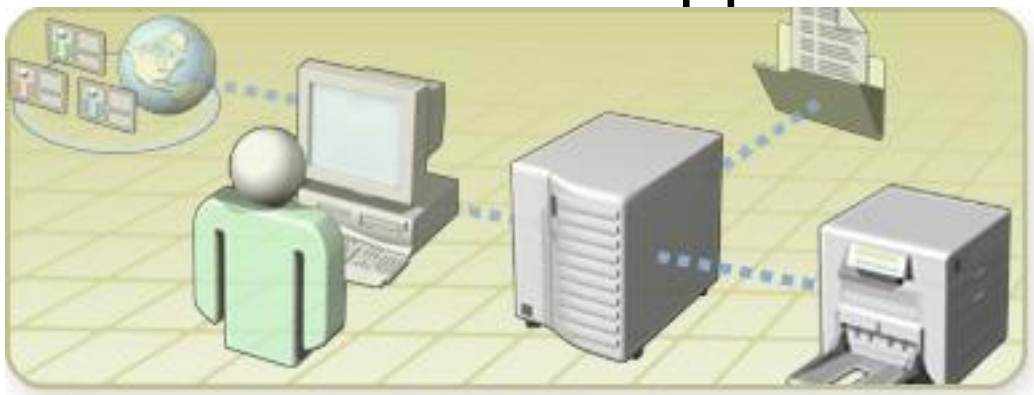
Group Policy за засилване на системната сигурност

Михаил Радев



План

- Преглед на Active Directory
  - Логически компоненти
  - Физически компоненти
  - Обекти
  - trust
- GPO
- Group Policy Management Tool
  - Създаване на GPO
  - Свързване на GPO
  - Редактиране и преглеждане на GPO настройки
  - Използване на Starter GPO
- Прилагане на GPO
- Изключения от правилата
  - Блокиране на наследяването
  - Enforced
  - Security Filtering
- Group Policy модели и резултати
- Използване на Password Setting Objects PSO

Какво е Active Directory?

- Това е името, дадено от MS на тяхната директорийна услуга/следва директорийния модел X.500/
- Обикновено се оприличава на телефонен указател – организация на хора, въз основа на различни полета (име, адрес, телефонен номер..). Но по-важно е, че AD служи за управление. AD позволява да създаваме обекти – потребителски акаунти, групи, компютри..., за които може да се дефинират атрибути – име, адрес, отдел и след това, понеже ще се използват в мрежа – да се определят login настройки, позволения за достъп до ресурси, настройки на политики, одит, .. Т.е. това не е статична, непроменяща се директория, а динамична и активна директорийна услуга.

Какво е AD?

- Active Directory е и йерархично хранилище за данни – съхранява информация за обектите в мрежата и прави лесно управлението им и търсенето в тях.
- Active Directory е централно хранилище за акаунт информация – потребители, групи и компютри.
- Самата AD се дефинира от schema, която указва как всеки обект е представен в хранилището за данни. Например, обектът user има първо име, фамилия, logon име, е-мейл адрес и парола. Или това е AD структурата.
- Щом AD е база данни, трябва да има индекс. Нарича се global catalog (GC) и съхранява подмножество от информация за всеки обект, което може да се използва за търсене в директорията. Информацията в GC се репликира към другите домейн контролери – промяна в един от тях автоматично се репликира на останалите.

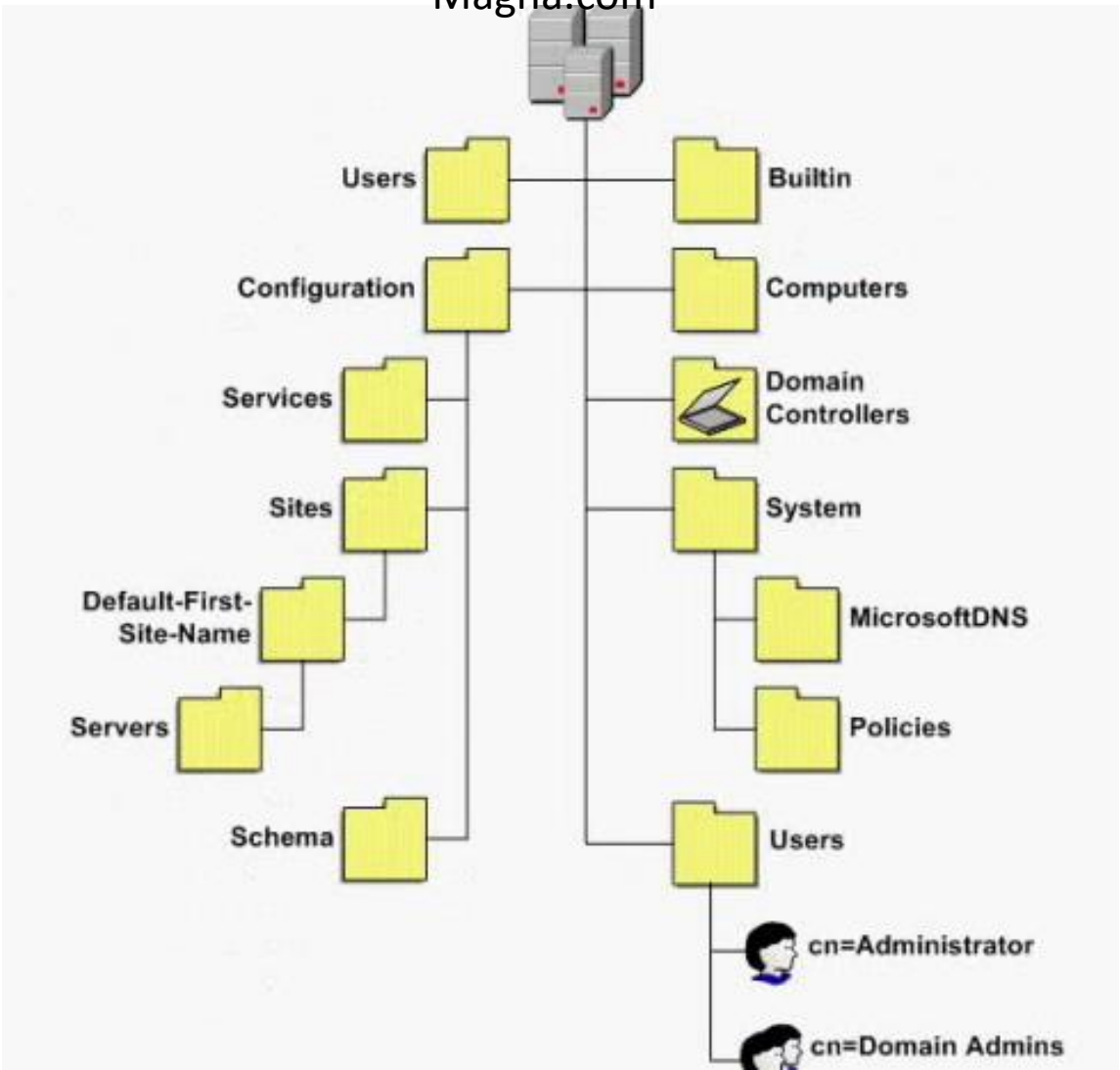
AD – предимства на използването й

- Централизираност
- Мащабируемост
- Разширяемост
- Управляемост
- Сигурност
- Интеграция с DNS
- Репликация
- GPO

Какво е AD?

- Файла на AD базата е ntds.dit

Magna.com



Физическа и логическа страна на AD

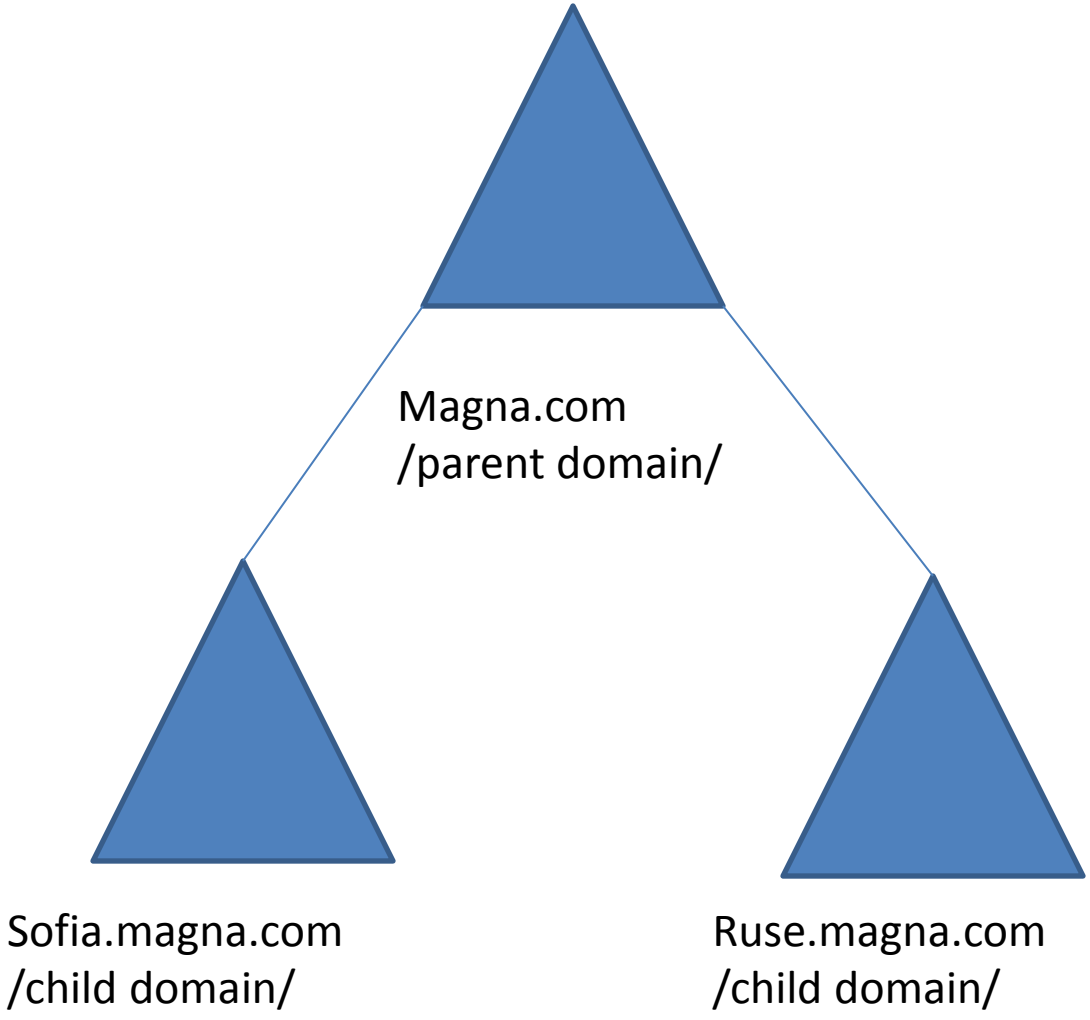
- От физическа гледна точка, AD позволява да се групират компютри (работни станции и сървъри) в сайтове (site). Сайтът обикновено включва една или няколко подмрежи, разположени в една физическа област. Ако имаме офис Варна и офис Шумен, това е очевидния пример на два отделни сайта. Но, може да имаме множество подмрежи във Варна поради големия размер на мрежата и да разделим това място на няколко допълнителни сайта.

- Сайтовете помагат да се ограничи репликацията, която се случва между тях и да се контролира използвания за репликация bandwidth.

Физическа и логическа страна на AD

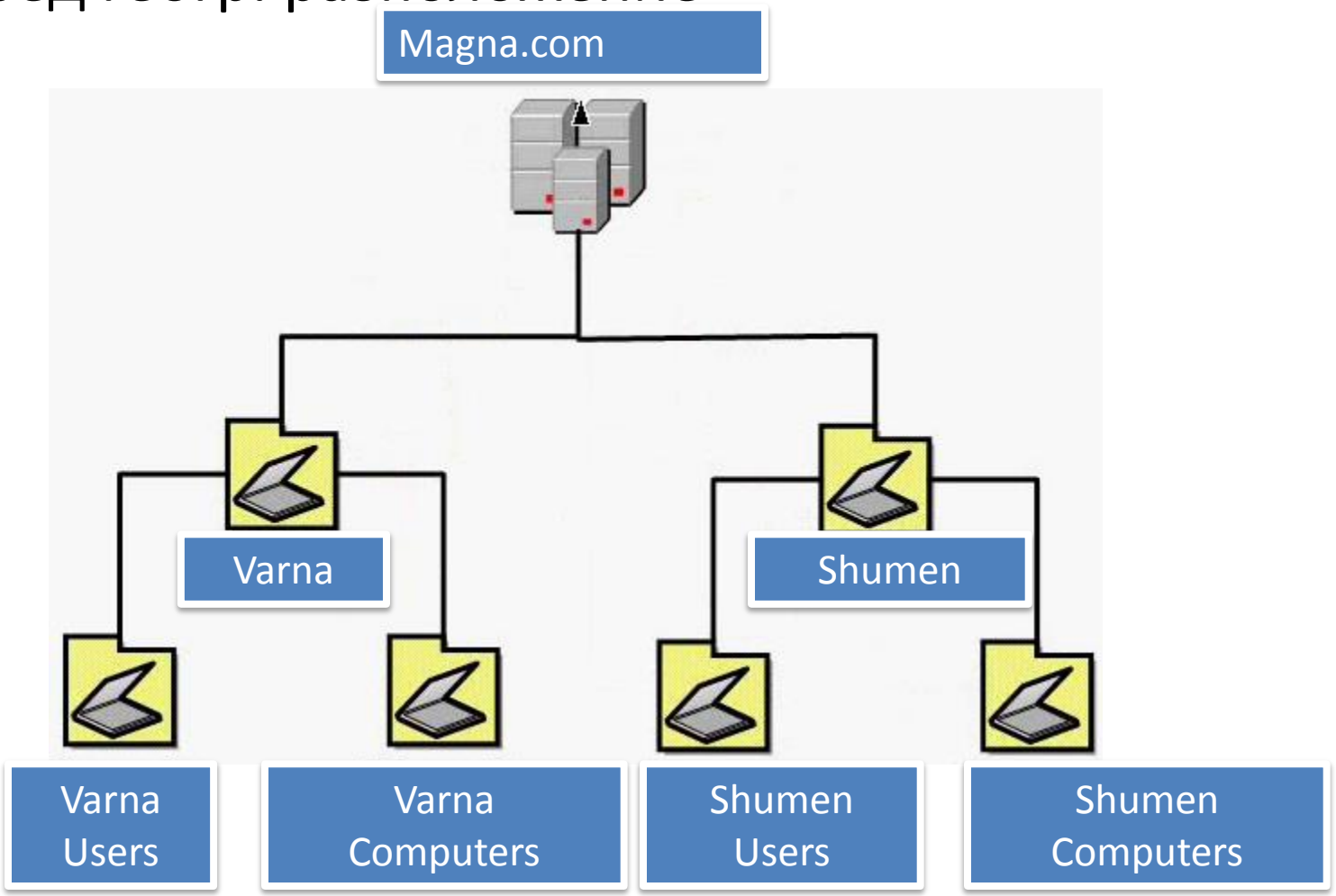
- Логическата страна на AD са forest, domain, organizational unit.
- Forest съдържа trees.
- Tree в случая с Магна е домейна. Ако имаше множество домейни с множество child домейни /всички свързани с transitive two-way trust/ те всички щяха да са tree.

Magna Forest



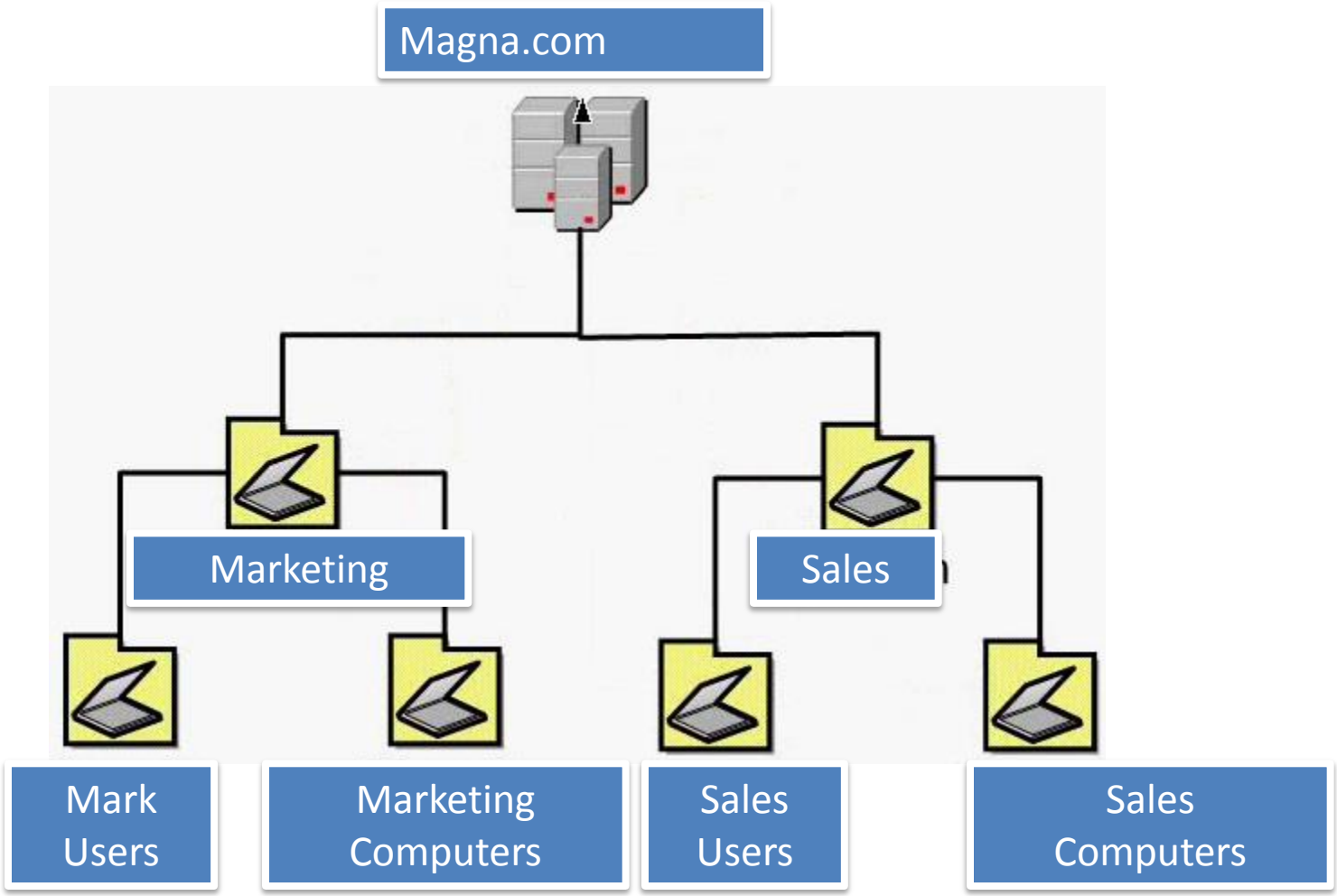
Organizational Unit OU

- Целта им е – чрез тях - по-лесно администриране на AD
- Според геогр. разположение



Organizational Unit OU

- Според отделите



Структура на домейн

- Domain
- Tree
- Forest
- Site

Преглед на Active Directory

- AD логическата структура се състои от Forests, Trees и Domains
- AD физическата структура се състои от sites и domain controllers
- AD database се състои от йерархическа структура от обекти. Тези обекти могат да са или контейнери (container), които се използват за съхранение на други обекти или leaf object, които представят цялостен обект и не съдържат други обекти.

AD логическа структура

- Domains – основен административен контейнер в AD
- Trees – област от namespace, съдържаща един или повече домейни
- Forest – съвкупност от trees. Най-отгоре е в AD инфраструктурата.

AD физическа структура

- Domain controllers – съхраняват копие на AD database
- Sites – представя физическото място, което съдържа домейн контролери. Отделните сайтове са свързани с бавни WAN връзки.

AD обекти

- Container – най-често използвания контейнер е OU – Organizational Unit. Чрез доброто им проектиране трябва да се постигне: добра организация, управление на груповите политики, делегиране на контрол
- Leaf – AD обект, който не съдържа други обекти. Например, обект user, обект computer.

AD trusts

- Parent/Child trust – по подразбиране всички домейни в рамките на 1 forest имат двупосочен транзитивен тръст с всеки друг домейн по-горе или по-долу в йерархията
- Shortcut trust – директен trust между два домейна. Обикновено се използва в голям forest.
- External trust – между домейн от форест и външен за този forest домейн, обикновено Windows NT домейн.
- Realm trust – trust между Windows домейн и Unix realm

AD trusts

- Forest trust – създава trust relationship между всички домейни в един forest и всички домейни в друг forest.
- Federated trust - за да могат да си комуникират през Интернет чрез достъп до ресурси през уеб приложения като например SharePoint. За създаването им се ползва AD Federation Services Role.

GPO

- Group policy object GPO е AD обект, който съдържа конфигурационни настройки за компютри и/или потребители.
- GPO облекчава администрирането и позволява да се направят настройките веднъж, а да се прилагат към множество компютри и/или потребители
- GPO настройките се прилагат към обекти потребител/компютър, които са в контейнер, към който съответния GPO е свързан.

Задача

- China.Magna.com
- В Шанхай имаме 53 потребители в следните групи:
  - 5 – Мениджърски отдел
  - 10 – отдел продажби
  - 3 - IT администратори
  - 30 - Call център оператори
  - 5 - Call център мениджъри
- Да се създадат в AD Users and Computers

Задача - продължение

- OU структура:
  - 2 top level OU – Шанхай и Пекин
  - В Shanghai OU има следните OU:
    - Sales, Operations, Management, Call Center
- Global security group, в която членуват IT администраторите

Задача - продължение

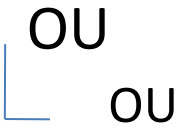
- Никой в домейна не трябва да може да използва removable device, освен членовете на групата IT Admins
- Всички членовете на Sales трябва да имат на десктопа си shortcut до 1 важен документ, който съвместно ползват
- Никой в домейна не трябва да може да използва Add/Remove Programs, освен членовете на Operations

Group Policy Management Tool

- За създаване и свързване на GPO
- За редактиране и преглеждане на GPO настройките
- Starter GPO

Прилагане на GPO

- Реда за прилагане на GPO е:
- **LSD OU**
  - Local
  - Site
  - Domain
  - OU



Правилото при конфликт е: последната приложена настройка е най-силна.

Изключение от правилата

- Block Inheritance– всички наследени от родителските контейнери GPO-та ще се игнорират.
- Enforced- когато се приложи към GPO линк всички негови настройки ще имат предимство при конфликт. Припокрива и Block Inheritance.
- Security filtering – да се забрани “Apply Group Policy” за потребител или група /от GPMC Delegation/.

Конфигуриране на User Account Control

- UAC добавя ауторизационен слой преди да може да се извърши действие, изискващо административни права
  - Ако UAC се игнорира за повече от 150 секунди заявката не се одобрява
- Само потребители с административни права могат да одобряват UAC съобщения
- По подразбиране UAC е пуснат по подразбиране в Windows 7
- Може да се конфигурира според политиката за сигурност на организацията

Конфигуриране на User Account Control

- Възможности

- Привилегии
  - Всички потребители работят със стандартни привилегии, включително и администраторите
  - Само когато задачата изисква административни права, тогава UAC прекъсва работата и временно увеличава привилегиите
    - напомняне /Prompt/ за съгласие
    - Промпт за удостоверяване на самоличност

Конфигуриране на User Account Control

- Настройки
  - Never notify me
  - Notify me only when programs try to make changes to my computer (do not dim my desktop)
  - Default - Notify me only when programs try to make changes to my computer (but don’t notify me when I make changes to Windows settings)
  - Always notify

Конфигуриране на User Account Control

- Group Policy/Local Group Policy/Local Security Policy
  - Computer Configuration> Windows Settings > Security Settings > Local Policies > Security Options
  - Local Group Policy: gpedit.msc
  - Local Security Policy : secpol.msc
- Позволява прецизен контрол над UAC политиките
  - Може да се конфигурира UAC да изисква аутентикация, вместо само да извежда прозорец за потвърждение

Конфигуриране на политики за removable devices

- С цел повишаване на сигурността, много организации забраняват използването на removable devices
- Group Policy / Local Group Policy
  - Computer Configuration -> Administrative Templates -> System -> Device Installation -> Device Installations Restrictions
  - Prevent installation of removable devices

Run as

- Позволява стартирането на програма чрез използване на различни от текущите потребителски пълномощия
- Runas /user:DOMAIN\USER “program” /параметри

- Runas /user:magna\kolev “mspaint”

- Runas /user:pc1\kolev “mspaint”

Account Policies и User Rights

- Account и password политики
  - Computer Configuration -> Windows Settings -> Security Settings -> Account Policies
  - Local Group Policy : gpedit.msc

  - Политиките за пароли включват:
    - Enforce password history
    - Maximum password age
    - Minimum password age
    - Password must meet complexity requirements
    - Store password using reversible encryption

Account Policies и User Rights

- Конфигуриране на account lockout policies:
  - Account lockout duration
  - Account lockout threshold
  - Reset account lockout

User rights:

Computer configuration -> Windows Settings -> Security Settings -> Local Policies - > User Rights Assignment

Въпроси?

Консултации
– сряда от 14:00 до 16:00 в кабинет 2-401
- петък от 13:00 до 15:00 в кабинет 530

Email: radev@ue-varna.bg