



## Windows Campus Treffen Oktober 2004

Gerd Hofmann

21. Oktober 2004

## Vorstellung



- Gerd Hofmann
- Novell-/Windowssysteme
- Kontakt
  - E-Mail: [gerd.hofmann@rrze.uni-erlangen.de](mailto:gerd.hofmann@rrze.uni-erlangen.de)
  - Telefon: 09131-85-28920
  - RRZE: Raum RZ 2.013

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

2

## Agenda



- Agenda
  - Windows XP Servicepack 2
    - Firewall
    - SecurityCenter
    - Internet Explorer
    - Bluetooth
    - Softwarekompatibilität
    - Rollout (FAUSUS)
  - SUS (FAUSUS)
  - SAV (FAUSAV / SAVRemoteUpdate)
  - Windows Sicherheit

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

3

## XP SP2 - Firewall



- Agenda
  - Stateful Filtering
    - TCP-Verbindungen von innen nach außen möglich
    - TCP-Verbindungen von außen nach innen geblockt, u.a. RPC (Remote Procedure Call), SMB (Datei- und Druckfreigabe), NetMeeting, ...
  - Boot Time Policy
    - Komplette Abschottung bis auf DHCP, DNS, AD (GPO) während Boot
    - Im Fehlerfall gilt Boot Time Policy!
  - Run Time Policy
    - Aktivieren der Konfiguration erst bei Start des Firewall-Dienstes

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

4

## XP SP2 - Firewall



- Agenda
  - Konfigurationsmöglichkeiten
    - XP SP2
      - Öffnen statischer Ports
      - Exceptions / Ausnahmen
        - Erlauben Anwendungen das Öffnen von Listening-Ports (Pfadangabe der ausführbaren Datei)
        - Gelten global (nicht pro Netzwerkkarte)!
    - Globale Konfiguration: Systemsteuerung / Control Panel
    - Konfiguration pro Netzwerkkarte: Einstellungsdialog der Netzwerkkarte

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

5

## XP SP2 - Firewall



- Agenda
  - Konfigurationsmethoden / -techniken
    - XP SP2
      - GUI: Systemsteuerung & Netzwerkkarteneinstellungen
      - Policy/ Richtlinie (%SystemRoot%\inf\system.adm)
      - netsh Kommando (Skripting)
 

```
$> netsh firewall help
```
      - Antwortendatei unattend.txt siehe netfw.inf


21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

6

## XP SP2 - Firewall



**Agenda**

- Konfigurationen an der FAU

**XP SP2**


- **Novell NDPS Notify**

```
netsh firewall add allowedprogram
program = "%WINDIR%\System32\dpmw32.exe"
name = "NDPS RPM & Notification Listener"
mode = ENABLE scope = ALL profile = ALL
```
- **Contivity VPN Client**

```
netsh firewall add allowedprogram
program = "%ProgramFiles%\Nortel Networks\Extranet.exe"
name = "Contivity VPN Client"
mode = ENABLE scope = ALL profile = ALL
```
- **Vorkonfigurierte Clients des RRZE schalten Firewall bereits bei der Installation frei**

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
7

## XP SP2 - Firewall



**Agenda**

- Konfigurationen an der FAU

**XP SP2**

- **Setzen der Standardberechtigungen des Firewall-Dienstes:**

```

Löschen des Registry-Keys
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Security]

```

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
8

## XP SP2 – Security Center




**Agenda**

- Zielgruppe: Heimanwender


**FAU: kann deaktiviert werden**

**XP SP2**



21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
9

## XP SP2 – Internet Explorer



**Agenda**


- Neues Zonenmodell: restriktivere lokale Zone (Local Machine Zone LockDown)

**XP SP2**

- **Verhinderung „Zone Elevation“: restriktivste Zone zahlt**
- **Pop-up Blocker (Tools->Pop-up Blocker...)**
- **Add-on Verwaltung und Add-on Crash Detection**

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
10

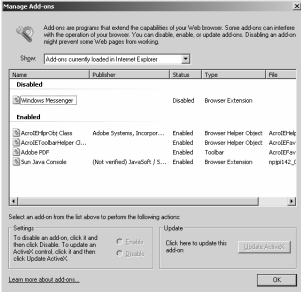
## XP SP2 – Internet Explorer



**Agenda**


- Add-on Verwaltung (Tools->Manage Add-ons...)

**XP SP2**



21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
11

## XP SP2 – Bluetooth





**Agenda**

- Nativer Bluetooth Support (signierter Treiber)


**XP SP2**

**Konflikt mit bereits installierten Bluetooth-Stacks (z.B. Widcomm nicht-signierter Treiber)**





Microsoft



Widcomm  
(rot: inaktiv)

- **Aktivieren des Widcomm Bluetooth-Stacks möglich: manuelles Zuweisen des nicht-signierten Treibers (siehe CT 2004/21, S.192 ff)**

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
12

## XP SP2 – Softwarekompatibilität

Agenda

XP SP2

- Probleme mancher Software / Tools:
  - Firewall Konfiguration (s.o.)
  - Verschärfte DCOM / RPC Sicherheitsrichtlinien
  - Bluetooth-Stack (s.o.)
  - Buffer-Overflow Schutzmechanismen (Lösung: Software Updates, falls vorhanden)
- ToDos für Adminsvor Rollout:
  - Test der eingesetzten Software auf SP2-Verträglichkeit
  - Konzeption und Implementation der Firewall und DCOM / RPC Konfiguration

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

13

## XP SP2 – Rollout

Agenda

XP SP2

- Installation von CD
- Windows Update (Verwendung des IE und der Microsoft Update Seite)
  - Software Update Service (Verwendung SUS-Client, z.B. FAUSUS)
  - Slipstream CD (Installations-CD mit integriertem SP2) originale Slipstream-CD von Microsoft am RRZE erhältlich

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

14

## XP SP2 – Rollout

Agenda

XP SP2

- Manuelle Nachinstallation
- Problem: viel Speicherbedarf (bis max. 2GB)
  - Lösung: Installation ohne Sicherung mit entpacktem Servicepack
    - Entpacken des Servicepacks:  
xpsp2.exe -x  
Der entpackte SP kann auf Server oder CD kopiert werden.
    - Aufruf des entpackten SPs ohne Sicherung:  
...\\1386\update\update.exe -n

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

15

## XP SP2 – Rollout

Agenda

XP SP2

- Automatische Installation über SUS-Client
- FAUSUS:
  - Freigabe erst Anfang Dezember bis dahin: Zeit für Tests und Vorbereitungen nutzen!
  - Microsoft SUS: VerzögerungsPatch (bis max. Mitte Dezember) von Microsoft erhältlich

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

16

## XP SP2 – Informationen im Web

Agenda

XP SP2

- RRZE Web Portal Dienstleistung -> Arbeiten & Rechnen -> Windows -> Aktuelle Informationen zum Windows XP Servicepack 2
- Microsoft XP SP2 Homepage: <http://www.microsoft.com/windowsxp/sp2/default.msp>

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

17

## System Update Service (SUS)

Agenda

XP SP 2

SUS

- FAUSUS.EXE (automatische Windows-Updates)
  - Web-Portal des RRZE Dienstleistung -> Arbeiten & Rechnen -> Windows -> FAUSUS
  - Nur für Windows 2000/XP/2003 nicht für Windows95/98/Me
  - Auf Arbeitsplatzrechnern innerhalb des Uni-Netzes
  - One Klick Setup => geeignet für automatische Installationen
  - Hotfixes werden vom RRZE vorgetestet (Arbeits-PCs der Administratoren + CIP-Pools)

21.10.04

gerd.hofmann@rrze.uni-erlangen.de

Windows Campus Treffen

18

## System Update Service (SUS)

Agenda  
 XP SP 2  
 SUS

**FAUSUS.EXE**  
(automatische Windows-Updates)

- Download über HTTP -Protokoll
- Updatecheck alle 17-24 Stunden => Geduld!
- Vorkonfiguration des Installationszeitpunktes täglich 10:00 (falls Hotfixes bereits verfügbar)
- Dialogmaske ermöglicht hinauszögern von Reboots (Reboot kann nicht verhindert werden)
- Windowsupdate mit Browser benötigt Administrator-Berechtigung  
Websurfen mit (IE und) administrativen Berechtigungen stellt großes Gefahrenpotential dar!

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
19

## Sophos Anti-Virus (SAV)

Agenda  
 XP SP 2  
 SUS  
 SAV

**FAUSAV.EXE**  
(Virens Scanner mit automatischem Update)

- Updates über SMB-Protokoll (Client für Windows Netzwerke, NetBIOS over TCP/IP)
- Updatecheck stündlich
- Vorkonfiguration des täglichen Intensivscans 10:30 / 15:00 oder 21:00 alle Dateien
- Vorkonfiguration des Echtzeitscans (Performanz)  
Schreiben, Umbenennen  
keine ZIP-Dateien (Entpacken == Schreiben)

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
20

## Sophos Anti-Virus (SAV)

Agenda  
 XP SP 2  
 SUS  
 SAV

**SAVRemoteUpdate.EXE**  
(Sophos@Home)

- Erhältlich über fauXpas
- Windows NT/2000/XP/2003 und Windows95/98/Me
- Auf Laptops oder Heim-PCs mit Internet-Verbindung und VPN-Client oder über Einwahl über die Uni

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
21

## Sophos Anti-Virus (SAV)

Agenda  
 WWW  
 SUS  
 SAV

**SAVRemoteUpdate.EXE**  
(Sophos@Home)

- Downloads über HTTP -Protokoll
- Updatecheck manuell & automatisch stündlich
- Keine Vorkonfiguration des Virens Scanners!  
*Ausnahme:*  
Konfiguration vorher installierter Sophos-Version (auch FAUSAV) wird übernommen

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
22

## Tipps zur Windows Sicherheit

Agenda  
 XP SP2  
 SUS  
 SAV  
 Sicherheit

**Benutzer mit eingeschränkten Rechten verwenden**

**Ausführen von Programmen mit Admin-Rechten:**  
runas-Befehl

**Alle kritischen / nicht benötigten Dienste deaktivieren, z.B.:**

- Server (+ Browser) Dienst (File- and Printsharing)
- Remote RegistryDienst
- Task Scheduler Dienst
- Messenger Dienst
- UPNP Dienst

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
23

## Sonstiges

Agenda  
 XP SP2  
 SUS  
 SAV  
 Sicherheit  
 Sonstiges

**Neue RRZE Internet CD**  
(VPN-Client, SAVRemoteUpdate)

**Campus Treffen am 11. November 2004, 14 Uhr c.t.:**  
Änderung der PC Hardware-Konfigurationen zum Jahreswechsel 2004/2005

21.10.04
gerd.hofmann@rrze.uni-erlangen.de
Windows Campus Treffen
24

**Ende**



- **Vielen Dank für Ihre Aufmerksamkeit**
- **Offene Fragen / Diskussion...**