

Freitag, 03.03.2006  
IT Security Day  
IT Security Day



## Windows Vista

Sicherheitsfeatures der neuen  
Microsoft® Windows® Client Plattform

Roland Taschler

MCSE MCT

Windows – Exchange - Security



# Security Experience

## mehr Vertrauen und Kontrolle



### Sicher

- 🔒 Secure Startup
- 🔒 Sicherer Betrieb mit geschützten User Accounts
- 🔒 Immer sicher und frei von malware



### Performant und zuverlässig

- 🔒 Geringe Antwortzeiten und Applikationsstart 15% schneller
- 🔒 2 sec. Resume von Standby und Boot PC 50% schneller
- 🔒 No crashes, no hangs und built-in Diagnostics



### Günstiges Deployment und Management

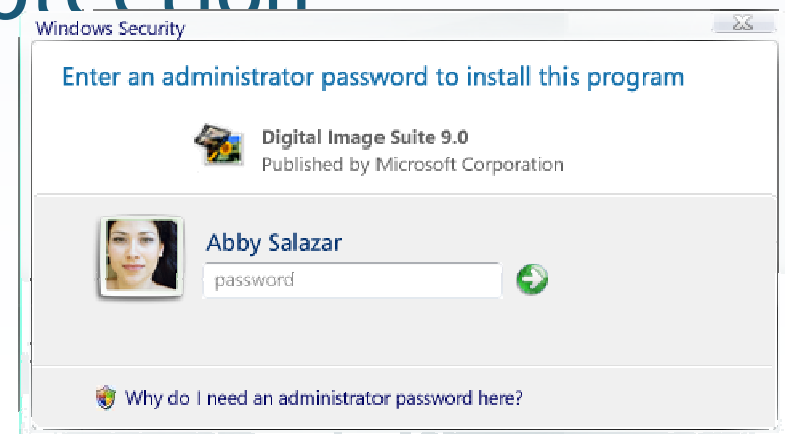
- 🔒 Patches mit 50% weniger Reboots
- 🔒 Anzahl der Systemimages um 50% niedriger
- 🔒 Migration der Anwender um 75% schneller



# Sicherheitsfeatures



- 🔒 Windows Services Hardening
- 🔒 Schutz vor Malware
- 🔒 Internet Explorer
- 🔒 Firewall
- 🔒 NAP Network Access Protection
- 🔒 Benutzerkonten Schutz
- 🔒 Datenschutz



# Windows Service Hardening



- 🔒 Windows Dienste wurden immer öfter Ziel von Angriffen, da sie meist als LocalSystem ausgeführt wurden und somit entsprechende Rechte hatten.
- 🔒 Verbesserungen:
  - Einführung von Service Security Identifier (SID). Jeder Dienst verfügt über eine Identität die über ACLs gesteuert werden kann
  - Den Diensten werden Firewall Netzwerkrichtlinien zugewiesen.
  - Unnötige Rechte werden für jeden Dienst einzeln entfernt.
  - Dienste werden unter Konten mit weniger Rechten ausgeführt als LocalService oder NetworkService

# Integrierte Anti-Malware



- 🔒 Integrierte Erkennung, Säuberung und Echtzeit Block:
  - Würmer, Viren und Trojaner
  - End Benutzer Lösung. Unternehmenslösung wird als eigenständiges Produkt erhältlich sein.
- 🔒 Bereits der Benutzerkontenschutz bietet höhere Sicherheit vor Malware
- 🔒 Integriertes Tool zur Entfernung gefährlicher Software (MSRT) entfernt Trojaner und Malware während Updates und mit Periodischen Scans.

# Internet Explorer



- 🔒 **Zusätzlich zum Benutzerkontenschutz bietet der IE**
  - Protected Mode (geplant für Vista Beta 2) Erlaubt dem IE das Browsen mit sehr eingeschränkten Rechten auch wenn der Benutzer höhere Rechte hat. (z.B. Software installieren)
  - “Read-only” mode, ausser für Temporäre Internet Dateien wenn sich der Benutzer in der Internet Sicherheitszone befindet.
  - Phishing Filter wird von Microsoft periodisch in kurzen Abständen aktualisiert aus verschiedenen Datenquellen.
    - Webseiten werden analysiert und geprüft ob sie irgendwelche Benutzerdaten identifizieren und weiterleiten.
  - Alle Cache Inhalte werden mit einem Klick gelöscht.

# Neue Windows Firewall



- 🔒 **Eingehende und ausgehende Sicherheit**
- 🔒 **Ausgehende Anwendungsfiler**
  - Richtlinienbasierte Installation und Konfiguration
    - Richtlinieneinstellungen verdoppelt auf ca. 3.500
  - Überprüft auch sog. Peer-2-Peer anwendungen auf Benutzer und Domänenebene.

# Network Access Protection

NAP



- 🔒 NAP ist eine Technologie die aus der VPN Welt kommt, wird jetzt aber auch auf das interne Netz ausgedehnt.
- 🔒 Es wird ein NAP fähiger Server benötigt, z. Zeit Windows Longhorn Server
- 🔒 Sie geben entsprechende Richtlinien vor:
  - Verbindliche OS Patches, aktuelle Antiviren Definition, aktuelle SPs usw.
- 🔒 ...und das System verhindert den Zugriff auf das gesamte Netzwerk für Clients die diesen Richtlinien nicht entsprechen:
  - Evtl. Zugriff auf Netzwerkreisourcen wo diese Patches und Updates heruntergeladen werden können.

Freitag, 03.03.2006

IT Security Day



# AIS & Benutzerkontenschutz





🔒 Neuer Windows Dienst der den Benutzerkontenschutz implementiert

🔒 Ziele:

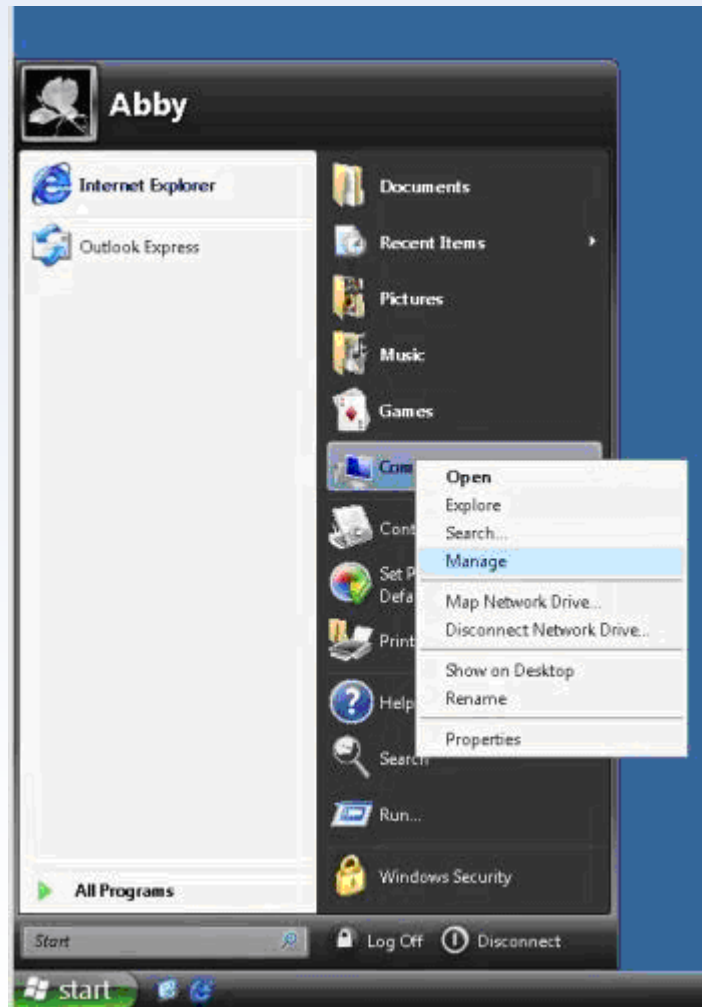
- Negative Auswirkungen von Malware einschränken, die vom System nicht erkannt wird

🔒 AIS ist im Kernel integriert.



- 🔒 Unterstützt das “Least Privileges Prinzip” auf 2 Arten:
  1. Benutzer brauchen keine administrativen Rechte für Aktionen die normalerweise Administrative Rechte erfordern, denn:
    - Sie werden bei Bedarf nach entsprechenden Kredentialien aufgefordert.
  2. Auch wenn ein Benutzer mit administrativen Rechten Aktionen ausführt, für die er Administrative Rechte benötigt, muss er dies bestätigen.
    - Hier wird nur die Zustimmung benötigt, keine alternativen Anmeldeinformationen.

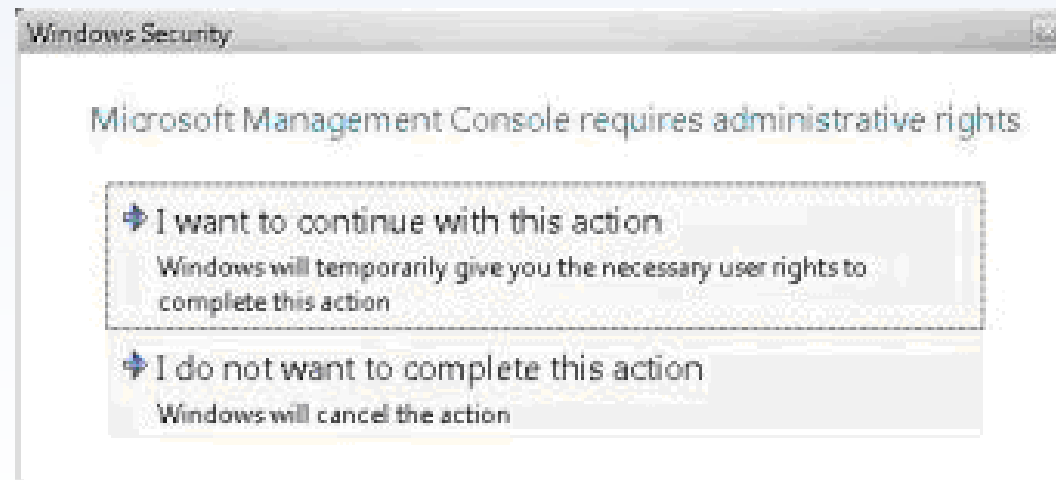
# Alternative Anmeldeinfo



# Zustimmung



- 🔒 Erfolgt in einer Situation wo ein Benutzer mit Administrativen Berechtigungen Aktionen ausführt für die Administrative Berechtigungen erforderlich sind.



# “Unlock” Schaltfläche für Änderungen am System



The image shows two overlapping windows from a Windows XP desktop. The background is a solid blue color.

The left window is titled "Date and Time Properties" and has two tabs: "Date & Time" and "Time Zone". The "Date & Time" tab is active, showing a date picker for June 2005, a calendar grid, and a clock face. The current time is 4:49:03 PM. Below the clock, it says "Current time zone: Pacific Daylight Time". There is a blue "Unlock" button at the bottom right of the dialog box.

The right window is titled "Windows Security" and contains the following text: "This action requires administrative rights. If you want to complete this action, choose an administrator account and enter its password." Below the text is a user selection area with a small icon of a rose and the name "Abby" next to a password input field. A "Cancel" button is at the bottom right of the dialog box.



- 🔒 Benutzerkontenschutz gilt nicht für den lokalen Administrator
  - Dieses Konto arbeitet “wie gehabt”
- 🔒 Steuerung über Richtlinien
  - Local Security Settings; Local Policies; Security Options; “LUA: Behavior of the elevation prompt”
    - No Prompt - Berechtigung wird automatisch erteilt
    - Prompt for Consent - Zustimmung wird eingeholt
    - Prompt for Credentials - Andere Anmeldeinformationen werden eingeholt. (Standard)

Freitag, 03.03.2006  
IT Security Day



# Integrierte Sicherheit





- 🔒 Kontrolle der Wechselmedien Geräteinstallation über Richtlinien
  - Nützlich zum Verhindern der Installation von USB Sticks
- 🔒 Genehmigte Treiber können in den Windows Trusted Driver Store integriert werden.
- 🔒 Wenn sich ein Treiber im Windows Trusted Driver Store befindet, kann er von jedem Benutzer unabhängig von seinen Rechten installiert werden.

# Client Security Scanner



- 🔒 Ermittelt den aktuellen Sicherheitsstand des Clients:
  - Patch und Update Status
  - Sicherheitsstatus
  - Signaturen
  - Anti-malware Status
- 🔒 Windows kann automatische Berichte selbst erstellen
- 🔒 Informationen können zentral gesammelt oder einach nur von Benutzern und Admins im Sicherheitscenter angezeigt werden.

# Restart Manager



- 🔒 Manche Updates erfordern Neustarts
- 🔒 Restart Manager:
  - Minimiert die Anzahl der Neustarts
  - Verwaltet die Neustarts von gesperrten PC's mit offenen Dokumenten.
    - Nach dem Neustart wird das Microsoft Word Dokument auf Seite 42 geöffnet, so wie es vor dem Neustart war.

Freitag, 03.03.2006

IT Security Day



## Sicherer Start - Datenschutz



# Trusted Platform Module

TPM Chip Version 1.2



- 🔒 Ein Hardware Chip auf der Hauptplatine von neuen PC's
- 🔒 Sicherheitsinformationen werden hier abgespeichert, Maschinenzertifikate, Verschlüsselungsschlüssel
  - Effectively, the essence of a smart smartcard
- 🔒 TPM kann für Codesignatur, Dateisignatur und Authentifizierung genutzt werden.

# Code Integrität



- 🔒 Alle DLL's und Ausführbare Dateien des Betriebssystems wurden digital signiert.
- 🔒 Signaturen werden überprüft bevor sie in den Speicher geladen werden.

# Full Volume Encryption

FVE



- 🔒 FVE verschlüsselt und signiert den gesamten Inhalt der Festplatte
- 🔒 TPM chip verwaltet die Schlüssel *dh*:
- 🔒 Jede ungewünschte Offline Änderung am den Daten oder am Betriebssystem wird erkannt und der Zugriff wird verweigert.
  - Verhindert Angriffe mit Tools auf die Daten während windows nicht ausgeführt wird.
- 🔒 Schutz vor Datendiebstahl wenn Laptops gestohlen werden.
- 🔒 Wesentlicher Teil des sicheren Starts

# Weitere Infos



- 🔒 [www.microsoft.com/windowsvista](http://www.microsoft.com/windowsvista)
- 🔒 Cebit (Hannover) 09.03 - 14.03.2006
- 🔒 Microsoft TechNet

Freitag, 03.03.2006  
IT Security Day  
IT Security Day



Vielen Dank für Ihre Aufmerksamkeit

Roland Taschler  
Net works KG  
roland.taschler@net-works.it

