

# Microsoft 365 - bezpečnost hybridního prostředí

Kód kurzu: GOC215

Pětidenní kurz se zaměřuje na porozumění bezpečnostní strategii a praktickou demonstraci jednotlivých bezpečnostních technologií určených pro Microsoft hybridních prostředí (prostředí s vlastní infrastrukturou a Microsoft365 cloudovými službami). Ve vysokém tempu a detailně probereme principy chování identit v hybridním prostředí, jednotlivé bezpečnostní technologie Microsoft365 a jejich aplikaci v oblasti ochrany uživatelů a citlivých dat, rozšíření bezpečnosti lokálního AD, pokročilé detekce hrozeb a externích přístupů. Na závěr se podíváme na možnosti integrace Azure MFA pro naše NPS servery, jak zamezit přístup k aplikacím a citlivým datům pro neschválená zařízení a jak můžeme publikovat intranetové aplikace bezpečně pro uživatele na home office.

## Předpokládané vstupní znalosti

Znalosti v rozsahu kurzů uvedených v sekcích **Předchozí kurzy** a **Související kurzy**

Dobrá znalost technologií TCP/IP a DNS

## Osnova kurzu

Attack vectors, security strategie pro Microsoft hybridní prostředí

Perimeter vs. Zero trust přístup

Azure AD vs ActiveDirectory – struktura, autentizace, objekty, tokeny

AzureAD Connect a jeho módy nasazení

Ochrana hybridní identity: MFA, SSO, conditional access, Windows Hello for business – jak zajistit ochranu účtů a zároveň dosáhnout zjednodušení přihlašovacího procesu pro uživatele

RBAC, PIM v hybridním prostředí, Identity protection

Práce s externími identitami

Politiky hesel, pokročilá ochrana hesel prostřednictvím Password protection a smart lockout

Zařízení v hybridním prostředí – rozdíly mezi stavy AzureAd registered, DomainJoined only, AzureAD Joined a HybridAzureADJoined

Úvod do Intune – device compliance, security profily

Pokročilé zabezpečení doménových řadičů – Microsoft Defender for identity

Microsoft information protection koncept a jednotlivé technologie – ochrana citlivých dokumentů, DLP v M365 a onprem prostředí

Obrana proti útokům na uživatele - Phishing, nebezpečné přílohy

Pokročilá detekce hrozeb EDR/XDR – jakou roli řešení zaujímá, detekce anomálií v systému

Azure AD Application Proxy – zpřístupnění intranet aplikací uživatelům z domu

Integrace Azure MFA a NPS serveru

## Příprava k certifikačním zkouškám

U certifikačních zkoušek Microsoft platí, že kromě certifikací MCM, není účast na oficiálním MOC kurzu nutnou podmínkou pro složení zkoušky

Oficiální kurzy MOC firmy Microsoft i naše vlastní kurzy GOC jsou vhodnou součástí přípravy na certifikační zkoušky firmy Microsoft, jako jsou MTA, MCP, MCSA, MCSE, nebo MCM

Primárním cílem kurzu ovšem není přímo příprava na certifikační zkoušky, ale zvládnutí teoretických principů a osvojení si praktických dovedností nutných k efektivní práci s daným produktem

### GOPAS Praha

Na Strži 2097/63  
140 00 Praha 4 - Krč  
Tel.: +420 226 201 390  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Brno

Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

### GOPAS Bratislava

Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2026 GOPAS, a.s.,  
All rights reserved

# Microsoft 365 - bezpečnost hybridního prostředí

MOC kurzy obvykle pokrývají téměř všechny oblasti, požadované u odpovídajících certifikačních zkoušek. Jejich probrání na kurzu ale nebývá dán vždy přesně stejný čas a důraz, jako vyžaduje certifikační zkouška

Jako další přípravu k certifikačním zkouškám lze využít například knihy od MS Press (tzv. Self-paced Training Kit) i elektronický self-test software

**GOPAS Praha**  
Na Strži 2097/63  
140 00 Praha 4 - Krč  
Tel.: +420 226 201 390  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Brno**  
Nové sady 996/25  
602 00 Brno  
Tel.: +420 530 513 590  
[info@gopas.cz](mailto:info@gopas.cz)

**GOPAS Bratislava**  
Dr. Vladimíra Clementisa 10  
Bratislava, 821 02  
Tel.: +421 902 903 132  
[info@gopas.sk](mailto:info@gopas.sk)



Copyright © 2026 GOPAS, a.s.,  
All rights reserved