Zabezpieczanie systemu Windows

Michał Melewski
carstein@man.poznan.pl

Poznańskie Centrum Superkomputerowo Sieciowe

Zespół Bezpieczeństwa

Plan wystąpienia

- Jak definiujemy bezpieczny system?
- Czy potrzebujemy bezpiecznego systemu?
- Co składa się na bezpieczny system?
- Zabezpieczanie stacji klienckiej.
- Zabezpieczanie serwerów.
  - Domena
  - Active Directory
  - Konta
  - Metody uwierzytelniania
  - Kontrola dostępu
  - *Group Policy Objects*
  - NTFS

Bezpieczny system komputerowy

- **Poufność** – tylko my znamy informację
- **Dostępność** – ciągle mamy dostęp do informacji
- **Integralność** – informacja nie zmieni się bez naszej wiedzy

Pozostałe cechy bezpieczeństwa

- **Kontrola dostępu** – możliwość kontrolowania dostępu poprzez identyfikacje i uwierzytelnienia
- **Uwierzytelnianie** – zapewnie autentyczności informacji i osób
- **Nienaruszalność** – zapewnia integralność komunikacji
- **Niezaprzeczalność** – niemożność zaprzeczania faktowi wysłania/odebrania informacji
- **Dyspozycyjność** – ograniczanie skutków ataków

Typowe zagrożenia

- Wirusy, robaki, spyware, adware
- Zmiana konfiguracji DNS
- Instalowanie rootkitów
- Atak na sieć wewnętrzną
- Kradzież danych
- Zniszczenie danych

Zintegrowane zagrożenia

- Wirus nimda
  - Infekowanie serwerów IIS
  - Propagacja przez HTTP i SMTP
  - Poszukiwanie udostępnionych zasobów lokalnych i atakowanie znajdujących się w nich plików wykonywalnych
  - Udostępnianie zasobów zainfekowanego komputera

Ochrona przed zagrożeniami

- Program antywirusowy
  - Blokuje wirusy i robaki
  - Skanuje ruch HTTP, SMTP, FTP itp.
- Firewall
  - Inspekcja niestandardowych pakietów
  - Inspekcja ruchu wchodzącego i wychodzącego
- IDS
  - Wykrywanie prób ataków
  - Blokowanie ataków
  - Analiza anomalii
- System aktualizacji oprogramowania

Spyware

- Wikipedia:
  - Programy gromadzące informacje o użytkowniku i wysyłające je często bez jego wiedzy i zgody autorowi programu.
- Najczęściej rejestrowane informacje:
  - Dane osobowe
  - Numery kart płatniczych
  - Hasła
  - Dane o komputerze (system operacyjny, przeglądarka internetowa)
  - Zainteresowania użytkownika (na podstawie wpisywanych słów w wyszukiwarkach internetowych)
  - Adresy email

Objawy spyware

- Zmiana strony domowej w przeglądarce
- Pojawiające się banery reklamowe
- Samoczynne uruchamianie się przeglądarki internetowej
- Spowolnienie pracy systemu

Ręczne zwalczanie

- Pliki: autoexec.bat, config.sys, win.ini
- Rejestr:
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
  - HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
  - HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
  - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
  - HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
  - HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
  - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows

Ręczne zwalczanie (2)

- Rejestr:
  - HKCU\Software\Microsoft\Internet Explorer\SearchUrl
  - HKLM\Software\Microsoft\Internet Explorer\Main
    - REG_SZ Search Bar
- Pliki:
  - %windir%\system32\drivers\etc\hosts
  - %windir%\system32\drivers\etc\lmhosts

Programy zwalczające

- Ad-Aware (www.lavasoftusa.com)
  - Licencja:
    - » Darmowa – Standard Edition
    - » Komercyjna $27
- Spybot Search & Destroy (spybot.eon.net.au)
  - Licencja:
    - » Darmowa
- AntiSpyware (www.microsoft.com)
  - Program istnieje w Beta wersji.

Aktualizacja oprogramowania

- Jak?
  - Usługa Automatyczna Aktualizacja
  - http://windowsupdate.microsoft.com/
  - http://office.microsoft.com/officeupdate/
  - http://www.microsoft.com/poland/security/protect/
- Jak często?
  - Najrzadziej co dwa tygodnie
- Informacje o nowych poprawkach:
  - http://www.microsoft.com/security/bulletins/

Bezpieczeństwo w praktyce: sufrowanie

- Utworzenie użytkownika w profilu którego będziemy uruchamiać przeglądarkę.
- Uruchamianie aplikacji poprzez mechanizm wtórnego logowania:
- runas /user:xxx program.exe

- Profil powinien mieć obcięte uprawnienia do zapisu na dysk oraz do zapisu do rejestru

Narzędzia

- Sysinternals (www.microsoft.com/technet/sysinternals/default.mspx)
  - Filemon
  - Regmon
  - Procmon
  - Procexp
  - TCPView
- Wbudowane
  - Regedit
  - Konsola MMC

Zabezpieczenia rejestru

- **Regmon** – sprawdzenie, które klucze rejestru są potrzebne do działania programu.
- **regedit32.exe** – Odebranie praw do gałęzi HKEY_USERS i HKEY_LOCAL_MACHINE oraz nadanie odpowiednich uprawnień do kluczy wyznaczonych przez aplikację regmon.

Zabezpieczenie filesystemu

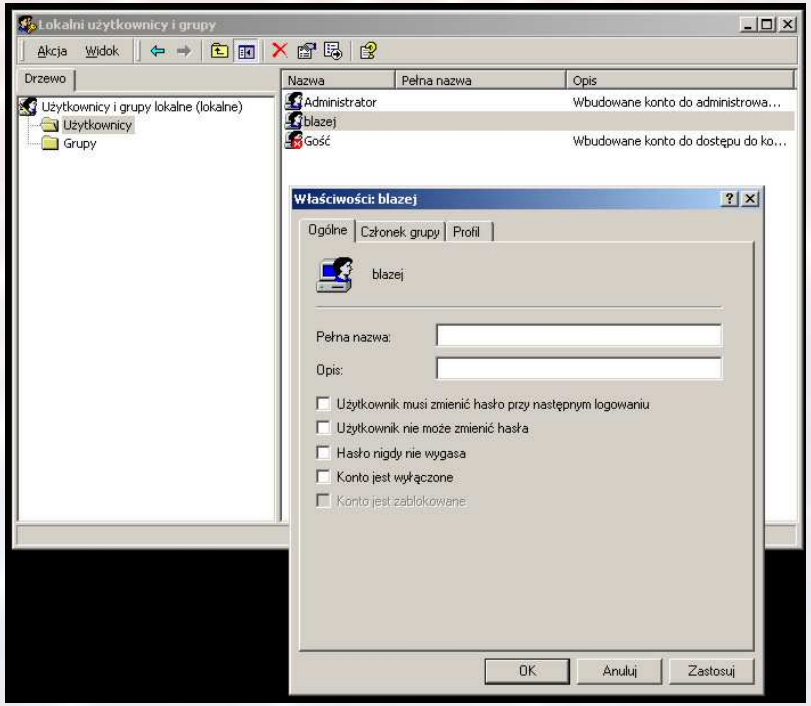
- **Filemon** – sprawdzenie, które katalogi i pliki są potrzebne do prawidłowego działania aplikacji.
- Odebranie uprawnień dla wszystkich dysków. Ustawienie odpowiednich uprawnień do katalogów i plików wskazanych przez aplikację filemon.

System bezpieczeństwa Windows 2000

- Konta użytkowników, komputerów, grupy
- Domeny
- Active Directory
- Kerberos
- Infrastruktura klucza publicznego
- Group Policy Object
- IPSEC
- NTFS

Konta użytkowników

- Typy kont
  - Konta użytkowników
  - Konta grup
  - Konta komputerów



Predefiniowane grupy

- Administratorzy
- Goście
- Operatorzy kopii zapasowej
- Użytkownicy
- Użytkownicy zaawansowani

Uwierzytelnianie

- Uwierzytelnianie Kerberos V5
- Uwierzytelnianie NTML
- Uwierzytelnianie SSL/TSL
- Uwierzytelnianie Passport (single sign-on)
- Uwierzytelnianie typu digest
- Uwierzytelnianie podstawowe

Prawa dostępu

- Prawa dostępu kontrolują dostęp do chronionych obiektów.
- Prawa dostępu Rejestru
- Prawa dostępu NTFS

Charakterystyka NTFS

- Rozbudowany system praw dostępu do plików
- Obsługa długich nazw
- Wielkość partycji do 2TB
- Quota
- Szyfrowanie plików
- Kompresja plików
- Linki twarde i miękkie

Atrybuty plików

- Standardowe informacje – data utworzenia, ostatnia modyfikacja
- Nazwa pliku (do 255 znaków Unicode)
- Dane – plik może posiadać wiele atrybutów danych (Multiple Data Stream)
- Deskryptor Bezpieczeństwa – kto jest właścicielem pliku i kto ma do niego dostęp

Kontrola dostępu

- Z każdym obiektem związany jest SID
- Prawa dostępu definiuje się w deskryptorach bezpieczeństwa związanych z każdym obiektem.
- Prawa dostępu można ustalić do plików, folderów, drukarek, kluczy rejestrów, usług.

Deskryptor bezpieczeństwa

- SID użytkownika
- SID Grupy
- Lista DACL
- Lista SACL

Listy DACL

- SID Użytkownika
- SID Grupy
- Wpisy odmowy skojarzone z obiektem
- Wpisy dostępu skojarzone z obiektem

Listy SACL

- Wpisy identyfikujące użytkowników, których pomyślne próby uzyskania dostępu mają zostać poddane inspekcji
- Wpisy identyfikujące użytkowników, których niepomyślne próby uzyskania dostępu mają zostać poddane inspekcji

Uprawnienia do plików i folderów

- Foldery:
  - Read,Write, List folder contents, Read & Execute
  - Modify, Full Control
- Pliki:
  - Read, Write, Read & Execute, Modify, Full Control
- Uprawnienia specjalne:
  - Change permissions, Take ownership

Multiple data streams

- Wielokrotne (alternatywne) strumienie danych
- Użycie:
  - echo abc >plik.txt:napis1
  - echo bbb>plik.txt:cos_innego
  - notepad plik.txt:cos_innego
- Strumienie omijają quote!

Quota

- Umożliwia ustalenie progów ograniczeń rozmiaru przestrzeni dyskowej przydzielonej użytkownikowi.
- Grupa Administratorzy nie posiada ustanowionego ograniczenia przestrzeni dyskowej.

Współdzielenie folderów

- Umożliwia użytkownikom sieciowym dostęp do danych lokalnych.
- Oprócz ustawienia właściwości kontroli dostępu do folderu, możliwe jest ustawienie docelowych uprawnień dostępu do współdzielonych obiektów sieciowych.

Zasady grup (Group Policy)

- Jest to zbiór ustawień konfiguracyjnych umożliwiających automatyczne konfigurowanie systemu zależnie od jego położenia w domenie oraz użytkownika, który się w nim loguje.

Konfiguracja zasad komputera

- Instalacja/konfiguracja/uaktualnianie oprogramowania
- Skrypty uruchamiane podczas startu/zamykania systemu
- Opcje Bezpieczeństwa
  - Polityka kont
  - Audyt uprawnień, konfiguracja bezpieczeństwa
  - Konfiguracja Zdarzeń
  - Zarządzanie grupami i użytkownikami
  - Zarządzanie serwisami systemowymi
  - Konfiguracja praw dostępu do rejestru i NTFS

Konfiguracja zasad użytkownika

- Instalacja/ reinstalacja/ uaktualnienie oprogramowania
- Opcje Internet Explorer
- Skrypty wykonywane w czasie logowania/wylogowania
- Opcje Bezpieczeństwa
- Przekierowanie katalogów (Moje Dokumenty, Menu Start)

Zarządzanie zasadami

- Przystawka zasad grup konsoli mmc
- %windir%\system32\GroupPolicy\Machine
- %windir%\system32\GroupPolicy\User

Filtr sieciowy

- Prosty filtr sieciowy umożliwiający blokowanie ruchu przychodzącego do komputera.
- Możliwość określenia portu TCP, UDP oraz protokołu IP.
- Ustawienie dotyczy wszystkich interfejsów.

IPSec

- Zapewnia:
  - Uwierzytelnianie połączenia
  - Poufność
  - Integralność
- Można skonfigurować jako:
  - Klient
  - Bezpieczny serwer
  - Serwer z zabezpieczeniami

Inspekcja systemu

- 6 dzienników inspekcji:
  - Aplikacja
  - Dziennik systemowy
  - Zabezpieczenia
  - Usługi katalogowe
  - Replikacja plików
  - DNS Server

Konfiguracja

- Inspekcja zdarzeń dotyczących logowania
- Inspekcja zarządzania kontami
- Inspekcja dostępu do usług katalogowych
- Inspekcja zdarzeń związanych z procesem logowania
- Inspekcja dostępu do obiektu
- Inspekcja zmiany zasad
- Inspekcja użycia uprawnień
- Inspekcja śledzenia procesów
- Inspekcja zdarzeń systemowych

Dziennik zdarzeń

- Dziennik jest pojedynczym zbiorem ważnych zdarzeń programowych i sprzętowych.
- Dziennik można przeglądać za pomocą przystawki Podgląd zdarzeń.

Dziękuje za uwagę

Pytania?