



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Mechanizmy naruszeń i zapewnienia bezpieczeństwa w Chmurze i Centrach Danych i bezpieczeństwo sieci definiowanych programowo [S2Inf1E-CYB>CLDC]

Przedmiot

Kierunek studiów

Informatyka/Computing

Rok/Semestr

1/2

Studia w zakresie (specjalność)

Cyberbezpieczeństwo

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

angielski

Forma studiów

stacjonarne

Wymagalność

obligatoryjny

Liczba godzin

Wykład

20

Laboratorium

30

Inne

0

Ćwiczenia

0

Projekty/seminaria

0

Liczba punktów ECTS

4,00

Koordynatorzy

dr inż. Marek Michalski

marek.michalski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student ma podstawową wiedzę i doświadczenie z zakresu komputerów, wirtualizacji, sieci komputerowych, protokołów IP (w tym protokołów routingu) oraz programowania

Cel przedmiotu

Przedstawienie studentom zagrożeń bezpieczeństwa i sposobów radzenia sobie z nimi w chmurowej realizacji usług oraz w data center

Przedmiotowe efekty uczenia się

Wiedza:

student rozumie mechanizmy, które są wykorzystywane podczas realizacji usług w chmurach i data center, ma świadomość ich słabości oraz sposobów podniesienia ich bezpieczeństwa

Umiejętności:

student umie przeanalizować system chmurowy oraz data center, wskazać ewentualne zagrożenia oraz zaproponować sposób ich eliminacji

Kompetencje społeczne:

student ma świadomość, że w zakresie bezpieczeństwa jego wiedza i doświadczenie mogą ulegać szybkiej dezaktualizacji i wymagają ciągłego uaktualniania

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Test pisemny, próg zaliczenia 51%

Treści programowe

Podstawy budowy chmur i usług chmurowych

Techniczne i nietechniczne aspekty usług chmurowych

Implementacja wybranych usług na przykładach z Google, MS, AWS i innych

Narzędzia i techniki realizacji usług chmurowych

Mechanizmy powstawania naruszeń bezpieczeństwa

Obszary niebezpieczeństwa

Mechanizmy ochrony oraz możliwość ich automatyzacji

Narzędzia dla operatorów, dostawców usług i klientów

Przykłady źródeł ujawnionych problemów

Ogólna budowa DC, Usługi i Mechanizmy DC

Zasady wirtualności, Charakterystyka klientów

Mechanizmy powstawania naruszeń bezpieczeństwa w DC

Kategoryzacja zagrożeń, command-and-control (C&C)

Mechanizmy obrony przed zagrożeniami oraz ich automatyzacja

Custom hardware for data Center (FPGA,option)

W ramach wykładu będzie wizyta w dwóch (lub więcej) data center w Poznaniu,

A także spotkanie z osobami pracującymi na co dzień z narzędziami zapewniającymi bezpieczeństwo

(integrator systemów bezpieczeństwa) oraz firmami świadczącymi usługi z zakresu testowania i

podnoszenia poziomu bezpieczeństwa (firmy z lokalnego rynku oraz znany ogólnopolski portal

poruszający tematykę bezpieczeństwa IT)

Laboratorium

Praktyczne zapoznanie się z testowym przykładowym środowiskiem Cloud, Data Center

Wirtualizacja systemów operacyjnych, sieci komputerowych, ich funkcjonalności (VM, NFV)

Zapoznanie się z typowymi rozwiązaniami typu WAF, narzędzia typu threat detection/threat protection,

IDS/IPS (Intrusion Detection Systems/Intrusion Protection Systems)

Wykrywanie mechanizmów command-and-control (C&C)

Tematyka zajęć

Podstawy budowy chmur i usług chmurowych

Techniczne i nietechniczne aspekty usług chmurowych

Implementacja wybranych usług na przykładach z Google, MS, AWS i innych

Narzędzia i techniki realizacji usług chmurowych

Mechanizmy powstawania naruszeń bezpieczeństwa

Obszary niebezpieczeństwa

Mechanizmy ochrony oraz możliwość ich automatyzacji

Narzędzia dla operatorów, dostawców usług i klientów

Przykłady źródeł ujawnionych problemów

Ogólna budowa DC, Usługi i Mechanizmy DC

Zasady wirtualności, Charakterystyka klientów

Mechanizmy powstawania naruszeń bezpieczeństwa w DC

Kategoryzacja zagrożeń, command-and-control (C&C)

Mechanizmy obrony przed zagrożeniami oraz ich automatyzacja

Custom hardware for data Center (FPGA,option)

W ramach wykładu będzie wizyta w dwóch (lub więcej) data center w Poznaniu,

A także spotkanie z osobami pracującymi na co dzień z narzędziami zapewniającymi bezpieczeństwo

(integrator systemów bezpieczeństwa) oraz firmami świadczącymi usługi z zakresu testowania i

podnoszenia poziomu bezpieczeństwa (firmy z lokalnego rynku oraz znany ogólnopolski portal

poruszający tematykę bezpieczeństwa IT)

Laboratorium

Praktyczne zapoznanie się z testowym przykładowym środowiskiem Cloud, Data Center

Wirtualizacja systemów operacyjnych, sieci komputerowych, ich funkcjonalności (VM, NFV)

Zapoznanie się z typowymi rozwiązaniami typu WAF, narzędzia typu threat detection/threat protection, IDS/IPS (Intrusion Detection Systems/Intrusion Protection Systems)

Wykrywanie mechanizmów command-and-control (C&C)

Metody dydaktyczne

Wykład z elementami dyskusji ze studentami, demonstracje i analizy

Laboratorium z eksperymentami na prawdziwej sieci oraz przykładach rozwiązań chmurowych i data center

Literatura

Podstawowa

Omar Santos, CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021

Uzupełniająca

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	50	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	50	2,00