Windows Server - Active Directory SAE, Tiering and Red Forest

Kód kurzu: GOC159

Třídenní kurz je určen správcům a architektům IT infrastruktury postavené na Active Directory a Azure Active Directory, kteří se chtějí dozvědět jak funguje bezpečnost uživatelských účtů, jak správně nakládat s privilegovanými účty správců, jak bezpečně spravovat celé on-prem i hybridní prostředí tak, aby nedocházelo ke kompromitacím přihlašovacích údajů správců a tím se buď úplně zamezilo, případně se alespoň izolovaly incidenty jako je ransomware a další dnešní nákazy i například se zabránilo vstupu a přežití APT.

Pro koho je kurz určen

Kurz je určen správcům a architektům bezpečnosti a IT infrastruktury primárně postavené na Active Directory (AD DS) a Azure Active Directory (AAD)

Co vás na kurzu naučíme

Pochopit proti jakým druhům útoků jsou principy SAE, tiering a red forest vhodné

Porozumnět základním bezpečnostním principům Active Diretory a Azure Active Directory, bezpečnosti jejich účtů a skupin/rolí, replikací a hesel a řízení přístupu uvnitř těchto adresářů

Porozumnět jejich schopnosti izolovat, nebo úplně omezit vstup malware obecně a zvláště ransomware, spyware, APT (advanced persistent threats) a jejich další šíření

Pochopit jak fungují bezpečnostní technická opatření jako je LDAPS, Kerberos Armoring, Kerberos Compound ID, Protected Users skupina, jak minimalizovat použití NTLM a dále zabezpečit přihlašovací údaje privilegovaných účtů

Jak vybudovat SAE (secure adminitrative environment) pro správu AD DS, serverů a stanic, Azure AAD, Office 365 i dalších a cizích cloudových služeb i ostatních systémů jako jsou síťové prvky, tiskárny apod.

Proč je zapotřebí a jak zavést tiering a účině separovat privilegované účty správců, jak k tomu využívat čipové karty a další více-faktorové přihlašovací metody (MFA - multi factor authentication)

Jak v takovém prostředí umožnit pohodlnou správu IT adminům i dodavatelům

Proč je forest tak zvaně security boundary, jak se kompromitují všechny domény v nich a proč je vhodné provozovat více oddělených forestů, například pro DMZ apod.

Jak a proč zavést red forest pro prostředí s více foresty

Předpokládané vstupní znalosti

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

Dobrá znalost technologií TCP/IP a DNS

Osnova kurzu

Příklady útoků, proti kterým se chceme bránit

Spyware, ransomware, keyloggery, rizika heslovníčků (password managers)

Rizika uložených přihlašovacích údajů, rizika slabých hesel, rizika (ne)zamykání účtů

SSO injections (single sign on), rizika impersonace, rizika Kerberos delegací a Kerberos protocol transition

Rizika spojená s Enteprise AD CS (certification services) a vydáváním přihlašovacích certifikátů do čipových karet (smart card logon)

Kompromitace Domain Admins účtu vede na kompromitaci celého forestu

Možnosti nasazení více-faktorového ověřování (multifactor authentication), smart-card logon (PKINIT), TPM virtuální čipové karty, tokeny, využití Azure MFA

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

Účty a skupiny s právy a přístupem na úrovni Domain Admins, anebo možnosti elevace na tuto úroveň

Principy synchronizace účtů a hesel AD DS a Azure AD, ověřování pomocí AD FS (federation services) pro Office365 a Kerberos pass-through ověřování pro Azure

Řízení přístupu uvnitř AD DS LDAP a Azure AD, AdminSDHolder, LDAP permissions

Řízení přístupu ke správě Group Policy a Intune a rizika a ochrany s tím spojené, plus Advanced GPM

Bezpečnost DNS a nebezpečnost DHCP

Více-doménová prostředí, forest trust (vztahy důvěry) a ověřování uživatelských účtů a bezpečné použití skupin mezi nimi

Identifikace tier0 (DC) zařízení a privilegovaných účtů správců

Identifikace tier1 (servers) zařízení a privilegovaných účtů správců

Idnetifikace tier2 (endpoint) zařízení a privilegovaných účtů správců

Izolace tier0-tier1-tier2 privilegovaných účtů správců pomocí User Rights Assignment, Kerberos Authentication Policies, Selective Autentication

Využití Windows Firewall nebo Private VLAN technologií k rozbíjení jednotlivých bezpečnostních zón (tier)

Budování bezpečného prostředí pro správu (SAE - secure administrative environment)

Technologie a vhodná bezpečnostní opatření pro jump servery (JS), privileged access workstation (PAW) a privileged access management servery (PAM)

Přístup a jeho ochrana na JS, PAW a PAM, zabezpečení přihlašovacích údajů správců v takovém prostředí, přístup přes VPN a dočasný nebo trvalý přístup cizích dodavatelů

Integrace identity (IDM) a red-forest scénáře pro více doménové prostředí, oddělené foresty pro DMZ a dalších izolované sítě, OT a výrobní sítě postavené na Windows

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

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
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk