Системна сигурност

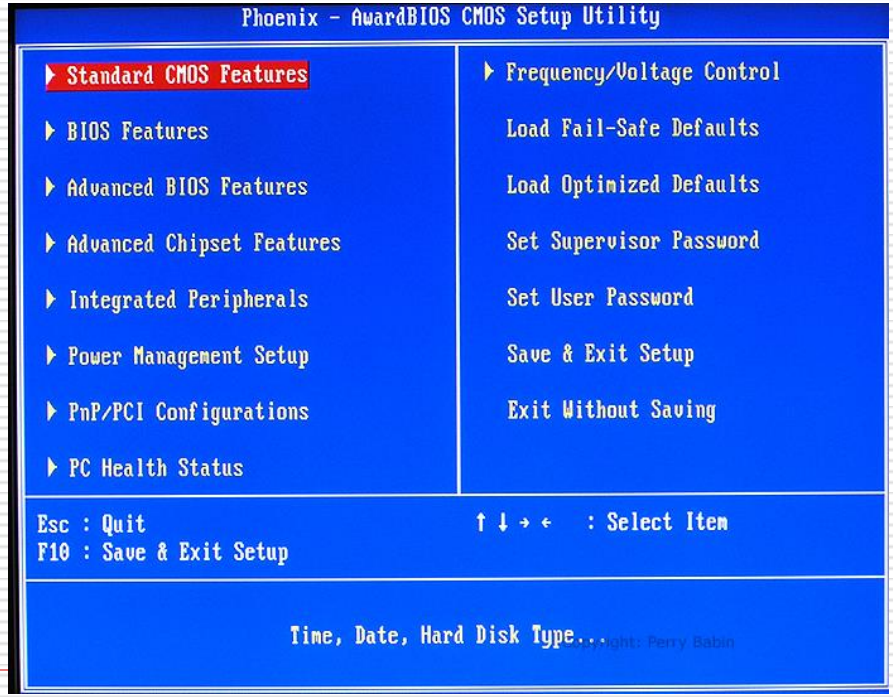
План

- Сигурност на системния хардуер - сървъри
- Сигурност и поддръжка на операционната система, на приложенията
- System Hardening

Сигурност на системния хардуер

BIOS

- Basic Input Output System
- Стартира се при пускане на машината
- Инструктира CPU как да комуникира с хардуера
- Дава възможност за конфигуриране на хардуерно ниво
- Защита с пароли
- Ако не защитите:



http://goo.gl/SkKsgk

http://www.piotrbania.com/all/kon-boot

Сигурност на системния хардуер

- USB устройства
  - Universal Serial Bus
- Какво може да се свърже
  - мишка
  - клавиатура
  - принтер
  - фотоапарати
  - Флаш устройства
  - Външен твърд диск

Сигурност на системния хардуер

- USB устройства

- USB портовете би трябвало да се изключат
  - Когато е възможно
  - Когато може да се достъпят чувствителни данни
  - Използването на USB устройства трябва да е описано в Политиката за приемлива употреба на компютърното оборудване

Поддръжка на операционната система

- Категории уязвимости на ОС:
  - Default инсталация
  - Service exploits (възползване)
  - Default protocols
  - Default accounts
  - Built-in applications
  - Remote administration
  - File access methods
  - Physical access
  - Buffer overflows

Поддръжка на операционната система

- Security Templates
  - Това е документ или конфигурационен файл, който съдържа настройки за сигурноста и може да бъде прилаган върху един или повече компютри
- Могат да се използват за контрол на:
  - Потребителски права
  - Политики за пароли
  - Позволения
  - Компютърна конфигурация
  - Софтуерна конфигурация
  - Ръчно (или чрез Group policy)

Базова конфигурация/configuration baseline/

- Това са минималните настройки по сигурността и конфигурацията, на които трябва да отговаря всяко мрежово устройство, за да бъде съвместимо с Политиката за IT сигурност

Базова конфигурация за ОС

- Базова конфигурация за ОС
  - Функционални изисквания
  - Бизнес нужди
- Управление на Базовата конфигурация
  - Трябва да се наблюдава
    - Напр. Qualys, Nessus, GFI LAN Guard, Retina, MS Baseline Security Analyzer
- Промените в Базовата конфигурация
  - Да се документират
  - Да се преглеждат
  - Да се одобряват

Таблица за проверка на сигурността на сървърите в Магна АД

#	Базова контрола	Да/ Не
1	Проверка всички дискови дялове да са форматирани с NTFS	
2	Проверка на акаунта Administrator – трябва да е със сложна парола	
3	Спиране или изтриване на неизползваните акаунти	
4	Спиране на ненужните услуги (services)	
5	Спиране на акаунта Guest	
6	Зададена политика за сложни пароли	
7	Зададена политика за заключване на акаунти	
8	Спиране на излишните шеъри	
9	Задаване на подходящите позволения на всички шеъри	
10	Инсталиране на последния ServicePack	
11	Инсталиране на security hotfix-овете след SP	
12	Включване на security auditing	
13	Инсталиран антивирусен софтуер и ъпдейти	
14	Сканиране на системата с MS Baseline Security Analyzer	

Административни права

- http://goo.gl/IL2nax

Поддръжка на ОС

- Hotfix
- Patch
- Service Pack

Hotfix

- Софтуерен пакет, чието предназначение е да разреши даден конкретен проблем, който е ограничен по обхват и се отнася специфична конфигурация на устройства. Може да е application hotfix (при някакъв софтуерен бъг) или OS hotfix и се прилага само в конкретен случай, при конкретен проблемсе използва само когато съответния проблем се появи на дадена машина, той не се прилага задължително.

Patch

- Софтуерен пакет, чието предназначение е да разреши един или повече проблеми, които възникват масово върху големи групи машини (напр. всички компютри с Windows XP SP2). Препоръчително е пачовете да се инсталират веднага след тяхното появяване, особено тези които са със статус „сигурност” и „критичен”

Service pack

- Софтуерен пакет, чието предназначение е:
  - да разпространи множество пачове наведнъж;
  - да подобри производителността на опер.система;
  - да внедри нова функционалност в опер.система.

Преди инсталация...

- Важен етап преди инсталация на пачове
  - Създаване на резервно копие на системни настройки на опер.система (например, създаване на Restore point)
  - Създаване на резервно копие на конфигурационни файлове на приложения;
  - Изготвяне на rollback процедура – какво се прави при неуспешен ъпдейт?
  - Тестване на пачове в тестова среда, различна от реалната

Patch management

- Разработване на писмена Patch Management стратегия
  - Оценка/тестване на всеки пакет
  - Определяне обхват на инсталиране /на кои машини/
- Използване на програмни средства за инсталиране на пачовете
- Тестване преди инсталиране
  - Четене на инструкциите
  - Backup на текущата конфигурация
  - Проверка на резултатите /логове.../
  - Проверка на процедури за деинсталиране

- Стратегия за deployment
  - Първо да се тестват на не-производствените машини
  - След това да се прилагат на потенциалните изложени на атаки машини
  - След това на не-критичните производствени машини
  - Последно на критичните за бизнеса машини

SMS

- **(Microsoft Systems Management Server) >>> SCCM (System Center Configuration Manager)** – многофункционална програма за инвентаризация на ИТ активи, разпространение на софтуер, разпространение на ъпдейти, инсталиране на Windows операционни системи, изготвяне на огромно количество отчети

•

SMS

- Проверка на конфигурацията на текущо инсталирания в компютъра софтуер и изготвяне на препоръки за корекция в случай на наличие на неправилни настройки.

- Инсталация на валидните за съответната система актуализации след одобрението им от потребителя или системния администратор.

0-day атаки

WSUS

- Автоматизирано изтегляне и инсталиране на пачове, отчети

Windows Server Update Services WSUS

- Предназначение и инсталиране на WSUS
- Конфигуриране на WSUS Server Options
- Конфигуриране на Computer groups
- Server-side targeting
- Client-side targeting
- Конфигуриране на клиенти с Group Policy
- Одобряване на ъпдейти

Софтуерни изисквания за WSUS

- Инсталиран Microsoft Internet Information Services (IIS) 7.0 (IIS Role) и следните му компоненти (features):

- Windows Authentication
- ASP.NET
- 6.0 Management Compatibility
- IIS Metabase Compatibility

Инсталиране на WSUS

- Инсталира се ролята WSUS

Конфигуриране на WSUS

System hardening

- *Hardening е общ термин за всяка security техника, при която default конфигурацията на системата се променя в опит да се затворят уязвимости или да се повиши защитеността й срещу атаки. Изпълнява се, за да се отговори на изискванията в Политиката за сигурност. Трябва да се балансира между hardening и изискванията за достъпност на услугите и ползваемост.*

System hardening

- Т.к. hardening се дефинира от конкретни security нужди в конкретна ситуация, то процедурите могат да са най-различни – от инсталиране на антивирусен софтуер и софтуерни ъпдейти на ОС до биометрична ауторизация за сървърното помещение.

System hardening

- Най-малките привилегии
- Спиране на не-необходимите компоненти:
  - Services
  - Protocols
  - Processes

Антивирусни програми

Кражба на данни

- Криптиране
- Пароли

Човешкият фактор

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