Standard bezpieczeństwa danych w branży kart płatniczych (PCI DSS) w AWS

Rok: 2020

Partner: SOFTPROM (softprom.com | info@softprom.com)

Status: Amazon Web Services Network – Advanced Consulting Partner

---

Wprowadzenie do standardu PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) to zastrzeżony standard w dziedzinie bezpieczeństwa informacji. Jest on zarządzany przez Radę ds. Standardów Bezpieczeństwa Branży Kart Płatniczych (PCI SSC), założoną przez firmy American Express, Discover Financial Services, JCB International, MasterCard Worldwide oraz Visa Inc.

Standard PCI DSS dotyczy wszystkich podmiotów prawnych, które zajmują się **przechowywaniem, przetwarzaniem lub przesyłaniem danych posiadaczy kart (CHD)** lub **wrażliwych danych uwierzytelniających (SAD)**. Obejmuje to m.in.:

- Firmy handlowe (merchantów),
- Centra procesingowe,
- Agentów rozliczeniowych (akwarystów),
- Emitentów kart,
- Dostawców usług (service providers).

> *Standard PCI DSS jest zatwierdzany bezpośrednio przez systemy płatnicze, natomiast jego administracją zajmuje się Rada ds. Standardów Bezpieczeństwa PCI.*

Zgodność AWS z wymaganiami PCI DSS

Amazon Web Services (AWS) jest certyfikowanym dostawcą usług **PCI DSS Level 1** — czyli najwyższego dostępnego poziomu oceny. Ocena zgodności infrastruktury AWS została przeprowadzona przez firmę Coalfire Systems Inc., która jest niezależnym, kwalifikowanym audytorem bezpieczeństwa (QSA).

Jak uzyskać dokumentację?

Certyfikat zgodności (AOC — *Attestation of Compliance*) PCI DSS dla AWS oraz szczegółowy przegląd zakresu odpowiedzialności można pobrać na żądanie za pośrednictwem portalu samoobsługowego **AWS Artifact** dostępnego w Konsoli zarządzania AWS.

Korzyści dla klientów:

- **Gotowa infrastruktura:** Wykorzystując usługi AWS do przechowywania, przetwarzania lub przesyłania danych kart płatniczych, możesz polegać na technologicznej infrastrukturze AWS podczas przechodzenia własnej certyfikacji PCI DSS.
- **Bezpieczna izolacja:** Platforma AWS to wirtualne środowisko wielodostępne (multi-tenant). Zastosowano w nim zaawansowane mechanizmy kontroli bezpieczeństwa, które skutecznie izolują klientów w ich własnych, chronionych środowiskach. Architektura ta została pomyślnie przetestowana przez niezależnego audytora QSA.
- **Brak bezpośredniego dostępu:** AWS nie zajmuje się bezpośrednim przechowywaniem, przesyłaniem ani przetwarzaniem danych kartowych Twoich klientów. Zamiast tego udostępnia usługi, na bazie których możesz zbudować własne środowisko danych kart płatniczych (CDE — *Cardholder Data Environment*).

> *Nawet jeśli Twoja organizacja nie wymaga certyfikacji PCI DSS, zgodność usług AWS z tym standardem potwierdza najwyższą dbałość o bezpieczeństwo informacji na wszystkich poziomach i zgodność z najlepszymi praktykami rynkowymi.*

Model wspólnej odpowiedzialności (Shared Responsibility)

Podczas wdrażania środowiska CDE w chmurze AWS, kwalifikowany audytor bezpieczeństwa (QSA) może polegać na certyfikacie AOC wydanym dla AWS bez konieczności przeprowadzania dodatkowych testów fizycznej infrastruktury chmurowej. Certyfikat AWS potwierdza m.in. pełną zgodność zarządzania bezpieczeństwem fizycznym

w centrach danych AWS, co oznacza, że audytor Twojej firmy nie musi ich osobiście kontrolować.

Pakiet zgodności AWS z PCI zawiera:

1. Certyfikat zgodności AWS z wymaganiami PCI DSS 3.2.1 (AOC).
2. Przegląd zakresu odpowiedzialności AWS w ramach zapewniania zgodności z PCI DSS 3.2.1.

AWS znajduje się w globalnym rejestrze dostawców usług Visa oraz na liście zatwierdzonych dostawców usług MasterCard.

Działania śledcze i operacyjne:

AWS **nie jest** uznawany za „Dostawcę hostingu współdzielonego" (Shared Hosting Provider) w rozumieniu standardu PCI DSS, w związku z czym wymaganie **DSS A1.4 nie ma zastosowania**. Zgodnie z Modelem wspólnej odpowiedzialności, AWS daje użytkownikom pełną swobodę w prowadzeniu działań śledczych (forensics) we własnym środowisku AWS bez konieczności angażowania wsparcia ze strony AWS. Służą do tego natywne usługi chmurowe oraz rozwiązania firm trzecich dostępne w AWS Marketplace.

Podejścia do rocznej certyfikacji

Istnieją dwie główne ścieżki potwierdzania zgodności z PCI DSS:

1. **Zewnętrzny audyt (QSA):** Przeznaczony dla organizacji przetwarzających duże wolumeny transakcji. Audytor QSA ocenia infrastrukturę i wystawia Raport ze zgodności (ROC) oraz Certyfikat zgodności (AOC).
2. **Kwestionariusz samooceny (SAQ):** Przeznaczony dla podmiotów o mniejszym wolumenie transakcji, polegający na samodzielnym wypełnieniu odpowiedniego formularza SAQ.

Uwaga: Za utrzymanie i egzekwowanie zgodności odpowiadają bezpośrednio systemy płatnicze oraz agenci rozliczeniowi, a nie Rada ds. Standardów Bezpieczeństwa PCI.

Przegląd wymagań standardu PCI DSS

| Obszar kontrolny | Szczegółowe wymagania standardu

|
| — | — |
| **Budowa i utrzymanie bezpiecznych sieci i systemów** | **1.** Instalowanie i utrzymywanie konfiguracji zapór sieciowych (firewalli) w celu ochrony danych posiadaczy kart.

2. Zmiana haseł systemowych dostarczonych przez producenta i innych domyślnych parametrów bezpieczeństwa. |
| **Ochrona danych posiadaczy kart** | **3.** Ochrona przechowywanych danych posiadaczy kart.

4. Szyfrowanie danych posiadaczy kart podczas ich transmisji w otwartych, publicznych sieciach. |
| **Zarządzanie podatnościami** | **5.** Ochrona wszystkich systemów przed złośliwym oprogramowaniem i regularne aktualizowanie programów antywirusowych.

6. Tworzenie i utrzymywanie bezpiecznych systemów oraz aplikacji. |
| **Wdrożenie rygorystycznej kontroli dostępu** | **7.** Ograniczenie dostępu do danych posiadaczy kart ściśle do celów biznesowych (zasada niezbędnej wiedzy).

8. Identyfikacja i uwierzytelnianie dostępu do komponentów systemu.

9. Ograniczenie fizycznego dostępu do danych posiadaczy kart. |
| **Regularne monitorowanie i testowanie sieci** | **10.** Śledzenie i monitorowanie całego dostępu do zasobów sieciowych i danych posiadaczy kart.

11. Regularne testowanie systemów i procesów bezpieczeństwa. |
| **Utrzymywanie polityki bezpieczeństwa informacji** | **12.** Utrzymywanie i zapewnianie polityki bezpieczeństwa informacji dla wszystkich pracowników. |

Obsługa protokołu TLS w AWS

AWS nie wycofuje globalnie obsługi protokołu TLS 1.0 ze wszystkich usług, ponieważ niektórzy klienci (niepodlegający restrykcjom PCI) wciąż go wymagają. Niemniej jednak, usługi AWS przeanalizowały wpływ wyłączenia TLS 1.0 na klientów i w określonych przypadkach oznaczają ten protokół jako przestarzały.

- **Punkty końcowe FIPS:** Klienci mogą korzystać z punktów końcowych FIPS, aby zapewnić silną kryptografię. AWS aktualizuje wszystkie punkty końcowe FIPS do wersji co najmniej TLS 1.2.
- **Zgodność z PCI:** Wszystkie usługi AWS zgodne z PCI domyślnie obsługują TLS 1.1 lub nowszy.
- **Konfiguracja Load Balancerów:** Klienci są zobowiązani do poprawnego skonfigurowania modułów równoważenia obciążenia (Application Load Balancer lub Classic Load Balancer). Aby wymusić bezpieczną komunikację (np. tylko TLS 1.2), należy wybrać predefiniowaną politykę bezpieczeństwa, np. `ELBSecurityPolicy-TLS-1-2-2018-06`.

Skanowanie ASV (Approved Scanning Vendor)

Jeśli skaner ASV wykryje obecność TLS 1.0 na punkcie końcowym API AWS, oznacza to, że interfejs API wciąż wspiera starszą wersję obok nowszych (TLS 1.1, TLS 1.2) ze względu na inne obciążenia robocze poza zakresem PCI. Klienci mogą udowodnić audytorowi ASV, że punkt końcowy obsługuje bezpieczne protokoły, używając narzędzi takich jak *Qualys SSL Labs*. Odpowiednia wczesna komunikacja z ASV i przedstawienie konfiguracji Elastic Load Balancera (np. z polityką `ELBSecurityPolicy-TLS-1-2-2017-01`) pozwala pomyślnie zamknąć proces sporny dotyczący podatności.

Gotowe szablony infrastruktury: AWS QuickStart dla PCI DSS

W ramach **AWS QuickStart** dostępny jest gotowy pakiet szablonów **AWS CloudFormation**, który pozwala na automatyczne wdrożenie wielowarstwowej architektury aplikacji internetowej opartej na systemie Linux, w pełni zgodnej z PCI DSS w wersji 3.2.1. Pakiet ten składa się z szablonu głównego (bazowego) oraz trzech szablonów dodatkowych.

Główne komponenty szablonu bazowego:

- **AWS Identity and Access Management (IAM):** Podstawowa konfiguracja polityk, grup, ról i profili instancji.
- **Polityka haseł:** Konfiguracja polityki haseł zgodna z rygorystycznymi wytycznymi PCI.

- **Virtual Private Cloud (VPC):** Architektura wielostrefowa (Multi-AZ) z odizolowanymi podsieciami publicznymi i prywatnymi (brak bezpośredniego routingu do internetu) dla baz danych i aplikacji.
- **Bramy NAT (NAT Gateways):** Zapewnienie bezpiecznego wyjścia do internetu dla zasobów z podsieci prywatnych.
- **Host Bastion (Bastion Host):** Bezpieczny punkt dostępowy do zarządzania instancjami Amazon EC2 za pomocą protokołu SSH.
- **Listy kontroli dostępu (Network ACL):** Filtrowanie ruchu sieciowego na poziomie podsieci.
- **Standardowe grupy bezpieczeństwa (Security Groups):** Kontrola ruchu na poziomie instancji EC2.

Dodatkowe pakiety szablonów (Opcje rozszerzone):

Szablon A: Logowanie, monitorowanie i alerty

- **Zasoby:** Konfiguracja systemów zbierania i analizy logów w oparciu o **AWS CloudTrail** oraz **AWS CloudWatch**.
- **Zarządzanie zasobami:** Centralne zarządzanie konfiguracją infrastruktury za pomocą **AWS Config**.
- **Analityka:** Integracja z Amazon ES (Elasticsearch) i interfejsem webowym Kibana do wizualizacji logów.
- **Przechowywanie:** Logi trafiają do centralnego koszyka Amazon S3 z regułami cyklu życia (Lifecycle Policy) przenoszącymi starsze dane do Amazon S3 Glacier.
- **Autoryzacja:** Dostęp autoryzowanych użytkowników realizowany poprzez **Amazon Cognito**.

Szablon B: Warstwa bazodanowa

- **Zasoby:** Uruchomienie bezpiecznego klastra relacyjnej bazy danych **Amazon Aurora** (w architekturze Multi-AZ).
- **Szyfrowanie danych:** Wykorzystanie usługi **AWS KMS** (Key Management Service) do szyfrowania danych w spoczynku (*encrypted data*).
- **Zarządzanie kluczami:** Integracja z **AWS Secrets Manager** do bezpiecznego przechowywania i rotacji poświadczeń.

Szablon C: Trójwarstwowa aplikacja webowa Linux

- **Skalowalność i wydajność:** Implementacja grup automatycznego skalowania (**Auto Scaling Groups**) dla instancji webowych oraz aplikacyjnych (EC2 instances Web / App).
- **Równoważenie obciążenia:** Ruch sieciowy dystrybuowany jest przez **Application Load Balancer**.
- **Ochrona aplikacji:** Wdrożenie zapory sieciowej **AWS WAF** (Web Application Firewall) w celu ochrony przed atakami z sieci.

Przydatne materiały i zasoby PCI DSS

- *Przewodnik dotyczący zapewnienia zgodności z wymaganiami: PCI DSS 3.2.1 w AWS*
- *Opis techniczny AWS PCI 3DS*
- *Szybki start: zgodność z wymaganiami PCI DSS w AWS*
- *Zalecenia dotyczące wirtualizacji PCI DSS*
- *Wytyczne PCI DSS dotyczące chmury obliczeniowej*
- *Przegląd narzędzi ochrony Amazon GuardDuty: zgodność z wymaganiami PCI DSS*