Zabezpečení

GPO Security Settings

- Comp Conf – Win Settings – Security Settings
- Account Policies
  - Password Policy – požadavky na hesla uživatelů
    - Doménová hesla nutno vynucovat v Default Domain Policy
  - Account Lockout Policy – podmínky zamknutí účtu v případě opakovaného nesprávného zadání hesla
- Local Policies
  - Audit Policy – nastavení logování událostí
  - User Rights Assignment – speciální oprávnění
  - Security Options – co se jinam nevešlo…

Firewall

- Blokuje nežádoucí síťový provoz
- Default
  - Příchozí provoz zakázán
  - Odchozí provoz povolen
- Nastavení přes GPO
  - Comp Conf > Windows Settings > Security Settings > Windows Firewall
  - Umožňuje doménovým správcům vynutit FW pravidla na stanicích

Updaty

- Počítače musí být udržovány v aktualizovaném stavu
- GPO
  - Computer Configuration – Administrative Templates – Windows Components – Windows Update
- Windows Server Update Services

Zálohování AD

- Ztráta dat vlivem přírodních jevů ale i cílených útoků
- Autoritativní x neautoritativní obnova
- Windows Server Backup, wbadmin
  - System State Backup
  - Propojení s Task Schedulerem

Delegace oprávnění

- Bezpečnost – Princip minimálních oprávnění
- Administrace
  - Odchod pracovníka
  - Výměna pracovníka
  - Přidání dalšího pracovníka

Princip minimálních oprávnění

- *Každý uživatel systému musí mít právo vykonávat pouze ty činnosti a přistupovat pouze k těm datům, které nezbytně potřebuje ke své práci.*

AGDLP

- AGDLP
  - A … Accounts
  - G … Global group
  - DL … Domain Local group
  - P … Permissions

AGDLP

1. Vytvoření Global skupiny v doméně uživatele
2. Vložení uživatele do Global skupiny
3. Vytvoření Domain Local skupiny v doméně zdroje
4. Vložení Global skupiny do Domain Local skupiny
5. Přidělení odpovídajících práv Domain Local skupině
   - Pozor na Advanced Features

AGDLP – Řetězení skupin

- Global
  - Vkládání skupin do sebe podle hierarchie organizace
  - Např. G_Zamestnanci obsahuje G_Marketing a G_Ekonomicke, G_Ekonomicke navíc obsahuje G_Ucetni
- Domain Local
  - Vkládání skupin do sebe podle úrovně přístupu ke zdroji
  - Např. DL_Pocitace_RW je vložena do skupin DL_Pocitace_R a DL_Pocitace_W, DL_Pocitace_W je navíc vlozena do DL_Pocitace_ResetPass

Fyzická bezpečnost

- Ochrana před
  - Krádeží (zámky, kontrola přístupu, uzavřené serverovny)
  - Poškozením
  - Výpadkem elektrického proudu (UPS, generátory)
  - Ztrátou konektivity (náhradní připojení)
  - Požárem (chlazení, požární hlásiče)
- **Redundance !!!**

Sociální inženýrství

- Útok na uživatele, ne přímo na systém
- Metody
  - Zastrašování
  - Krytí se autoritou
  - Předstírání bezradnosti
  - Zneužívání informací
- Ochrana
  - Školení uživatelů
  - Legislativa, vnitřní předpisy

Písemné dokumenty

- Každé významnější bezpečnostní nastavení by mělo být vynucováno písemnými nařízeními managementu / informačního oddělení
- Umožňuje postižitelnost
- Psychologický význam

Obecné rady pro práci

- Silná hesla
  - Pozor na řetězení připojení – rozhodující je nejslabší heslo „na cestě“
- Nepřihlašovat se z nezabezpečených počítačů
- Zamykat session vždy když nesedím u počítače
- Přihlašovat se jako běžný uživatel, pod administrátora přejít pouze pro vykonání konkrétní činnosti
- Používat šifrované připojení

Úkoly

1. Vytvořit OU CallCentrum a uživatele UserA a UserB
2. Přiřadit uživateli UserA právo Write na OU CallCentrum
3. Přiřadit uživateli UserB právo Write na OU CallCentrum
4. Odebrat uživateli UserA právo Write na OU CallCentrum
5. Otevřít port 80 na klientské stanici pomocí GPO
6. Povolit automatické instalace updatů pomocí GPO
7. Zazálohovat AD