Bezpečnostné mechanizmy v OS Windows

Obsah

Skupinové politiky

Skupinové politiky predstavujú možnosti pre centralizáciu správy počítačov a obmedzení používateľov. Správcovia môžu nastaviť automatickú aplikáciu potrebných nastavení pre počítače, používateľov s cieľom vybudovať štandardizované prostredie v zmysle štandardov v oblasti riadenia informačnej bezpečnosti. Nastavenia sú rozsiahle (viac ako 6 000 možností), dajú sa nastavovať hierarchie – resp. poradie aplikovania, aktivovať alebo deaktivovať dedičnosť v rámci organizačných jednotiek domény ale aj využiť automatické možnosti reaplikácie politík na klientskych operačných systémoch po uplynutí stanoveného časového limitu.

Nastavenie politík je rozdelené do dvoch častí. Osobitne je možné nastaviť politiky pre počítač, ktoré sú aplikované na stroj ako celok bez ohľadu na prihláseného používateľa a politiky pre používateľov, ktorí sa prihlásia na daný počítač.

Pre účely zabezpečenia domény môžeme využiť nástroj `gpmgmnt.msc` a nastaviť politiky centralizovane pre všetky počítače a používateľov. V prípade potreby zabezpečenia lokálneho stroja môžeme použiť nástroj `gpedit.msc` a politiky budú aplikované na danom konkrétnom stroji. Obe možnosti sa dajú kombinovať, t. j. niektoré politiky budú prevzaté z domény a zvyšné z lokálnej politiky daného stroja. Prednosť však majú doménové politiky.

Princíp fungovania väčšiny skupinových politík, ktoré slúžia na nastavovanie vlastností operačného systému je založený na ovplyvňovaní hodnôt v registroch systému Windows. Pre ilustráciu uvažujme Windows 10 nepripojený do domény. V umiestnení `%SystemRoot%\PolicyDefinitions\` možno nájsť definičné súbory politík typu ADMX. Štruktúru tohto súboru ilustruje nasledujúci príklad. Vlastnosť, ktorej text môže byť preložený pre jednotlivé jazykové mutácie (`dispalyname`) má v časti `key` uloženú informáciu o ceste v registroch systému Windows, ktorú treba ovplyvniť.

```
<policy name="HostToRealm" class="Machine"
displayName="$(string.hosttorealm)"
explainText="$(string.hosttorealm_explain)"
presentation="$(presentation.hosttorealm)"
key="Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos"
valueName="domain_realm_Enabled">
      <parentCategory ref="kerberos" />
      <supportedOn ref="windows:SUPPORTED_WindowsVista" />
      <elements>
        <list id="hosttorealm"
key="Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\dom
ain_realm" additive="true" explicitValue="true" />
      </elements>
    </policy>
```

Obrázok 1 - Výber z definičného súboru skupinovej politiky

Správa počítača (Computer Management)

Konzola správy počítača (Computer Management Console) je sada nástrojov na správu Windows. Nástroje sú rozdelené do troch kategórií:

- Systémové nástroje (System Tools)
- Úložisko (Storage)
- Služby a aplikácie (Services and Applications)

Systémové nástroje

- Zobrazenie udalostí (Event Viewer) – správa a zobrazenie udalostí zaznamenaných v logoch.
- Zdieľané priečinky (Shared Folders) – vytváranie, zobrazenie a správa zdieľaných priečinkov.
- Lokálni používatelia a skupiny (Local Users and Groups) – správa lokálnych používateľov a skupín.
- Výkon (Performance) – monitorovanie výkonu a stavu počítača.
- Správca zariadení (Device Manager) – správa hardvérových zariadení pripojených k počítaču.

Úložisko

- Odpojiteľné zariadenia (Removable storage) – správa odpojiteľných úložných médií.
- Defragmentácia disku (Disk Defragmenter) – defragmentácia oddielov na diskoch.
- Správa diskov (Disk Management) – operácie spojené s diskami.

Služby a aplikácie

- Služby (Services) – správa služieb na lokálnom a vzdialených počítačoch.
- Ovládanie WMI (WMI Control) – konfigurácia Windows Management Instrumentation (WMI)

Správca servera (Server Manager)

Server Manager je správcovská konzola dostupná vo Windows Server, ktorá umožňuje jednoduchý prístup k nástrojom na správu a provisioning lokálnych aj vzdialených serverov.

Prístupové oprávnenia NTFS

4.3 KONFIGURÁCIA RIADENIA PRÍSTUPU K DÁTAM

Každý súbor a priečinok uložený na súborovom systéme NTFS má bezpečnostný deskriptor na kontrolu prístupu k dátam. Táto štruktúra obsahuje dve dôležité štruktúry a to diskrétny zoznam kontroly prístupu a systémový zoznam kontroly prístupu, spolu s identifikátorom vlastníka dát. Vlastník dát je používateľský účet, ktorý má absolútny prístup k dátam, čo zahŕňa aj schopnosť prideľovať či odoberať tento prístup ostatným účtom. V praxi to potom vyzerá asi tak, že aj pokiaľ vlastníkovi dát odoberieme prístup k dátam, má právo si tento prístup zasa obnoviť. Na druhú stranu členovia skupiny administrátorských používateľských účtov môžu prebrať vlastníctvo hociktorých dát. Toto zabezpečuje pohodlnú obnovu dát, napríklad pokiaľ používateľ účtu odišiel zo spoločnosti, či napríklad pokiaľ sa nesprávne nakonfiguroval prístup k dátam.

Riadiť prístup k dátam sa dá na úrovni priečinkov a na úrovni súborov. Operačný systém Windows XP ponúka základné nastavenia prístupu k dátam, ktoré sú preddefinované najzákladnejšie kombinácie špeciálnych oprávnení k dátam. Ide o tieto možnosti: plný prístup, modifikácia, čítanie a vykonanie, zobrazenie obsahu priečinka, čítanie a posledná možnosť je zápis. Jednotlivé špeciálne oprávnenia môžeme vidieť v tabuľke 01[3]:

	Základné kombinácie					
Špeciálne oprávnenia	plný prístup	modifikácia	čítanie a vykonanie	zobrazenie obsahu priečinka	čítanie	zápis
prechádzaj priečinok / vykonaj súbor	x	x	x	x		
obsah priečinka / čítaj dáta	x	x	x	x	x	
čítaj vlastnosti	x	x	x	x	x	
čítaj rozšírené vlastnosti	x	x	x	x	x	
vytváraj súbory / zapisuj dáta	x	x				x
vytváraj priečinky / pridávaj dáta	x	x				x
zapisuj vlastnosti	x	x				x
zapisuj rozšírené vlastnosti	x	x				x
zmazanie podpriečinkov a súborov	x					
zmazanie	x	x				
čítaj oprávnenia	x	x	x	x	x	x
meň oprávnenia	x					
prevzatie vlastníctva	x					

Tabuľka č. 01 – Základné kombinácie prístupu k dátam

Prechádzaj priečinok: dovoľuje používateľovi prechádzať cez priečinok, aj keď používateľ nemá právo na čítanie. Týka sa len priečinkov.

Vykonaj súbor: povoľuje alebo zakazuje vykonanie spustiteľných súborov a týka sa iba súborov.

Obsah priečinka: povoľuje, alebo zakazuje zobrazenie súborov a podpriečinkov v danom priečinku. Týka sa len priečinka.

Čítaj dáta: povoľuje zobrazenie dát v súboroch, týka sa len súborov

Čítaj vlastnosti : povoľuje alebo zakazuje zobrazenie vlastnosti súboru alebo priečinku, ako napríklad len-na-čítanie.

Čítaj rozšírené vlastnosti: povoľuje alebo zakazuje čítanie rozšírených vlastností. Tieto vlastnosti sú definované špecifickými programami a líšia sa medzi programami.

Vytváraj súbory/zapisuj dáta: povoľuje alebo zakazuje vytváranie súborov v priečinku (pre priečinok). Povoľuje alebo zakazuje menenie a prepisovanie dát v súbore (pre súbor).

Windows Firewall

V prípade podnikovej siete možno považovať bránu Firewall servera alebo pracovnej stanice ako poslednú líniu obrany (ak uvažujeme o modeli defense-in-depth).

Všeobecnou úlohou brány firewall je na základe určitých pravidiel povoľovať alebo zakazovať prechod údajov prostredníctvom počítačovej siete. Jej hlavnou úlohou je regulovať tok údajov medzi počítačovými sieťami s rôznymi úrovňami dôvery. Funkciou brány firewall je teda zamedziť prieniku nevyžiadaných údajov z počítačovej siete s nízkou dôverou do počítačovej siete s vyššou dôverou.

Brána firewall systému Windows je navrhnutá na ochranu jediného osobného počítača alebo servera. Prednastavenou konfiguráciou brány firewall je blokovanie všetkej komunikácie smerom z pripojenej počítačovej siete ku klientskej stanici, okrem predvolených služieb, predovšetkým na serveri.

V praxi na Windows Serveri v podnikovom prostredí beží služba DNS, LDAP - kvôli adresárovej službe Active Directory, príp. služba DHCP.

Z používateľského hľadiska je nutné vytvoriť výnimky pre určité aplikácie, ktoré následne brána firewall prepustí zo siete do klientskej stanice.

Zdroje

Administrative Tools

https://docs.microsoft.com/en-us/windows/client-management/administrative-tools-in-windows-10

Server Manager

https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager

Windows Security

https://docs.microsoft.com/en-us/windows/security/

Windows Server Security

https://docs.microsoft.com/en-us/windows-server/security/security-and-assurance

Windows Server 2008 Documentation

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc772323(v=ws.10)

Windows Server 2012 Documentation

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh801901(v=ws.11)

Firewall best practice

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring

M. Pavelka: KOMPLEXNÝ NÁSTROJ NA AUTOMATIZOVANÉ ZABEZPEČOVANIE OPERAČNÉHO SYSTÉMU VO FIREMNOM PROSTREDÍ. Bakalárska práca. FIIT STU, 2021.