformatycznego (BSI). Stworzono go, aby pomóc organizacjom zapewnić bezpieczeństwo operacyjne przed powszechnymi atakami cybernetycznymi w kontekście zaleceń niemieckiego rządu dotyczących bezpieczeństwa dostawców usług w chmurze, czyli Security Recommendations for Cloud Providers.

Techniczne i organizacyjne środki ochrony danych oraz środki służące do zabezpieczenia informacji są ukierunkowane na bezpieczeństwo danych w celu zapewnienia poufności, integralności i dostępności. C5 określa wymogi bezpieczeństwa, które mogą być również istotne dla ochrony danych. Certyfikat C5 może być wykorzystywany przez klientów AWS i ich doradców ds. zgodności w celu zapoznania się z zakresem usług związanych z zapewnieniem bezpieczeństwa IT oferowanych przez AWS, gdy klienci przenoszą swoje pliki do chmury. C5 wprowadza zdefiniowany prawnie poziom bezpieczeństwa IT równoważny z poziomem bezpieczeństwa IT-Grundschutz, z dodatkiem środków kontroli specyficznych dla chmury.

C5 zawiera więcej środków kontroli, które dostarczają informacji dotyczących lokalizacji danych, świadczenia usług, miejsca jurysdykcji, istniejącej certyfikacji, obowiązków w zakresie ujawniania informacji oraz opisu pełnego zakresu usług. Korzystając z tych informacji, można ocenić, w jaki sposób regulacje prawne (takie jak prywatność danych), własne zasady lub środowisko zagrożenia odnoszą się do korzystania z usług przetwarzania w chmurze.

Kodeks postępowania CISPE

GDPR rozważa zatwierdzenie kodeksów postępowania, aby pomóc administratorom i podmiotom przetwarzającym dane w wykazaniu zgodności z rozporządzeniem. Jednym z takich kodeksów, który oczekuje na oficjalne zatwierdzenie przez organy UE odpowiedzialne za ochronę danych, jest *CISPE Code of Conduct for Cloud Infrastructure Service Providers* (Kodeks, Kodeks postępowania CISPE)[4]. Kodeks daje klientom poczucie bezpieczeństwa, że ich dostawca usług chmurowych stosuje odpowiednie standardy ochrony danych, które są zgodne z GDPR.

Poniżej przedstawiono kilka kluczowych korzyści płynących z Kodeksu:

- **Precyzuje, kto jest odpowiedzialny za które aspekty ochrony danych** – Kodeks wyjaśnia rolę zarówno dostawcy chmury, jak i klienta w odniesieniu do GDPR, szczególnie w kontekście usług infrastruktury chmury.
- **Określa zasady, których muszą przestrzegać dostawcy** – Kodeks rozwija kluczowe zasady zawarte w GDPR dotyczące jednoznacznych działań i zobowiązań, które powinni podjąć dostawcy w celu wykazania zgodności z wymogami GDPR i pomocy klientom w ich przestrzeganiu. Klienci mogą wykorzystać te konkretne korzyści we własnych strategiach zapewniania zgodności i ochrony danych.
- **Dostarcza klientom informacji dotyczących prywatności i bezpieczeństwa niezbędnych do osiągnięcia zgodności z przepisami** – Kodeks wymaga od dostawców przejrzystości w zakresie kroków podejmowanych w celu wywiązania się ze zobowiązań dotyczących prywatności i bezpieczeństwa. Kilka z tych kroków obejmuje wdrożenie zabezpieczeń prywatności i bezpieczeństwa, powiadamianie o naruszeniach danych, usuwanie danych oraz przejrzystość podwykonawstwa przetwarzania danych przez osoby trzecie. Wszystkie te zobowiązania są weryfikowane przez zewnętrzne, niezależne organy monitorujące. Klienci mogą korzystać z tych informacji, aby w pełni zapoznać się z wysokim poziomem oferowanego bezpieczeństwa.

W chwili publikacji do zarejestrowanych usług AWS w pełni spełniających wytyczne Kodeksu należą Amazon EC2, Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS), AWS Identity and Access Management (IAM), AWS CloudTrail oraz Amazon Elastic Block Store (Amazon EBS). Więcej informacji znajdziesz na stronie CISPE Public Register. Daje to klientom AWS dodatkowe gwarancje, że kiedy korzystają z AWS, mają kontrolę nad swoimi danymi w bezpiecznym, chronionym i zgodnym środowisku. Zgodność z Kodeksem dopełnia listę

uznanych międzynarodowo certyfikatów i akredytacji, które uzyskało AWS. Należą do nich między innymi: ISO 27001, ISO 27018, ISO 9001, SOC 1, SOC 2, SOC 3, PCI DSS Poziom 1.

Kontrola dostępu do danych

Artykuł 25 GDPR stanowi, że administrator „wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania”. Poniższe mechanizmy kontroli dostępu AWS mogą pomóc klientom spełnić ten wymóg, umożliwiając dostęp do zasobów AWS i danych klientów wyłącznie autoryzowanym administratorom, użytkownikom i aplikacjom.

Zarządzanie tożsamością i dostępem AWS

Podczas tworzenia konta AWS automatycznie tworzone jest również konto użytkownika *root*. To konto użytkownika ma pełny dostęp do wszystkich usług AWS i zasobów na koncie AWS. Nie używaj tego konta do wykonywania codziennych zadań, a jedynie do wstępnego tworzenia dodatkowych ról i kont użytkowników oraz do czynności administracyjnych, które tego wymagają. AWS zaleca od samego początku stosowanie zasady najmniejszych uprawnień: zdefiniowanie różnych kont użytkowników i ról dla różnych zadań oraz określenie minimalnego zestawu uprawnień wymaganych do wykonania każdego zadania. Podejście to jest mechanizmem służącym dostrojeniu kluczowej koncepcji wprowadzonej przez GDPR: ochrony danych już w fazie projektowania. AWS Identity and Access Management (IAM) jest usługą sieciową, którą można wykorzystać do bezpiecznej kontroli dostępu do swoich zasobów AWS.

Użytkownicy i role definiują tożsamości IAM z określonymi uprawnieniami. Dzięki usłudze IAM Roles (role IAM) możesz pozwolić każdemu użytkownikowi na wykonywanie określonych zadań, aby mogli je przejąć i wykorzystać tymczasowe uprawnienia do sesji ról. Możesz użyć ról IAM, aby bezpiecznie nadać aplikacjom działającym w Amazon EC2 poświadczenia wymagane do uzyskania dostępu do innych zasobów AWS, takich jak wiadra Amazon S3 oraz bazy danych Amazon RDS lub DynamoDB.

Tymczasowy dostęp do tokenów poprzez AWS STS

Usługę tokenów bezpieczeństwa AWS Security Token Service (AWS STS) można wykorzystać do tworzenia i udostępniania zaufanym użytkownikom tymczasowych poświadczeń bezpieczeństwa, które umożliwiają dostęp do zasobów AWS. Tymczasowe poświadczenia bezpieczeństwa działają niemal identycznie jak poświadczenia klucza dostępu długoterminowego, które podajesz użytkownikom IAM, przy czym występują następujące różnice:

- Tymczasowe poświadczenia bezpieczeństwa są przeznaczone do użytku krótkotrwałego. Można skonfigurować czas ich ważności – od kilku minut do kilku godzin. Po wygaśnięciu tymczasowych poświadczeń AWS nie rozpoznaje ich ani nie zezwala na dostęp z żądań API, które zostały złożone przy ich użyciu.
- Tymczasowe poświadczenia bezpieczeństwa nie są przechowywane na koncie użytkownika. Są generowane dynamicznie i dostarczane użytkownikowi na żądanie. Kiedy (lub zanim) tymczasowe poświadczenia bezpieczeństwa wygasną, użytkownik może zażądać nowych poświadczeń, jeśli ma do tego uprawnienia.

W przypadku korzystania z poświadczeń tymczasowych zróżnicowanie to zapewnia poniższe korzyści:

- Nie musisz rozpowszechniać lub osadzać długoterminowych poświadczeń bezpieczeństwa AWS w aplikacji.
- Poświadczenia tymczasowe są podstawą dla ról i federacji tożsamości. Możesz zapewnić użytkownikom dostęp do swoich zasobów AWS poprzez zdefiniowanie ich tymczasowej tożsamości AWS.
- Tymczasowe poświadczenia bezpieczeństwa mają ograniczony okres użytkowania, który można dostosowywać. Z tego powodu nie musisz ich rotować ani jednoznacznie odwoływać, kiedy nie są już potrzebne. Po wygaśnięciu tymczasowych poświadczeń bezpieczeństwa nie mogą być one ponownie wykorzystane. Możesz określić maksymalny czas ważności danych uwierzytelniających.

Uwierzytelnianie wieloczynnikowe

Dla dodatkowego bezpieczeństwa możesz dodać do swojego konta i indywidualnych kont użytkowników uwierzytelnianie dwuskładnikowe. Przy włączonym uwierzytelnianiu wieloczynnikowym (MFA), po zalogowaniu się na stronę internetową AWS, pojawia się prośba o podanie nazwy użytkownika i hasła (pierwszy składnik), a także odpowiedzi uwierzytelniającej z urządzenia AWS MFA (drugi składnik). Możesz włączyć MFA dla swojego konta AWS i dla indywidualnych użytkowników IAM, których stworzyłeś(-aś) na swoim koncie. Możesz również użyć MFA do kontrolowania dostępu do API usług AWS.

Możesz na przykład zdefiniować zasadę, która pozwala na pełny dostęp do wszystkich operacji AWS API w Amazon EC2, ale jednoznacznie odmawia dostępu do określonych operacji API – takich jak *StopInstances* i *TerminateInstances* – jeśli użytkownik nie jest uwierzytelniony przez MFA.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllActionsForEC2",
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
            "Effect": "Deny",
            "Action": [
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
            }
        }
    ]
}
```

Rysunek 1 – Wymóg MFA dla konkretnych operacji API Amazon EC2

Dostęp do zasobów obiektów AWS

Aby wprowadzić granularny dostęp do swoich obiektów AWS, możesz przyznać różne poziomy uprawnień różnym osobom dla różnych zasobów.
Możesz na przykład zezwolić tylko niektórym użytkownikom na pełny dostęp do Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), Amazon DynamoDB, Amazon Redshift czy innych usług AWS.

W przypadku innych użytkowników możesz zezwolić na dostęp tylko do odczytu tylko do niektórych wiader Amazon S3, administrowanie tylko niektórymi instancjami Amazon EC2 lub na dostęp tylko do informacji o rozliczeniach.

Poniższe zasady to przykład jednej z metod, które można wykorzystać, aby umożliwić wszystkie działania na konkretnym wiadrze Amazon S3 i jednoznacznie odmówić dostępu do każdej usługi AWS różnej od Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        },
        {
            "Effect": "Deny",
            "NotAction": "s3:*",
            "NotResource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*"
            ]
        }
    ]
}
```

Rysunek 2 – Zarządzanie ograniczone do konkretnego wiadra Amazon S3

Możesz dołączyć zasadę do konta użytkownika lub roli. Inne przykłady zasad IAM znajdziesz na stronie Example IAM Identity-Based Policies (Przykładowe zasady IAM oparte na tożsamości).

Dostęp do danych operacyjnych i konfiguracyjnych

Możesz użyć managera systemów AWS (AWS Systems Manager), aby zobaczyć operacje swojej infrastruktury AWS i zarządzać nimi. Możesz audytować i egzekwować zgodność ze zdefiniowanymi stanami. AWS Systems Manager Parameter Store (pamięć parametrów managera systemów AWS) może centralnie zarządzać danymi definiującymi parametry. Pozwala to na wprowadzenie granularnego dostępu do danych parametrów, niezależnie od tego, czy są to dane tekstowe (takie jak ciągi baz danych) czy też dane tajne (takie jak hasła). Możesz zapewnić kontrolę dostępu poprzez indywidualne uprawnienia dla użytkowników i zasobów (takich jak instancje) w celu uzyskania dostępu do parametrów i wykorzystania integracji z IAM. Na przykład w środowisku programistycznym dane uwierzytelniające są często zapisywane na stałe. Zamiast zapisywać swoje poświadczenia bezpieczeństwa na stałe, możesz użyć Parameter Store do zapisywania haseł i umożliwienia deweloperom dostępu do poświadczeń za pomocą usługi AWS API get-parameter.

Poniższy wycinek API pokazuje sposób odzyskiwania hasła *get-parameter*:

```
password=$(aws ssm get-parameters --region us-east-1 --names MySecureSQLPassword
```

Inną dostępną opcją ochrony tajnych informacji potrzebnych do uzyskania dostępu do aplikacji, usług i zasobów IT jest usługa AWS Secrets Manager. Usługa umożliwia łatwe rotowanie, zarządzanie i pobieranie danych uwierzytelniających bazy danych, kluczy API i innych informacji tajnych przez cały ich cykl życia. Użytkownicy i aplikacje pobierają informacje tajne, wywołując interfejsy API Secrets Manager, czym eliminują potrzebę kodowania informacji wrażliwych na stałe w zwykłym tekście. Secrets Manager oferuje tajne rotowanie z wbudowaną integracją dla Amazon RDS, Amazon Redshift i Amazon DocumentDB.

Ograniczenia geograficzne

Możesz użyć ograniczeń geograficznych, zwanych również geoblocking, aby uniemożliwić użytkownikom w określonych lokalizacjach geograficznych dostęp do treści dystrybuowanych za pośrednictwem dystrybucji internetowej Amazon CloudFront.

Istnieją dwie możliwości zastosowania ograniczeń geograficznych:

- **CloudFront geo-restriction feature** – wybierz tę opcję, aby ograniczyć dostęp do wszystkich plików związanych z dystrybucją CloudFront oraz aby ograniczyć dostęp na poziomie krajowym.
- **Third-party geolocation service** – wybierz tę opcję, aby ograniczyć dostęp do podzbioru plików związanych z dystrybucją lub aby ograniczyć dostęp na poziomie granularności niższym niż poziom krajowy.

Poza tymi dwiema opcjami dla nowo uruchomionych Regionów istnieją możliwości geo-limitingu. Podczas gdy regiony AWS Regions wprowadzone przed 20 marca 2019 r. są automatycznie aktywne, regiony wprowadzone po 20 marca 2019 r., np. Azja–Pacyfik (Hongkong) i Bliski Wschód (Bahrajn) są domyślnie nieaktywne. Zanim będziesz mógł korzystać z tych regionów, musisz je aktywować. Jeśli region AWS jest domyślnie nieaktywny, możesz użyć konsoli AWS Management Console, aby go aktywować lub dezaktywować. Aktywowanie i dezaktywowanie regionów AWS pozwala na kontrolę, czy użytkownicy na Twoim koncie AWS mają dostęp do zasobów w danym regionie.[5]

Kontrola dostępu do aplikacji internetowych i aplikacji mobilnych

AWS świadczy usługę zarządzania kontrolą dostępu do danych w ramach swoich aplikacji. Jeśli musisz dodać funkcje logowania użytkownika i kontroli dostępu do aplikacji internetowych i aplikacji mobilnych, możesz użyć Amazon Cognito. Amazon Cognito User Pools oferuje bezpieczny katalog użytkownika, który skaluje się do setek milionów użytkowników. Aby chronić tożsamość użytkowników, można do puli użytkowników dodać uwierzytelnianie wieloczynnikowe (MFA). Można również użyć uwierzytelniania adaptacyjnego, które wykorzystuje model oparty na ryzyku, aby przewidzieć, kiedy może być potrzebny inny czynnik uwierzytelniający.

Dzięki Amazon Cognito możesz sprawdzić, kto uzyskał dostęp do Twoich zasobów i skąd pochodzi dostęp (aplikacja mobilna czy internetowa). Informacje te można wykorzystać do tworzenia zasad bezpieczeństwa, które umożliwiają lub uniemożliwiają

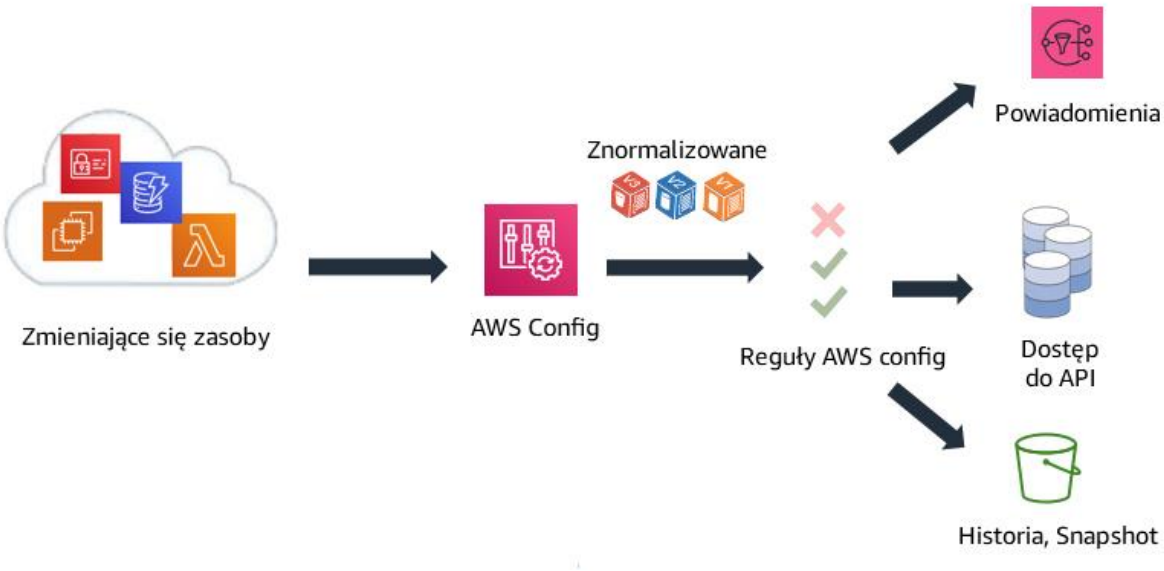
dostęp do zasobów w zależności od rodzaju źródła dostępu (aplikacja mobilna lub internetowa).

Monitorowanie i logowanie

Artykuł 30 GDPR stanowi, że „każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają”. Ten artykuł zawiera również szczegółowe informacje o tym, które informacje muszą być rejestrowane podczas monitorowania przetwarzania wszystkich danych osobowych zgodnie z wymogami GDPR. Administratorzy i podmioty przetwarzające dane są również zobowiązani do terminowego wysyłania powiadomień o naruszeniach, dlatego ważne jest szybkie wykrywanie incydentów. Aby pomóc klientom wywiązać się z tych zobowiązań, AWS oferuje następujące usługi monitorowania i logowania.

Zarządzanie zasobami i ich konfiguracja z AWS Config

AWS Config umożliwia szczegółowy wgląd w konfigurację zasobów AWS na Twoim koncie AWS. Obejmuje to sposób, w jaki zasoby są powiązane ze sobą i jak były wcześniej skonfigurowane, aby można było zobaczyć, jak konfiguracje i relacje zmieniają się w czasie.



Rysunek 1 – Monitorowanie zmiany konfiguracji w czasie z AWS Config

Zasobem AWS jest jednostka, z którą można pracować w AWS, np. instancja Amazon Elastic Compute Cloud (EC2), wolumin Amazon Elastic Block Store (EBS), grupa zabezpieczeń czy Amazon Virtual Private Cloud (VPC). Pełna lista zasobów AWS

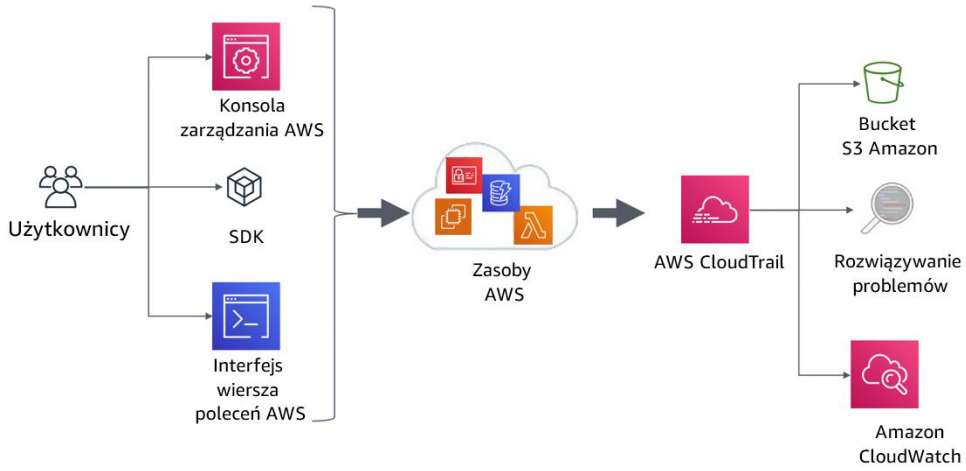
obsługiwanych przez AWS Config znajduje się na stronie internetowej Supported AWS Resource Types.

Zastosowanie AWS Config pozwala na wykonanie następujących działań:

- Ocena konfiguracji zasobów AWS w celu sprawdzenia, czy ustawienia są poprawne.
- Uzyskanie zrzutu bieżących konfiguracji obsługiwanych zasobów, które są powiązane z Twoim kontem AWS.
- Uzyskanie konfiguracji jednego lub więcej zasobów, które istnieją na Twoim koncie.
- Uzyskanie historycznych konfiguracji jednego lub więcej zasobów.
- Otrzymanie powiadomienia o utworzeniu, modyfikacji lub usunięciu zasobu.
- Sprawdzenie relacji między zasobami. Na przykład w sytuacji gdy chcesz znaleźć wszystkie zasoby, które korzystają z określonej grupy zabezpieczeń.

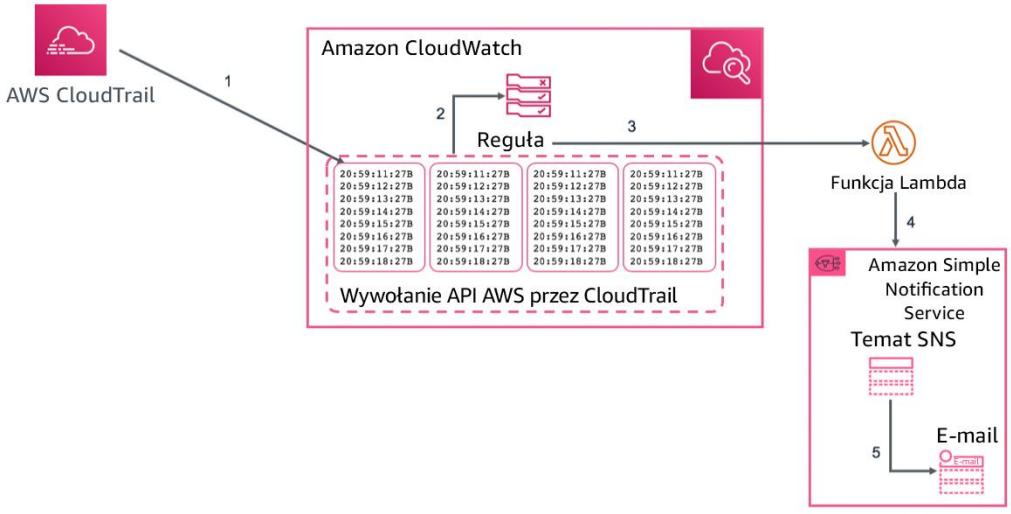
Audyt zgodności i analiza bezpieczeństwa z AWS CloudTrail

Dzięki AWS CloudTrail możesz na bieżąco monitorować aktywność swojego konta AWS. Przechwytywana jest historia wywołań API AWS dla Twojego konta, w tym wywołań API wykonywanych przez konsolę AWS Management Console, AWS SDK, narzędzia wiersza poleceń i usługi AWS wyższego rzędu. Możesz określić, którzy użytkownicy i konta wywołali API AWS dla usług obsługujących CloudTrail, źródłowy adres IP, z którego wykonano wywołania i kiedy wywołania zostały wykonane. Możesz zintegrować CloudTrail z aplikacjami za pomocą API, zautomatyzować tworzenie ścieżek dla swojej organizacji, sprawdzić status swoich ścieżek oraz kontrolować, w jaki sposób administratorzy aktywują i dezaktywują logowanie CloudTrail. Do celów audytowych lub rozwiązywania problemów możesz organizować i przechowywać logi CloudTrail w wiadrze Amazon S3.



Rysunek 2 – Przykładowa architektura audytu zgodności i analizy bezpieczeństwa w AWS CloudTrail

Logi AWS CloudTrail mogą również wyzwalać wstępnie skonfigurowane zdarzenia Amazon CloudWatch. Możesz użyć tych zdarzeń w celu powiadomienia użytkowników lub systemów o wystąpieniu zdarzenia lub w celu przeprowadzenia działań naprawczych. Na przykład jeśli chcesz monitorować działania w instancjach Amazon EC2, możesz utworzyć regułę CloudWatch Event. W przypadku gdy na instancji Amazon EC2 ma miejsce określona czynność i zdarzenie jest przechwycone w logach, reguła wyzwala funkcję AWS Lambda, która wysyła do administratora wiadomość e-mail z powiadomieniem o zdarzeniu (kiedy nastąpiło, który użytkownik wykonał akcję, szczegóły Amazon EC2 itp.). Poniższy schemat przedstawia architekturę powiadamiania o zdarzeniu.



Rysunek 3– Przykład powiadomienia o zdarzeniu AWS CloudTrail

Formaty logów

Kiedy aktywujesz logowanie, możesz uzyskać szczegółowe logi dostępu dla żądań, które są wysyłane do Twojego wiadra Amazon S3.
Zapis w logu dostępu zawiera szczegóły dotyczące żądania, takie jak typ żądania, zasoby określone w żądaniu oraz godzinę i dzień przetworzenia żądania. Więcej informacji na temat zawartości komunikatu logu znajdziesz w części Amazon S3 Server Access Log Format przewodnika *Amazon Simple Storage Service Developer Guide*.

Dzienniki dostępu do serwera są przydatne dla wielu aplikacji, ponieważ dają właścicielom wiader wgląd w charakter żądań klientów, którzy nie są pod ich kontrolą. Domyślnie Amazon S3 nie gromadzi logów dostępu do usług, ale gdy aktywujesz logowanie, Amazon S3 co godzinę przekazuje logi dostępu do wiadra.

Informacja taka obejmuje:

- Granularne logowanie dostępu do obiektów Amazon S3
- Szczegółowe informacje na temat przepływów w sieci poprzez VPC-Flow Logs
- Weryfikację konfiguracji w oparciu o reguły i działania z wykorzystaniem reguł AWS Config Rules
- Filtrowanie i monitorowanie dostępu HTTP do aplikacji z funkcjami WAF w CloudFront

Logi są również użytecznym źródłem informacji do wykrywania zagrożeń. Amazon GuardDuty analizuje logi z AWS CloudTrail, VPC Flow Logs i AWS DNS, co pozwala na bieżące monitorowanie kont AWS i ich obciążenie. W celu dostarczenia w każdej chwili szczegółowych ostrzeżeń z możliwością działania w przypadku wykrycia złośliwej aktywności lub nieautoryzowanego zachowania, usługa ta wykorzystuje uczenie się maszynowe, analizę zagrożeń i wykrywanie anomalii.

Scentralizowane zarządzanie bezpieczeństwem

Wiele organizacji stoi przed wyzwaniami związanymi z widocznością i scentralizowanym zarządzaniem swoim środowiskiem.
W miarę jak rośnie Twój ślad operacyjny, to wyzwanie może się nasilać, chyba że uważnie przeanalizujesz swoje zabezpieczenia. Brak wiedzy, zdecentralizowane i nierównomierne zarządzanie procesami administracji i zabezpieczeń może narazić Twoje środowisko na niebezpieczeństwo.

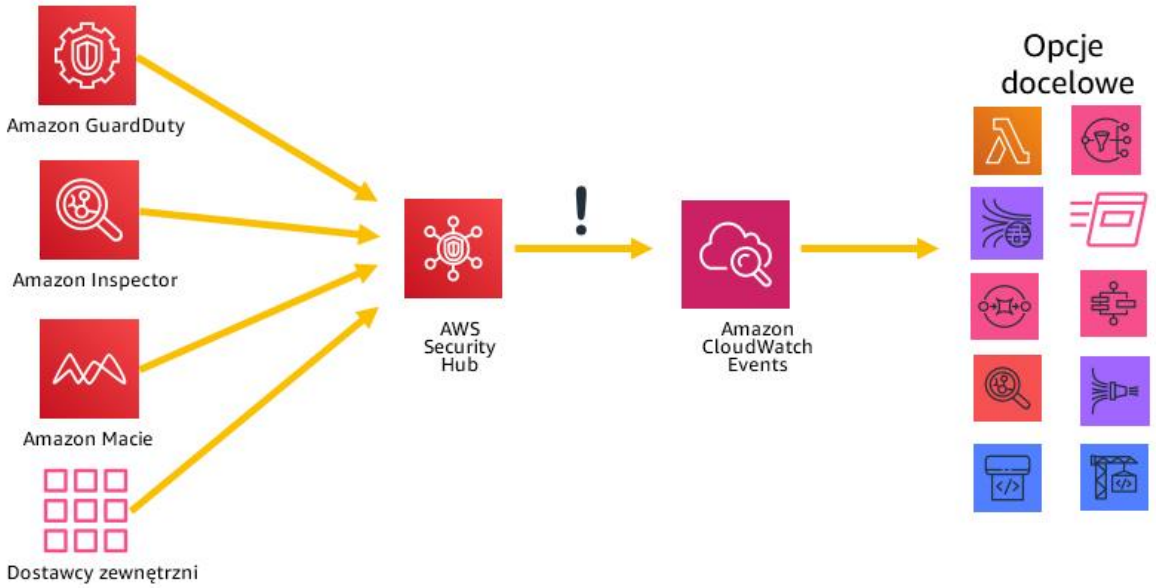
AWS oferuje narzędzia, które pomogą Ci sprostać niektórym z najbardziej wymagających zadań w zakresie zarządzania i administrowania IT oraz służące ochronie danych poprzez podejście uwzględniające bezpieczeństwo już na etapie projektowania.

AWS Control Tower zapewnia łatwą metodę konfigurowania i administrowania nowym, bezpiecznym, środowiskiem AWS obsługującym wiele kont. Automatyzuje konfigurację strefy docelowej [6] będącej środowiskiem składającym się z wielu kont, która jest oparta na najlepszych praktykach i umożliwia administrowanie przy użyciu osłon zabezpieczających, które można wybrać z wcześniej przygotowanej listy. Osłony wdrażają reguły administrowania w zakresie bezpieczeństwa, zgodności i operacji. AWS Control Tower umożliwia zarządzanie tożsamością przy użyciu domyślnego katalogu AWS Single Sign-On oraz audyt krzyżowy kont przy użyciu AWS SSO i AWS IAM. Centralizuje również logi pochodzące z logów Amazon CloudTrail i AWS Config, które są przechowywane w Amazon S3.

AWS Security Hub to kolejna usługa, która usprawnia centralizację i może poprawić widoczność w organizacji.
Usługa Security Hub centralizuje i nadaje priorytet ustaleniom dotyczącym bezpieczeństwa i zgodności z przepisami kont i usług AWS. Można ją także zintegrować z oprogramowaniem zabezpieczającym innych partnerów, aby pomóc w analizowaniu trendów w zakresie bezpieczeństwa i identyfikowaniu problemów dotyczących bezpieczeństwa o najwyższym priorytecie.

Usługa **Amazon CloudWatch Events** umożliwia skonfigurowanie konta AWS do wysyłania zdarzeń na inne konta AWS lub pełnienie funkcji odbiorcy zdarzeń z innych kont lub organizacji. Mechanizm ten może być bardzo przydatny przy wdrażaniu krzyżowych scenariuszy reagowania na incydenty poprzez podejmowanie w odpowiednim czasie działań naprawczych (na przykład poprzez wywołanie funkcji

Lambda lub uruchomienie polecenia na instancji EC2), w zależności od potrzeb, w każdym przypadku wystąpienia zdarzenia zagrażającego bezpieczeństwu.



Rysunek 4 – Podejmowanie działań z AWS Security Hub i Amazon CloudWatch Events

AWS Organizations pomaga w centralnym zarządzaniu i administrowaniu bardzo złożonymi środowiskami. Zapewnia kontrolę dostępu, zgodność i bezpieczeństwo w środowisku obsługującym wiele kont. AWS Organizations wspomaga zasadę kontroli usług, czyli Service control Policy (SCP), która określa działania usług AWS dostępne dla różnych kont w organizacji.

Ochrona danych w AWS

Artykuł 32 GDPR wymaga od organizacji, żeby wdrożyły „odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi… pseudonimizację i szyfrowanie danych osobowych…”. Ponadto organizacje muszą zabezpieczyć się przed nieuprawnionym ujawnieniem lub dostępem do danych osobowych.

Szyfrowanie zmniejsza ryzyko związane z przechowywaniem danych osobowych, ponieważ bez właściwego klucza dane są nieczytelne. Szczegółowa strategia szyfrowania może pomóc złagodzić wpływ różnych zdarzeń związanych z bezpieczeństwem, w tym niektórych naruszeń bezpieczeństwa.

Szyfrowanie danych w spoczynku

Encrypting data at rest (szyfrowanie danych w spoczynku) ma zasadnicze znaczenie dla zgodności z przepisami i ochrony danych. Pomaga zagwarantować, że żaden użytkownik lub aplikacja nie będzie mogła odczytać wrażliwych danych zapisanych na dyskach bez ważnego klucza. AWS oferuje wiele opcji szyfrowania w spoczynku i zarządzania kluczami szyfrowania. Na przykład do szyfrowania dowolnych danych można użyć usługi AWS Encryption SDK z kluczem głównym klienta (CMK) utworzonym i zarządzanym w AWS Key Management Service (AWS KMS).

Zaszyfrowane dane można bezpiecznie przechowywać w spoczynku i rozszyfrować tylko przez stronę posiadającą autoryzowany dostęp do CMK. W rezultacie otrzymujesz poufne dane zaszyfrowane dynamicznie, mechanizmy reguł autoryzacji i szyfrowania uwierzytelnionego, a także logowanie audytów poprzez AWS CloudTrail. Niektóre usługi podstawowe AWS mają wbudowane funkcje szyfrowania w spoczynku, które umożliwiają szyfrowanie danych przed zapisaniem ich do nieulotnej pamięci masowej. Na przykład za pomocą szyfrowania AES-256 możesz zaszyfrować woluminy Amazon Elastic Block Store (Amazon EBS) i skonfigurować wiadra Amazon Simple Storage Service (Amazon S3) do szyfrowania po stronie serwera (SSE). Usługa Amazon

Relational Database Service (Amazon RDS) wspomaga także szyfrowanie Transparent Data Encryption (TDE).

Inną metodą szyfrowania danych w bazach instancji Linux EC2 jest wykorzystanie wbudowanych bibliotek Linuksa.
Metoda ta szyfruje pliki w sposób przezroczysty, co chroni poufne dane. W rezultacie aplikacje przetwarzające dane nie posiadają informacji na temat szyfrowania na poziomie dysku.

Do szyfrowania plików w bazach instancji można zastosować dwie metody. Pierwszą metodą jest pełne szyfrowanie dysku (disk encryption), w którym cały dysk lub blok w obrębie dysku jest szyfrowany przy użyciu jednego lub więcej kluczy szyfrujących. Pełne szyfrowanie dysku działa poniżej poziomu systemu plików. Jest to funkcja działająca w dowolnym systemie operacyjnym i ukrywa katalogi i informacje o plikach, takie jak nazwa i rozmiar. Przykładowo pełne szyfrowanie dysku oferuje Encrypting File System, który jest rozszerzeniem Microsoft do systemu operacyjnego Windows NT New Technology File System (NTFS).

Drugą metodą jest *szyfrowanie na poziomie systemu plików* (file-system-level encryption).
Dzięki tej metodzie szyfrowane są pliki i katalogi, a nie cały dysk lub partycja. Szyfrowanie na poziomie systemu plików działa na szczycie systemu plików i można je przenosić między systemami operacyjnymi.

W przypadku woluminów non-volatile memory express (NVMe, woluminów pamięci nieulotnej express) SSD instance store volumes (woluminy pamięci masowej na dyskach SSD), domyślną opcją jest szyfrowanie. Dane w pamięci masowej instancji NVMe są szyfrowane przy użyciu szyfru blokowego XTS-AES-256 wprowadzonego w module sprzętowym na instancji. Klucze szyfrujące są generowane przy użyciu modułu sprzętowego i są unikalne dla każdego urządzenia pamięci masowej NVMe. Wszystkie klucze szyfrujące są niszczone, gdy instancja jest zatrzymana lub zamknięta, i nie można ich odzyskać. Nie możesz używać własnych kluczy szyfrujących.

Szyfrowanie danych w tranzycie

AWS stanowczo zaleca szyfrowanie danych w tranzycie z jednego systemu do drugiego, łącznie z zasobami w obrębie systemu AWS i poza nim.

Podczas tworzenia konta AWS, przydziela się mu logicznie wyodrębnioną sekcję chmury AWS Cloud, czyli Amazon Virtual Private Cloud (Amazon VPC). Możesz tam uruchomić zasoby w sieci wirtualnej, którą sam definiujesz. Masz pełną kontrolę nad wirtualnym środowiskiem sieciowym, włącznie z wyborem własnego zakresu adresów IP, tworzeniem podsieci oraz konfiguracją tabel tras i bramek sieciowych. Możesz również utworzyć sprzętowe połączenie sieci Virtual Private Network (VPN, wirtualnej sieci prywatnej) pomiędzy firmowym centrum danych a Amazon VPC, dzięki czemu możesz używać chmury AWS Cloud jako rozszerzenia firmowego centrum danych.

W celu ochrony komunikacji między centrum danych Amazon VPC i firmowym centrum danych możesz wybrać jedną z kilku opcji łączności VPN i wybrać taką, która najlepiej odpowiada Twoim potrzebom. Przy użyciu AWS Client VPN możesz włączyć bezpieczny dostęp do zasobów AWS, korzystając z usług VPN opartych na kliencie. Możesz również użyć innego oprogramowania urządzenia VPN, które możesz zainstalować na instancji Amazon EC2 w swoim Amazon VPC. Możesz też utworzyć połączenie IPsec VPN w celu ochrony komunikacji między VPC a siecią zdalną. Aby utworzyć dedykowane połączenie prywatne z sieci zdalnej do sieci Amazon VPC, możesz użyć usługi AWS Direct Connect. W celu utworzenia połączenia szyfrowanego przez IPsec możesz łączyć to połączenie z AWS Site-to-Site VPN.

AWS udostępnia do komunikacji punkty końcowe HTTPS z wykorzystaniem protokołu TLS (Transport Layer Security), co zapewnia szyfrowanie w tranzycie podczas korzystania z AWS API. Z usługi AWS Certificate Manager (ACM) możesz korzystać w celu generowania, zarządzania i wdrażania prywatnych i publicznych certyfikatów, których używa się w celu utworzenia dla swoich zadań zaszyfrowanego transportu między systemami. Usługa Amazon Elastic Load Balancing jest zintegrowana z ACM i służy do obsługi protokołów HTTPS. Jeśli Twoje treści są dystrybuowane przez Amazon CloudFront, usługa ta obsługuje zaszyfrowane punkty końcowe.

Narzędzia szyfrujące

AWS oferuje różne wysoce skalowalne usługi, narzędzia i mechanizmy szyfrowania danych, które pomagają chronić dane przechowywane i przetwarzane w AWS. Informacje na temat funkcji i prywatności AWS Service można znaleźć w AWS Service Capabilities for Privacy Considerations (Możliwości serwisowe AWS w zakresie ochrony prywatności)[7].

Usługi kryptograficzne AWS wykorzystują szeroki zakres technologii szyfrowania i przechowywania danych, które zostały zaprojektowane w celu zachowania integralności

danych w spoczynku lub w tranzycie. Dla operacji kryptograficznych AWS oferuje cztery podstawowe narzędzia.

- **AWS Key Management Service (AWS KMS)** jest usługą zarządzaną przez AWS, która generuje i zarządza zarówno kluczami głównymi, jak i kluczami danych. Usługa AWS KMS jest zintegrowana z wieloma usługami AWS, co umożliwia szyfrowanie danych po stronie serwera za pomocą kluczy KMS z kont klientów. Sprzętowe moduły bezpieczeństwa KMS (HSM) są zgodne z normą FIPS 140-2 Poziom 2.
- **AWS CloudHSM** oferuje HSM-y, które są zgodne z normą FIPS 140-2 Poziom 3. Przechowują bezpiecznie różne klucze kryptograficzne zarządzane we własnym zakresie, w tym klucze główne i klucze danych.
- **Usługi i narzędzia kryptograficzne AWS**
  - **AWS Encryption SDK** udostępnia bibliotekę szyfrującą po stronie klienta, umożliwiającą wykonywanie operacji szyfrowania i odszyfrowywania *wszystkich* typów danych.
  - **Amazon DynamoDB Encryption Client** udostępnia bibliotekę szyfrującą po stronie klienta do szyfrowania tabel danych przed wysłaniem ich do usługi bazodanowej, np. Amazon DynamoDB.

Usługa zarządzania kluczami AWS

AWS Key Management Service (AWS KMS) jest usługą zarządzaną, która ułatwia tworzenie i kontrolowanie kluczy szyfrujących stosowanych do szyfrowania danych oraz do ochrony kluczy wykorzystuje Hardware Security Modules (HSM-y, sprzętowe moduły bezpieczeństwa).
AWS KMS jest zintegrowana z kilkoma innymi usługami AWS, aby pomóc Ci chronić dane, które są dzięki nim przechowywane. AWS KMS jest również zintegrowana z AWS CloudTrail, aby zapewnić Ci logi wszystkich kluczowych zastosowań do realizacji Twoich potrzeb w zakresie regulacji i zgodności.

Możesz w prosty sposób tworzyć, importować i rotować klucze, a także definiować zasady użytkowania i wykorzystania audytu dzięki AWS Management Console lub korzystając z usługi AWS SDK czy AWS Command Line Interface (AWS CLI).

Klucze główne w AWS KMS, importowane przez użytkownika lub tworzone w jego imieniu przez AWS KMS i nazywane kluczami głównymi klienta (CMK), są przechowywane w bardzo trwałej pamięci masowej w zaszyfrowanym formacie, co

pozwala na ich wykorzystanie kiedy zajdzie taka potrzeba.
W AWS KMS możesz wybrać opcję automatycznego rotowania kodów CMK utworzonych w AWS KMS raz w roku bez konieczności ponownego szyfrowania danych, które zostały już zaszyfrowane kluczem głównym. Nie musisz już śledzić starszych wersji swoich CMK, ponieważ AWS KMS przechowuje je w celu automatycznego odszyfrowania wcześniej zaszyfrowanych danych.

Dla każdego CMK w KMS możesz kontrolować, kto ma dostęp do tych kluczy i z jakimi usługami można je wykorzystać poprzez szereg środków kontroli dostępu, w tym przeniesień i warunków w ramach zasad kluczowych lub zasad IAM. Możesz również importować klucze z własnej infrastruktury zarządzania kluczami i używać ich w usłudze KMS.

Na przykład do poniższej zasady stosuje się warunek *kms:ViaService*, aby umożliwić wykorzystanie klucza CMK zarządzanego przez klienta do określonych działań tylko wtedy, gdy żądanie pochodzi z Amazon EC2 lub Amazon RDS w określonym regionie (*us-west-2)* w imieniu określonego użytkownika (*ExampleUser*).

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:ViaService": [
        "ec2.us-west-2.amazonaws.com",
        "rds.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

Rysunek 7– Przykładowa zasada dla Amazon KMS

Integracja usług AWS

Usługa AWS KMS jest zintegrowana z szeregiem usług AWS (w momencie pisania tego artykułu jest ich ponad pięćdziesiąt). Integracje te pozwalają na łatwe korzystanie z

zestawów kluczy CMK AWS KMS do szyfrowania danych przechowywanych za pomocą tych usług. Oprócz korzystania z CMK zarządzanych przez klienta, szereg zintegrowanych usług umożliwia korzystanie z CMK zarządzanego przez AWS, który został stworzony i jest zarządzany automatycznie, ale może być wykorzystany tylko w ramach konkretnej usługi, która go stworzyła.

Możliwości audytowe

Jeśli na Twoim koncie AWS jest aktywna chmura AWS CloudTrail, każde użycie klucza, który przechowujesz w KMS, jest zapisywane w pliku logu, który jest dostarczany do wiadra Amazon S3 zdefiniowanego przy aktywowaniu chmury AWS CloudTrail. Zapisane informacje zawierają szczegóły dotyczące użytkownika, godziny, dnia i użytego klucza.

Bezpieczeństwo

Usługa AWS KMS została zaprojektowana tak, aby zagwarantować to, że nikt nie ma dostępu do Twoich kluczy głównych. Jest zbudowana na systemach zaprojektowanych, aby chronić klucze główne za pomocą rozbudowanych technik hartowania. Należą do nich: nieprzechowywanie kluczy tekstowych na dysku, nieutrzymywanie ich w pamięci i ograniczanie liczby systemów, które mogą uzyskać dostęp do hostów, które używają kluczy. Cały dostęp do oprogramowania aktualizującego w usłudze jest kontrolowany przez wielostronną kontrolę dostępu, która jest audytowana i weryfikowana przez niezależną grupę w firmie Amazon.

Więcej informacji na temat AWS KMS znajdziesz w białej księdze AWS Key Management Service.

AWS CloudHSM

Usługa AWS CloudHSM pomaga spełnić firmowe, umowne i regulacyjne wymogi zgodności w zakresie bezpieczeństwa danych dzięki zastosowaniu dedykowanych urządzeń modułu bezpieczeństwa sprzętu (HSM) w chmurze AWS Cloud.
Dzięki CloudHSM możesz sterować kluczami szyfrowania i operacjami kryptograficznymi wykonywanymi przez HSM.

Partnerzy AWS i AWS Marketplace oferują różnorodne rozwiązania w zakresie ochrony wrażliwych danych w ramach platformy AWS, ale w przypadku aplikacji i danych podlegających rygorystycznym wymogom umownym lub regulacyjnym w zakresie zarządzania kluczami kryptograficznymi, czasami konieczna jest dodatkowa ochrona. Wcześniej jedyną opcją przechowywania poufnych danych (lub kluczy szyfrujących

chroniących poufne dane) mogło być przechowywanie ich w centrach danych na terenie obiektu. Mogło to uniemożliwić migrację tych aplikacji do chmury lub znacznie spowolnić ich wydajność. Dzięki AWS CloudHSM możesz chronić klucze szyfrujące w systemach HSM zaprojektowanych i zatwierdzonych zgodnie z rządowymi standardami bezpiecznego zarządzania kluczami. Klucze kryptograficzne używane do szyfrowania danych możesz bezpiecznie generować i przechowywać oraz nimi zarządzać, aby mieć pewność, że tylko Ty masz do nich dostęp. AWS CloudHSM pomaga w spełnieniu rygorystycznych wymagań w zakresie zarządzania kluczami bez poświęcania wydajności aplikacji.

Usługa AWS CloudHSM działa z Amazon Virtual Private Cloud (Amazon VPC). Instancje CloudHSM są dostarczane w chmurze Amazon VPC z podanym przez Ciebie adresem IP, co gwarantuje prostą i prywatną łączność sieciową z instancjami Amazon Elastic Compute Cloud (Amazon EC2). Gdy umieszczasz instancje CloudHSM w pobliżu instancji Amazon EC2, zmniejszasz opóźnienie sieci, co może poprawić wydajność aplikacji. AWS oferuje dedykowany i wyłączny (pojedynczy najemca) dostęp do instancji CloudHSM, które są izolowane od innych klientów AWS. Dostępna w wielu regionach i strefach dostępności chmura CloudHSM umożliwia dodanie bezpiecznej i trwałej pamięci masowej kluczy do Twoich aplikacji.

Integracja z usługami AWS i zewnętrznymi aplikacjami

Chmury CloudHSM możesz używać z Amazon Redshift, Amazon Relational Database Service (Amazon RDS) dla Oracle lub aplikacjami innych firm (takimi jak SafeNet Virtual KeySecure) jako Root of Trust, Apache (zakończenie połączenia SSL) lub Microsoft SQL Server (przezroczyste szyfrowanie danych). Możesz jej także użyć, gdy tworzysz własne aplikacje i nadal korzystasz ze znanych Ci standardowych bibliotek kryptograficznych, m.in. PKCS#11, Java JCA/JCE, Microsoft CAPI i CNG.

Działania audytowe

Jeśli musisz śledzić zmiany w zasobach lub audytować działania w celach bezpieczeństwa i zgodności, możesz przejrzeć wszystkie wywołania API CloudHSM wykonane z Twojego konta przez AWS CloudTrail. Dodatkowo możesz audytować operacje na urządzeniu HSM za pomocą sysloga lub wysyłać komunikaty logów do swojego własnego kolektora logów.

Usługi i narzędzia kryptograficzne AWS

AWS oferuje mechanizmy spełniające szereg standardów bezpieczeństwa kryptograficznego, które można wykorzystać do wdrożenia najlepszych praktyk szyfrowania. AWS Encryption SDK[8] to biblioteka szyfrująca po stronie klienta, dostępna w językach Java, Python, C, JavaScript oraz interfejs wiersza poleceń obsługujący systemy Linux, MacOS i Windows. AWS Encryption SDK oferuje zaawansowane funkcje ochrony danych, w tym bezpieczne, uwierzytelnione, symetryczne zestawy algorytmów klucza, takie jak 256-bit AES-GCM z pochodną i podpisywaniem kluczy. W związku z tym, że została zaprojektowana specjalnie dla aplikacji wykorzystujących Amazon DynamoDB, DynamoDB Encryption Client [9] umożliwia użytkownikom ochronę danych z tabeli przed wysłaniem ich do bazy danych. Sprawdza również i odszyfrowuje dane podczas ich pobierania. Klient jest dostępny w języku Java i Python.

Infrastruktura kryptograficzna systemu Linux DM-Crypt

Dm-crypt to mechanizm szyfrowania na poziomie jądra Linuksa, który umożliwia użytkownikom zamontowanie zaszyfrowanego systemu plików. Montowanie systemu plików jest procesem, w którym system plików jest dołączany do katalogu (punktu montowania), który udostępnia go systemowi operacyjnemu. Po zamontowaniu wszystkie pliki w systemie plików są dostępne dla aplikacji bez dodatkowej interakcji. Jednak przy zapisywaniu na dysku pliki te są szyfrowane.

Device mapper to infrastruktura w jądrze Linux 2.6 i 3.x, która umożliwia tworzenie wirtualnych warstw urządzeń blokowych. Device mapper crypt target zapewnia przezroczyste szyfrowanie urządzeń blokowych przy użyciu kernel crypto API. Rozwiązanie wykorzystuje dm-crypt w połączeniu z systemem plików z kopii zapasowej dysku mapowanym do logicznego woluminu przez Logical Volume Manager (LVM). LVM zapewnia logiczne zarządzanie woluminem dla jądra Linuksa.

Ochrona danych w fazie projektowania i domyślnie

Za każdym razem, gdy użytkownik lub aplikacja próbuje korzystać z konsoli AWS Management Console, API AWS lub AWS CLI, do AWS wysyłane jest żądanie. Usługa AWS otrzymuje żądanie i wykonuje zestaw kilku kroków w celu ustalenia, czy należy na nie zezwolić, czy odrzucić, zgodnie z określoną logiką oceny zasad. Wszystkie żądania w AWS są domyślnie odrzucane (stosowana jest domyślna zasada *odrzucania*). Oznacza to, że wszystko, co nie jest jednoznacznie dozwolone przez zasadę, jest odrzucane. AWS sugeruje, zgodnie z definicją zasad i jako najlepszą praktykę, że

należy stosować zasadę najmniejszych przywilejów, co oznacza, że każdy składnik (taki jak użytkownicy, moduły lub usługi) musi mieć dostęp tylko do zasobów niezbędnych do wykonania swoich zadań.

Ta zasada jest zgodna z artykułem 25 GDPR, który stanowi, że administrator „wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania”.

AWS dostarcza również narzędzi do wdrażania infrastruktury jako kodu, co stanowi silny mechanizm włączania zabezpieczeń od samego początku projektowania architektury. AWS CloudFormation określa wspólny język opisujący i udostępniający wszystkie zasoby infrastrukturalne, w tym zasady i procesy dotyczące bezpieczeństwa. Dzięki tym narzędziom i praktykom zabezpieczenia stają się częścią Twojego kodu i można je wersjonować, monitorować i modyfikować (za pomocą systemu wersjonowania) zgodnie z wymaganiami Twojej organizacji. Umożliwia to *ochronę danych już w fazie projektowania*, ponieważ w definiowaniu architektury można uwzględnić procesy i zasady dotyczące bezpieczeństwa, a także stale monitorować za pomocą zabezpieczeń stosowanych w organizacji.

W jaki sposób usługi AWS są pomocne

Obszar	Opis	Usługi i narzędzia AWS
Ramy ścisłej zgodności	Odpowiednie środki techniczne i organizacyjne mogą wymagać uwzględnienia „zdolności do zapewnienia ciągłej poufności, integralności, dostępności i niezawodności systemów i usług przetwarzania danych”.	SOC 1 / SSAE 16 / ISAE 3402 (dawniej SAS 70) / SOC 2 / SOC 3 PCI DSS Poziom 1 ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018 NIST FIPS 140-2 Common Cloud Computing Controls Catalog (C5)
Kontrola dostępu do danych		AWS Identity and Access Management (IAM) Amazon Cognito

Obszar	Opis	Usługi i narzędzia AWS
	Administrator „wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania”.	 AWS WAF
		 AWS CloudFormation
		 AWS Systems Manager
Monitorowanie i logowanie	„Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają”.	 AWS CloudTrail
		 AWS Config
		 Amazon CloudWatch
		 AWS Control Tower
		 Amazon GuardDuty
		 AWS Security Hub
Ochrona danych w AWS	Organizacje muszą „wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi pseudonimizację i szyfrowanie danych osobowych”.	 AWS Tools and SDKs
		 AWS CloudHSM
		 AWS Key Management Service

Współautorzy

Do współautorów tego dokumentu należą między innymi:

- Tim Anderson, Technical Industry Specialist, Amazon Web Services
- Carmela Gambardella, Public Sector Solutions Architect, Amazon Web Services
- Giuseppe Russo, Security Assurance Manager, Amazon Web Services
- Marta Taggart, Senior Program Manager, Amazon Web Services

Zmiany w dokumencie

Data	Opis
Październik 2019	Zaktualizowano w celu uwzględnienia nowych usług AWS.
Wrzesień 2019	Drobne zmiany.
Listopad 2017	Pierwsza publikacja.

Notes

[1] https://ec.europa.eu/info/law/law-topic/data-protection_en

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[3] https://aws.amazon.com/compliance/programs/

[4] https://cispe.cloud/

[5] https://docs.aws.amazon.com/general/latest/gr/rande-manage.html

[6] https://aws.amazon.com/solutions/aws-landing-zone/

[7] https://aws.amazon.com/compliance/data-privacy/service-capabilities/

[8] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-encrypt.html

[9] https://docs.aws.amazon.com/crypto/latest/userguide/awscryp-service-ddb-client.html