Tytuł szkolenia: Security on AWS

Kod szkolenia: AWS

Wprowadzenie

Wraz z rozrastaniem się infrastruktury i zwiększonej ilości posiadanych kont w chmurze AWS, rośnie potrzeba bezpiecznej komunikacji pomiędzy nimi. Niezależnie od komunikacji wewnątrz wirtualnej serwerowni, niezbędne jest też odpowiednie zabezpieczenie od strony sieciowej wszystkich punktów styku z publicznym Internetem swoich aplikacji. Wraz z mnogością dostępnych narzędzi w Amazonie, rośnie ilość opcji na bezpieczne prowadzenie swoich projektów bez nadmiernego narzutu ze strony zarządzania. Dobre podsumowanie z praktycznym przetestowaniem tych możliwości może okazać się dobrą inwestycją na przyszłość.

Adresaci szkolenia

Szkolenie skierowane jest głównie do:
- osób zarządzających wieloma kontami AWS w swojej firmie (Cross-account access, AWS Organizations),
- osób chcących poznać mechanizmy sieciowe AWS od strony bezpieczeństwa
(NACLs, Security Groups, WAF),
- osób chcących poznać mechanizmy zarządzania dostępem do zasobów w AWS
(resource-based policies, IAM policies, presigned URLs, etc.)
- osób nastawionych na mocno praktyczne szkolenia.

Cel szkolenia

Szkolenie ma na celu teoretyczne omówienie oraz praktyczne przećwiczenie najpopularniejszych scenariuszy takich zagadnień jak - bezpieczna konfiguracja sieciowa zasobów wrażliwych (np. baz danych - RDS/EC2), zarządzanie dostępem do zarządzalnych usług AWS (S3, DynamoDB) oraz centralizacja zarządzania wieloma kontami w ramach AWS Organizations.

Czas i forma szkolenia

- 14 godzin (2 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

1. Omówienie globalnej infrastruktury sieciowej chmury AWS
 • regiony
 • Availability Zones
 • Edge Locations
2. Krótkie omówienie podstawowych protokołów sieciowych
 • wyrównanie wiedzy przed omawianiem bardziej szczegółowych zagadnień
3. Szczegółowe objaśnienie usług sieciowych
 • VPC
 • interfejsy sieciowe
 • tablice routingu
 • NACL
 • Security Groups oraz ćwiczenia z Security Groupami
4. Szczegółowe omówienie usługi IAM oraz STS
 • ćwiczenia praktyczne
5. Szczegółowe omówienie Resource-based policies
 • ćwiczenia praktyczne
6. Szczegółowe omówienie Cross-Account Access
 • ćwiczenia praktyczne
7. Omówienie usługi WAF
 • proste ćwiczenie praktyczne ilustrujące działanie
8. Bezpieczne przechowywanie haseł w środowisku AWS
 • SSM Parameter Store/Secrets Manager