Der Landesbeauftragte für den Datenschutz
Mecklenburg-Vorpommern

Datenschutz bei Windows XP Professional

Orientierungshilfe

Stand: 2003

Postanschrift
Schloss Schwerin
19053 Schwerin

Hausanschrift
Johannes-Stelling-Str. 21
19053 Schwerin

Kommunikation
Telefon (03 85) 5 94 94-0
Telefax (03 85) 5 94 94-58
E-Mail datenschutz@mvnet.de
Internet http://www.lfd.m-v.de

PGP-Fingerprint
ADB5 030A C111
388C A8FD
92B7 EF40 56E6
71DA 3ABA

Inhalt

1 Einleitung

Windows XP wird in zwei Versionen angeboten: Windows XP Home und Windows XP Professional. Wie schon der Name vermuten lässt, ist Windows XP Professional für den professionellen Gebrauch besser geeignet als die Home Version, da bestimmte Funktionen mit der Home-Version nicht ausführbar sind (siehe Punkt 13). Die nachfolgenden Ausführungen beziehen sich deshalb hauptsächlich auf Windows XP Professional.

Die Orientierungshilfe richtet sich deshalb auch in erster Linie an versierte Anwender wie Administratoren aus dem Bereich der professionellen Datenverarbeitung, denen der Umgang mit Windows vertraut ist und die somit auch die Schwachstellen älterer Windows-Betriebssysteme bereits kennen. Das Papier ist im Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder beraten und zustimmend zur Kenntnis genommen worden.

Windows XP Professional tritt die Nachfolge von Windows 2000 Professional an. Die neue Benutzeroberfläche, die erweiterte Hilfe und viele Assistenten sind die auf den ersten Blick auffälligsten Veränderungen bei Windows XP. Die Assistenten sollen den gestiegenen administrativen Aufwand eingrenzen. Insbesondere für erfahrene Benutzer sind sie gewöhnungsbedürftig und oft etwas zuviel des Guten, zumal automatisierte Vorgänge schlechter nachvollziehbar und dadurch undurchsichtiger werden. Die enge Anbindung an das Internet macht das Betriebssystem besonders leicht angreifbar.

Im Mittelpunkt dieser Betrachtung des neuen Betriebssystems von Microsoft sollen datenschutzrelevante Aspekte stehen. Der Benutzer soll auf bestehende Mängel in der Sicherheit des Betriebssystems aufmerksam gemacht werden. Es sollen Hinweise gegeben werden, wie diese Mängel eingeschränkt oder umgangen werden können. Darüber hinaus werden wesentliche Sicherheitsaspekte des Betriebssystems erklärt, damit bestimmte sicherheitsrelevante Einstellungen vorgenommen werden können.

2 Was ist neu bei Windows XP

2.1 Neue Benutzeroberfläche

Das Startmenü ist vollkommen neu gestaltet, bietet den Zugriff auf den Programmpfad und auch auf häufig genutzte Programme

2.2 Hilfe und Supportcenter

Mit dem Hilfe- und Supportcenter wurde der Zugriff auf die Onlinehilfe intensiviert.

2.3 Vereinfachungen für die Administration

Da der administrative Aufwand sehr gestiegen ist, werden Assistenten bereitgestellt.

2.4 Schneller Benutzerwechsel

Mehrere Benutzer können sich gleichzeitig anmelden, der Desktop und alle Tasks bleiben erhalten.

2.5 Neue Sicherheitsmechanismen

Mit Windows XP Professional wartet das Betriebssystem mit zahlreichen neuen Sicherheits-Funktionen auf. Zu den Wichtigsten zählen:

- die Verschlüsselung von Dateien und Ordnern auch für mehrere Benutzer,
- Analysefunktionen für Angriffe, Firewallfunktionen,
- automatische Konfiguration sicherheitsrelevanter Einstellungen.

Eine weitere aus datenschutzrechtlicher Sicht bedeutende Neuerung bei Windows XP ist die so genannte **Produktaktivierung** (siehe Punkt 5).

3 Vorteile und Nachteile von Windows XP

3.1 Vorteile

Durch die neue Treiberarchitektur wurde die Stabilität des Betriebssystems verbessert. Die veränderte Benutzeroberfläche ist eher umstritten. Für Computerneulinge vereinfacht sie sicher die Nutzung, für erfahrene Benutzer ist sie jedoch gewöhnungsbedürftig, weil vieles völlig anders als bisher ist. Immerhin kann auch die gewohnte, klassische Windows-Oberfläche gewählt werden. Da der administrative Aufwand gestiegen ist, werden einige erleichternde Hilfen durch Windows zur Verfügung gestellt:

- mehr Assistenten für Basisaufgaben,
- Zusammenfassung von Verwaltungsaufgaben in der Managementkonsole,
- kontextorientierte Aufgabenlisten in den Standardordnern,
- neue Ansicht der Systemsteuerung,
- Verlagerung von bestimmten Aufgaben in das Hilfe- und Supportcenter.

3.1.1 Verbesserte Hilfe

Die Suchfunktion ist deutlich leistungsfähiger als seine Vorgänger. So kann über den Suchdialog direkt nach Dokumenten, Computern, Druckern oder Personen gesucht werden. Neu ist der Start der Suchfunktion für das Internet. Die enge Verflechtung mit dem Internet spart zwar Zeit und Arbeit, ist jedoch nicht ganz unbedenklich. Nachteilig ist allerdings, dass kein Handbuch mehr zur Verfügung gestellt wird.

3.1.2 Verbesserte Systemwiederherstellung

Die Systemwiederherstellung kann im Falle eines Systemproblems einen früheren Zustand des Computers wiederherstellen, ohne dass die persönlichen Datendateien (z. B. Dokumente, Internetfavoriten und E-Mail) verloren gehen. Die Systemwiederherstellung überwacht Änderungen auf dem Computer und erstellt regelmäßig leicht identifizierbare Wiederherstellungspunkte. Darüber hinaus kann der Nutzer selbst jederzeit eigene Wiederherstellungspunkte erstellen und benennen.

3.1.3 Onlineunterstützung

Mit Hilfe der Remoteunterstützung kann anderen Personen gestattet werden, eine Verbindung mit dem eigenen Computer über das Internet herzustellen, sich in einem Chat mit dem Nutzer zu unterhalten und dessen Computerbildschirm einzusehen. Außerdem kann dieser Assistent nach entsprechender Zustimmung die Tastatur des Nutzers und dessen Maus steuern und somit bei der Problembehandlung helfen. Zusätzlich werden auch die Dateisysteme des Client-Geräts

auf den Windows XP Rechner übertragen, damit dieser Rechner auf die Laufwerke des Clients zugreifen kann (siehe dazu auch Punkt 6.4). Die Supportseite ermöglicht es, sich direkt an den Computerhersteller oder, falls Windows XP separat erworben wurde, an Microsoft zu wenden. In der Support-Newsgroup kann der Austausch von Informationen und Hilfe mit anderen Benutzern erfolgen.

3.1.4 Offline-Unterstützung

Falls keine Internetverbindung zur Verfügung steht, können andere Tools für die Problembehandlung genutzt werden: Die so genannten Computerinformationen zeigen Informationen über die zurzeit installierte Software und Hardware an. Die erweiterten Systeminformationen und das Systemkonfigurationsprogramm bieten technische Details, mit denen Mitarbeiter vom technischen Support Probleme beheben können.

3.1.5 Schnelle Benutzerumschaltung

Windows XP führt mit Hilfe der Terminaldiensttechnologie eindeutige Benutzersitzungen aus, wodurch die Daten der einzelnen Benutzergruppen eindeutig voneinander getrennt bleiben. Durch das verwendete Benutzerkennwort werden die Daten separat voneinander geschützt, sofern sie sich auf einer NTFS-Partition befinden. Die schnelle Benutzerumschaltung ist nur bei Computern einer Arbeitsgruppe oder bei eigenständigen Computern möglich. Gehört der Computer zu einer Domäne, erfolgen die Optionen für die Anmeldung nach den vom Administrator festgelegten Richtlinien (siehe auch Punkt 9).

Die neue Benutzerumschaltung ermöglicht es, schnell zwischen Benutzern umzuschalten, ohne sich am Computer abzumelden. Mehrere Benutzer können einen Computer gemeinsam nutzen und ihn gleichzeitig verwenden, wobei die Benutzer wechseln können, ohne die Programme, die sie ausführen, zu schließen (z. B. ein Computer für alle Mitarbeiter einer Lagerverwaltung).

3.2 Nachteile

Windows XP ist das wohl neugierigste Betriebssystem aller Zeiten. Der Internet-Explorer suchte schon vor XP automatisch nach Updates. Aber in keiner der vorherigen Windows-Versionen hat Microsoft so viele Komponenten eingebaut, die über das Internet Kontakt mit den Microsoft-Servern aufnehmen, wie z. B. das Windows-Update, die Fehlerberichterstattung und die Zeitsynchronisation.

Den Messenger von Microsoft musste sich bisher jeder auf seinen PC laden, der ihn einsetzen wollte. Bei XP sind jetzt diese Anwendungen und Funktionen Standard. Windows XP schreibt einen Fehlerbericht, sobald ein Programm abstürzt, und gibt dem Anwender die Möglichkeit, diesen per Internet an Microsoft zu senden (siehe Abb.1). Immerhin könnte der Anwender davon indirekt profitieren, da Microsoft mit der so entstehenden Datenbank unter anderem natürlich auch das Betriebssystem verbessern kann.

Abb.1

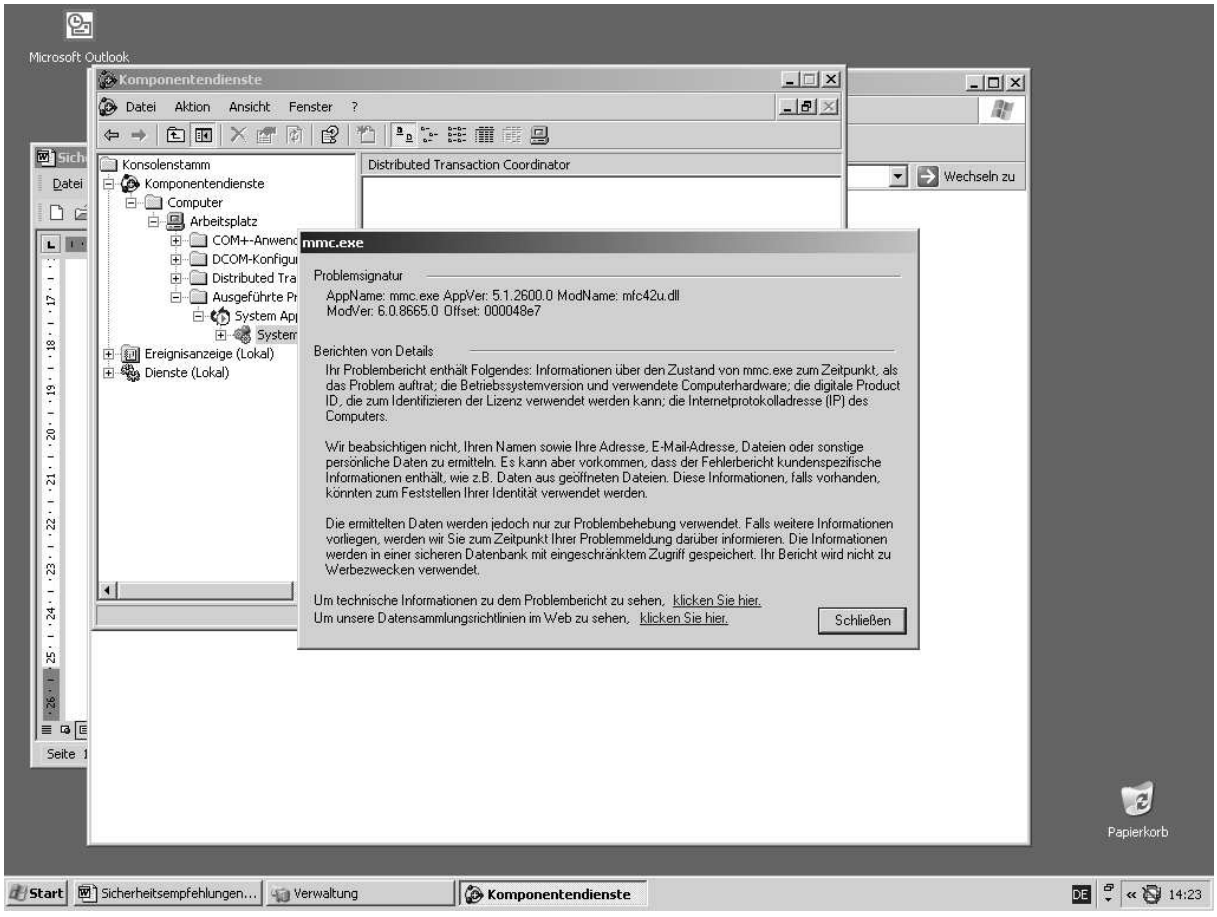


Abb. 1 zeigt eine typische Fehlermeldung mit Hinweisen zu den übertragen Daten. Mit dem Hinweis, dass die Informationen „auf einer sicheren Datenbank mit eingeschränktem Zugriff gespeichert werden“ und dass der „Bericht nicht zu Werbezwecken verwendet wird“ soll möglicherweise der datenschutzgerechte Umgang mit diesen Daten suggeriert werden, nachprüfbar ist jedoch keine dieser Aussagen.

Der über das Netz übertragene Fehlerbericht enthält folgende Informationen:

- Informationen über den Zustand der Datei zum Zeitpunkt, als das Problem auftrat,
- die Betriebssystemversion und die verwendete Computerhardware,
- die digitale Produkt-ID die zum Identifizieren der Lizenz verwendet werden kann,
- die Internetprotokolladresse (IP).

Es kann aber auch vorkommen, dass der Fehlerbericht kundenspezifische Informationen enthält, wie z. B. Daten aus geöffneten Dateien. Diese Informationen, falls vorhanden, können zum Feststellen der Identität verwendet werden.

3.2.1 So schützen Sie sich

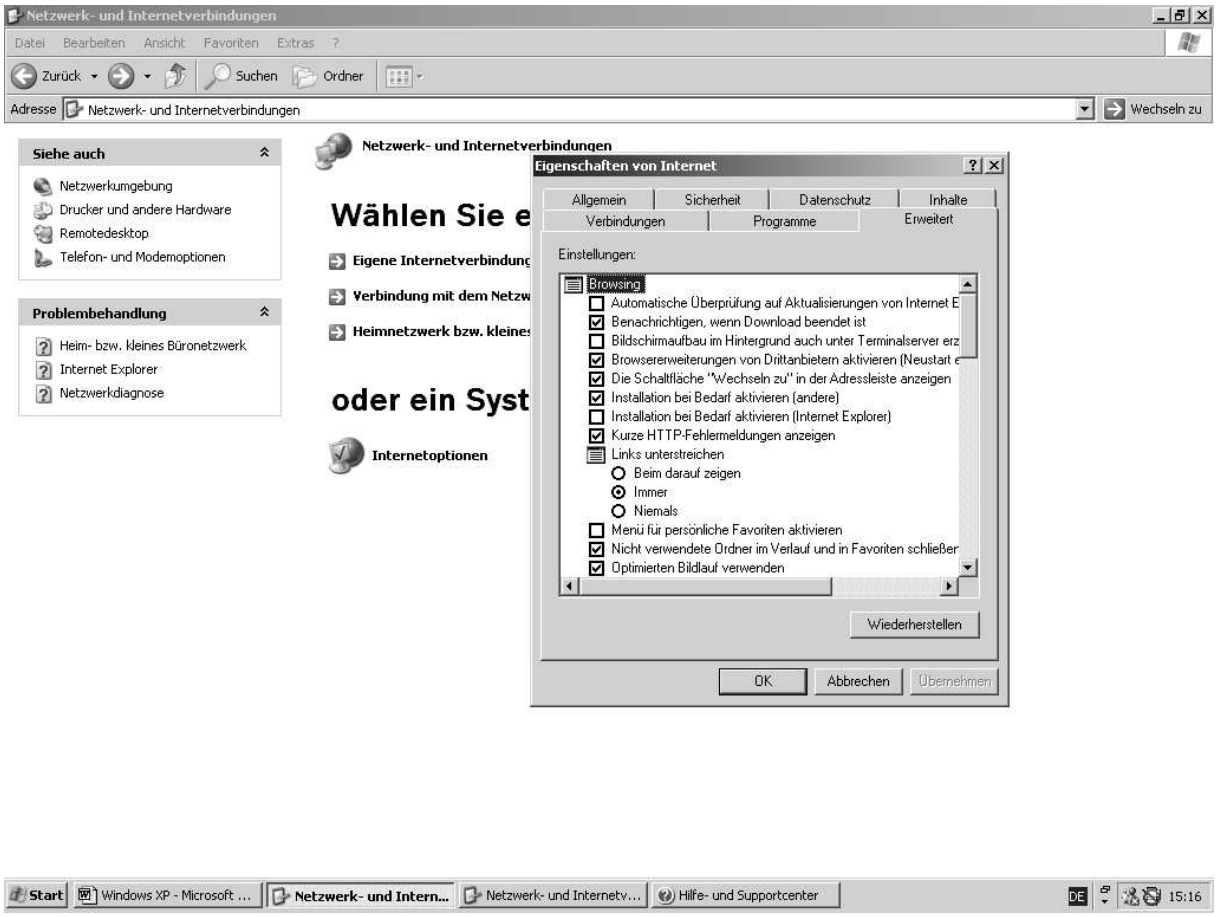
Grundsätzlich gilt: Alle genannten Funktionen lassen sich über die Systemsteuerung abschalten (siehe Abb.2)

Automatische Aktualisierung abschalten

Die Automatische Aktualisierung lässt sich über Systemsteuerung/Netzwerk und Internetverbindungen/Internetoptionen auf der Karte erweitert abschalten.

Wurden die automatischen Aktualisierungen nicht abgeschaltet, können sie über Systemsteuerung/Software jederzeit wieder entfernt werden. Alle Aktualisierungen werden dort verwaltet.

Abb.2



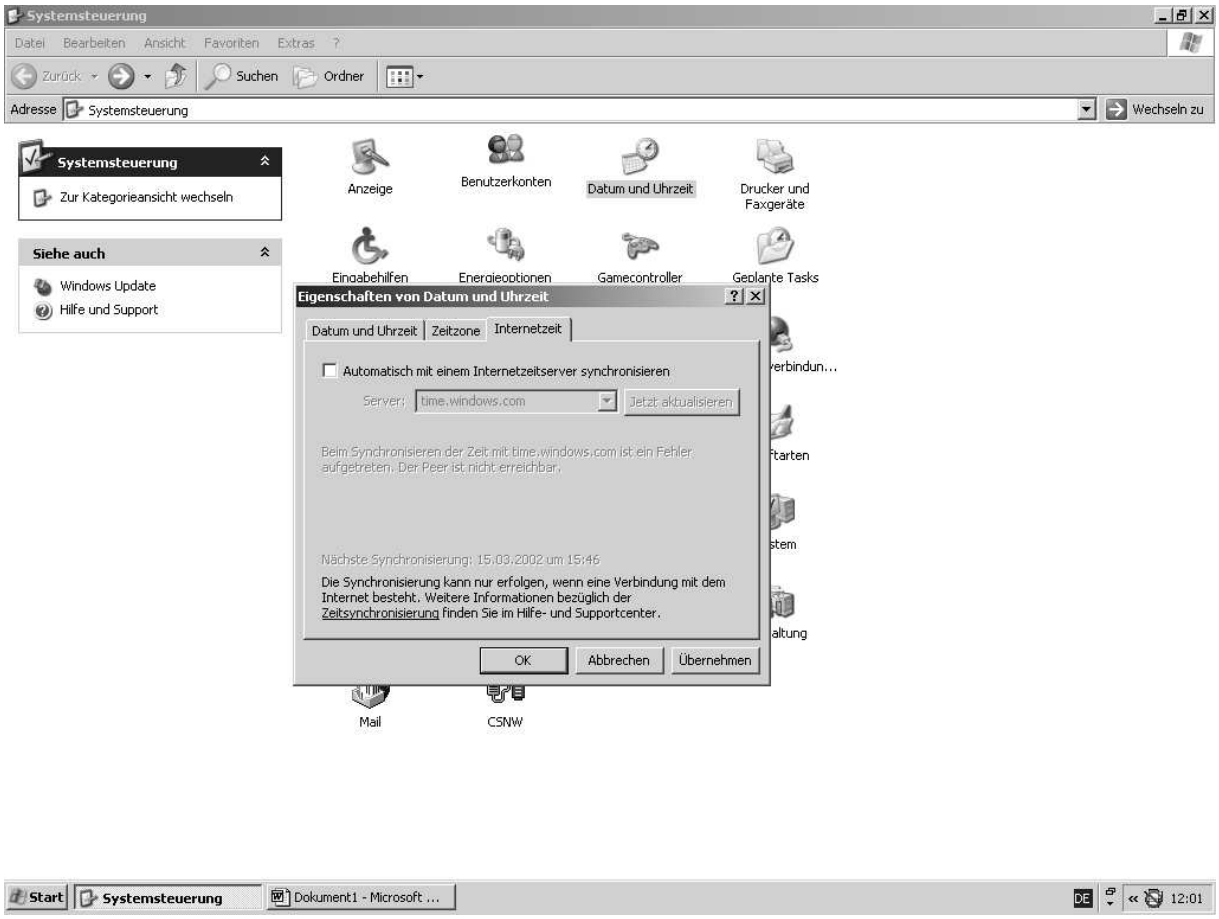
Empfehlung: Die automatische Überprüfung auf Aktualisierungen vom Internet Explorer sollte deaktiviert sein.

Abschalten der Zeitsynchronisation

Bei der Funktion Zeitsynchronisation stimmt Windows XP die Uhrzeit des PCs mit einer Uhr im Internet ab. Dazu wird ein Internet-Server von Microsoft kontaktiert. Als Standardserver kann jedoch auch ein anderer Server eingetragen werden.

Ein Entfernen des Häkchens bei „Automatisch mit einem Internetserver synchronisieren“ verhindert diese ständigen Kontaktaufnahmeversuche (siehe Abb. 3).

Abb.3

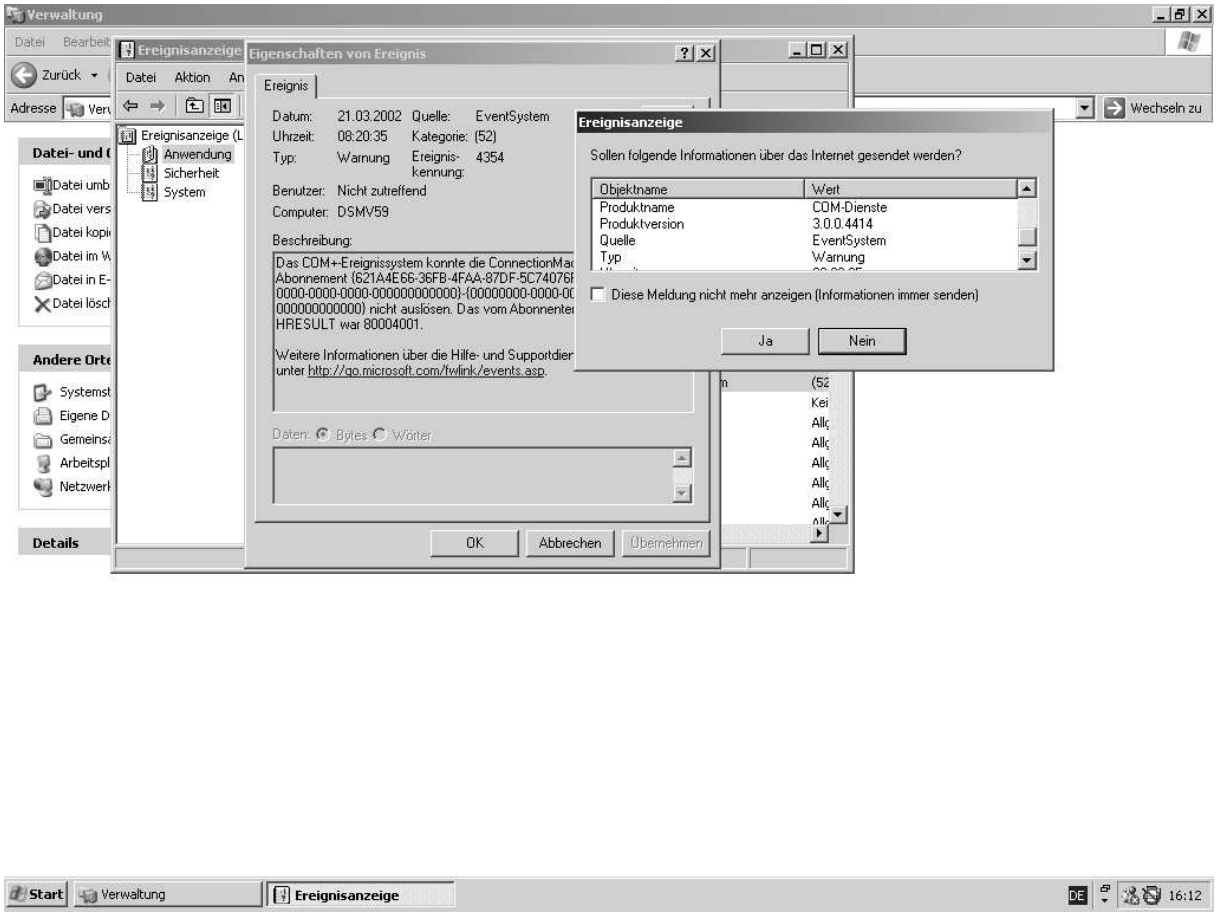


Die Zeitsynchronisation lässt sich unter Datum und Uhrzeit abschalten oder auf einen anderen Internet-Server umlenken.

Fehlerprotokoll aufrufen/Kontrolle der übertragenen Daten über die Hilfe und Supportdienste

Zur besseren Kontrolle der übertragen Daten sollte die entsprechende Mitteilung immer angezeigt bleiben (siehe Abb. 4). Nur so lässt sich einschätzen, welche Informationen wann übertragen werden.

Abb.4

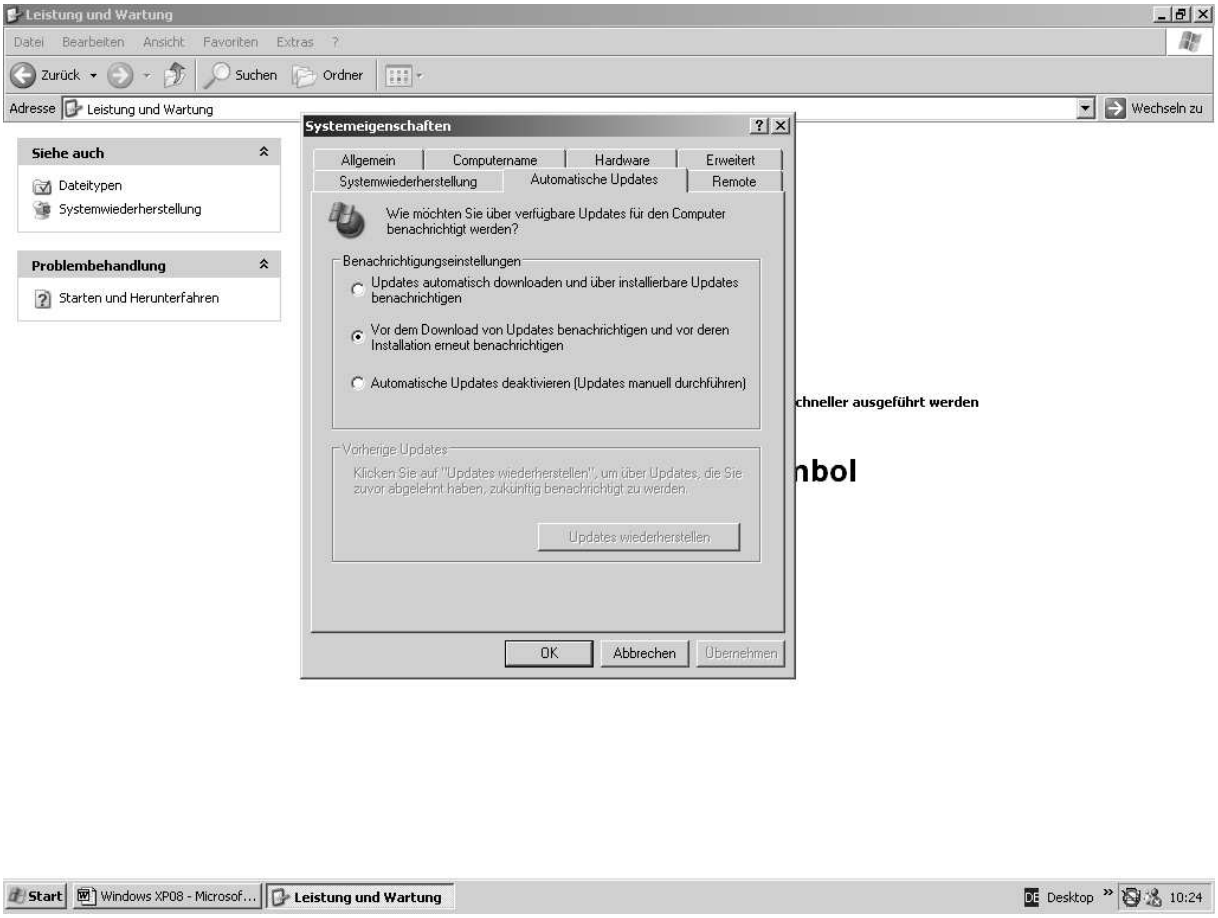


Empfehlung: Das Feld „Diese Meldung nicht mehr anzeigen“ sollte deaktiviert bleiben.

Automatische Updates

Auch Updates können so eingestellt werden, dass sie nicht automatisch erfolgen, und der Nutzer den Überblick behält, wann welches Update erfolgt (siehe Abb. 5).

Abb.5



Empfehlung: Automatische Updates sollten deaktiviert sein, mindestens jedoch sollte vorher eine Benachrichtigung erfolgen.

3.2.2 Softwareunterstützung

Einen guten Überblick über die in Punkt 3.2.1genannten datenschutzrelevanten Einstellungen kann man sich auch mit Hilfe zusätzlicher Software verschaffen. Das – allerdings nur für die private Nutzung kostenlos – aus dem Internet herunter zu ladende Programm XPAntiSpy beispielsweise ermöglicht ein sehr komfortables Konfigurieren dieser Systemeinstellungen über die Windows-Oberfläche oder im Befehlszeilenmodus.

4 Die Installation von Windows XP

4.1 Anforderungen an Hardware

Folgende Mindestvorrausetzungen bzw. Empfehlungen für die Hardware sollten berücksichtigt werden, um flüssiges Arbeiten zu gewährleisten:

Hardware	Mindestanforderungen	Empfohlen
CPU	266 MHz Pentium	500 MHz Pentium III
RAM	64 MB	256 MB
Festplatte	2 GB; min.1,2 GB Frei	Ab 4 GB
Netzwerk	PCI 10 MBit	PCI 100 MBit
Grafikkarte	PCI-Grafikkarte	AGP-Grafikkarte
CD-ROM	12-fach	32-fach
Floppy	1,44 MB	1,44 MB

Das Vorhandensein der Maus ist Bedingung.

Es gibt drei verschieden Möglichkeiten, Windows XP zu installieren: Update-, Neu-, und Parallelinstallation. Für die Parallelinstallation muss für Windows XP eine eigene Partition eingerichtet sein.

Die Produktaktivierung kann telefonisch oder online über das Internet erfolgen (siehe Punkt 5).

Alle Benutzer, die bereits während der Installation von Windows XP eingerichtet wurden, erhalten zunächst automatisch die Rechte eines System-Administrators. Es sind nicht nur „Benutzer“, wie das dazugehörige Dialogfenster vermuten lässt, sondern „Administratoren“ mit entsprechenden Privilegien. Diese lassen sich zwar im Nachhinein einschränken, besser ist es aber, bestimmte Rechte von vornherein auszuschließen. Dabei ist jedoch zu berücksichtigen, dass sich einige Applikationen ohne Administrator-Rechte nicht sinnvoll betreiben lassen. Eine Abwägung zwischen Produktivität und Sicherheit ist deshalb immer notwendig.

4.2 Automatisierte Installation

Die komplette Installation vieler identischer Computer bedeutet hohen zeitlichen Aufwand und entsprechend hohe Kosten. Der schnellstmögliche Ersatz bei Ausfall eines Computersystems in einem Unternehmen ist ein weiterer Grund für eine Arbeitserleichterung auf diesem Gebiet.

Für die automatisierte Installation gibt es mehrere Möglichkeiten:

- **Mit Hilfe von Antwortdatei für WINNT.EXE/WINNT32.EXE**
    - Über Antwortdateien wird das Setup von Windows XP gesteuert. In normalen Textdateien werden in einer bestimmten Syntax die Antworten eingetragen, die normalerweise durch den Benutzer eingegeben werden. Das automatisch ablaufende Setup verkürzt die benötigte Zeit für die Installation. Das Administratorkennwort wird unverschlüsselt im Klartext in der Antwortdatei (siehe Punkt 4.2) abgelegt und kann damit leicht missbräuchlich genutzt werden. Man sollte deshalb hier noch kein reales, sicherheitsrelevantes Passwort festlegen, sondern zunächst nur eines für den jeweiligen lokalen Zugriff auf den Computer definieren und nach Abschluss der Installation sofort ändern.

- **Mit Hilfe von Verteilung von Disk-Images**
    - Bei dieser Methode wird über spezielle Programme ein bitweises Abbild (Image) der spezifizierten Partition erzeugt, welches auf einem anderen Computersystem wieder auf der Festplatte eingefügt werden kann.
- **Über Remoteinstallationsdienste** (siehe auch Punkt 3.1.3)

5 Produktaktivierung

5.1 Produktaktivierung

Windows XP lässt einen Start ohne Produktaktivierung nur während der ersten 30 Tage zu. Danach muss das Produkt durch entsprechende Registrierung aktiviert werden. Diese Zwangsaktivierung soll Microsoft vor Raubkopieren schützen.

Bei der Produktaktivierung wird ein 50-stelliger Code per Web oder Telefon an Microsoft übermittelt. Darin sind verschiedene Merkmale des Computers gespeichert. Die 50 Stellen reichen allerdings nicht aus, um das genaue Modell zu übermitteln.

Folgende Daten prüft und verschickt Windows XP:

- Seriennummer der Windows-Partition
- MAC-Adresse der Netzwerkkarte
- CD-ROM-ID-Nummer
- Grafikkarten-ID-Nummer
- Prozessor-ID-Nummer
- Festplatten-ID-Nummer
- SCSI-Adaptter-ID-Nummer
- IDE-Controller-ID-Nummer
- Modell des Prozessors
- Größe des RAM

Nachdem Windows XP aktiviert wurde, dürfen laut Hersteller nur noch geringfügige Änderungen am System vorgenommen werden, bevor eine erneute Aktivierung fällig wird. Dabei ist wichtig, ob am normalen PC oder am Notebook mit Dockingstation gearbeitet wird. Am normalen PC sind bis zu 3 Änderungen möglich, am Notebock können es bis zu 6 Änderungen an der Hardware sein. (Bei einem Notebook, das an eine Docking-Station anschließbar ist, werden Grafikkarte und SCSI-Host-Adapter nicht in die Berechnung einbezogen.)

Die Microsoft Produktaktivierung ist bei Paket-, OEM-, System Builder-Produkten und Lizenzen für Schüler, Studierende und Lehrkräfte erforderlich. Die Microsoft Volumenlizenzprogramme sind hiervon ausgenommen, das heißt, sie müssen nicht aktiviert werden.

5.2 Übertragung personenbezogener Daten bei der Produktaktivierung

Der TÜViT hat im Auftrag der Microsoft Deutschland GmbH die Produktaktivierung der Microsoft Produkte Windows XP, Office XP und Visio 2002 geprüft. Dabei sind die Mitarbeiter zu folgendem Resultat gekommen:

In den untersuchten Programmteilen wurden keinerlei Anhaltspunkte gefunden, dass personenbezogenen Daten automatisch über das Internet übertragen werden. Erst wenn ein Benutzer

auch eine freiwillige Registrierung durchführt, werden nach Abfrage der expliziten Zustimmung personenbezogene Daten übertragen. Dies gilt entsprechend auch für eine telefonische Registrierung.

Der Technische Überwachungsverein stellte dem Betriebssystem Windows XP in Bezug auf die Produktaktivierung zwar eine Unbedenklichkeitsbescheinigung in Sachen Datenschutz aus. Fragwürdig bleibt diese Zwangsregistrierung dennoch, insbesondere weil Microsoft nichts zur Art und Weise der künftigen Verwendung der gesammelten Informationen sagt. Dass die Nutzung vieler verbesserter Merkmale von Windows XP eine Internet-Verbindung quasi zwingend voraussetzt, macht viele Anwender zusätzlich skeptisch, da Sicherheitsprobleme bei der Internetanbindung die Schwachstelle des Systems zu sein scheinen.

6 Sicherheit im Netzwerk

6.1 Schutz nach außen

Der Schutz vertraulicher Daten bei der Übermittlung über das Internet von einem lokalen Computer oder einem Büronetzwerk ist heute zunehmend schwierig. Durch Festverbindungen und Flatrates sind Ports auf lokalen Rechnern mit entsprechender Software wie Portscannern leicht zu orten. Auch dynamische IP-Adressen bieten keinen Schutz davor, dass inzwischen ganze Netzwerke gescannt werden. Es ist beobachtet worden, dass bereits nach 20 Minuten Online-Zeit erste Scannerzugriffe erfolgten. Erkennt der Angreifer dann offene Ports, die Systemdienste anbieten, kann er darüber versuchen, Zugriff auf das System zu erlangen.

Grundsätzlich gilt: Je länger die Verbindung, desto größer die Angriffswahrscheinlichkeit.

Gefährdet sind Computer und Netzwerke aber auch oft durch mangelnde Sensibilität der Anwender. Die Meinung: „Wer sollte mich schon angreifen?“ ist nach wie vor sehr verbreitet, angesichts der Möglichkeiten von Windows XP jedoch völlig fehl am Platz. Die zahlreichen, scheinbar ziellosen Portscans zeigen, dass zunächst keine auf bestimmte Personen bezogene Angriffe gefahren werden. Oft werden einfach irgendwelche offene Computer gesucht, um dort trojanische Pferde zu installieren. Diese schaden nicht zwangsläufig direkt den befallenen Computer, sondern greifen nach entsprechenden Anweisung von außen das eigentliche Opfer an. Selbst stark abgesicherte Systeme sind angreifbar, indem extrem viele Anfragen, möglichst mit fehlerhaften Paketen, gestartet werden (Denial-of-Service-Attacken). Dass hierbei die Angriffe von unwissenden Anwendern weltweit verteilt sind, macht eine Abwehr fast unmöglich. Dem Angegriffenen bleibt oft keine andere Wahl als den Server abzuschalten.

6.2 Sicherheitsprotokolle für das Netzwerk

6.2.1 Kerberos – sichere Authentifizierung

Wie schon Windows 2000, so verwendet auch XP zur sicheren Authentisierung im Netzwerk das Kerberos-Protokoll. Kerberos ist als zentraler Sicherheitsstandard in Windows 2000/XP und in Active Directory (siehe auch Punkt 11) implementiert. Kerberos verwendet zum einen ein Verschlüsselungsverfahren für die Schlüssel selbst, zum anderen so genannte Zeittickets, die den Ablauf der Übertragung kontrollieren. Microsoft hat den Kerberos-Standard weiter entwickelt, so dass nun auch Zertifikate mit öffentlichen Schlüsseln eingesetzt werden können. Diese Schlüssel werden mit dem Zertifikatserver erstellt, der nur in der Windows 2000 Server-Familie verfügbar ist.

6.2.2 Sicherer Datentransfer – IPSec

Mit IPSec (IPSecurity) ist in Windows XP wie bereits in Windows 2000 eine Technologie implementiert, die Daten auf IP-Ebene verschlüsselt, und somit vor Abhörangriffen und unbefugten Veränderungen schützen soll. Für Applikationen bleibt dieser Vorgang transparent. IPSec erlaubt den einfachen Aufbau sicherer Verbindungen auf Betriebssystemebene, ohne dass die Anwendungen speziell dafür ausgelegt sein müssen. Mit IPSec lässt sich der Datenverkehr im LAN (Lokal Network Area) und im WAN (Wide Area Network) schützen. Es schützt gleichermaßen vor den Angriffen Interner und Externer. Diese Dienstesammlung basiert auf der DES (Data Encryption Standard) – oder 3DES-Verschlüsselung und kann auch auf getunnelte Verbindungen wie z. B. L2TP (Layer 2 Tunneling Protocol) aufsetzen (siehe auch Punkt 6.2.3). IPSec bietet ein höheres Maß an Sicherheit als PPTP (Point to Point Tunneling Protocol) und wird wohl langfristig PPTP ablösen. IPSec bietet zwei verschiedene Betriebsmodi: den Transportmodus und den Tunnelmodus. Im Transportmodus wird nur der Datenteil des zu transportierenden IP-Paketes verschlüsselt, im Tunnelmodus wird das komplette IP-Paket verschlüsselt und mit einem neuen IP-Kopf und dem IPSec-Kopf versehen.

6.2.3 L2TP (Layer 2 Tunneling Protocol)

Das Tunneling von Datenpaketen über IP gewinnt immer mehr Bedeutung für den Aufbau Virtueller Privater Netzwerke (VPN). Der Transport von Daten erfolgt hierbei über das Netzwerk in abgeschlossenen (privaten) Einheiten. Damit die Daten auch sicher sind, werden sie einzeln verpackt und über TCP/IP-Protokoll „getunnelt“ verschickt. Bisher wurde bei Windows das Point-to-Point Tunneling Protocol (PPTP) verwendet. Da andere Systeme aber auch mit anderen Standards arbeiten, unterstützt Microsoft mit Windows XP neben PPTP jetzt auch L2TP. Da dieses Protokoll von sich aus keine Verschlüsselung unterstützt, kann hierbei IPSec zum Einsatz kommen (siehe auch Punkt 6.2.2).

Vergleich von **PPTP gegenüber L2TP**

L2TP unterscheidet sich nur in wenigen Punkten von PPTP. PPTP und L2TP verwenden die Datenverbindungsschicht (Ebene 2) und packen die Datenpakete in Frames des Punkt-zu-Punkt-Protokolls. L2TP unterstützt mehrere Tunnel. PPTP arbeitet nur über IP-Netzwerke. Der Vorteil von L2TP gegenüber PPTP ist, dass es direkt über die verschiedenen WAN übertragen werden kann, aber optional auch über den Umweg IP funktioniert.

6.3 Internetverbindungsfirewall

Die Internetverbindungsfirewall soll den Computer schützen, auf dem sie aktiviert ist. Bei den meisten Heim- bzw. kleinen Büronetzwerken ist dies der so genannte ICS-Hostcomputer (Internet Connection Sharing), also der Computer, der die DFÜ-Verbindung zum Internet herstellt. Ohne dass weitere DFÜ-Verbindungen aufgebaut werden müssen, können alle Computer im Heim- oder im kleinen Büronetzwerk mit dem Internet verbunden werden, da sie die vom ICS-Host aufgebaute Verbindung gemeinsam nutzen können. Eine Internetverbindung über die vorhandene DFÜ-Verbindung können andere Computer im Netzwerk nur dann herstellen, wenn ICS auf dem ICS-Host aktiviert ist. Die Adressen der Clientcomputer erscheinen nicht im Internet, nur der gemeinsam genutzte Host ist öffentlich sichtbar.

Die Firewall schützt dann bei Aktivierung jede beliebige Internetverbindung. Die Firewall speichert Kommunikationsdaten, Sende- und Empfangsadressen von jeder Verbindung zwischen dem Internet und dem Computer und verwaltet sie in einer Tabelle. Daten von nicht erwarteten Adressen werden abgewiesen. Sind Zugriffe auf den Computer aus dem Internet beispielsweise über http, ftp oder andere Dienste gewollt, so müssen diese extra konfiguriert werden.

Die Remoteunterstützung wird hingegen nicht eingeschränkt (siehe auch Punkt 6.4). Sie ist immer in beiden Richtungen möglich. Während eines Remotezugriffs ist der Schutz durch die Firewall weitgehend aufgehoben, und das gesamte System ist dadurch verwundbar.

Die Windows XP Firewall bietet kleinen Netzwerken, die mit dem Internet verbunden sind, nur eine sehr trügerische Sicherheit. Wird nämlich der Windows Messenger oder andere MS Software gestartet, dürfen Multimedia-Dateien die Firewall ungehindert passieren. Das Desinteresse ausgehenden IP-Paketen gegenüber stellt ein erhebliches Sicherheitsrisiko dar. Ins System eingedrungene Trojaner können trotz der integrierten Firewall ungehindert eine Verbindung ins Netzwerk oder Internet aufnehmen. Der Schutz durch die integrierten Firewall ist zwar besser als gar kein Schutz. Trotzdem sollte das System zusätzlich mit einer externen Firewall abgesichert werden, die auch ausgehende Daten kontrolliert, damit beide Richtungen abgesichert sind.

Standardmäßig ist die in Windows XP integrierte Firewall abgeschaltet. Unter Systemsteuerung/Netzwerk- und Internetverbindungen/Netzwerkverbindungen rechte Maustaste Eigenschaften Registrierkarte Erweitert sollte sie zugeschaltet werden.

6.4 Remote Zugriff

Bei der Remoteunterstützung wird einem bestimmten autorisierten Personenkreis gestattet, über das Web, auf den entfernten Computer zuzugreifen. Die Autorisierung der Remotebenutzer erfolgt in den Systemeinstellungen/Leistung und Wartung/System Registerkarte Remote unter Remotedesktop, Remotebenutzer auswählen.

Vorraussetzungen für einen Remote-Zugriff sind:

- Der Clientcomputer sowie der Remotecomputer müssen entweder Windows Messenger oder ein MAPI-kompatibles E-Mail-Konto, wie z. B. Microsoft Outlook oder Outlook Express, verwenden.
- Der Clientcomputer sowie der Remotecomputer müssen über eine Internetverbindung verfügen, während Sie die Remoteunterstützung verwenden.

Externe Firewalls können bei entsprechender Konfiguration die Remoteunterstützung verhindern.

Eine Anmeldung ohne Kennwort kann bei Windows XP nur direkt an der Konsole des physischen Computers erfolgen. Standardmäßig können Konten mit leeren Kennwörtern nicht mehr für eine Remoteanmeldung an dem Computer verwendet werden. Die Einschränkung, die eine Anmeldung über ein Netzwerk verhindert, kann aufgehoben werden, indem einem lokalen Konto ein Kennwort zugewiesen wird.

Remoteinstallation

Über die Remotinstallationsdienste kann Windows XP Professional auf einem Computer über das Netzwerk installiert werden. Der zu installierende Client-PC wird über eine bootfähige Netzwerkkarte oder eine spezielle Bootdiskette gestartet und kann nach der Verbindung mit dem RIS-Server (**R**emote **I**nstallation **S**ervices) mit Windows XP installiert werden.

Risiken eines Remotezugriffs

Schon allein die zusätzliche Schnittstelle gefährdet die Sicherheit und Zuverlässigkeit der Ressourcen, unabhängig vom verwendeten Remote System. Zum einen besteht eine erhöhte Virengefahr, zum anderen ein erhöhtes Risiko des Zugriffs durch unbefugte Benutzer auf das Unter-

nehmensnetzwerk. Neben der obligatorischen Authentisierung durch Benutzernamen und Passwort sollten unbedingt weitere Möglichkeiten zum Schutz der Ressourcen genutzt werden (z. B. Smartcards). Wichtig ist in diesem Zusammenhang auch der Schutz offen zugänglicher Telefonanschlüsse, die zum übertragen von Codes genutzt werden.

Ein Remotezugriff sollte nur dann eingerichtet werden, wenn dies zwingend erforderlich ist und nach Abwägung der damit verbundenen Risiken vertretbar ist.

6.5 Der Internet Explorer 6

Da der Internet Explorer 6 standardmäßig mit Windows XP ausgeliefert wird, folgt hier eine kurze Sicherheitsbetrachtung.

Der Internet Explorer unterteilt das Internet in Zonen, so dass jeder Web-Seite eine Zone mit einer geeigneten Sicherheitsstufe zugewiesen werden kann. Bei dem Versuch, Inhalte aus dem Web zu öffnen oder herunter zu laden, überprüft der Internet Explorer die Sicherheitseinstellungen für die Zone dieser Web-Seite. Das Einstellen der Internetoptionen erfolgt auf der Registrierkarte SICHERHEIT.

Es gibt vier verschiedene Zonen:

- Internet
- Lokales Intranet
- Vertrauenswürdige Sites
- Eingeschränkte Sites

Für jede Zone gibt es Sicherheitsstufen von „SEHR NIEDRIG“ bis „HOCH“ sowie „BENUTZERDEFINIERT“. Unter anderem lässt sich einstellen, ob aktive Inhalten ausgeführt werden dürfen. Da kaum nachvollzogen werden kann, welche Auswirkungen aktive Inhalte haben können, sollten sie grundsätzlich deaktiviert werden. Je mehr Sicherheitsfunktionen zur Minimierung Sicherheitsrisiken aktiviert werden, um so stärker können natürlich die Nutzmöglichkeiten einiger Websites eingeschränkt werden.

6.6 Cookies

Auf der Registerkarte DATENSCHUTZ können Sie das Verhalten des Internetexplorers gegenüber Cookies einstellen. Folgende Cookieeinstellungen sind verfügbar:

ALLE ANNEHMEN	Alle Cookies werden ohne Rückfrage akzeptiert.
NIEDRIG	Cookies, die nicht zur aufgerufenen Webseite passen, werden abgelehnt.
MITTEL	Cookies, die nicht zur aufgerufenen Webseite passen, werden abgelehnt. Außerdem werden Betreiber der Website gesperrt, wenn bekannt ist, dass diese persönliche Informationen verwenden.
MITTELHOCH	Cookies werden abgelehnt, wenn Drittanbieter, die nicht zur aufgerufenen Website passen, keine ausdrückliche Zustimmung des Benutzers anfordern.
HOCH	Ebenso wie MITTELHOCH, jedoch auch für den Betreiber der aufgerufenen Website selbst geltend.
ALLE SPERREN	Alle Cookies werden gesperrt.

Die automatische Verwaltung von Cookies sollte aus Sicherheitsgründen abgeschaltet werden.

7 Passport- der Weg zum gläsernen Internet-Surfer?

Um die Einwahl in verschieden Internetdienste zu vereinfachen, bietet Windows XP die Anmeldung über den Dienst „Passport“ an. Durch einen Passport kann dann ausschließlich durch Verwendung einer E-Mail-Adresse auf alle MSN Internetzugangs-Websites und anderen Dienste und Websites, die Passports unterstützen, zugegriffen werden. Passport implementiert einen Anmeldedienst, der es ermöglicht, mit einem Benutzernamen und einem Kennwort alle .NET-Passport-kompatiblen Dienste nutzen.

Die Nutzung von Passport ist aus datenschutzrechtlicher Sicht nicht unbedingt zu befürworten. Hier teilen sich alle Anbieter ein und dieselbe Datenbank, denselben Login-Mechanismus und dieselbe Sicherheitstechnik. Die Weiterleitung im Browser erfolgt ohne SSL, was bereits ausreicht, um in einen Account einzudringen.

Experten warnen davor, bei der Passport-Anmeldung die geforderten persönlichen Daten einzugeben. Damit könnte Microsoft jeden Computernutzer zusammen mit der eindeutigen 64-Bit-Nummer identifizieren. Sobald sich der Verbraucher bei einer Website anmeldet, die mit Microsoft kooperiert, wird seine Identifizierung an den Betreiber dieser Website übermittelt. Hinzu kommt, dass das Netz der über diesen Dienst zugänglichen Anbieter noch nicht sehr weit ausgebaut ist, so dass es sich für den Nutzer bisher kaum lohnt, diesen Dienst in Anspruch zu nehmen.

Wenn der Passport-Dienst nicht genutzt wird, stehen alle weiteren Funktionen von Windows XP uneingeschränkt zur Verfügung.

8 Gravierendes Sicherheitsleck: UPnP (Universal Plug and Play)

UPnP gehört zu den Innovationen, die den Umgang mit Hardware im Netzwerk vereinfachen sollen. Vernetzte Geräte teilen automatisch ihre Anwesenheit anderen UPnP-fähigen Geräten mit, die sich daraufhin bereitwillig auf die Zusammenarbeit einlassen. UPnP wird bei jeder Standard-Installation von Windows XP eingerichtet und aktiviert, und kann auch Microsofts früheren Betriebssystemversionen Windows 98, 98SE oder ME manuell hinzugefügt werden.

UPnP erfordert keinerlei Interaktion mit dem Benutzer. Aufgrund schwerwiegender Fehler in der UPnP-Implementierung in Windows XP kann ein Angreifer durch einen Puffer-Überlauf uneingeschränkte Kontrolle über das System erlangen, Daten lesen und löschen, Programme installieren und DDoS-Angriffe ausführen, sogar ohne in das System einzudringen. Von diesem Problem ist laut Microsoft jede Installation von Windows XP betroffen, denn die UPnP-Funktionalität ist standardmäßig aktiviert. Der Hersteller selbst veröffentlichte am 20. Dezember 2001 eine deutschsprachige Reparatursoftware für XP für diesen von unabhängigen IT-Sicherheitsforschern entdeckten Fehler.

Der von Microsoft zur Verfügung gestellte Patch kümmert sich jedoch lediglich um die Verwundbarkeit; UPnP wird dadurch nicht deinstalliert. Am sichersten ist es UPnP vollständig zu entfernen und die Ports 5000 und 1900 zu schließen.

9 Interne Sicherheit

9.1 SmartCards

Unter XP ist die Unterstützung von SmartCards direkt im Betriebssystem integriert. Die kleinen scheckkartengroßen Kärtchen eignen sich beispielsweise zum Speichern von Sicherheitszertifikaten, Anmeldekennwörtern, privaten Schlüsseln sowie anderen persönlichen Informationen. Im Gegensatz zu einem Kennwort wird die PIN, die den Zugriffsschutz zur SmartCard realisiert, niemals im Netzwerk weitergeleitet, und bietet somit einen höheren Schutz als ein herkömmliches Kennwort.

SmartCards lassen nur eine beschränkte Anzahl von fehlgeschlagenen Versuchen zur Eingabe der richtigen PIN zu. Dann werden sie gesperrt und funktionieren dann auch bei Eingabe der richtigen PIN nicht mehr. Der Benutzer muss sich zum Entsperren der Karte an den Systemadministrator wenden.

Vorteil bei der Verwendung dieser Technologie ist die stark vereinfachte Authentifizierungsprozedur, besonders wenn im Active Directory (siehe Punkt 11) die Anmeldung für verschiedenste Dienste zusammengefasst wird.

9.2 Integrierte „Sandbox“

Windows XP verfügt über eine integrierte „Sandbox“, um Anwendungen in einem geschützten Bereich ablaufen zu lassen und somit Manipulationen und Beschädigungen am System zu verhindern.

9.3 Windows-Dateischutz

Bei Windows-Versionen vor Windows 2000 war nicht auszuschließen, dass bei der Installation von Software, die zusätzlich zum Betriebssystem gebraucht wurde, freigegebene Systemdateien, z. B. Dynamic Link Libraries (DLL-Dateien) und ausführbare Dateien (EXE-Dateien), ohne jede Nachfrage überschrieben wurden. Wenn Systemdateien überschrieben werden, wird die Leistung des Systems unvorhersehbar, Programme können sich fehlerhaft verhalten und das Betriebssystem kann versagen.

In Windows 2000 und Windows XP verhindert der Windows-Dateischutz, dass geschützte Systemdateien, z. B. Dateien mit den Erweiterungen SYS, DLL, OCX, TTF, FON und EXE, überschrieben werden. Der Windows-Dateischutz wird im Hintergrund ausgeführt und schützt alle Dateien, die durch das Windows Setup-Programm installiert wurden. Der Windows-Dateischutz erkennt auch Versuche von anderen Programmen, eine geschützte Systemdatei zu ersetzen oder zu verschieben. Um festzustellen, ob es sich bei der neuen Datei um die korrekte Microsoft-Version handelt, wird ihre digitale Signatur vom Windows-Dateischutz überprüft. Falls die Datei nicht die korrekte Version aufweist, ersetzt der Windows-Dateischutz diese Datei entweder durch die Sicherungskopie, die im Ordner **Dllcache** gespeichert ist, oder durch die entsprechende Datei von der Windows-CD. Wenn der Windows-Dateischutz die entsprechende Datei nicht finden kann, werden Sie aufgefordert, den Speicherort anzugeben. Zusätzlich wird der versuchte Dateiaustausch vom Windows-Dateischutz im Ereignisprotokoll aufgezeichnet.

Der Windows-Dateischutz ist standardmäßig aktiviert und ermöglicht es, vorhandene Dateien durch digital signierte Windows-Dateien zu ersetzen. Derzeit werden signierte Dateien auf folgenden Wegen bereitgestellt:

- Windows Service Packs,
- Hotfix-Distributionen,
- Betriebssystemupdates,
- Windows-Aktualisierung,
- Windows Geräte-Manager/Klasseninstallationsprogramm.

9.4 Offline Dateien

Offline Dateien werden verwendet, um auf dem Netzwerk gespeicherte Dateien und Programme auch dann noch nutzen zu können, wenn keine Internetanbindung mehr besteht. Temporäre Offlinedateien werden auch als automatisch zwischengespeicherte Dateien bezeichnet. Diese freigegebenen Netzwerkdateien werden automatisch gespeichert. Diese Dateien müssen nicht gesondert offline verfügbar gemacht werden. Windows kann sie jederzeit von Ihrem lokalen Cache entfernen, wenn mehr Speicherplatz für weitere temporäre Dateien benötigt wird. Die freigegebenen Netzwerkdateien, die ausdrücklich offline verfügbar gemacht worden sind, stehen immer zur Verfügung. Diese Dateien werden erst dann vom Computer entfernt, wenn sie gelöscht werden. Wenn man sichergehen will, dass z. B. bei Übergabe eines Notebooks an eine andere Person keine Daten im Offline-Cache verbleiben, sollte der Cache gelöscht werden.

9.5 EFS (Encrypting File Systems)

Mit Hilfe von EFS können Daten auf der Festplatte vor unbefugtem Zugriff wirksam geschützt werden. Eine direkte Integration in den Windows Explorer gestattet die einfache Nutzung der Datenverschlüsselungsfunktion. Allein das Aktivieren des entsprechenden Kontrollkästchens reicht aus, um einen Ordner oder eine Datei verschlüsseln zu lassen. Dabei arbeitet der Dateisystemfilter des EFS völlig transparent, Ver- und Entschlüsselungsvorgänge laufen unsichtbar im Hintergrund ab.

Die verschlüsselte Datei kann nur noch durch die berechtigten Benutzer geöffnet, umbenannt, kopiert oder verschoben werden. Alle anderen Benutzer werden abgewiesen. Neu ist bei Windows XP, dass Sie mehr als einem Benutzer den Zugriff auf eine EFS-verschlüsselte Datei gestatten können.

Beim EFS wird die Datei zunächst symmetrisch mit einem FEK (File Encryption Key) verschlüsselt. Der FEK wird wiederum mit einem öffentlichen Schlüssel aus dem öffentlichen/privaten Schlüsselpaar des Anwenders verschlüsselt. Um eine Wiederherstellung verschlüsselter Daten auch ohne den privaten Schlüssel des Anwenders zu ermöglichen, z. B. nach Verlust des Schlüssels oder dem Ausscheiden eines Mitarbeiters, wird der FEK auch mit dem öffentlichen Schlüssel des öffentlichen/privaten Schlüssels des Wiederherstellungsagenten verschlüsselt. Entschlüsseln können diese Daten nur autorisierte Benutzer und designierte Wiederherstellungsagenten. Die Datei selbst kann auch vom Nutzer mit Administratorrechten nicht geöffnet werden, wenn er nicht als Wiederherstellungsagent bestimmt wurde.

Das Wiederherstellungsrecht besitzt unter Windows XP der Administrator standardmäßig. Für eine Sicherung der verschlüsselten Dateien vor dem Zugriff des Administrators kann das Wiederherstellungszertifikat des Administrators gelöscht werden. Dann sind die verschlüsselten Dateien eines Benutzers nur noch mit dessen Zertifikat entschlüsseln. Zusätzlich oder alternativ zu den genannten Administratoren können weitere Benutzer als Wiederherstellungs-Agenten bestimmt werden; dies geschieht durch Eintragen in der Sicherheitsrichtlinie unter Richtlinien öffentlicher Schlüssel/Agenten für Wiederherstellung verschlüsselter Daten. Als Wiederherstellungs-Agenten können nur einzelne Benutzer, nicht jedoch ganze Gruppen bestimmt werden. Zur Sicherheit sollten so wenig Wiederherstellungsagenten eingerichtet werden wie möglich.

Im Regelfall ist eine entsprechende Berechtigung ausreichend. In der verschlüsselten Datei kann der Benutzer unter Eigenschaften/erweitert/Details Verschlüsselungsdetails einsehen, Zugriffsrechte für weitere Benutzer festlegen und Informationen zum den Wiederherstellungsagenten erhalten.

Alle EFS-Vorgänge werden auf dem Computer ausgeführt, auf dem sie gespeichert sind. Beim Kopieren einer verschlüsselten Datei über das Netzwerk wird sie entschlüsselt und im Zielordner wieder verschlüsselt. Sie ist damit auf dem Transportweg über das lokale Netzwerk oder die Datenfernverbindung prinzipiell lesbar. Für einen sicheren Netztransfer sollte deshalb beispielsweise IPSec genutzt werden (siehe Punkt 6.2.2).

10 ASR (Automated System Recovery)

In regelmäßigen Abständen sollten zur eigenen Sicherheit automatische Systemwiederherstellungssätze im Rahmen eines Gesamtplanes zur Systemwiederherstellung bei Systemversagen erstellt werden.

ASR ist ein zweiteiliges Wiederherstellungssystem, das aus den Teilen ASR-Sicherung und ASR-Wiederherstellung besteht. Die Sicherung erfolgt durch den Assistenten für die automatische Systemwiederherstellung, der im Sicherungsdienstprogramm zu finden ist. Der Assistent sichert Systemstatus, Systemdienste und alle mit den Betriebssystemkomponenten verknüpften Datenträger. Er erstellt auch eine Datei mit Informationen zur Sicherung, zur Datenträgerkonfigurationen (einschließlich Basisvolumes und dynamischer Volumes) und zur Durchführung einer Wiederherstellung.

Die automatische Systemwiederherstellung sollte erst als letztes Mittel zur Systemwiederherstellung eingesetzt werden, wenn andere Möglichkeiten, wie Starten im abgesicherten Modus und Wiederherstellen der letzten als funktionierend bekannten Konfiguration, nicht greifen.

Um Datenverluste zu vermeiden, sollten Dateien, die nicht dem von Microsoft vorgeschriebenen Dateitypen entsprechen bzw. nicht in den von Microsoft dargebotenen Verzeichnissen gespeichert werden, auf einer anderen Partition gespeichert werden, die dann von der Wiederherstellung ausgenommen wird.

11 Active Directory

Active Directory ist ein Verzeichnisdienst, der Informationen zu Objekten und Subjekten in einem Netzwerk speichert, und diese Informationen Benutzern und Netzwerkadministratoren zur Verfügung stellt. Active Directory ermöglicht Netzwerkbenutzern über einen einzigen Anmeldevorgang den Zugriff auf zugelassene Ressourcen im gesamten Netzwerk. Es stellt Netzwerkadministratoren eine anschauliche, hierarchische Ansicht des Netzwerkes und einen einzigen Verwaltungspunkt für alle Netzwerkobjekte zur Verfügung.

Zur Pflege des Directorys gehören das Erstellen, Löschen, Ändern und Verschieben von Objekten sowie das Festlegen von Berechtigungen für Objekte, die im Verzeichnis gespeichert sind. Diese Objekte umfassen Organisationseinheiten, Benutzer, Kontakte, Gruppen, Computer, Drucker und freigegebene Dateiobjekte. Für die Wahrung der Sicherheit im Active Directory sollte die entsprechende primäre Netzwerkanmeldung mit den betreffenden Gruppenrichtlinien abgestimmt sein.

Die dem Active Directory (AD) zugrunde liegenden Überlegungen führen mitunter zu sehr umfassende AD-Strukturen. So werden in zunehmendem Maße landesweite, ressortübergreifenden AD angelegt. Dabei können Client-Server-Systeme, die bislang unabhängig voneinander zum

Teil von der Verwaltung und zum Teil auch von externen Dienstleistern administriert wurden, in einer Administrationsstruktur zusammengefasst werden. Die Active Directory Technik sieht standardmäßig die Rolle der so genannter Enterprise-Administratoren vor. Diese haben Administrationsberechtigungen für das gesamte AD. Damit können die Enterprise-Administratoren auf sämtliche Daten zugreifen, die in den angeschlossenen Client-Server-Systemen gespeichert sind. Zwar kann man die damit verbundenen Zugriffsberechtigungen einschränken, jedoch können sich die Enterprise-Administratoren die entsprechenden Zugriffsberechtigungen jederzeit wieder selbst gewähren. Es ist daher notwendig, die Nutzung der „allmächtigen“ Enterprise-Administrator-Kennungen einzugrenzen. Dazu bieten sich mehrere Ansatzpunkte:

- Verzicht auf „integrative“ AD, in denen bislang separat administrierte Client-Server-Systeme zusammengefasst werden,
- möglichst weitgehender Verzicht auf Enterprise-Administrator-Kennungen im Tagesbetrieb; stattdessen werden dafür Kennungen mit (beschränkten) Administrationsrechten verwendet; ob die damit einhergehenden funktionalen Beschränkungen tragbar sind, ist von Fall zu Fall zu entscheiden,
- sollen nur zwei bislang unabhängig voneinander administrierte Client-Server-Systeme in einem AD zusammengefasst werden, kann als organisatorische Maßnahme die Nutzung der Enterprise-Administrator-Kennung nach dem Vier-Augen-Prinzip in Betracht kommen.

12 Sicherheitsempfehlungen

Nutzer sollten der Benutzergruppe für Remotedesktop auf dem eigenen Computer angehören. Sie müssen keinesfalls als Administrator angemeldet sein, um Remotezugriff auf den Computer zu haben. Standardnutzer sollten prinzipiell nicht der Gruppe **Administratoren** angehören und den Computer nicht als Administrator starten, es sei denn, sie müssen Aufgaben wahrnehmen, für die Administratorrechte erforderlich sind. Für die meisten Computeraufgaben reicht jedoch die Mitgliedschaft in der Gruppe **Benutzer** oder **Hauptbenutzer**. Wenn jedoch eine administratorspezifische Aufgabe ausgeführt werden muss, sollte man sich so kurzzeitig wie möglich als Administrator anmelden, und sofort nach der Erledigung der entsprechenden Aufgabe abmelden.

Alle Remotedesktopbenutzer sollten sich nur mit einem sicheren Kennwort anmelden. Dies ist besonders wichtig, wenn Ihr Computer direkt über ein Kabelmodem oder eine DSL-Verbindung an das Internet angeschlossen ist.

12.1 Warum man sich an seinem Computer nicht standardmäßig als Administrator anmelden sollte

Wenn Windows 2000 oder Windows XP mit Administratorrechten gestartet wird, ist das System besonders hohen Sicherheitsrisiken ausgesetzt. Viren oder trojanische Pferde könnten auf dem System dann wesentlich schwerwiegendere Probleme verursachen, als bei einer weniger hoch privilegierten Anmeldung.

Wenn man sich als Mitglied der Gruppe **Benutzer** anmeldet, kann man bereits sehr viele Routineaufgaben durchführen, wie das Ausführen von Programmen und das Besuchen von Internetseiten, ohne den Computer einem unnötigen Risiko auszusetzen. Als Mitglied der Gruppe **Hauptbenutzer** können neben diesen Routineaufgaben auch Programme installiert, Drucker hinzugefügt und die meisten Programme der Systemsteuerung verwendet werden. Administra-

toraufgaben, wie das Aktualisieren des Betriebssystems oder das Konfigurieren von Systemparametern, können dann nur durchgeführt werden, nachdem sich der Anwender als Standardnutzer abgemeldet und erneut als Administrator anmeldet hat.

12.2 Tipps zum Testen der Systemsicherheit

Mit einem simulierten Angriff von außen können Sicherheitseinstellungen des Systems schnell getestet werden. Bevor man mit der Konfiguration beginnt, sollte beispielsweise folgende Website besucht werden: https://grc.com/x/ne.dll?bh0bkyd2 (Testseite der Gibson Research Corporation). Auf dieser Seite kann mit den Funktionen „TEST MY SHIELDS“ oder “PROBE MY PORTS“ die Sicherheit des Systems getestet werden. Der gesamte Test dauert – über eine DSL-Verbindung – nur wenige Sekunden. Genauso schnell wäre bei entsprechender Fehlkonfiguration auch ein Angreifer über alle Schwachstellen des Systems im Bilde. Der Test eignet sich auch gut zur Kontrolle der Protokollierungsfunktion der Firewall, da die IP-Adressen, von denen der simulierte Angriff erfolgt, offen gelegt werden. Dadurch ist gut nachvollziehbar, wann die Aktion vom berechtigten Nutzer ausgelöst und welche Wirkung erzielt wurde.

Weitere Hinweise zu Selbsttests sind auch beim „Landesbeauftragten für den Datenschutz Niedersachsen“ unter www.lfd.niedersachsen.de/service/service_selbstt.html/ oder beim Schweizer Datenschutzbeauftragten unter www.datenschutz.ch zu erhalten.

13 Windows XP Home

Um die Sicherheit der Version XP Home einschätzen zu können, sollte man wissen, dass die folgenden im vorangegangenen Text beschriebenen Merkmale nicht zur Verfügung stehen:

- EFS
- Kerberos
- IPSec
- Internet Information Server
- Remotedesktop
- Automatische Installation
- Remotinstallationsdienste
- Offline-Dateien und Ordner
- Gruppenrichtlinien
- Managementkonsole

14 Der Windows XP Media Player

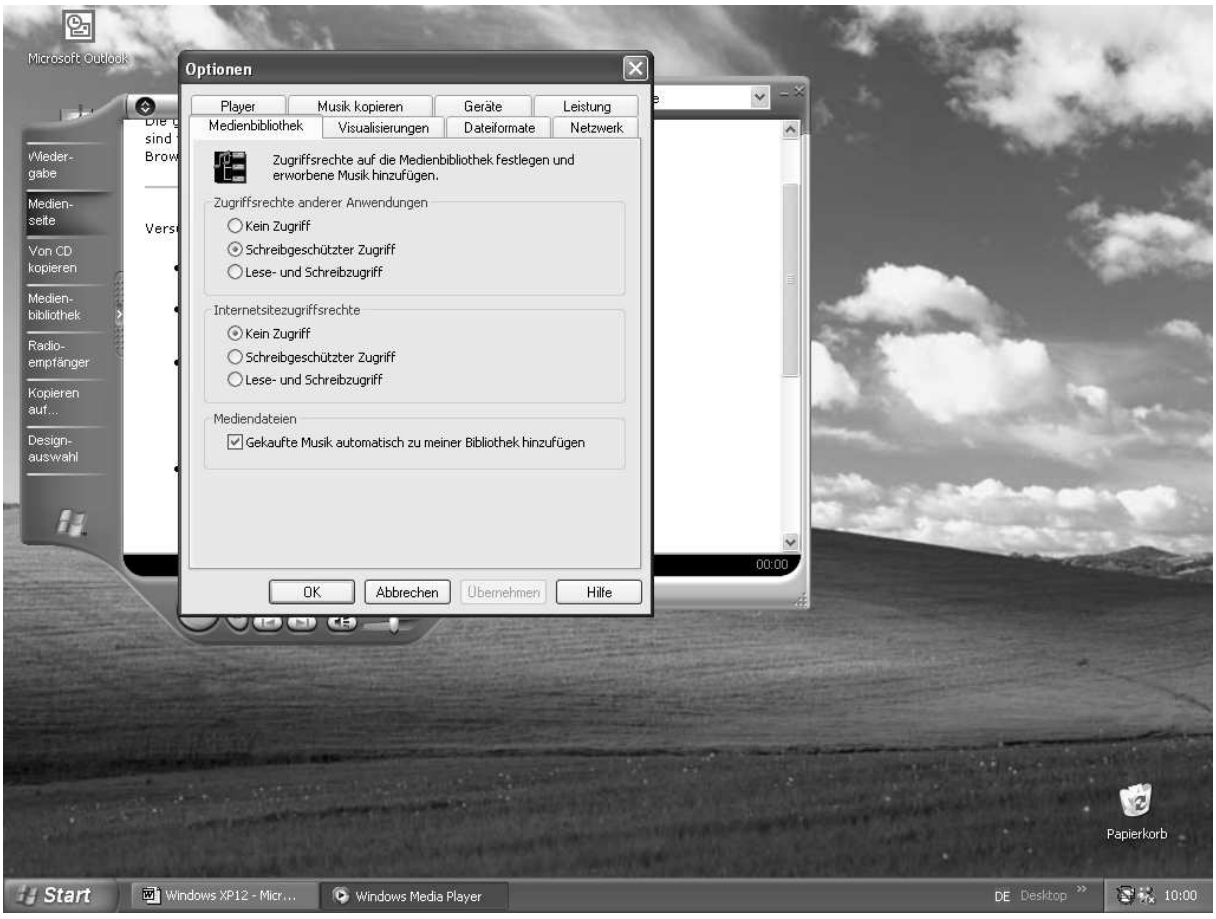
Der Media Player dient der Wiedergabe vielfältiger Sound- und Videoformate. Der Einsatz des XP Media-Players bietet Microsoft die Möglichkeit, über die Internetverbindung seinen Nutzer zu identifizieren. Microsofts Mediaplayer für Windows XP verrät, welcher Anwender welche Musikstücke und Videos abspielt. Die Software identifiziert zugleich mit dem Anmeldenamen des jeweiligen Windows-Benutzers die abgespielten Stücke, und schreibt diese Informationen hinter dem Rücken des Anwenders in eine Logdatei auf die Festplatte. Das geht einen Schritt weiter als etwa Office-Programme, die sich maximal neun zuletzt bearbeitete Dokumente merken, um dem Anwender das wiederholte Eintippen von Dateinamen zu ersparen.

14.1 Welche Daten erhält Microsoft tatsächlich?

Der Multimediaplayer zieht sich aus dem Netz die Angaben zum gespielten Titel und zum entsprechenden Künstler. Gleichzeitig verschickt das Programm die Medien-ID der eingelegten CD, den der Mediaplayer von der CD ausliest, sowie die Identifikationsnummer des installierten Mediaplayers. Die Übermittlung der Identifikationsnummer gibt zunächst keine Auskunft über den Benutzer und verstößt somit nicht gegen Datenschutzauflagen. Bedenklich ist jedoch, dass dieselbe Identifikationsnummer z. B. bei der Anmeldung für den Windows Media Newsletter zusammen mit Name und E-Mail Adresse genutzt wird, und auf diesem Wege sehr wohl personenbezogene Daten preisgibt.

Microsoft Sprecher Jonathan Usher erklärte, der Konzern plane derzeit nicht, gesammelte Daten über die Seh- und Hörgewohnheiten von Kunden zu vermarkten, wolle das aber für die Zukunft auch nicht ausschließen. Vor diesem Hintergrund sollte die Nutzung eines anderen Players erwogen werden. Wer nicht auf den Multimediaplayer von Windows XP verzichten will oder kann, sollte wenigstens die CD-Datenbankabfrage deaktivieren. Allerdings kann der Benutzer erst dann wieder im Internet surfen, wenn diese Einstellung aufgehoben ist. Sicherheit vor ungewollter Datenübertragung bietet da nur das Abschalten des Internetzugriffsrechts unter Extras/Optionen/Medienbibliothek (siehe Abb. 5)

Abb.5



15 Fazit

Bisher gibt es zum Thema XP sehr viele widersprüchliche Aussagen. Es ist nicht völlig klar, welche Daten tatsächlich an Microsoft übertragen werden und ob sich aus diesen Daten Nutzungsprofile der Anwender erstellen lassen. Deshalb sollte insbesondere bei der Nutzung des Internet sorgfältig zwischen einer höheren Benutzerfreundlichkeit und Einbußen bei der Sicherheit abgewogen werden.

Die Vielfalt, mit der das Betriebssystem versucht, mit dem Hersteller Kontakt aufzunehmen, macht es schwierig, wirklich alle risikobehafteten Funktionen abzuschalten und dabei noch effizient zu arbeiten. Natürlich wird die Sicherheit beim Nutzen von Windows XP größer, wenn der Zugang zum Internet völlig gesperrt wird. Aber gerade die enge Verknüpfung mit dem Internet soll ja den Vorteil gegenüber älteren Systemen ausmachen.

Die enge Verzahnung mit der vielfältigen Nutzung des Internets und mit dem Active Directory führen dazu, dass sich beim Einsatz von Windows XP komplexe datenschutzrechtliche Problemstellungen ergeben können, für die vor dem Einsatz von Windows XP angemessene Lösungen gefunden werden müssen. Bei der Einsatzplanung von Windows XP wird deshalb die Erstellung eines Sicherheitskonzepts empfohlen.

Quellen

Der Hamburgische Datenschutzbeauftragte: Datenschutz bei Windows 2000, 2002.

Uwe Brünning, Jörg Krause - Windows XP Professional - Carl Hanser Verlag

http://www:heise.de/newsticker/data/hps-21.02.02-000/ Verlag Heinz Heise, 2002.

http://www.microsoft.com/windows/windowsmedia/windowsxpwhatsnew.asp

http://www.sun.de/SunPR/Pressemitteilungen/2001/PM01

Martins/Kobylinska -„Auf IP-Nummer sicher“,“Sicherheit an Bord“- PC INTERN 02/02