Macrosoft
Vzdelávanie s trvalým efektom

Macrosoft s.r.o.
Štefánikova 47
811 04 Bratislava

tel: 02/ 55 410 308,
0948 88 40 88
e-mail: macrosoft@macrosoft.sk

Bezpečnostné mechanizmy Active Directory

Ste administrátor Active Directory? Chcete vylepšiť Vašu bezpečnostnú stratégiu tak, aby bola odolná voči súčasným typom útokov? Na rozšírenom kurze o pokročilých bezpečnostných mechanizmoch AD Vám predstavíme nové možnosti, ktorými možno zlepšiť zabezpečenie AD infraštruktúry pre malé a stredné podniky.

- Kurz o pokročilých bezpečnostných mechanizmoch Active Directory poteší každého administrátora, ktorý má záujem inovovať celkovú úroveň bezpečnosti a konceptu svojej AD domény. Predstavíme Vám množstvo oblastí a opatrení, ktoré častokrát chýbajú a spôsobia prienik do AD domény a kompromitujú infraštruktúru. V neposlednom rade nás čaká veľa spoločného brainstormingu a diskusií.
- Upozornenie: Jedná sa o rozšírený kurz - oproti štandardnému kurzovému dňu je na tento kurz vyčlenených 6 hodín (nakoľko počítame s aktívnou diskusiou účastníkov)

Bezpečnostné mechanizmy systému Windows Server - opakovanie

- GPO - možnosti, odkiaľ čerpať námety
- Windows Firewall (a jeho úskalia v prípade použitia antimalvérových produktov s podobnou funkciou)
- Windows Defender a ostatné antimalvérové nástroje

Resuscitácia AD

- Dôležité miesta v doméne, ktoré je potrebné kontrolovať a monitorovať

Bezpečné DNS

- Využitie DNS proxy a rozličné scenáre ochrany DNS.
- Nastavenie bezpečnej replikácie DNS záznamov.

Bezpečná sieť

- Cez ktoré protokoly potrebujú naši používatelia komunikovať?

Firewall pre klientov, servery, radiče AD

- Nastavenie pravidiel prostredníctvom GPO

Používateľské účty a skupiny používateľov

- Prečo každý nemusí byť Domain User?

Model vrstvenia

- Ako ochrániť administrátorské konto pred „šikovným“ používateľom?
- Využitie vybraných skupín v AD

Problematika lokálneho administrátora

- Nástroj Local Admin Password Solution - áno alebo nie?
- Ochrana procesu LSASS

Čo všetko môžu naši používatelia?

- Čítanie z LDAP, resp. čítanie databázy AD
- Čítanie a parsovanie skupinových politík
- Spúšťanie programov, exfiltrácia

Ako získať večný život?

- Perzistencia na pracovnej stanici, serveri
- Perzistencia v AD
- Odhaľovanie perzistencie základnými ale aj sofistikovanými postupmi

Záverečné zhrnutie

Macrosoft s.r.o.
Štefánikova 47
811 04 Bratislava

tel: 02/ 55 410 308,
0948 88 40 88
e-mail: macrosoft@macrosoft.sk

- diskusia o možných ďalších opatreniach na zvýšenie bezpečnosti domény
- záver

Upozornenie

- Jedná sa o rozšírený kurz - oproti štandardnému kurzovému dňu je na tento kurz vyčlenených **6 hodín** (nakoľko počítame s aktívnou diskusiou účastníkov).
- V prípade záujmu je možné prispôsobiť témy kurzu na mieru a prispôsobiť ho potrebám konkrétnej inštitúcie (napr. pre účely školenia IT oddelení, Manažérov informačnej bezpečnosti a pod.)