

Zgłoszenie tematu pracy dyplomowej :: STUDIA II STOPNIA ::

rok akademicki 2025/26

Promotor:	prof. dr hab. Oleksandr Korchenko
Temat pracy magisterskiej (j. polski, j.angielski):	Referencyjna architektura Zero Trust dla korporacyjnych aplikacji .NET w chmurze Microsoft Azure <i>Reference Zero Trust Architecture for Corporate .NET Applications in the Microsoft Azure Cloud</i>
Zakres pracy i oczekiwane rezultaty praktyczne:	Praca obejmuje zaprojektowanie i implementację referencyjnej architektury Zero Trust dla korporacyjnych aplikacji .NET uruchamianych w chmurze Microsoft Azure. W ramach pracy zostaną: • zdefiniowane wymagania bezpieczeństwa oraz założenia architektury Zero Trust dla aplikacji .NET, • zaprojektowana architektura referencyjna z wykorzystaniem usług Azure (m.in. App Service lub AKS, Azure SQL, Azure Storage, Azure Key Vault, Azure Active Directory/Entra ID, Azure Application Gateway/WAF, Private Endpoints, Conditional Access), • przygotowana infrastruktura jako kod (IaC) do automatycznego wdrażania środowiska, • opracowany pipeline CI/CD „bez sekretów” (z użyciem Managed Identity/Key Vault), • zaimplementowana przykładowa aplikacja referencyjna .NET ilustrująca zastosowanie architektury. Rezultatem praktycznym będzie gotowa, udokumentowana architektura referencyjna wraz z działającym środowiskiem demonstracyjnym w Azure, możliwa do wykorzystania jako wzorzec w projektach korporacyjnych oraz jako element portfolio.
Aspekt naukowy, problemowy, innowacyjny pracy:	Aspekt naukowy pracy dotyczy praktycznego zastosowania zasad Zero Trust w projektowaniu i wdrażaniu korporacyjnych aplikacji .NET w chmurze Azure, z uwzględnieniem podejścia security by design. Praca zakłada: • analizę wybranych modeli zagrożeń i typowych podatności aplikacji chmurowych (m.in. w odniesieniu do OWASP Top 10 i misconfigurations w chmurze), • opracowanie modelu architektonicznego integrującego kontrolę dostępu opartą na tożsamości (Azure AD/Entra ID, RBAC), segmentację sieci (Private Link/Private Endpoints, deny-by-default), ochronę na poziomie brzegowym (WAF) oraz bezpieczne zarządzanie sekretami (Key Vault), • ocenę skuteczności zaproponowanych rozwiązań poprzez analizę konfiguracji, testy bezpieczeństwa oraz porównanie z podejściem tradycyjnym (perimeter-based). Innowacyjność pracy polega na opracowaniu kompletnej, praktycznej architektury referencyjnej Zero Trust, uwzględniającej zarówno warstwę aplikacyjną (.NET), jak

Zgłoszenie tematu pracy dyplomowej :: STUDIA II STOPNIA ::

rok akademicki 2025/26

	i infrastrukturę chmurową (Azure) oraz proces wdrażania (IaC, CI/CD bez sekretów).
*Oprogramowanie, język programowania, środowisko systemowe:	Oprogramowanie, język programowania, środowisko systemowe: • Języki programowania: C# (.NET), SQL, TypeScript/JavaScript, • Frameworki i platformy: ASP.NET Core, Entity Framework Core, • Narzędzia chmurowe: Microsoft Azure (App Service lub Azure Kubernetes Service, Azure SQL Database, Azure Storage, Azure Key Vault, Azure Active Directory/Entra ID, Azure Application Gateway/WAF, Azure Monitor/Application Insights), • Infrastruktura jako kod: Bicep / ARM / Terraform, • CI/CD: Azure DevOps, • Systemy operacyjne: Windows i/lub Linux,
*Środowisko uruchomieniowe	Aplikacja i komponenty architektury będą uruchamiane w chmurze Microsoft Azure (m.in. App Service, Azure SQL Database, Azure Storage, Application Gateway/WAF, Private Endpoints), z integracją z Azure Active Directory/Entra ID. Środowisko deweloperskie: stacje robocze z systemem Windows, przeglądarka internetowa oraz lokalne narzędzia deweloperskie dla .NET.
Dodatkowe wymagania i uwagi:	OWASP Foundation – OWASP Top Ten (najnowsza wersja). Microsoft – oficjalna dokumentacja Zero Trust oraz Azure Security Benchmark. Dokumentacja Microsoft Azure Architecture Center (Identity, Security, Zero Trust, Reference Architectures).
*Literatura:	

*pola opcjonalne