Manželka pošle svého manžela informatika nakoupit se slovy: "Kup chleba a když budou mít rohlíky, vezmi jich deset."
Manžel přijde z obchodu a donese deset chlebů, protože rohlíky měli.

Podzim 2008

PV175 SPRÁVA MS WINDOWS I

Řízení přístupu

Motivace

- Systémové naplnění principu minimálních oprávnění
  - Každý uživatel by měl mít možnost vykonávat pouze ty činnosti, které nezbytně potřebuje ke své práci
- Záznamy o přístupech ke zdrojům jsou základem auditu

Práva a oprávnění

- Diskrétní řízení přístupu – vlastník objektu rozhoduje o povolení přístupu
- NTFS permissions – oprávnění přiřazovaná složkám a souborům na úrovni souborového systému NTFS
- share permissions – oprávnění přiřazovaná zdrojům sdíleným v síti
- AD user rights – práva uživatelů nebo skupin provést v AD určitý úkon

ACL (Access Control List)

- Seznam uživatelských účtů a jim přidělených oprávnění, připojený k objektu (souboru, složce, klíči registru, sdílené položce,…)
- ACE (Access Control Entry)
  - Obsahuje SID, oprávnění, příznaky dědičnosti a omezení působnosti
- Windows Vista
  - http://technet.microsoft.com/en-us/magazine/cc138011.aspx

Dědičnost

- Defaultně se oprávnění z nadřazených složek dědí do podsložek
- Je možné zakázat dědění oprávnění, v takovém případě se složka stává novým kořenem oprávnění
- Je možné vynutit, aby se oprávnění na podsložkách a souborech shodovala s těmi na nadřazené složce

Vlastnictví

- Každý soubor nebo složka má svého vlastníka
- Vlastník má vždy neodstranitelné právo přidělovat oprávnění
- Vlastnictví může převzít člen skupiny Administrators nebo osoba s právem Take Ownership
- Na základě množství vlastněných souborů je možné specifikovat diskové kvóty

Uplatňování oprávnění

- Implicitní je Deny
- K povolení přístupu na dané úrovni stačí aspoň jedno Allow
- K nepovolení přístupu stačí jediné Deny
- Deny má vždy přednost před Allow
- Uživatel může efektivně využívat sjednocení všech ACE, pro která má Allow, pokud nemá ani jedno Deny

NTFS

- New Technology File System
- Nejběžnější souborový systém u počítačů s Windows
- Každá partition může využívat jiný souborový systém
- NTFS je vyžadován pro:
  - Řízení přístupu, šifrování, diskové kvóty, kompresi na úrovni FS…

NTFS oprávnění na soubory

- Read
  - Číst soubor, zobrazit jeho atributy a ACL
- Write
  - Přepsat soubor
- Read & Execute
  - Jako read a navíc je možné soubor spustit
- Modify
  - Read, write, smazání souboru
- Full Control
  - Cokoliv, včetně změn oprávnění a převzetí vlastnictví

NTFS oprávnění na složky

- Read
  - číst soubory, podsložky a atributy složky
- Write
  - read + vytvořit nové soubory, měnit atributy
- List Folder Contents
  - vidět jména souborů a podsložek
- Read & Execute
  - read, LFC + procházet složku a podsložky
- Modify
  - Write, R&E + smazat složku
- Full Control

Ověření oprávnění

1. Přihlášení uživatele a vytvoření jeho access tokenu (SIDy uživatele a všech skupin, kterých je členem)
2. Pokus o přístup ke zdroji. Porovnání SIDů v jednotlivých ACE se SIDy v access tokenu.

   Pokud je nalezen aspoň jeden záznam (SID, oprávnění, Allow) a zároveň žádný (SID, oprávnění, Deny), je uživateli povolena požadovaná akce.

Share

- Zařízení nebo informace dostupná z jiného počítače, typicky v LAN
- př.: sdílené složky, disky, tiskárny
- Share může být skrytý ($)
- Přístup k sharu může být omezen přístupovými právy (FC, Read, Modify)
  - Pokud se jedná o disky nebo soubory, tak jsou skutečná práva rovna průniku práv na sharu a na NTFS

Obecná práva uživatelů

- GPO: Computer Configuration – Windows Settings – User rights assignment
- Zde je možné specifikovat činnosti, které mohou provádět uživatelé nebo skupiny uživatelů (př. kdo může provádět zálohování, kdo se může přihlásit lokálně, přes síť atd.)

Best practices

- Každé významnější bezpečnostní nastavení by mělo být vynucováno písemnými nařízeními managementu nebo informačního oddělení
  - Postižitelnost
  - Psychologický efekt
- Vždy přidělovat oprávnění skupinám, ne přímo jednotlivcům
- Vyvarovat se použití Deny

Best practices

- Vhodně využívat dědičnost pro minimalizaci velikostí ACL
  - Nastavovat oprávnění na úrovni složek, nikoliv jednotlivých souborů
- Adresářům s aplikacemi přiřadit práva podle masky:
  - Users: Read & Execute
  - Administrators: Full Control
- Poučit uživatele o právech ☺

Windows 7

- 28.10. poprvé představeno
- Změny oproti Vistě víceméně pouze vzhledové
- http://www.winsupersite.com/win7/win7_preview.asp
- http://www.winsupersite.com/win7/win7_preview_02.asp
- http://blogs.technet.com/sieben/archive/2008/10/29/windows-7-installation-walkthrough.aspx
- http://www.neowin.net/news/live/08/10/28/introducing-the-windows-7-ui

Dotazy?

Díky za pozornost