KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Zarządzanie bezpieczeństwem systemów IT oraz testy penetracyjne [S2Inf1E-CYB>ISSM]

Przedmiot

Kierunek studiów
Informatyka/Computing

Rok/Semestr
2/3

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
30

Laboratorium
30

Inne (np. online)
0

Ćwiczenia
0

Projekty/seminaria
30

Liczba punktów ECTS

6,00

Koordynatorzy

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

dr hab. inż. Sławomir Hanczewski
slawomir.hanczewski@put.poznan.pl

dr inż. Michał Apolinarski
michal.apolinarski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Student ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie architektury systemów komputerowych, zasad działania systemów operacyjnych i ich rodzajów, zna i rozumie podstawowe procesy zachodzące w cyklu życia sys. komp. i sys. operacyjnych. Student ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie podstaw teleinformatyki, protokołów i usług w sieciach telekomunikacyjnych. Zna podstawy z zakresu ochrony danych w syst. inf.. Student potrafi pozyskiwać informacje z literatury, baz danych i innych źródeł; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, a także wyciągać wnioski oraz formułować i uzasadniać opinie. Student potrafi pracować indywidualnie i w zespole. Student ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera-informatyka i związaną z tym odpowiedzialność za podejmowane decyzje. Powinien również rozumieć konieczność poszerzania swoich kompetencji. Ponadto w zakresie kompetencji społecznych student musi prezentować takie postawy jak uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

Cel przedmiotu

W ramach przedmiotu studenci zapoznają się z problematyką zarządzania bezpieczeństwem teleinformatycznym w firmie lub instytucji, a więc w oparciu o normy i standardy, sposobami przeprowadzania analizy ryzyka i odpowiednim doborem zabezpieczeń (minimalizujących prawdopodobieństwo i/lub skutki zagrożeń), metod reagowania na incydenty oraz przywracania systemu informatycznego do stanu sprzed incydentu.

Przedmiotowe efekty uczenia się

Wiedza:
student ma uporządkowaną i podbudowaną teoretycznie wiedzę w zakresie ochrony danych, bezpieczeństwa systemów informatycznych, analizy ryzyka w sys. inf.
student ma podstawową wiedzę w zakresie administrowania systemami informatycznymi oraz jest świadomy obowiązków spoczywających na administratorach systemów inf.
student ma zaawansowaną i szczegółową wiedzę z zakresu szeroko rozumianych testów penetracyjnych sieci komputerowych. wiedza obejmuje: 1. zasady testów penetracyjnych 2. planowanie i przeprowadzanie testów (wewnętrznych i zewnętrznych), 3. dokumentacja potestowa.
student posiada wiedzę o trendach rozwoju testów penetracyjnych i sieci komputerowych.

Umiejętności:
student potrafi zastosować odpowiednie metody ochrony danych i zapewnić bezpieczeństwo systemu informatycznego, potrafi opracować dokumentację dotyczącą realizacji zadania inżynierskiego i przygotować tekst zawierający omówienie wyników realizacji tego zadania oraz potrafi dokonać krytycznej analizy istniejących rozwiązań.
student potrafi pozyskiwać informacje o testach penetracyjnych i sieciach komputerowych z literatury, baz danych oraz innych źródeł (w języku polskim i angielskim). student potrafi również integrować wiedzę na temat testów penetracyjnych oraz potrafi ocenić przydatność metod i narzędzi do przygotowania i przeprowadzenia testów. potrafi też współdziałać w zespole, przyjmując w nim różne role i wyznaczać kierunki dalszej nauki.

Kompetencje społeczne:
student rozumie, że w informatyce wiedza i umiejętności bardzo szybko stają się przestarzałe, w szczególności technologie związane z bezpieczeństwem, sieciami komputerowymi i testami penetracyjnymi.
student ma świadomość ważności i rozumie pozatechniczne aspekty i skutki działalności inżyniera-informatyka i związaną z tym odpowiedzialność za podejmowane decyzje.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wykład - wiedza zdobyta na wykładach weryfikowana jest na zaliczeniu, które ma formę pisemną lub ustną. Próg zaliczenia to 50%. Zagadnienia końcowe, na podstawie których przygotowywane są pytania, zostaną rozesłane do studentów pocztą elektroniczną z wykorzystaniem uczelnianego systemu poczty elektronicznej. W przypadku egzaminu ustnego każdy student odpowiada na trzy pytania z zestawu 40 (są one znane studentom).Oceniana jest poprawność odpowiedzi oraz stopień zrozumienia problemu przez studenta.
Projekt i ćwiczenia laboratoryjne - na podstawie wykonanego ćwiczenia lub oceny bieżącego postępu realizacji zadań. Brak zaliczenia ćwiczenia powoduje konieczność powtórzenia go w wyznaczonym przez prowadzącego terminie.

Treści programowe

Treści programowe
Analiza ryzyka. Reguły bezpieczeństwa. Analiza podatności. Analiza i modelowanie zagrożeń. Testy penetracyjne

Tematyka zajęć

Wykłady:
Wprowadzenie - określenie co oznacza, że system informatyczny jest systemem bezpiecznym,

wiarygodnym, jak oceniamy bezpieczeństwo, relacje pomiędzy elementami bezpieczeństwa, standardy, miary, normy i najlepsze praktyki (TCSEC, ITSEC, ISO, CC). Środki ochrony i ocena ich skuteczności. Certyfikacja systemów informatycznych (w tym ISO 15408). Kryteria oceny zabezpieczeń. Klasyfikacja zagrożeń zarówno sieciowych, kryptograficznych jak i eksploatacyjnych systemów komputerowych. Określanie stopnia podatności systemów na zagrożenia (metody ilościowe i jakościowe).
Analiza i zarządzanie ryzykiem. Definiowanie oraz dyskusja nad sposobami osiągania i utrzymywania założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności . Dobór odpowiednich środków zabezpieczających. Przykłady procesów zarządzania
ryzykiem w firmie, w konkretnym systemie informatycznym. Polityka bezpieczeństwa - przykładowe dokumenty wchodzące w skład polityki bezpieczeństwa Audyt -przykład wdrożenia systemu zarządzania bezpieczeństwem (COBIT, MARION, TISM, OSSTM, LP-
A) Modele systemów zaufania (płaski, hierarchiczny, zdecentralizowany, zorientowany na użytkownika). Problemy związane z zaufaniem (błędy poznawcze). Implementacje modeli zaufania (w tym w systemach PKI). Modele wyboru strategii bezpieczeństwa (security by obscurity, open security) Wymagania prawne związane z zarządzaniem bezpieczeństwem. Problem czynnika ludzkiego w ochronie danych. Ekonomiczne aspekty bezpieczeństwa w systemach informatycznych (finansowe skutki naruszeń bezpieczeństwa, koszt zabezpieczeń). Wspomaganie użytkowników systemów informatycznych. Organizacja szkoleń z zakresu ochrony danych. Zasady redagowania instrukcji użytkowania. Mnemotechniki w systemach haseł. Informatyczne narzędzia wspierające procesy zarządzania bezpieczeństwem, w tym zastosowania sztucznej inteligencji w ochronie danych. Metodologie prowadzenia testów penetracyjnych (wprowadzenie do testów penetracyjnych,
podstawowe definicje, rodzaje testów penetracyjnych - białej-, czarnej- i szarej-skrzynki, techniki socjotechniczne, koszty i korzyści testu penetracyjnego, rekonesans pasywny). Klienci i umowy prawne (konieczność testów penetracyjnych, etapy testów penetracyjnych i wymagania klientów, zasady zachowania i ryzyka związane z testami penetracyjnymi, umowy prawne związane z testami penetracyjnymi). Obowiązki licencjonowanego testera (LPT - Licensed Penetration Tester) (obowiązki zawodowe LPT, normy prawne dla LPT, listy kontrolne zgodności niezbędne do przeprowadzenia testu penetracyjnego, zasady współpracy pomiędzy organizacją a testerami penetracyjnymi). Planowanie i harmonogramowanie testów penetracyjnych (faza planowania testów penetracyjnych, zespół testów penetracyjnych).
Lista kontrolna testów penetracyjnych (lista kontrolna testów penetracyjnych, wymagania dotyczące testów penetracyjnych, rodzaje testów). Zbieranie informacji i testy penetracyjne inżynierii społecznej (kroki w procesie zbierania informacji, socjotechnika, zbieranie informacji o docelowej firmie, archiwalne
strony) Analiza podatności (ocena podatności, klasyfikacja podatności, raport z oceny podatności, harmonogram oceny podatności) Zewnętrzne testy penetracyjne (mapy topologiczne sieci, fizyczna lokalizacja serwerów docelowych, różnorodność skanowań portów w sieci docelowej, rekord DNS domeny, banery różnych serwerów, odpowiedzi ICMP) Wewnętrzne testy penetracyjne (mapowanie sieci wewnętrznej, skanowanie portów poszczególnych maszyn, umieszczanie wirusów, trojanów i rootkitów na maszynie docelowej, MitM) Wyniki testów penetracyjnych (elementy składowe raportu z testów penetracyjnych, jak dostarczyć raport klientowi, jak długo przechowywać informacje związane z testem penetracyjnym). Działania po testach (rekomendacje zespołu testów penetracyjnych, plan działania na rzecz poprawy bezpieczeństwa, proces minimalizacji przypadków błędnych konfiguracji, wyciągnięte wnioski i najlepsze praktyki) Zaawansowane exploity i narzędzia

Projekt
Opracowanie projektu oraz dokumentacji systemu zarządzania bezpieczeństwie w wybranym środowisku informatycznym uwzględniając m.in. inwentaryzację zasobów IT, rodzaj przetwarzanych danych, analizę ryzyka wraz z propozycją zmian, analizę powdrożeniową. Zastosowane metody kształcenia: praca w zespołach maksymalnie 2 osobowych, prezentacje postępu prac nad dokumentacją systemu, dyskusje nad proponowanymi rozwiązaniami na forum całej grupy oraz indywidualnie z zespołem

Metody dydaktyczne

Wykład: wykład prowadzony w sposób interaktywny z formułowaniem pytań do grupy studentów lub do wskazywanych konkretnych studentów, uwzględnia się aktywność studentów w czasie zajęć przy wystawianiu oceny końcowej, w trakcie wykładu inicjowanie dyskusji;.

Projekt: projekt - szczegółowe recenzowanie dokumentacji projektowej przez prowadzącego projekt i dyskusje nad komentarzami, praca w zespołach dwuosobowych.

Ćwiczenia laboratoryjne: prezentacja multimedialna, prezentacja ilustrowana przykładami podanymi na tablicy oraz wykonanie zadań podanych przez prowadzącego - ćwiczenia praktyczne.

Literatura

Podstawowa
1. Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Białas A. WNT, Warszawa 2017.
2. Bezpieczeństwo informacyjne : nowe wyzwania, Liderman K, PWN Warszawa 2017.
3. Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy, NIST 800-37 rev.2, 2018
4. EC-Council, Penetration Testing: Procedures & Methodologies, Cengage Learning 2011
5. Wnag J., Computer network security : theory and practice, Higher Education Press 2009.
6. Tanenbaum A. S., Wetherall D. J., Computer networks, Pearson Longman 2014 .
Uzupełniająca
1. Normy ISO (13335, 2700x),
2. Audyt bezpieczeństwa systemów IT-ścieżka techniczna (rekonesans i skanowanie), Księżopolski B., Szałachowski P., Wyd. Uniwersytetu Marii Curie-Skłodowskiej, Lublin, 2011.
3. www.cisco.com

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	150	6,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	90	3,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	60	2,50