



Sicherheits-Schulung
Windows Datensicherheit

Sicherheits-Schulung

Gesamtüberblick I

- Allgemeines
- Installation
- Services
- Registry
- Kontorichtlinien
- Auditing
- Netzwerkeinstellungen

Sicherheits-Schulung

Gesamtüberblick II

- IIS installieren
- IIS Dateizuordnungen
- IIS Einstellungen
- IIS NTFS Einstellungen

- NTLMv2 Authentisierung
- Tools

Sicherheits-Schulung

Windows Sicherheit

- Ist Windows sicher?



Windows Sicherheit
Axel Neimke
WiSE 2005
Folie 4

- Die meisten Services/Programme laufen als "local system". Der mächtigste Account auf einem Rechner.
- Über 3900 Systemaufrufe
- Proprietäre Verschlüsselung
- Unveröffentlichte Algorithmen
- Undokumentierte Systemaufrufe

Datensicherheit Windows

Installation und Patches

- Installation OHNE Netzwerkzugang
- Neueste Patch-CD bereit halten
- CD mit Zusatz-Software bereithalten
- Netzwerk erst am Ende nach der Sicherung einstecken

Datensicherheit Windows

ALLGEMEINE SICHERHEITSRICHTLINIEN

- Gib den Leute was sie brauchen, nicht was Du hast !
- Benutzergruppen und Berechtigungen planen
- Vertrauensstellung (zwischen Domänen) begrenzen
- RAS sichern (Einwählrechte nur für Benutzer, die es unbedingt brauchen)
- Zugriff auf Netzwerkmonitor begrenzen
- Authentifizierung von Drittanbietern benutzen
- System aktualisieren

RAS nur mit GlobalRemote

Datensicherheit Windows

MASCHINEN EINSTELLUNGEN

- Physikalische Absicherung der Server.
- System schützen vor unerwünschtem Booten
- Verschlüsselung einstellen für Back-up Bänder

-Server in abschließbaren Schrank installieren

-Zutrittsicherung für Serverraum

-BIOS Passwort setzen und an "sicherem" Ort hinterlegen

-BIOS Verbot von Booten von Diskette und CD

Datensicherheit Windows

Eine sichere Windows Installation

- Neue Installation
- Isolierte Installation
- Server oder Workstation?
- Software von original CD installieren
- NTFS
- KEIN ADMINISTRATOR PAßWORT während der Installation!
- PDC, BDC oder Standalone ?
- Kein Multimedia, keine Kommunikation und keine Erreichbarkeit

Windows Sicherheit
Axel Neimke
WiSE 2005
Folie 8

- Setzen Sie immer neu auf. Keine alten Systeme wiederverwenden
- Verbinden Sie den Server erst dann mit dem Netzwerk, nachdem er gesichert wurde
- NT Server in englisch, weil patche schneller verfügbar sind
- Niemals FAT, sondern immer NTFS installieren. FAT ist nicht sicher.
- Nicht convert zum Konvertieren von FAT nach NTFS benutzen, da nicht alle ACLs richtig gesetzt werden
- Trennen von "system" und "Nutzer/Applikations"-Platten
- Wenn möglich ein "standalone" System installieren
- Keine zusätzlichen Betriebssysteme installieren
- Unnötige Software nicht installieren
 - Nur wordpad drauflassen, vielleicht nicht einmal das
- Unnötige Software deinstallieren
- Als Netzwerkprotokoll ausschließlich TCP/IP installieren

Datensicherheit Windows

Services ausschalten

- Folgende Dienste sind, wenn möglich, auszuschalten:
 - Remote Access Service RAS
 - DHCP Relay Agent
 - Einfache TCP/IP Dienste
 - Gateway Service für Netware
 - MS DHCP Server
 - MS DNS Server
 - RIP IP
 - RIP IPX
 - RPC für Banyan und Vines
 - Services für Macintosh
 - WINS nur auf Domaincontrollern installieren
 - SNMP nur installieren, wenn es auch benutzt wird

-Bei SNMP die "communities (read/write) in zufällige Werte umbenennen.
NICHT public oder private verwenden.

-<http://www.securityfocus.com/infocus/1301>

Datensicherheit Windows

Registry Sicherheit I

- Zuletzt angemeldete Benutzer nicht anzeigen
- Anmelde Warnung
- Laufwerke und Laufwerksbuchstaben
- Schwierige Passwörter erzwingen

Windows Sicherheit
Axel Neimke
WiSE 2005
Folie 10

- Dies ist wichtig, da das Administratorkonto umbenannt wurde! .

Schlüssel	HKEY_LOCAL_MACHINE\SOFTWARE\WINDOWS
NT\CURRENTVERSION\Winlogon\DontDisplayLastUsername	
Typ	REG_SZ
Wert	1

- Schlüssel
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

	LegalNoticeCaption
Typ	REG_SZ
Wert	VORSICHT
Schlüssel	HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

	LegalNoticeText
Typ	REG_SZ
Wert	Dies ist ein überwachte System. Nicht autorisierter Zugriff ist nicht erlaubt.

- Schlüssel
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\NotificationPacka
ges

Typ	REG_MULTI_SZ
Wert	* PASSFILT einfügen *

Weiter ist über den Benutzermanager folgendes einzustellen:

- Maximales Kennwortalter = 45 - 90 Tagen
- Minimale Kennwortalter = 1-5 Tagen
- Minimale Kennwortlänge = 8 Zeichen
- Kennwortzyklus = 8 - 13 Kennwörter
- Benutzer muss sich anmelden, um Kennwort zu ändern = yes

Datensicherheit Windows

Registry Sicherheit II

- Druckertreiber absichern
- Überwachung der Backup und Wiederherstellen
- Beschränken der Informationen, für anonym angemeldete Benutzer
- Kontrollieren des entfernte Zugriffs auf der Registry

Windows Sicherheit
Axel Neimke
WiSE 2005
Folie 11

- Wenn man Druckeradministratoren nicht traut, sollte die Installation neuer Treiber verhindert werden, da die Treiber im Kernel laufen und alles dürfen. ACLs ändern!

Schlüssel

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanManPrintServices\Servers

AddPrintDrivers

Typ

REG_DWORD

Wert

1

- Anonymen Netzzugriff verbieten!

Schlüssel

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

RestrictAnonymous

Typ

REG_DWORD

Wert

1; ab windows 2000 auf 2 setzen

- Setzen Sie die ACLs für

Schlüssel

KEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\

winreg

So, dass nur Administratoren und System Vollzugriff besitzen.

Datensicherheit NT

Registry Sicherheit III

- Einschränken der anonyme entfernte Zugriffe auf der Registry und andere named pipes
- Kontrollieren des Zugriffs auf den command scheduler

Windows Sicherheit
Axel Naimark
WISE 2005
Folie 12

- Anonymen Zugriff über das Netz einschränken

Schlüssel KEY_LOCAL_MACHINE\System\CurrentControlSet\Services\

LanManServer\Parameters\RestrictNullSessAccess

Typ REG_DWORD

Wert * Namen von der Liste entfernen um Null

- Session Zugriff darauf zu verhindern *

Schlüssel HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\

LanManServer\Parameters\NullSessionPipes

Typ REG_MULTI_SZ

Wert * Namen von der Liste entfernen um Null

- Session Zugriff darauf zu verhindern *

<http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/Default.asp?url=/resources/documentation/Windows/2000/server/reskit/en-us/regentry/58643.asp>

- Nur Administratoren sollen auf den Command scheduler zugreifen können, da Programme, die von dort gestartet werden zu große Macht besitzen.

Schlüssel

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\

SubmitControl

Typ REG_DWORD

Wert * Ein Wert von 0 bedeutet, dass nur

- Administrators und Hauptbenutzer dürfen

Jobs in der Scheduler zufügen Ein Wert von 1

- bedeutet, dass Serveroperatoren

können auch Jobs in der Scheduler zufügen. *

- Weiter können die Rechte auf den scheduler durch ACLs auf folgenden Schlüssen gesteuert werden:

Schlüssel HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Schedule

- *Security Configuration Wizard für windows 2003 SP1*

- <http://go.microsoft.com/fwlink/?linkid=43450>

Datensicherheit Windows

Registry Sicherheit V

- **Automatische Generierung der Shares C\$, Admin\$, IPC\$ verhindern (Autoshare)**

- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters`
AutoShareServer für Server und
AutoShareWks für Workstations
DWORD auf 0 setzen

Datensicherheit Windows

Registry Sicherheit IV

Berechtigungen für den Zugriff auf die Registry einstellen

Blockieren des 8.3 Angriffs

Windows Sicherheit
Axel Neimke
WISE 2005
Folie 14

- Den Nutzer "Everyone" durch die wirklichen Nutzer des Rechners ersetzen
Der Nutzer "system" ist ein solcher Nutzer, den man nicht vergessen darf.
Wenn es viele Nutzer gibt, dann Everyone durch "Authenticated Users" ersetzen.
- Die Gruppe "Administrators" durch die wirklichen Administratoren ersetzen, oder durch eine Gruppe der Administratoren, die per Hand gepflegt wird.

Schlüssel	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\Win31FileSystem
	* Für FAT Datesystem*
	NtfsDisable8dot3NameCreation
	* Für NTFS Datesystem*
Typ	REG_DWORD
Wert	1
	Performancegewinn, da unnütze Namen nicht mehr generiert werden

- *Security Configuration Manager*(SCM) Utility
<http://www.microsoft.com/ntserver/nts/downloads/recommended/scm/default.asp>
- Security Configuration Wizard
<http://www.microsoft.com/windowsserver2003/technologies/security/configwiz/default.msx>

Datensicherheit Windows

Kontorichtlinien

- Konto sperren nach einer Reihe von ungültige Kennworteingaben.
- Administrator Kontosperrern aktivieren
- Separate Konten für Administratoren errichten
- Einen Administrator-Passwortkontrolleprozess einrichten
- Das Benutzen der Gruppe Jeder verschärfen, und deaktivieren des Gast Kontos
- Das Geben von Administratorprivilegien für die meisten Aufgaben vermeiden
- Sichern und Verwalten der Ereignisprotokolle
- Die gemeinsame Nutzung von Konten vermeiden
- ACL Protokollierung
- Die SAM Datei verschlüsseln

Windows Sicherheit
Axel Neimke
WiSE 2005
Folie 15

- Benutzermanager / Richtlinien / Konto
- PASSPROP.EXE Utility von NT Resource Kit
 - Passprop /adminlockout
 - Server bleibt über Konsole administrierbar, auch wenn Admin über Netz ausgesperrt ist.
- Administratorkonto umbenennen und auch Kommentar ändern. CSM schlägt admin-Computernamen vor.
- Dem Konto "Administrator" alle Rechte nehmen und verfolgen, wer versucht mit diesem Konto sich anzumelden
- Kein Mensch sollte das umbenannte Administratorkonto benutzen. Stattdessen Konten mit Administrator-Rechten einrichten.

- Jeder (Everybody) ist WIRKLICH jeder; Deshalb Rechte von Jeder durch AuthorizedUsers ersetzen. Aber vorsichtig.
- Ausführen der Applikation syskey.exe bewirkt das Verschlüsseln der SAM Datei und ihrer Kopien

Datensicherheit Windows

Auditing einschalten

- Überwachung einschalten
- Überwachungsprotokolle kontrollieren

Datensicherheit Windows

Security Configuration Wizard for Windows2003



Datensicherheit Windows

NETWORKING AND INTERNET SECURITY SETTINGS

- **Nicht benötigte Dienste deaktivieren und benötigte Dienste sicher ausführen**
- **Bekanntes IIS Sicherheitslücken blockieren, wenn IIS benutzt werden soll**
- **Ungeschützte Ports absichern durch Firewall (oder Screening Router)**

Windows Sicherheit
Axel Neimke
WiSE 2005
Folie 18

```
; Enable TCP/IP Filtering oder heutzutage besser mit ipsec filtern  
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]  
"EnableSecurityFilters"=dword:00000001
```

```
; Disable ICMP Redirect  
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]  
"EnableICMPRedirect"=dword:00000000
```

```
; 'Disable' IP source routing  
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]  
"DisableIPSourceRouting"=dword:00000001
```

```
; Disallow Fragmented IP  
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\IPFilterDriver\Parameters]  
"EnableFragmentChecking"=dword:00000001
```

```
; Disable forwarding of fragmented IP packets  
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\IPFilterDriver\Parameters]  
"DefaultForwardFragments"=dword:00000000
```

```
; Disable IP Forwarding  
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]  
"IPEnableRouter"=dword:00000000
```

```
; Fix for MS DNS Compatibility with BIND versions earlier than 4.9.4  
;[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters]  
;"BindSecondaries"=dword:00000001
```

Datensicherheit Windows

NETWORKING AND INTERNET

W2K IPSEC-Filter

- Können im Gegensatz zu TCP/IP-Filtern auch rausgehende Verbindungen filtern
- Einstellung über local security policy oder ipsecpol.exe
- IPSEC-Filter filtern nicht: multicast, broadcast, QoS RSVP, IKE 500/udp, Kerberos 88/tcp/udp (Q253169)

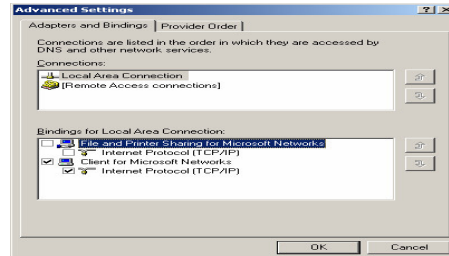
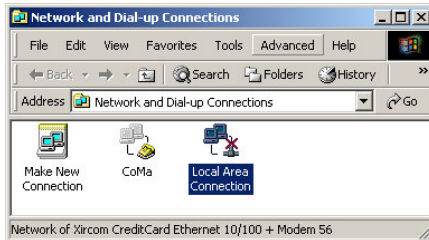
Entweder GUI oder ipsecpol verwenden
Unbenutzte Regeln disablen und löschen

```
Ipsecpol \\computername -w REG -p "Web" -o  
Ipsecpol \\computername -x -w REG -p "Web" -r "BlockAll" -n Block -f 0+*  
Ipsecpol \\computername -x -w REG -p "Web" -r "OkHTTP" -n PASS -f 0:80+*::TCP
```

Datensicherheit Windows

NETWORKING AND INTERNET

NetBIOS/SMB ausschalten



- RestrictAnonymous
 - Wird bei W2K auf 2 gesetzt, das bedeutet „No Access Without Explicit Anonymous Permission“

Datensicherheit Windows

Nach der Installation

- Kennwort für Bildschirmschoner
- Virusschutzsoftware installieren
- Windows Update Service konfigurieren

- <http://www.microsoft.com/windowsserversystem/updateservices/default.aspx>

Datensicherheit Windows

IIS installieren

- <http://www.microsoft.com/technet/security/checklists/default.aspx>
- Microsoft Papier „Securing Your Webserver“ beachten
- Windows 2003 - ‚sicher‘ installieren und patchen
- IIS installieren; Beispiele nicht installieren
- MBSA benutzen -> erneut patchen
- Alle Verzeichnisse löschen, die „sample“ im Namen tragen
 - inetpub\iissamples
 - inetpub\AdminScripts
 - Program Files\Common Files\System\msadc\Samples
- Das virtuelle Verzeichnis IISADMPWD löschen

- Checkliste benutzen:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod104.asp>

- Securing Your Webserver:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod89.asp>

Datensicherheit Windows

IIS Dateizuordnungen

- **Dateizuordnungen, die nicht benutzt werden, löschen**
 - **Internet Database Connector**
(new Web sites don't use this, they use ADO from Active Server Pages)
.idc
 - **Web-based Password Reset** .htr
 - **Server-side includes** .shtm, .stm, .shtml
- **Bei ASP-Seiten ausführliche Fehlermeldungen ausschalten.**
- **Bei allen Dateizuordnungen "check that file exists" anklicken.**

Datensicherheit Windows

IIS Allgemeines zur Sicherheit

- Als "Operators" die "Administrators" entfernen und durch WebAdmins ersetzen
- Directory listings verbieten
- Home Directory auf eigene Partition
- Logging einschalten, auf eigene Partition, NTFS Rechte einschränken
- Logfile-Überwachung regeln -> Eventcomb, Intrusion Detection System

- Microsoft sagt, dass man keine Windows-Administratorrechte braucht, um IIS zu administrieren.
- Verhindern, dass man mit ".." im Verzeichnisbaum rauf gehen kann
- Wenn es doch jemanden gelingt im Verzeichnisbaum rauf zu gehen, dann kann er nicht in die System-Verzeichnisse

Datensicherheit Windows

IIS Einstellungen

- **Verbot der Benutzung von „..“ (parent path)**
Die Verwendung von „..“ in Pfadangaben ist per default erlaubt. Dies muss geändert werden, indem in den Eigenschaften der webroot in „Home Directory | Configuration | App Options“ die checkbox „Enable Parent Paths“ ausgeschaltet wird.
- **Ausschalten des Headers „Content-Location“**
Dieses http-header feld verrät den Ort interner IP-Adressen. Dies sollte ausgeschaltet werden:
<http://support.microsoft.com/?scid=kb%3Ben-us%3B218180&x=7&y=10>

Datensicherheit Windows

IIS NTFS Einstellungen

- Die Rechte der IIS Verzeichnisse werden so gesetzt, dass der Nutzer Everyone nur die Rechte besitzt, die zum einwandfreien Betrieb des IIS notwendig sind. Script-Verzeichnisse dürfen niemals schreibbar sein. Verzeichnisse ohne ausführbaren Inhalt sind niemals „ausführbar“.
- Bei unterschiedlichen NTFS und IIS Rechten gewinnt das Recht, das weniger erlaubt
- MS empfiehlt jede Dateiart in eigene Verzeichnisse zu speichern und die Rechte entsprechend der Art zu setzen z.B. nur X für Scripte

Datensicherheit Windows

Microsoft Sicherungstools

- <http://www.microsoft.com/technet/security/tools/default.aspx>

- **IIS Lockdown Tool**
 - <http://www.microsoft.com/technet/security/tools/locktool.aspx>
 - **Jetzt mit URLSCAN Integration**
 - **Template basiert**
 - **Answerfile für unattended install**

- **URLSCAN**
 - <http://www.microsoft.com/technet/security/tools/urlscan.aspx>

Datensicherheit NT

NTLMv2 Authentisierung

- Wenn alle Clients W2k oder NT4.0SP4+ sind, dann kann der Server auf „use NTLMv2/refuse LM & NTLM “ Authentisierung gestellt werden.
- Für Windows9x steht NTLMv2 nach der Installation und Deinstallation (!) der Directory Services von W2K CD (Clients\Win9x\Dslclient.exe) zur Verfügung
- <http://support.microsoft.com/kb/q239869/>

Datensicherheit Windows

Windows Security Tools

- Microsoft Management Console mit Security Management Snap-In
- L0phtcrack2.5, LC5
- Netcat (nc11)
- sacls, cacls
- Pwdump3
- Isadump2
- Foundstone Tools (fport, ...)

- <http://www.bindview.com/Services/Razor/Utilities/>
- <http://www.foundstone.com/>

Datensicherheit Windows

Security Recources

- **Securing Microsoft Windows**
<http://www.microsoft.com/technet/security/>
- <http://www.sans.org/>
- www.foundstone.com
- Hacking Exposed Windows 2003; Joel Scambray, Stuart McClure
 - www.hackingexposed.com

Datensicherheit Windows

Ansprechpartner

Axel Nennker

T-Systems Enterprise Services GmbH

SSC ENPS / Technologiezentrum

Tel: 030 / 34 97 - 3256

Fax: 030 / 34 97 - 3257

email: axel.nennker@t-systems.com

Datensicherheit Windows

Fragen

Zusammenfassung

Fragen???