KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo w systemach chmurowych [S1Cybez1>BSCh]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
24

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
16

Liczba punktów ECTS

4,00

Koordynatorzy

dr inż. Michał Weissenberg
michal.weissenberg@put.poznan.pl

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten kurs powinien posiadać podstawową wiedzę z zakresu, sieci teleinformatycznych, systemów operacyjnych, systemów chmuorowych oraz posiadać podstawowe umiejętności programowania. Powinien także posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł. Student powinien wykazywać takie cechy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla drugiego człowieka oraz gotowość do pracy w grupie.

Cel przedmiotu

Zapewnienie studentom teoretycznych podstaw dotyczących systemów chmurowych. 2. Zapoznanie studentów z teoretycznymi informacjami na bezpieczeństwem infrastruktury systemów chmurowych. 3. Zapoznanie studentów z podstawowymi informacjami dotyczącymi zarządzania bezpieczeństwem systemów chmurowych oraz szacowaniem ryzyka. 4. Zapoznanie studentów z podstawowymi informacjami dotyczącymi bezpieczeństwa danych w systemach chmurowych. 5. Zapoznanie studentów z podstawowymi pojęciami dotyczącymi operacji bezpieczńestwa w chmurze oraz zarządzeniem tożsamością i dostępem

Przedmiotowe efekty uczenia się

Wiedza:
Student ma poszerzoną i pogłębioną wiedzę w zakresie urządzeń sieciowych znajdujących zastosowanie w systemach chmurowych [K2_W07]
Student rozumie metodykę projektowania złożonych systemów infomatyczncych; zna języki opisu sprzętu i komputerowe narzędzia do projektowania i symulacji systemów chmurowych [K2_W14]
Zna i rozumie zagrożenia, na które narażona jest współczesna cywilizacji masowo wykorzystująca usługi cyfrowe, a w szczególnosci usługi chmurowe [K2_W22]

Umiejętności:
Student potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji i krytycznej oceny, a także wyciągać wnioski oraz formułować i wyczerpująco uzasadniać opinie [K2_U01]
Potrafi zaproponować ulepszenia lub rozwiązania alternatywne dla istniejących rozwiązań projektowych i systemów teleinformatycznych w obszarze systemów chmurowych [K2_U09]
Potrafi ocenić przydatność i możliwość wykorzystania nowych osiągnięć w zakresie technik, metod projektowania do projektowania i wytwarzania układów i systemów teleinformatycznych zawierających rozwiązania o charakterze innowacyjnym w obszarze systemów chmurowych [K2_U11]

Kompetencje społeczne:
Jest gotów do uznawania znaczenia wiedzy w rozwiązywaniu problemów poznawczych i praktycznych oraz do krytycznej oceny odbieranych treści [K2_K02]
Jest gotów do myślenia i działania w sposób przedsiębiorczy [K2_K04]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
Wykład: Egzamin pisemny sprawdzający wiedzę studentów w formie pytań otwartych oraz pytań testowych wielokrotnego wyboru. Podczas egzaminu nie wolno używać żadnych materiałów.
Ćwiczenia laboratoryjne: na podstawie oceny postępów prac dokonywanych na każdych laboratoriach
Projekt: Na podstawie przygotowanych raportów i prezentacji z realizacji studium przypadku w zakresie inicjowania, planowania, realizacji i monitorowania oraz zakończenia projektu.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 51% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

W ramach przedmiotu omówione zostaną zagrożenia i ataki na infrastrukturę chmurową. Wyjaśniony zostanie model określający podział obowiązków między dostawcą chmury a użytkownikiem. Studenci poznają mechanizmy ochrony danych, w tym szyfrowanie, zarządzanie kluczami kryptograficznymi oraz kontrolę dostępu. Przedstawione zostanie monitorowanie bezpieczeństwa poprzez systemy SIEM oraz integracja DevSecOps w procesie tworzenia oprogramowania. Omówione będą zasady zgodności z regulacjami prawnymi oraz strategie Disaster Recovery i Business Continuity w chmurze.

Tematyka zajęć

1. Wprowadzenie do bezpieczeństwa systemów chmurowych
- Definicja i modele chmury (IaaS, PaaS, SaaS)
- Modele wdrożenia chmury (publiczna, prywatna, hybrydowa, multi-cloud)
- Korzyści i zagrożenia wynikające z korzystania z chmury
- Przepisy prawne i regulacje (RODO, HIPAA, ISO 27001, NIST)
2. Zagrożenia i ataki na systemy chmurowe
- Ataki na warstwę infrastruktury (DDoS, ataki na API, exploity VM)
- Ataki na aplikacje chmurowe (injection, XSS, CSRF)
- Zagrożenia związane z przechowywaniem i transmisją danych (man-in-the-middle, ransomware, utrata kontroli nad danymi)
- Insider threats - zagrożenia wewnętrzne
3. Model Shared Responsibility w chmurze
- Zakres odpowiedzialności dostawcy chmury i użytkownika
- Przykłady odpowiedzialności w AWS, Azure i Google Cloud
- Strategie minimalizacji ryzyka
4. Mechanizmy ochrony danych w chmurze
- Szyfrowanie danych w spoczynku i w tranzycie
- Zarządzanie kluczami kryptograficznymi (KMS)
- Maskowanie danych i tokenizacja
5. Kontrola dostępu i zarządzanie tożsamością (IAM)
- Role i polityki IAM w AWS, Azure i GCP
- Multi-Factor Authentication (MFA)
- Least Privilege Access i Zero Trust Security
- Federacja tożsamości i SSO
6. Monitorowanie i detekcja zagrożeń
- Systemy SIEM (Security Information and Event Management)
- Usługi monitorowania w chmurze (AWS CloudTrail, Azure Security Center, Google Security Command Center)
- Wykrywanie anomalii i incydentów
7. Disaster Recovery i Business Continuity w chmurze
- Backup i odzyskiwanie danych
- Projektowanie systemów odpornych na awarie
- Strategie redundancji i failover
8. Audyt i zgodność z regulacjami
- Frameworki zgodności w chmurze (CIS, NIST, GDPR, SOC 2)
- Narzędzia do audytu i oceny bezpieczeństwa chmury
- Case studies - analiza rzeczywistych przypadków naruszeń bezpieczeństwa
Ćwiczenia laboratoryjne i projekty grupowe: Tematyka zgodna z treścią wykładów

Metody dydaktyczne

Wykład: prezentacja multimedialna, ilustrowana przykładami podawanymi na tablicy oraz pokazami praktycznymi.
Ćwiczenia laboratoryjne: ćwiczenia praktyczne wykonywane samodzielne lub w grupach z wykorzystaniem komputera
Projekty grupowe.

Literatura

Podstawowa:
Chris Dotson, Bezpieczeństwo w chmurze, Wydawnictwo Naukowe PWN, 2020 Omar Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021

Uzupełniająca:
Uzupełniająca
P. Mishra, E. S. Pilli, R. C. Joshi, “Cloud Security: Attacks, Techniques, Tools, and Challenges”, CRC Press.,
2021 (https://www.amazon.com/Cloud-Security-Attacks-Techniques-Challengesebook/dp/B09MTT5D3T) J. R. Vacca, “Cloud Computing Security: Foundations and

Challenges”. CRC Press, 2016 (https://www.amazon.com/Cloud-Computing-Security-Foundations-Challenges/dp/1482260948) C. Dotson, “Practical Cloud Security: A Guide for Secure Design and Deployment”, O'Reilly Media, 2019 (https://www.amazon.com/Practical-Cloud-Security-Secure-Deployment/dp/1492037516)

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	119	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	64	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	55	2,00