KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo sieci LAN i WAN [S1Cybez1>BSLiW]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/5

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
16

Inne
0

Ćwiczenia
0

Projekty/seminaria
16

Liczba punktów ECTS

4,00

Koordynatorzy

dr hab. inż. Maciej Sobieraj
maciej.sobieraj@put.poznan.pl

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Wykładowcy

Wymagania wstępne

Wiedza z zakresu funkcjonowania lokalnych i rozległych sieci pakietowych; umiejętność konfiguracji urządzeń sieciowych

Cel przedmiotu

• Zdobycie zaawansowanej wiedzy na temat nowoczesnych zagrożeń i technik zabezpieczania sieci LAN i WAN • Nabycie praktycznych umiejętności w konfiguracji i zarządzaniu dedykowanymi systemami bezpieczeństwa różnych producentów • Przygotowanie do projektowania i wdrażania kompleksowych rozwiązań bezpieczeństwa w środowiskach sieciowych • Poznanie nowoczesnych technologii i narzędzi dedykowanych do ochrony infrastruktury sieciowej

Przedmiotowe efekty uczenia się

Wiedza:
• Zna zaawansowane zagrożenia i ataki sieciowe oraz metody ich przeciwdziałania [K1_W10]

• Rozumie działanie i konfigurację nowoczesnych systemów bezpieczeństwa (NGFW, IPS, ATP) [K1_W07]
• Posiada wiedzę na temat rozwiązań bezpieczeństwa oferowanych przez Cisco, Palo Alto Networks, Check Point, Juniper [K1_W20]

Umiejętności:
• Potrafi konfigurować i zarządzać zaawansowanymi urządzeniami bezpieczeństwa sieciowego [K1_U02]
• Umie projektować kompleksowe systemy zabezpieczeń sieci LAN i WAN [K1_U11]
• Jest w stanie integrować różnorodne technologie i systemy bezpieczeństwa w spójne rozwiązanie [K1_U11]

Kompetencje społeczne:
• Rozumie potrzebę ciągłego doskonalenia wiedzy w dynamicznie rozwijającej się dziedzinie bezpieczeństwa sieciowego [K1_K01]
• Potrafi efektywnie pracować w zespole nad zaawansowanymi projektami bezpieczeństwa [K1_K05]
• Jest świadomy odpowiedzialności za bezpieczeństwo informacji i infrastruktury w organizacji [K1_K05]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

1. Wiedza: Egzamin pisemny zawierający pytania otwarte i testowe dotyczące zaawansowanych technologii bezpieczeństwa
2. Umiejętności: Ocena zadań laboratoryjnych oraz projektu grupowego pod kątem poprawności, efektywności i innowacyjności zastosowanych rozwiązań.
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 50% 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

Przedmiot „Bezpieczeństwo sieci LAN i WAN” dostarcza studentom zaawansowanej wiedzy i praktycznych umiejętności w zakresie zabezpieczania sieci lokalnych (LAN) i rozległych (WAN). Kurs koncentruje się na identyfikacji zaawansowanych zagrożeń, implementacji nowoczesnych technologii bezpieczeństwa oraz konfiguracji dedykowanych systemów oferowanych przez wiodących producentów, takich jak Cisco, Palo Alto Networks, Check Point czy Juniper Networks. Studenci poznają zaawansowane techniki ochrony sieci, w tym Next-Generation Firewalls (NGFW), systemy zapobiegania włamaniom (IPS), zaawansowaną ochronę przed zagrożeniami (ATP) oraz rozwiązania do zarządzania tożsamością i dostępem (IAM).

Tematyka zajęć

I. Zaawansowane zagrożenia i ataki sieciowe (4x45 minut)
1. Nowoczesne zagrożenia sieciowe
o Ataki typu Advanced Persistent Threats (APT)
o Ransomware, botnety i malware wielowektorowe
o Ataki na infrastrukturę sieciową: BGP hijacking, DNS spoofing
2. Aktualne rozwiązania bezpieczeństwa
o Przegląd technologii zabezpieczeń od Cisco, Palo Alto Networks, Check Point, Juniper
o Wprowadzenie do standardów bezpieczeństwa (ISO/IEC 27001, NIST)
II. Zaawansowane techniki zabezpieczania sieci LAN (6x45 minut)
1. Zabezpieczanie warstwy 2
o Ochrona przed atakami ARP spoofing i MAC flooding
o Techniki Port Security w urządzeniach Cisco i Juniper
o Implementacja DHCP Snooping, Dynamic ARP Inspection
2. Uwierzytelnianie i kontrola dostępu
o Wdrożenie 802.1X z wykorzystaniem Cisco Identity Services Engine (ISE)
o Rozwiązania Network Access Control (NAC) od Juniper (Juniper Unified Access Control)
o Zarządzanie tożsamością z wykorzystaniem Active Directory i LDAP

3. Segmentacja sieci
o Mikrosegmentacja z wykorzystaniem technologii VLAN i Private VLAN
o Implementacja Virtual Routing and Forwarding (VRF) w urządzeniach Cisco
III. Zaawansowane techniki zabezpieczania sieci WAN (6x45 minut)
1. Next-Generation Firewalls (NGFW)
o Koncepcja NGFW i ich rola w ochronie sieci
o Konfiguracja i zarządzanie Cisco Firepower, Palo Alto Networks NGFW, Check Point Quantum Security Gateways
2. Systemy wykrywania i zapobiegania włamaniom (IPS)
o Implementacja IPS w urządzeniach Cisco (Firepower), Palo Alto Networks (Threat Prevention), Juniper (Junos IPS)
o Analiza sygnatur i zachowań anomalii sieciowych
3. Zaawansowane wirtualne sieci prywatne (VPN)
o Technologie VPN: IPSec, SSL/TLS, FlexVPN
o Implementacja VPN site-to-site i remote access z wykorzystaniem Cisco AnyConnect, Palo Alto GlobalProtect
o Zastosowanie GETVPN w środowiskach korporacyjnych
IV. Nowoczesne systemy i technologie bezpieczeństwa (8x45minut)
1. Zaawansowana ochrona przed zagrożeniami (ATP)
o Wykorzystanie Cisco Advanced Malware Protection (AMP)
o Palo Alto Networks WildFire, Check Point SandBlast
o Analiza i sandboxing plików w celu wykrycia zaawansowanych zagrożeń
2. Zarządzanie bezpieczeństwem i analiza zdarzeń
o Systemy SIEM: Splunk, IBM QRadar
o Integracja urządzeń bezpieczeństwa z SIEM
o Analiza logów i korelacja zdarzeń
3. Kontrola aplikacji i filtrowanie treści
o Implementacja Application Control w NGFW
o Filtrowanie URL i antywirus na poziomie sieciowym
o Ochrona przed zagrożeniami webowymi z wykorzystaniem Secure Web Gateway (SWG)

Metody dydaktyczne

• Wykłady: Prezentacje multimedialne z przykładami praktycznymi i studiami przypadków, online
• Laboratoria: Ćwiczenia praktyczne z wykorzystaniem urządzeń i oprogramowania od różnych producentów
• Projekt: Praca zespołowa nad kompleksowym rozwiązaniem bezpieczeństwa sieciowego

Literatura

Podstawowa:
1. Santos, O., Kampanakis, P., & Woland, A. (2016). Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. Cisco Press. ISBN: 9781587144462.
2. Oficjalna dokumentacja Cisco dla ASA, Firepower i ISE dostępna na stronie Cisco:
[Cisco ASA](https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/tsd-products-support-series-home.html),
[Cisco Firepower](https://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html),
[Cisco ISE](https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html).
3. Piens, T. (2022). Mastering Palo Alto Networks: Build, configure, and deploy network solutions for your infrastructure using features of PAN-OS (2nd ed.). Packt Publishing. ISBN: 9781803241418.
4. Materiały szkoleniowe Palo Alto Networks dostępne na stronie: [Palo Alto Networks Education](https://www.paloaltonetworks.com/services/education).
5. Check Point Firewall Administration R80.10" - Guide dostępny na stronie Check Point: [Check Point R80.10 Administration Guide](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk116515).
6. Dokumentacja Check Point Infinity dostępna na stronie: [Check Point Infinity Documentation](https://www.checkpoint.com/support-services/documentation/).

7. Woodberg, B., & Cameron, R. (2013). *Juniper SRX Series: A Comprehensive Guide to Security Services on the SRX Series*. O'Reilly Media. ISBN: 9781449339029.
8. Materiały techniczne Juniper Networks dostępne na stronie: [Juniper Networks Technical Documentation](https://www.juniper.net/documentation/).

Uzupełniająca:
1. Dokumentacja i whitepapers producentów urządzeń i rozwiązań sieciowych
2. Materiały przygotowane przez prowadzących

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	116	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	56	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	60	2,00