



Ralf Feest

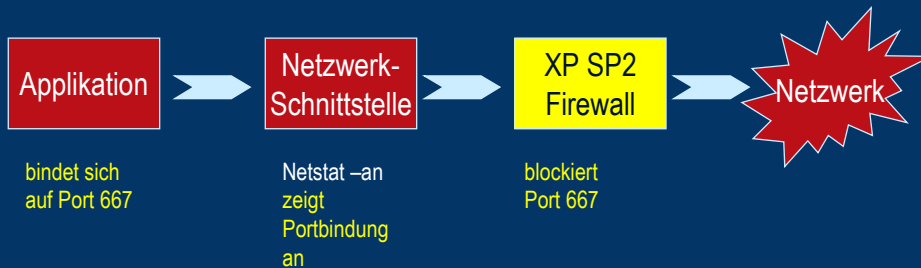
Director Enterprise Services bei AddOn

Ist die Windows XP SP2 Firewall sicher?

Die XPSP2 Firewall

- Statusbehaftete Hostfirewall
- überwacht Quell- und Zieladresse, UDP und TCP Ports
- blockiert keinen ausgehenden Datenverkehr (Ausnahme: einige ICMP Meldungen)
- standardmäßig aktiviert für LAN, DFÜ und VPN
- Über Gruppenrichtlinien konfigurierbar
`Computerkonfiguration\Administrative Vorlagen\Netzwerk\Netzwerkverbindungen\Windows-Firewall`
 - **Domänenprofil**
wenn mit Netzwerk der eigenen Active Directory Domäne verbunden
 - **Standardprofil**
alle anderen Netzwerkverbindungen; i. d. R. restriktiver
- Einführung und Hintergrundinfos: TechNet Artikel
<http://www.microsoft.com/germany/technet/datenbank/articles/600522.mspx>

Wo klinkt sich die Firewall ein?



3/20

AddOn 2006

Port-Analyse

- Sicherheitstools von Microsoft
<http://www.microsoft.com/germany/technet/sicherheit/tools/default.mspx>
- Prozesse auflisten, die Ports geöffnet haben
 - Netstat -an | more
 - PortQry.exe -local | more

```
Processing local system's ports...
TCP/UDP Port to Process Mappings
39 mappings found

PID      Port      Local IP      State          Remote IP:Port
4        TCP 445     0.0.0.0       LISTENING     0.0.0.0:36985
4        TCP 2798     192.168.0.25 ESTABLISHED   192.168.0.223:445
2828    TCP 2936     192.168.0.25 ESTABLISHED   192.168.0.225:1433
2904    TCP 2829     192.168.0.25 ESTABLISHED   207.46.114.30:1863

Process ID: 2904 (Msmmsgs.exe)
Process doesn't appear to be a service
PID      Port      Local IP      State          Remote IP:Port
2904    TCP 2829     192.168.0.25 ESTABLISHED   207.46.114.30:1863

C:\>nslookup 207.46.114.30
Name:    by2m6-cs10.msgr.hotmail.com
Address: 207.46.114.30
```

4/20

AddOn 2006

Firewall Kommandozeilenschnittstelle

- netsh firewall
 - Konfiguration auslesen und anzeigen: **netsh firewall show config**
 - Aktueller Firewallstatus: **netsh firewall show state**
 - Erlaubtes Programm hinzufügen: **netsh firewall add allowedprogram**
 - Port öffnen: **netsh firewall add portopening**

```

C:\>netsh firewall show config

Profilkonfiguration "Domäne":
-----
Betriebsmodus           = Aktiv
Ausnahmemodus           = Aktiv
Benachrichtigungsmodus = Aktiv

C:\>netsh firewall show state

Firewallstatus:
-----
Profil                   = Domäne
Betriebsmodus            = Inaktiv
Ausnahmemodus            = Aktiv
Multicast-/Broadcastantwortmodus = Aktiv
Benachrichtigungsmodus  = Aktiv
Gruppenrichtlinienversion = Windows-Firewall
Remoteverwaltungsmodus  = Inaktiv

Ports, die momentan auf allen Netzwerkschnittstellen offen sind:
-----
Port  Protokoll Version  Programm
-----
137   UDP    IPv4    (null)
139   TCP    IPv4    (null)
138   UDP    IPv4    (null)
445   TCP    IPv4    (null)
8081  TCP    IPv4    C:\Programme\McAfee\Common Framework\FrameworkService.exe
8081  UDP    IPv4    C:\Programme\McAfee\Common Framework\FrameworkService.exe
8082  UDP    IPv4    C:\Programme\McAfee\Common Framework\FrameworkService.exe
                    
```

Vorsicht! Dies ist die Konfiguration, nicht der aktuelle Status

Diese Programme dürfen von außen angesprochen werden

Einstellung kommt durch Gruppenrichtlinie. Ansonsten steht hier: "keine"

Offene P

5/20 Add On 2006

Wichtige Gruppenrichtlinien für Firewall

Richtlinieneinstellung	Beschreibung
Alle Netzwerkverbindungen schützen	Aktiviert die Windows-Firewall und verhindert, dass lokale Administratoren sie deaktivieren können
Keine Ausnahmen zulassen	Setzt sämtliche konfigurierten Ausnahmen außer Kraft
Programmausnahmen festlegen	Zwei Programmausnahmelisten werden verwendet: eine Liste durch die Gruppenrichtlinien, die andere durch den lokalen Administrator in der Systemsteuerung
Portausnahmen festlegen	Portausnahmen durch Gruppenrichtlinien definieren
Ausnahmen für lokale Programme zulassen	Lokale Administratoren dürfen eine lokale Programmausnahmeliste definieren
Remoteverwaltungsausnahme zulassen.	Öffnet TCP-Ports 135 und 445 für WMI, RPC und DCOM
Ausnahme für Datei- und Druckerfreigabe zulassen	Öffnet UDP-Ports 137 und 138 sowie TCP-Ports 139 und 445
Authentifizierter IPSec durchlassen	IPSec-geschützter Datenverkehr von bestimmten Benutzern/Gruppen umgeht die Windows-Firewall

- Gruppenrichtlinien-Einstellungen kommen nach **HKLM\Software\Policies\Microsoft\WindowsFirewall**
- Lokale Einstellungen werden abgelegt unter **HKLM\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy**

6/20

Add On 2006

Benachrichtigungen durch die Firewall

- Wann kommen diese Meldungen?



Wenn sich ein Programm auf einen Port einer IP Adresse des eigenen PCs im "Abhören"-Modus binden möchte, um eingehenden Netzwerkverkehr anzunehmen ▶ [Winsock.dll](#)

7/20

AddOn 2006

Demo 1 - SuperClock1a

- Benachrichtigungen durch die Firewall
 - Start eines Programms
 - durch Endbenutzer ohne besondere Rechte
 - durch Benutzer mit lokalen Administratoren-Rechte
- Netsh firewall
- Portqry -local

8/20

AddOn 2006

Warnung: Programme modifizieren Firewall

- Beachte: Auch Programme können die Firewall per Befehl öffnen, wenn Sie es als Administrator starten!
- Beispiel: Skype – fügt folgende Regeln ohne Nachfrage ein:

```
netsh firewall set allowedprogram program=C:\Programme\Skype\Phone\Skype.exe name=Skype profile=Domain Mode=ENABLE
```



Von Skype automatisch eingetragen

```
C:\>netsh firewall show allowedprogram

Zugelassene Programmkonfiguration für Profil "Domäne"
Modus      Name/Programm
-----
Aktiv      Skype / C:\Programme\Skype\Phone\Skype.exe

C:\>netsh firewall show state

Firewallstatus:
-----
Profil                        = Domäne
Betriebsmodus                 = Aktiv
Ausnahmemodus                 = Inaktiv
Benachrichtigungsmodus       = Aktiv

Ports, die momentan auf allen Netzwerkschnittstellen offen sind:
Port  Protokoll Version  Programm
-----
80    TCP      IPv4     C:\Programme\Skype\Phone\Skype.exe
443   TCP      IPv4     C:\Programme\Skype\Phone\Skype.exe
11990 UDP      IPv4     C:\Programme\Skype\Phone\Skype.exe
11990 TCP      IPv4     C:\Programme\Skype\Phone\Skype.exe
```

Abhilfe: Per Gruppenrichtlinie den Ausnahmemodus deaktivieren.

Keine Ausnahmen zulassen

9/20

AddOn 2006

Demo 2 – SuperClock1B

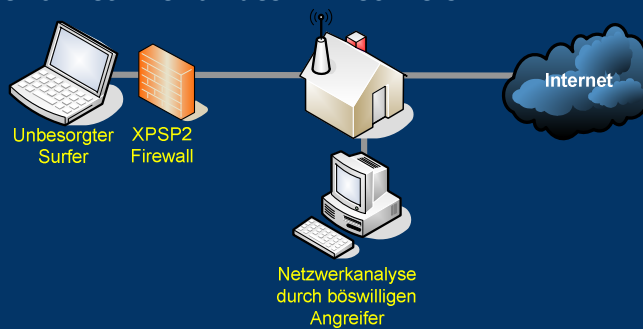
- Automatische Konfiguration der Firewall durch Trojaner verhindern
- Netsh firewall show state

10/20

AddOn 2006

Warnung vor Public WiFi Access Points

- Gefahr: Public oder „Scheinbar ungewollte Public“ WLANs
- Access Point Betreiber analysiert Netzwerkverkehr
- Angreifer ermittelt Daten, die zum Öffnen der Firewall von extern ermittelt werden können
- Angreifer öffnet Firewall des XP Rechners



11/20

AddOn 2006

Demo 3 – SuperClock1

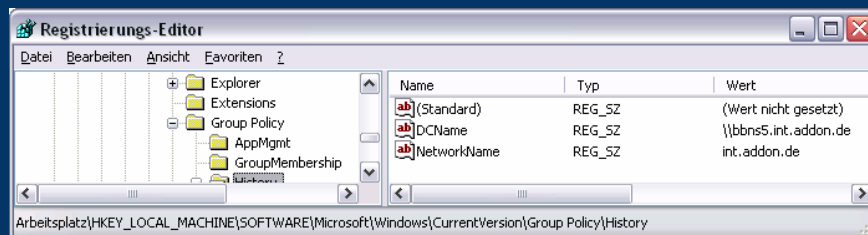
- Analyse des Netzwerkverkehrs am Access Point
- Wie von extern die Firewall u. U. geöffnet werden kann
- Algorithmus „Profilwechsel“

12/20

AddOn 2006

Algorithmus „Profilwechsel“

- Prüft verbindungsabh. **DNS suffix Informationen** (des DHCP-Servers) und vergleicht diese mit **HKLM\Software\Microsoft\Windows\Current Version\Group Policy\History\NetworkName**
 - NetworkName = DNS suffix ▶ Domänenprofil
 - NetworkName ≠ DNS suffix ▶ Standardprofil



- MS-Doku: <http://tinyurl.com/qyj9j>

13/20

AddOn 2006

Empfohlene Strategien für XP Firewall

- Firewall für Standard- und Domänenprofil konfigurieren, dabei beide recht restriktiv vorgeben
- Wenige Ausnahmeregeln
 - Bevorzugt **Programmausnahmen** definieren
Ports sind dadurch nicht ständig offen, sondern nur, wenn die Anwendung sie benötigt, d.h. wenn das Programm läuft und auf die Verbindung von außen wartet
 - Lokalen Administratoren **Verändern der Ausnahmeregeln** verbieten
 - Nicht mehr benötigte Ausnahmen sofort löschen
- Protokollierung einschalten
Und stichprobenhaft zyklisch Protokolle lesen!



14/20

AddOn 2006


Demo 4 – SuperClock2

- Wie Trojaner die Firewall umgehen können

15/20

AddOn 2006

Die neue Firewall von Windows Vista

- blockiert jeglichen eingehenden Netzwerkverkehr außer: Ausnahmen sind konfiguriert
- lässt ausgehenden Netzwerkverkehr zu außer: Ausnahmen sind konfiguriert 
- Ausnahmenregeln unterstützen Active Directory Konten und Windows Dienste und werden mit Hilfe von Assistenten konfiguriert
- Neue MMC: "Windows Firewall with Advanced Security" und neue Kommandozeile `netsh advfirewall`
- Neue Gruppenrichtlinien unterstützen die neue Firewall

16/20

AddOn 2006

Tools entwickeln – AD 429/431

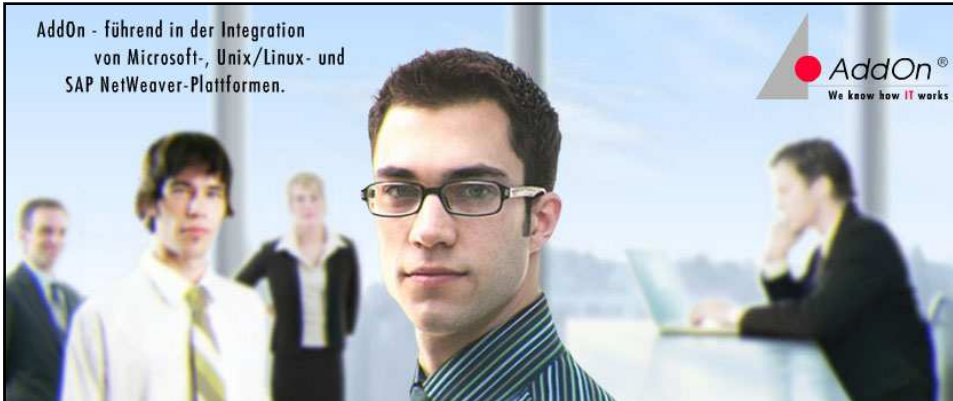


- AD429: „Visual Basic 2005 für Administratoren“
- Zielgruppe: Administratoren, die Tools zur Erleichterung der administrativen Arbeit entwickeln möchten
 - Leichter und verständlicher Einstieg – auch ohne Vorkenntnisse
 - Zugriff auf Active Directory, WMI, SQL-Datenbanken etc.
 - Viele Beispiele und nützliche Tools
- Zwei Alternativen:
 - TN **ohne** Vorkenntnisse
Dauer: 4 Tage, Preis: 2.200 € (für NT-AGler: 1.870 €)
 - TN hat schon **AD409** besucht oder hat fundierte WSH-Kenntnisse
Dauer: 2 Tage, Preis: 1.250 € (für NT-AGler: 1.060 €)

19/20

AddOn 2006

AddOn - führend in der Integration
von Microsoft-, Unix/Linux- und
SAP NetWeaver-Plattformen.



Vielen Dank für Ihre Aufmerksamkeit!

