

Практически насоки при внедряване на система за управление сигурността на информацията в съответствие с изискванията на ISO 27001:2005

Конференция за Информационна Сигурност
Септември 2009



Борис Гончаров, CISSP

Certified Information Systems Security Professional

Четири въпроса



- За какво става въпрос?
- Защо има значение за нас?
- Как работи?
- Какво трябва да направим?

Какво е сигурност на информацията?



- **Използване на СУСИ (Система за Управление Сигурността на Информацията) в дадена организация за **систематичното** опазване на**
 - Наличността
 - Поверителността
 - Цялостносттана нейните информационни активи (и информационни системи)
- **Риск за информацията**
 - Всички информационни системи имат уязвимости, които могат да бъдат използвани от определени заплахи по начин, който би имал значително въздействие върху ефективността, доходността, стойността и дългосрочното оцеляване на дадената организация
- **Също включва**
 - Достоверност
 - Отговорност
 - Неотменимост
 - Надеждност

За какво ни е СУСИ?



- **Разполагаме с ценни активи**
 - Интелектуална собственост
 - Търговски тайни
 - Данни относно служители, клиенти, доставчици
 - Организационно ноу-хау
- **Имаме законови и регулаторни изисквания**
 - ЗЗЛД
 - Други специфични (Sarbanes-Oxley)
- **Зависими сме от ИТ**
 - Сливът в ИТ (хардуер, електричество, природно бедствие) е и бизнес слив
 - ИТ не са напълно сигурни
 - ИТ не са взаимно съвместими

Защо сигурността на информацията е от значение?



■ Външни заплахи

- Вируси, червеи, троянски коне
 - 100 000+
- Хакери + автоматизирани атаки
 - Понастоящем огромен бизнес (botnets, zero-day атаки...)
- СПАМ – 80%+ от електронната поща
- Кибер престъпници – phishing, identify theft...
- Измами, кибертероризъм
- Конкуренти
- Всеки с компютър!

■ Вътрешни заплахи

- Измами, грешки, неоторизирана или нелегална употреба на системи, кражба на данни
- Недостатъчно обучение
- Невнимание

Какво е ISO 27001?



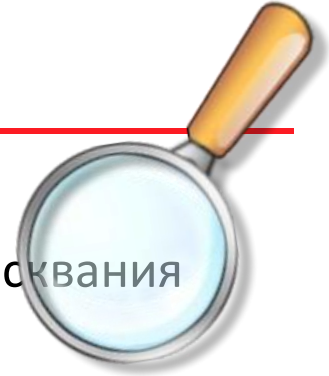
- Международен стандарт
- Ръководство и спецификация на най-добри практики
- **СИСТЕМА ЗА УПРАВЛЕНИЕ**
 - НЕ е технологична
 - НЕ е обвързана с конкретна нормативна уредба
- Систематичен и изчерпателен
- Приложим за всички организации, независимо от бизнеса и размера им
- Международно разбираем
- Годен за външна сертификация
- Общо приети най-добри практики
- 200+ нови ISO27001 сертификации/месец
- ISO27001 и ISO9001

Какво е СУСИ?



- **Дефинирана, документирана система за управление (в дадена организация-обхват), съдържаща:**
 - Одобрена от ръководството политика за сигурност
 - Дефинира сигурността на информацията, компонентите и целите на СУСИ и свидетелства, че подходът на мениджмънта по отношение сигурността на информацията е определен и систематичен
 - План за въздействие върху рисковете
 - Описва как различните типове рискове ще бъдат третирани
 - Списък на всички важни информационни активи (данни и системи)
 - Оценка на уязвимости, заплахи и рискове (преценяване на риска) за тези активи
 - Наръчник по СУСИ, съдържащ Декларация за приложимост
 - Определя контролите, които отговарят на всеки идентифициран риск
 - Изчерпателен комплект от процеси, политики, процедури и работни инструкции
- **СУСИ трябва да е**
 - Систематично внедрена и управлявана
 - Преглеждана, одитирана и проверявана
 - Непрекъснато подобрявана
- **Сертификация**
 - Финален етап
 - Извършва се от външен сертифициращ орган
 - Доказателство за пълнотата и качеството на СУСИ

ISO 27001 от близо



- ISO 27001:2005 - настояща версия
- Системи за управление сигурността на информацията - изисквания
- Спецификация на изискванията за
 - Създаване и управление на СУСИ
 - Внедряване и функциониране на СУСИ
 - Наблюдение и преглед на СУСИ
 - Поддържане и подобряване на СУСИ
 - Управление на документите
 - Отговорност на ръководството
 - Преглед от ръководството на СУСИ
 - Подобряване на СУСИ
 - Цели по контрола и механизми за контрол (Приложение А)
 - Не е изчерпателно

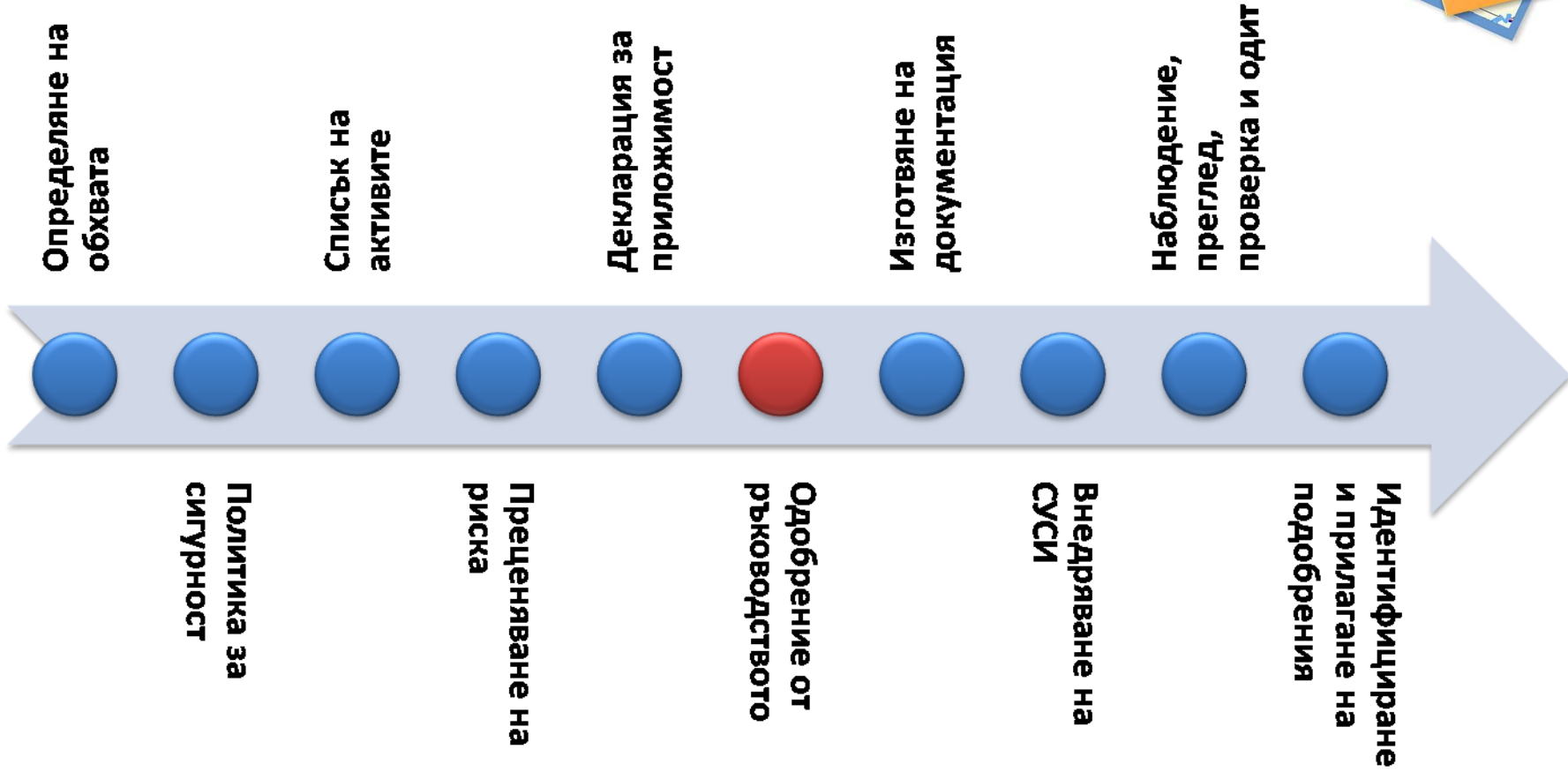
Какво е механизъм за контрол?



- Уязвимостта поражда заплаха
 - Заплахата може да прояви нежелано въздействие (финансово, оперативно) ако се материализира
 - Рискът е вероятността да се реализира дадената заплаха
 - Рисовете имат различни нива (напр. висок/катастрофален, среден/допустим, нисък/незначителен)
- Механизмът за контрол е отговорът на или ответната на мярка спрямо даден риск
 - (заплаха ≠ риск)
 - Механизмите за контрол намаляват риска но не го елиминират
- Механизмите за контрол се въвеждат единствено в отговор на специфични, идентифицирани рискове
- Комбинация от технология, поведение и процедура
 - Например Антивирус:
 - Инсталиран софтуер
 - Процедура за регулярно обновяване на вирусни сигнатури
 - Не се отварят съмнителни приложени файлове
- Стойност на механизма за контрол \leq стойност на нежеланото въздействие
- За всеки актив съществуват множество рискове
- Срещу всеки риск има механизъм за контрол
- Някои механизми за контрол се прилагат срещу множество рискове

Създаване на СУСИ

Пътна карта



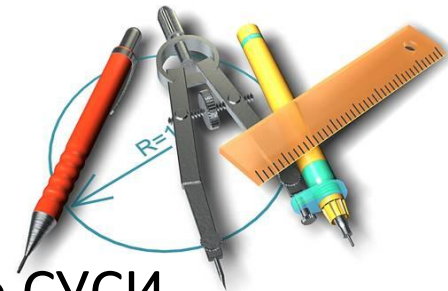
Какво трябва да направим?

Или как да превърнем теоретичните брътвежи в практика



Създаване на СУСИ

Ден 1



- Не си и помисляйте да внедрявате формално СУСИ
- Купете си стандарта на български език
- Намерете някой, който да е “в час” и който да знае как функционира организацията
- Намерете някой, който да може да пише (би било прекрасно ако е същият, който е “в час”)
- Научете се да разбирате стандарта
- Уверете се, че ръководството е готово да налага предложените решения

Създаване на СУСИ

Кое е задължително и кое по-задължително?

- Изключения от изискванията по точки от 4 до 8 **не се приемат**
 - Система за управление на сигурността на информацията
 - Отговорност на ръководството
 - Вътрешни одити на СУСИ
 - Преглед от ръководството на СУСИ
 - Подобряване на СУСИ
- Могат да бъдат изключвани (само в резултата от преценяването на рисковете) механизми за контрол от **Приложение А**



Изисквания по точка 4

Как да определим обхвата на СУСИ?

- На кои места се обработва информация (местоположение)?
- Кои дейности са свързани с информационни активи?
- Кой и какво обработва информация?



Изисквания по точка 4

Политика за сигурност



- Ръководството декларира как ще отделя от безценното си време и ще се ангажира със сигурността на информацията
- Определя се как ще се управлява СУСИ
- Указва се обхватът на СУСИ
- Посочва се “клетникът”, който ще носи отговорност за поддържането на СУСИ

Изисквания по точка 4

Преценяване на рисковете (модел)



Изисквания по точка 4

Преценяване на рисковете

- Използване на стандарта за определяне на заплахи, уязвимости и механизми за контрол:
- А.9.1 Сигурни зони
Цел: Да се предотврати **неразрешен физически достъп, вреда, вмешателство** в **помещенията и информацията** на организацията
- Точка А.9.1.2 Механизми за контрол на физическото влизане

Активи

Заплахи

Контрол

Сигурните зони трябва да бъдат защитени със съответни **механизми за контрол на входа**, за да се гарантира, че само упълномощеният персонал има **разрешен достъп**.

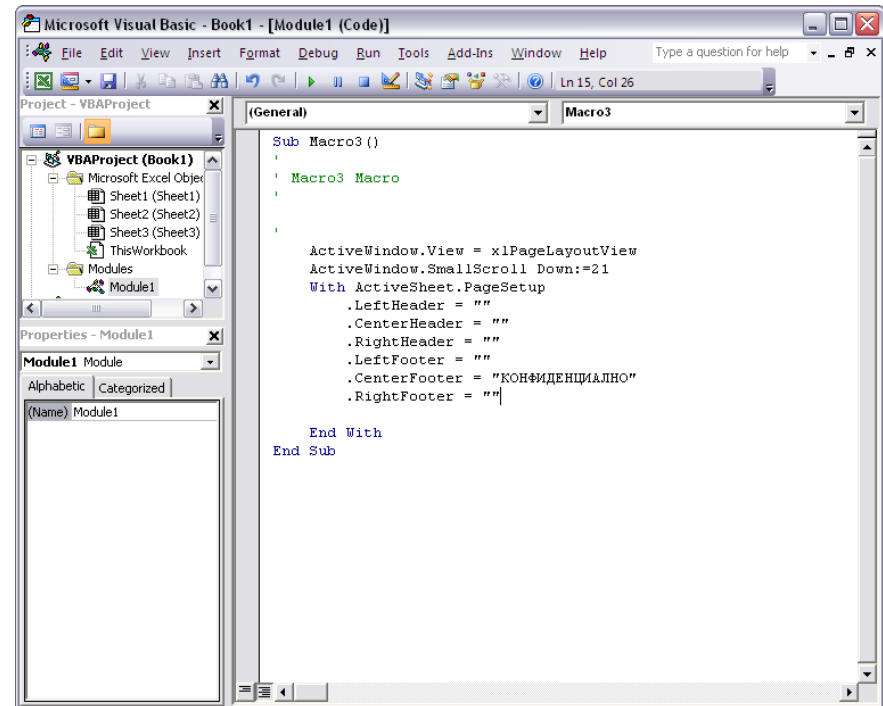
Уязвимост: Липса на механизми за контрол на входа

Заплаха: Неразрешен достъп

Приложение А

А.7.2 Класифициране на информацията

- Избира се класификационна схема, която да кореспондира с бизнес практиката на дадената организация
- 80% от информацията се отнася до оперативните аспекти на дейността и не трябва да е с високо ниво на класификация
- Означаването на документи в електронен вид може да се извършва автоматизирано чрез макроси в съответните офис приложения



The screenshot shows the Microsoft Visual Basic for Applications (VBA) editor window. The title bar reads "Microsoft Visual Basic - Book1 - [Module1 (Code)]". The menu bar includes File, Edit, View, Insert, Format, Debug, Run, Tools, Add-Ins, Window, and Help. The Project Explorer on the left shows a project named "VBAProject (Book1)" containing "Microsoft Excel Objects" (Sheet1, Sheet2, Sheet3, ThisWorkbook) and "Modules" (Module1). The Properties window below it shows "Module1 Module". The main code editor displays the following VBA code for a macro named "Macro3":

```
Sub Macro3 ()  
    Macro3 Macro  
  
    ActiveWindow.View = xlPageLayoutView  
    ActiveWindow.SmallScroll Down:=21  
    With ActiveSheet.PageSetup  
        .LeftHeader = ""  
        .CenterHeader = ""  
        .RightHeader = ""  
        .LeftFooter = ""  
        .CenterFooter = "КОНФИДЕНЦИАЛНО"  
        .RightFooter = ""  
    End With  
End Sub
```

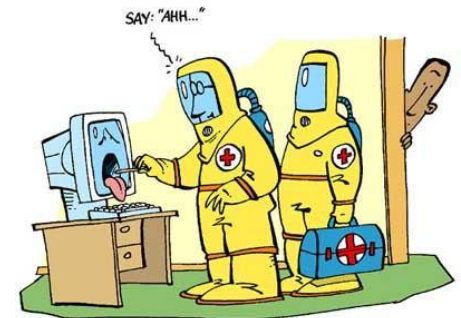
Приложение А

А.10.4 Защита от зловреден и мобилен код

Конкретното решение е въпрос на избор и финансови възможности, но това, което ви е необходимо е:



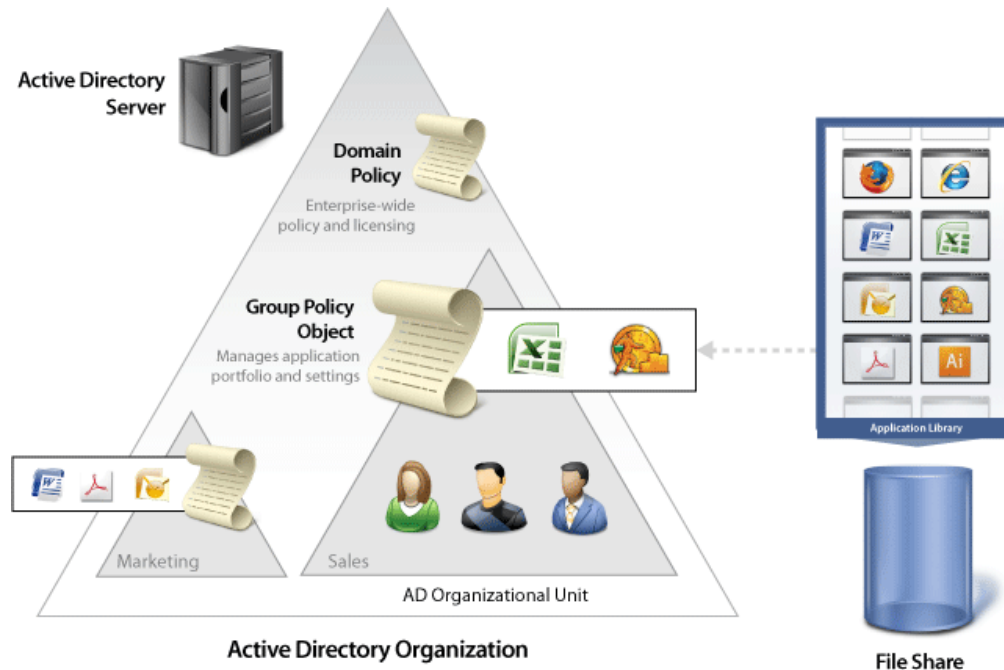
- Anti-virus
- Anti-Spyware
- Anti-Phishing
- Anti-Rootkit
- Anti SPAM
- Firewall



Приложение А

А.11 Контрол на достъпа

- А.11.2 Управление на достъпа на потребителите

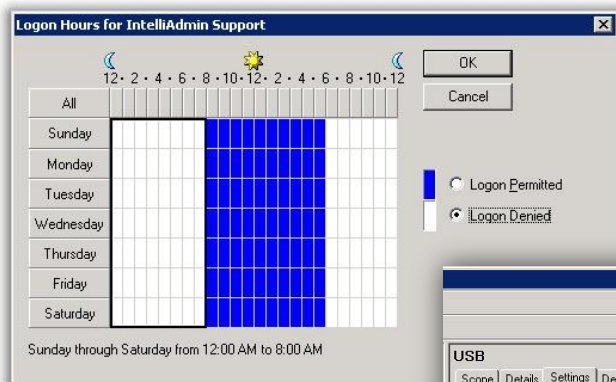


Достатъчно е наличие на **правилно** конфигурирана Active Directory

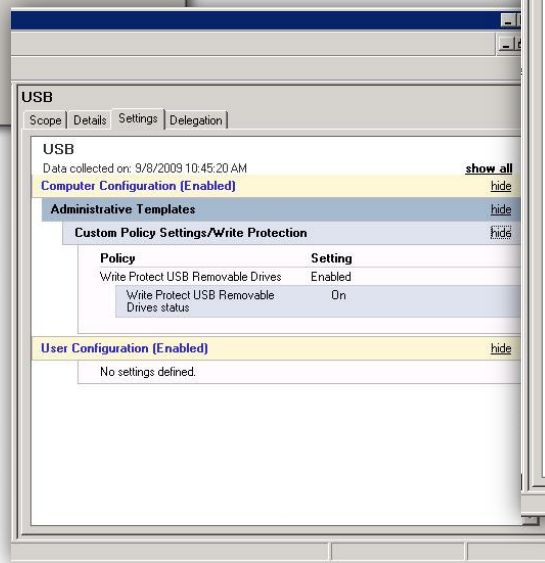
Приложение А

А.11 Контрол на достъпа

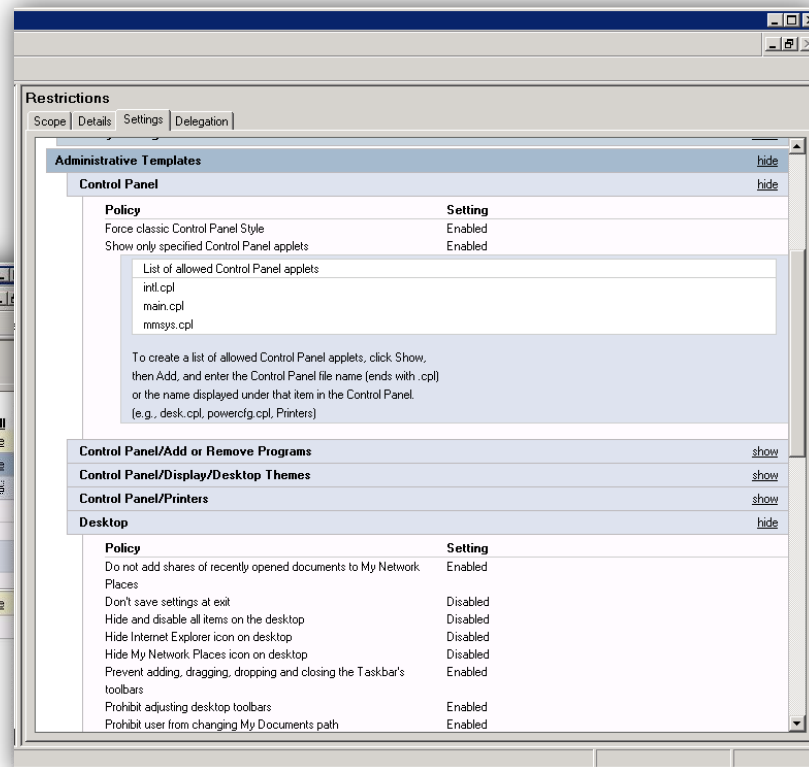
- А.11.2 Управление на достъпа на потребителите
Примери за ефективни рестрикции в Active Directory



- Logon hours restrictions



- USB Restrictions



- User Restrictions

Приложение А

А.11 Контрол на достъпа

- А.11.2 Управление на достъпа до мрежи

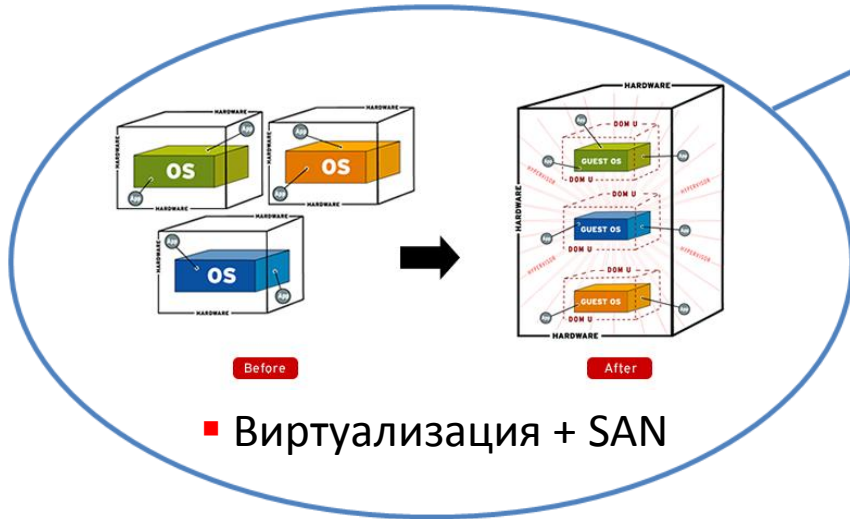


Необходимо ви е:

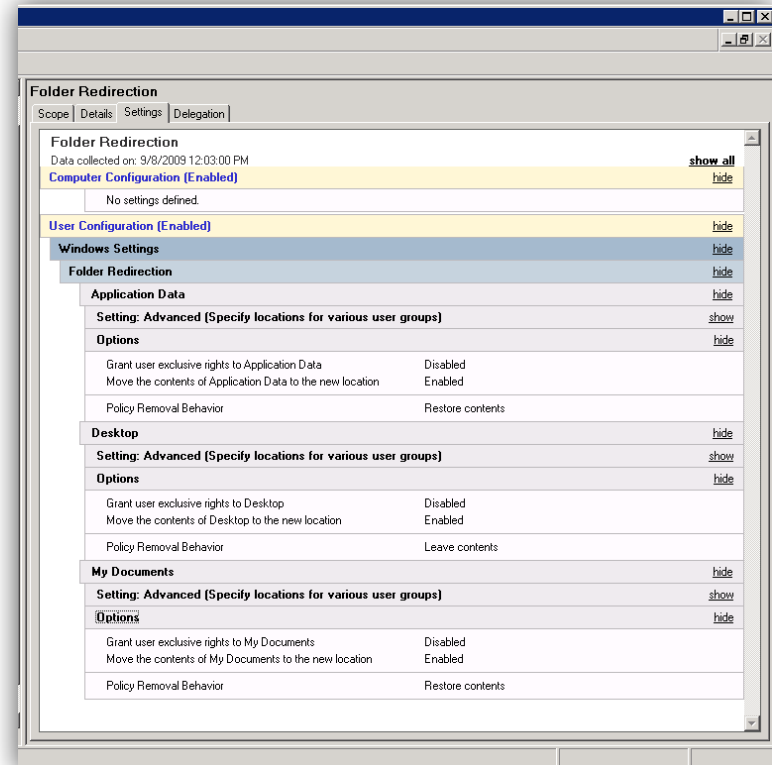
- Firewall & VPN
 - Разделяне и сегментация
 - Intrusion prevention
 - Web & Email filtering
 - Malware protection
-
- За достъп до критична информация – криптиране на трафика
 - При наличие на уеб приложения за външен достъп - защита от специализирани атаки като кражба на сесии, кражба на удостоверения за самоличност, износ на данни директно от базата и др.

Приложение А

А.10.4 Резервиране



Само ако можете да си го позволите



- Folder redirection policy



- Архивиране върху лента

Какво трябва да запомним?

Изискванията на ISO 27001:2005 **могат да бъдат** изпълнени чрез използване на добре познати и използвани принципи, механизми и средства за защита





Въпроси и отговори...



Благодаря за Вниманието!

boris.goncharov@bg.g4s.com

Securing Your World

