Ото переведенный документ на польский язык, отформатированный для удобного чтения в любом Markdown-редакторе:

Szyfrowanie danych w AWS

2020 SOFTPROM (softprom.com | info@softprom.com)

Amazon Web Services Network Partner (Advanced Consulting Partner)

Szyfrowanie danych w AWS

Utrzymanie zaufania klientów to niezmienny priorytet Amazon Web Services (AWS). AWS informuje swoich klientów o politykach ochrony prywatności i bezpieczeństwa danych, a także o stosowanych metodach i technologiach.

AWS przyjmuje na siebie następujące zobowiązania i zapewnia następujące możliwości:

-

Dostęp: Klient przejmuje całkowitą kontrolę nad swoimi treściami i ponosi odpowiedzialność za konfigurację dostępu do usług i zasobów AWS. Aby skutecznie realizować to zadanie, AWS zapewnia rozszerzony zestaw narzędzi do zarządzania dostępem, szyfrowania i rejestrowania zdarzeń (np. AWS Identity and Access Management, AWS Organizations oraz AWS CloudTrail). Ponadto AWS udostępnia interfejsy API do konfiguracji zarządzania uprawnieniami dostępu do wszelkich usług, które klienci tworzą lub wdrażają w środowisku AWS. AWS nie uzyskuje dostępu do treści klientów ani nie wykorzystuje ich do jakichkolwiek celów bez odpowiedniej zgody. AWS w żadnym wypadku nie wykorzystuje treści klientów ani powiązanych z nimi informacji w celach marketingowych i reklamowych.

-

Przechowywanie: Klienci wybierają regiony AWS do przechowywania swoich treści, a także typ pamięci masowej. Klienci mogą replikować treści między regionami AWS i tworzyć kopie zapasowe w wielu regionach. AWS nie będzie przenosić ani replikować treści poza wybrane przez klienta regiony AWS bez jego zgody, z wyjątkiem nielicznych przypadków, gdy wymagają tego przepisy prawa lub wiążący nakaz organu państwowego.

-

Bezpieczeństwo: Klienci wybierają sposoby ochrony swoich treści. AWS oferuje niezawodne środki szyfrowania treści podczas przesyłania i przechowywania, a także zapewnia klientom możliwość korzystania z własnych kluczy szyfrujących.

Nowe możliwości

- Funkcje szyfrowania danych dostępne w usługach AWS dla pamięci masowych i baz danych, takich jak Amazon Elastic Block Store, Amazon Simple Storage Service, Amazon Relational Database Service i Amazon Redshift.
- Elastyczne opcje zarządzania kluczami, w tym AWS Key Management Service (KMS), pozwalające klientom decydować, czy chcą zachować pełną kontrolę nad kluczami szyfrującymi, czy też przekazać zarządzanie kluczami do AWS.
- Klienci AWS mogą zapewnić szyfrowanie po stronie serwera (SSE) za pomocą kluczy zarządzanych przez Amazon S3 (SSE-S3), AWS KMS (SSE-KMS) lub przy użyciu własnych kluczy (SSE-C).

Ujawnianie treści klientów

AWS pod żadnym pozorem nie ujawnia treści klientów, z wyjątkiem przypadków, gdy wymaga tego prawo lub wiążące postanowienie wydane przez organ państwowy.

Jeśli organ państwowy kieruje do AWS żądanie udostępnienia treści klienta, AWS zawsze sugeruje, aby zwrócił się o te dane bezpośrednio do klienta. Jeśli AWS będzie zmuszony ujawnić treści klienta organowi państwowemu, klient otrzyma uzasadnione powiadomienie o tym żądaniu, aby mógł przygotować zabezpieczający nakaz sądowy lub inny instrument ochrony prawnej, o ile AWS ma do tego prawo.

Gwarancja bezpieczeństwa

Opierając się na międzynarodowych wytycznych dotyczących ochrony danych i prywatności, AWS opracował program zapewnienia bezpieczeństwa, który pomaga klientom bezpiecznie pracować w AWS i w pełni korzystać z naszego środowiska zarządzania bezpieczeństwem. Procesy zapewniania bezpieczeństwa w AWS oraz zarządzania nim były wielokrotnie weryfikowane przez niezależnych specjalistów zewnętrznych.

Jak AWS klasyfikuje dane klientów

W AWS dane klientów dzielą się na dwie kategorie: **treść klienta** (customer content) oraz **dane konta** (account data).

-

Treść klienta: Obejmuje oprogramowanie (w tym obrazy maszyn), dane, pliki tekstowe, audio, wideo oraz obrazy, które klient lub jakikolwiek użytkownik końcowy przenosi do naszego systemu w celu przetwarzania, przechowywania lub hostowania za pomocą usług AWS w ramach konta klienta, a także wszelkie wyniki obliczeń, które klient lub użytkownik końcowy uzyskuje w wyniku korzystania z usług AWS. Na przykład treść klienta obejmuje wszelkie informacje, które klient lub użytkownicy końcowi przechowują w Amazon Simple Storage Service (S3). Treść klienta nie obejmuje danych konta. Do treści klienta mają zastosowanie warunki Umowy Klienta AWS oraz Warunki Korzystania z Usług AWS.

-

Dane konta: To informacje o kliencie, które przekazuje on w celu utworzenia konta lub administrowania nim. Dane konta obejmują na przykład: imiona i nazwiska, nazwy użytkowników, numery telefonów, adresy e-mail oraz informacje o płatnościach powiązane z kontem klienta. Do danych konta stosuje się metody pracy z informacjami opisane w Oświadczeniu AWS o ochronie prywatności.

Zgodność ze standardami

Amazon Web Services (AWS) umożliwia klientom szyfrowanie danych za pomocą usług szyfrowania zgodnych z wymaganiami FIPS 140-2 (dla danych w podróży) oraz standardu FIPS-197 (dla danych w spoczynku).

AWS Key Management Service (KMS) pozwala bez trudu tworzyć klucze kryptograficzne dla wszystkich procesów szyfrowania, zarządzać nimi i używać ich w aplikacjach oraz różnych usługach AWS. Usługa AWS KMS charakteryzuje się niezawodnością i odpornością na awarie; do ochrony kluczy wykorzystuje sprzętowe moduły bezpieczeństwa (HSM), które zostały zweryfikowane lub są w trakcie weryfikacji pod kątem zgodności ze standardem FIPS 140-2. Klucze te nigdy nie opuszczają sprzętowych modułów bezpieczeństwa AWS KMS (zgodnych z FIPS) w postaci niezaszyfrowanej i nie są przekazywane personelowi AWS.

AWS KMS jest zintegrowany z usługą AWS CloudTrail i dostarcza dzienniki użycia kluczy w celu zapewnienia zgodności z przepisami i standardami.

Środki zarządzania bezpieczeństwem i jakością usługi AWS KMS zostały potwierdzone i certyfikowane w ramach następujących programów zgodności:

- **SOC 1, SOC 2 i SOC 3:** Raporty z audytów Service Organization Controls. Kopię tych raportów można pobrać w AWS Artifact.
-

PCI DSS Level 1: Szczegółowe informacje na temat zgodności usług AWS ze standardem PCI DSS znajdują się na stronie pytań i odpowiedzi dotyczących PCI DSS.

-

FIPS 140-2: Wszystkie moduły kryptograficzne AWS KMS zostały już zweryfikowane lub są w trakcie weryfikacji pod kątem zgodności z normą FIPS 140-2 Level 2, a w niektórych aspektach (w tym ochrony fizycznej) – Level 3. Szczegóły można znaleźć w certyfikacie FIPS 140-2 dla modułów HSM usługi AWS KMS oraz w odpowiedniej polityce bezpieczeństwa.

-

FedRAMP: Więcej informacji na stronie zgodności z FedRAMP.

-

HIPAA: Więcej informacji na stronie zgodności z HIPAA.

Własny magazyn kluczy (Custom Key Store)

AWS KMS pozwala na utworzenie własnego magazynu kluczy z wykorzystaniem sprzętowych modułów HSM zarządzanych przez klienta. Dla każdego własnego magazynu kluczy klaster AWS CloudHSM tworzy kopię zapasową.

Podczas tworzenia klucza Customer Master Key (CMK) we własnym magazynie kluczy, usługa generuje materiał klucza i zapisuje go w klastrze AWS CloudHSM, który znajduje się pod pełną kontrolą klienta. Kiedy używasz CMK z własnego magazynu kluczy, wszystkie operacje kryptograficzne z tym kluczem są wykonywane w Twoim klastrze AWS CloudHSM.

Klucze CMK zapisane we własnym magazynie i zarządzane przez klienta – podobnie jak każde inne CMK – mogą być używane w dowolnej usłudze AWS zintegrowanej z AWS KMS. Korzystanie z własnego magazynu kluczy wiąże się jednak z dodatkowymi kosztami za klaster AWS CloudHSM. Odpowiedzialność za dostępność materiału klucza w tym klastrze ponosi sam klient.

AWS CloudHSM to chmurowy sprzętowy moduł bezpieczeństwa (HSM), który pozwala bez trudu generować i stosować własne kluczy szyfrujące w chmurze AWS. Za pomocą CloudHSM można zarządzać kluczami, korzystając z modułów HSM zweryfikowanych pod kątem zgodności ze standardem FIPS 140-2 Level 3. CloudHSM zapewnia elastyczność integracji z aplikacjami za pomocą standardowych interfejsów API, takich jak PKCS#11, Java Cryptography Extensions (JCE) oraz biblioteki Microsoft CryptoNG (CNG).

Architektura AWS CloudHSM

AWS CloudHSM działa wewnątrz chmury użytkownika – Amazon Virtual Private Cloud (VPC), co pozwala na łatwe użycie modułów HSM z aplikacjami uruchomionymi na instancjach Amazon EC2. Podczas pracy z CloudHSM można korzystać ze standardowych narzędzi bezpieczeństwa sieciowego VPC do zarządzania dostępem do modułów HSM.

Aplikacje klienta łączą się z modułami HSM za pomocą kanałów SSL z dwustronną uwierzytelnieniem, które są ustanawiane przez oprogramowanie klienckie HSM. Ponieważ moduły HSM znajdują się w centrach danych Amazon w bezpośrednim sąsiedztwie instancji EC2, opóźnienia sieciowe między aplikacjami a modułami HSM są znacznie mniejsze w porównaniu z użyciem modułów lokalnych (on-premise).

Kluczowe założenia architektury (Diagram komponentów):

-

A. AWS zarządza samym sprzętem modułu bezpieczeństwa (HSM), ale nie ma dostępu do kluczy klienta.

-

B. Użytkownik w pełni kontroluje swoje klucze i zarządza nimi.

-

C. Wydajność aplikacji wzrasta ze względu na bliską odległość od środowisk roboczych AWS.

-

D. Klucze są bezpiecznie przechowywane w odpornych na manipulacje modułach sprzętowych w wielu strefach dostępności (AZ).

-

E. Moduły HSM znajdują się wewnątrz Virtual Private Cloud (VPC) i są odizolowane od innych sieci AWS.

W architekturze usługi AWS CloudHSM przewidziano podział obowiązków oraz kontrolę dostępu opartą na rolach (RBAC). AWS monitoruje stan techniczny i dostępność sieciową modułów CloudHSM, ale nie uczestniczy w tworzeniu danych kluczy ani w zarządzaniu nimi. Klient samodzielnie zarządza modułami HSM, generuje i wykorzystuje swoje klucze.

Klucze asymetryczne

AWS KMS zapewnia możliwość tworzenia i używania asymetrycznych kluczy CMK oraz asymetrycznych par kluczy danych. Możesz wyznaczyć CMK do roli pary kluczy do podpisywania lub do szyfrowania. Generowanie par kluczy oraz asymetryczne operacje kryptograficzne na takich kluczach CMK są wykonywane bezpośrednio w sprzętowych modułach HSM.

Możesz zażądać części publicznej asymetrycznego klucza CMK do użytku w aplikacjach lokalnych, natomiast część prywatna nigdy nie opuszcza granic usługi.

Za pomocą usługi możesz również utworzyć asymetryczną parę kluczy danych. Taka operacja zwraca kopię klucza publicznego i prywatnego w formacie czystego tekstu (plaintext), a także kopię klucza prywatnego zaszyfrowaną dostarczonym przez Ciebie symetrycznym kluczem CMK. Wersje kluczy w formacie czystego tekstu możesz wykorzystać w aplikacji lokalnej, a zaszyfrowaną kopię klucza prywatnego zapisać osobno do użycia w przyszłości.

Wykaz wspomnianych usług AWS

Przykład użycia	Usługa AWS
Przechowywanie kluczy i zarządzanie nimi	**AWS Key Management Service (KMS)**

|
| Sprzętowy magazyn kluczy dla zgodności z przepisami |
AWS CloudHSM

|
| Rotacja, pobieranie i zarządzanie poufnymi danymi (sekretami) |
AWS Secrets Manager

|
| Bezpieczne zarządzanie dostępem do usług i zasobów |
AWS Identity & Access Management (IAM)

|
| Bezpłatny portal samoobsługowy z dostępem na żądanie do raportów zgodności AWS |
AWS Artifact

|