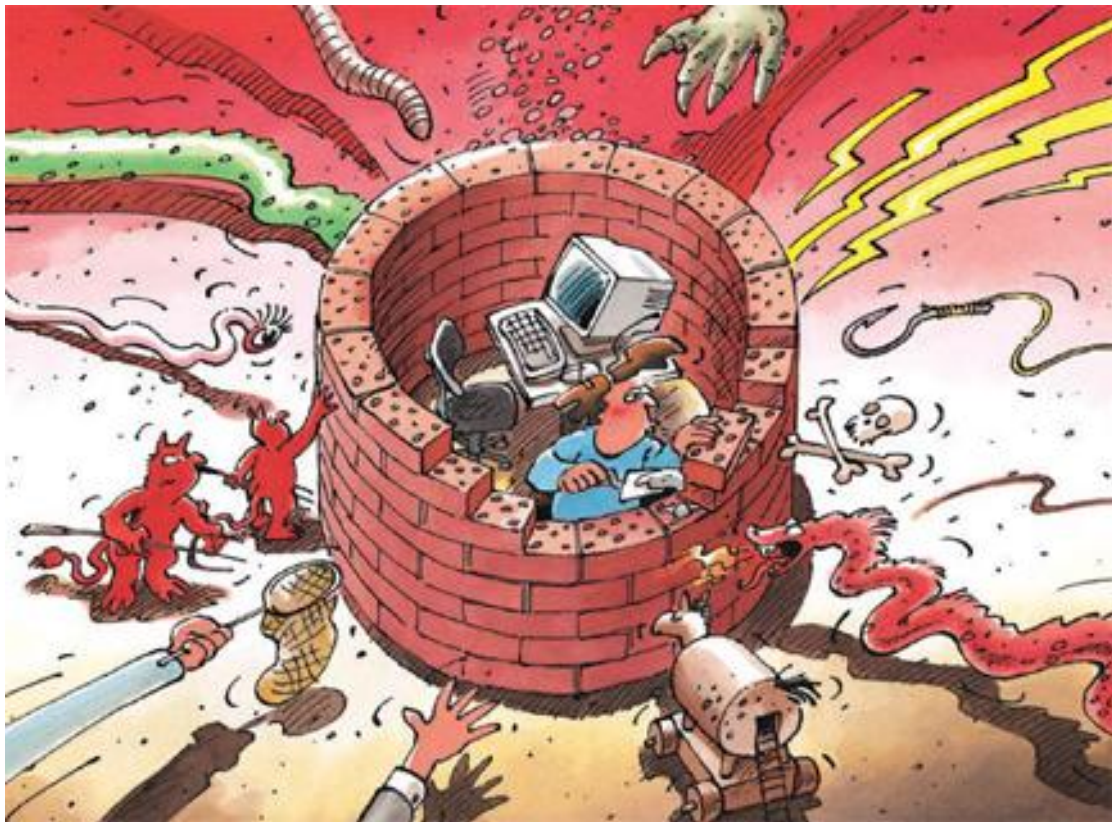


Sicherheitseinstellungen für Windows XP

Dokument verfügbar unter: www.melani.admin.ch



Checkliste „Sicherheitseinstellungen für Windows XP“

Die einzelnen Punkte sind auf den nachfolgenden Seiten Schritt für Schritt erklärt.

Personal Firewall

Überprüfen Sie regelmässig, ob die bei Windows XP vorhandene Firewall aktiviert ist und lassen Sie keine Ausnahmen zu. Dies lässt sich über den entsprechenden Punkt im Sicherheitscenter kontrollieren und umsetzen (*Systemsteuerung* → *Sicherheitscenter* → *Windows-Firewall*)

Software Updates

Aktivieren Sie die automatische Updatefunktion, deren Konfigurationsmenü ebenfalls über das Sicherheitscenter zugänglich ist (*Systemsteuerung* → *Sicherheitscenter* → *Automatische Updates*).

Vergessen Sie nicht, übrige Software (z.B. MS Office, Audio Player, usw.) ebenfalls regelmässig zu aktualisieren.

Antiviren-Software

Stellen Sie sicher, dass eine Antiviren-Software installiert ist und halten Sie diese über die automatische Updatefunktion aktuell.

Verwaltung von Benutzerkonten

Versehen Sie sämtliche Benutzerkonten mit einem starken Passwort.

Datensicherung

Führen Sie regelmässige Datensicherungen auf externe Speichermedien durch und versuchen Sie von Zeit zu Zeit, ob die Daten wieder hergestellt werden können.

Bewahren Sie die Speichermedien an einem sicheren Ort auf.

INHALT

<u>EINLEITUNG</u>	1
<u>GRUNDSCHUTZ</u>	2
PERSONAL FIREWALL	2
SOFTWARE UPDATES	3
ANTIVIREN-SOFTWARE (SCHUTZ VOR MALICIOUS CODE)	4
INTERNETOPTIONEN	5
VERWALTUNG VON BENUTZERKONTEN	7
WINDOWS XP HOME	7
WINDOWS XP PROFESSIONAL	9
DATENSICHERUNG	11
<u>ZUSÄTZLICHE SICHERHEITSEINSTELLUNGEN</u>	12
ANMELDEOPTIONEN	12
LOKALE SICHERHEITSEINSTELLUNGEN UNTER WINDOWS XP PROFESSIONAL	13
KENNWORTRICHTLINIEN	13
KONTOSPERRUNGSRICHTLINIEN	15
ÜBERWACHUNGSRICHTLINIEN	16
ZUWEISEN VON BENUTZERRECHTEN	16
SICHERHEITSOPTIONEN	17
DIENSTE	17
KONTROLLE UND EINSCHRÄNKEN VON AUSGEHENDEN VERBINDUNGEN	17
DATENVERSCHLÜSSELUNG UNTER WINDOWS XP PROFESSIONAL	18
DATEI- UND DRUCKERFREIGABE DEAKTIVIEREN	19
DESKTOPSPERRUNG UND BILDSCHIRMSCHONER	21
<u>ÜBERPRÜFUNG DER SYSTEMSICHERHEIT MIT HILFE VON TOOLS</u>	21
MICROSOFT BASELINE SECURITY ANALYZER (MBSA)	21
ENTDECKEN UND ENTFERNEN VON SPY- UND ADWARE	22
<u>REFERENZEN UND WEITERFÜHRENDE LINKS</u>	23
<u>ANHANG A: ERMITTELN DES INSTALLIERTEN SERVICE PACKS</u>	24
<u>ANHANG B: INFORMATIONEN ÜBER DAS FILESYSTEM ANZEIGEN</u>	24

Einleitung

Durch befolgen einiger weniger Massnahmen und Verhaltensregeln ist Ihr Windows XP System bereits gut vor unautorisierten Zugriffen und vor den Auswirkungen von Viren, Wurmern und Trojanischen Pferden geschützt. Diese Massnahmen umfassen

- Personal Firewall
- Software Updates
- Antiviren-Software
- Datensicherung

und werden im ersten Kapitel „Grundschutz“ beschrieben. Das daran anschliessende Kapitel "Zusätzliche Sicherheitseinstellungen" richtet sich an den erfahrenen Windows-Benutzer. Die dort aufgeführten Empfehlungen tragen dazu bei, die Systemicherheit über den Grundschutz hinaus zu erhöhen.

Wichtige Hinweise:

- Windows XP gibt es in einer Home Edition und einer Professional Edition. Die beiden Versionen unterscheiden sich in einigen Punkten. Die vorliegende Anleitung trägt diesem Umstand so weit als möglich Rechnung.
- Dieses Dokument gilt ausschliesslich für Windows XP Systeme, die nicht Bestandteil einer Windows-Domäne sind. Dies ist bei Privatanwendern stets der Fall.
- Es wird ferner davon ausgegangen, dass sich das Windows XP System auf dem aktuellen Stand bezüglich des Service Packs (derzeit SP2) sowie allfälliger Sicherheits-Updates befindet¹ und dass es sich beim Filesystem um NTFS² handelt.

¹ Wie dies überprüft werden kann, wird im „Anhang A: Ermitteln des installierten Service Packs“ aufgezeigt.

² Wie dies überprüft werden kann, wird im „Anhang B: Informationen über das Filesystem anzeigen“ aufgezeigt.

Grundschutz

Windows XP ist das derzeit aktuellste Client-Betriebssystem von Microsoft. Mit dem Service Pack 2 (SP2) wurde das Sicherheitscenter mit den drei Schwerpunkten *Firewall*, *Automatische Updates* und *Virenschutz* hinzugefügt. Die Benutzeroberfläche ist über den Menüpunkt „Systemsteuerung → Sicherheitscenter“ erreichbar.

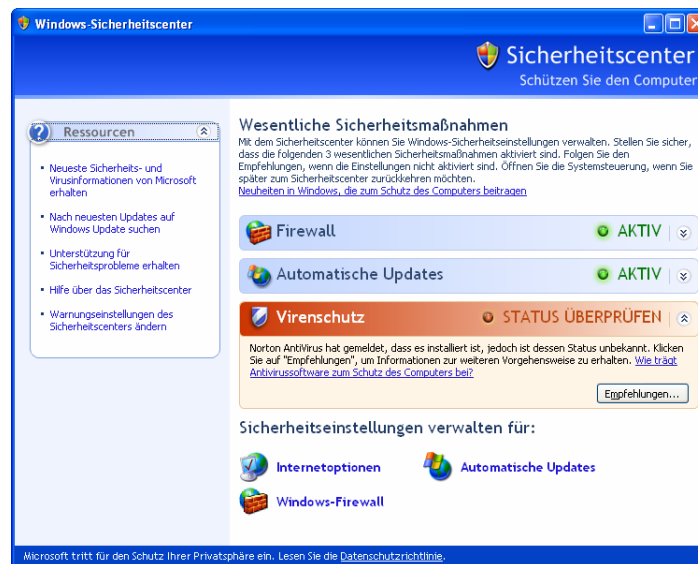


Abbildung 1: Das Windows Sicherheitscenter

Auf die einzelnen Punkte des Sicherheitscenters und seine Funktionen wird auf den folgenden Seiten eingegangen.

Personal Firewall

Eine Personal Firewall schützt ein Computersystem, indem sie ein- und eventuell auch ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Die Entscheidung darüber erfolgt anhand einfacher Regeln, die bei jedem Verbindungsaufbau konsultiert werden.

Mit dem Einspielen des Service Packs 2 wird die in Windows XP integrierte Firewall standardmässig aktiviert. Das Konfigurationsmenü der Windows-Firewall kann über das Sicherheitscenter (siehe Abbildung 1) erreicht werden. Über die drei Register „Allgemein“, „Ausnahmen“ und „Erweitert“ lassen sich die gewünschten Einstellungen vornehmen (siehe Abbildung 2).

- Überprüfen Sie im Register „Allgemein“, ob der Punkt „Aktiv“ im Fenster von Abbildung 2 markiert ist und setzen Sie ein Häkchen bei „Keine Ausnahmen zulassen“.

Erfahrene Benutzer können benötigte Dienste unter dem Register „Ausnahmen“ freischalten, falls zum Beispiel Dienste wie Datei- und Druckerfreigabe verwendet werden.

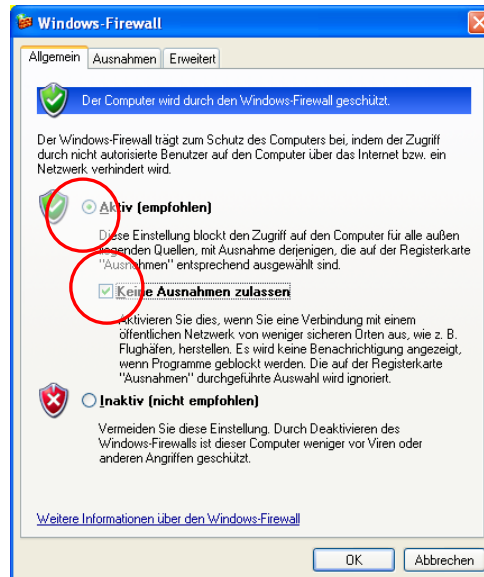


Abbildung 2: Konfiguration der Windows-Firewall

Wichtiger Hinweis: Die Windows-Firewall ermöglicht nur die Kontrolle von eingehenden Verbindungen. Vom System ausgehende Verbindungen lassen sich so nicht kontrollieren und überwachen! Weitere Informationen dazu sind im Abschnitt „Kontrolle und Einschränkungen von ausgehenden Verbindungen“ auf [Seite 17](#) aufgeführt.

Software Updates

Sicherheitslücken können unrechtmässige Zugriffe auf Daten oder die Ausbreitung von Würmern ermöglichen und sind sowohl in Betriebssystemen (z.B. Windows XP, Windows 2000, Mac OS X, Linux usw.) wie auch in Anwendungen (z.B. Internet Explorer, Media Player usw.) vorhanden. Um die Sicherheit Ihrer Daten (und der anderen Internet-Nutzer) zu erhöhen, kommt dem regelmässigen Einspielen von Sicherheits-Updates, welche diese Sicherheitslücken schliessen, eine grosse Bedeutung zu.

Die automatische Updatefunktion von Windows XP lässt sich ebenfalls über das Sicherheitscenter vornehmen und sollte unbedingt aktiviert werden (siehe Abbildung 3). Beachten Sie, dass diese Updatefunktion nur das Betriebssystem, den Internet Explorer, den Media Player usw. abdeckt, nicht aber MS Office (Word, Excel, PowerPoint, Access, Outlook). Diese Updates müssen separat über die Webseite von Microsoft eingespielt werden, die Sie zu diesem Zweck regelmässig konsultieren sollten:

<http://office.microsoft.com/de-de/officeupdate/default.aspx>

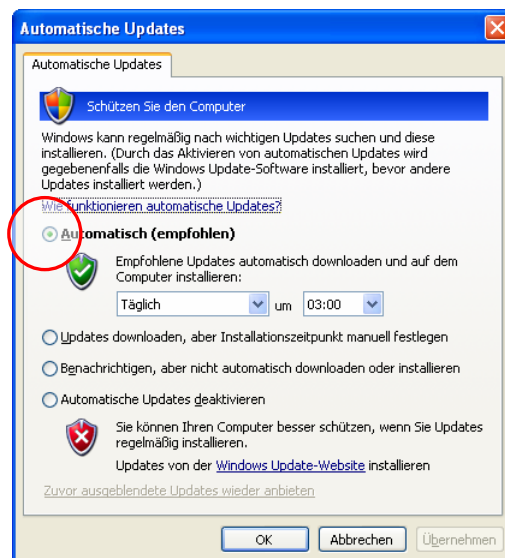


Abbildung 3: Automatisches Softwareupdate

Neben dem Betriebssystem und den Office-Anwendungen sind auch Softwareprodukte von Drittanbietern (z.B. Entpacksoftware, Dokument Reader usw.) periodisch auf deren Aktualität hin zu prüfen. Bei denjenigen Programmen, die über keine automatische Updatefunktion verfügen, sind regelmässige Besuche der entsprechenden Hersteller-Webseite empfehlenswert.

Antiviren-Software (Schutz vor Malicious Code)

Malicious Code ist der Oberbegriff für Software, die schädliche Funktionen auf einem System ausführt. Dieser Gruppe gehören neben Viren unter anderem auch Würmer und Trojanische Pferde an. Detaillierte Informationen zu diesen Begriffen sind auf der Webseite von MELANI unter dem folgenden Link zu finden:

<http://www.melani.admin.ch/themen/00103/index.html?lang=de>

Sorgen Sie unbedingt dafür, dass eine aktuelle Antiviren-Software auf Ihrem System vorhanden ist. Diese schützt nicht nur die Daten auf Ihrem System, sondern auch Systeme und Daten anderer Internetnutzer. Beispielsweise erfolgt das Versenden von Spam vielfach über unzureichend geschützte Systeme, ohne dass der Benutzer etwas davon bemerkt. Mit einem aktuellen Virenschutz werden auch solche Gefahren minimiert.

Windows XP versucht, die installierte Antiviren-Software zu erkennen und deren Aktualität zu prüfen. Scheitert dieser Versuch oder ist der Virenschutz nicht auf dem aktuellsten Stand beziehungsweise nicht vorhanden, wird dies dem Benutzer durch ein Symbol in der Taskleiste angezeigt und der Menüpunkt „Virenschutz“ im Sicherheitscenter rot hervorgehoben (Abbildung 4).

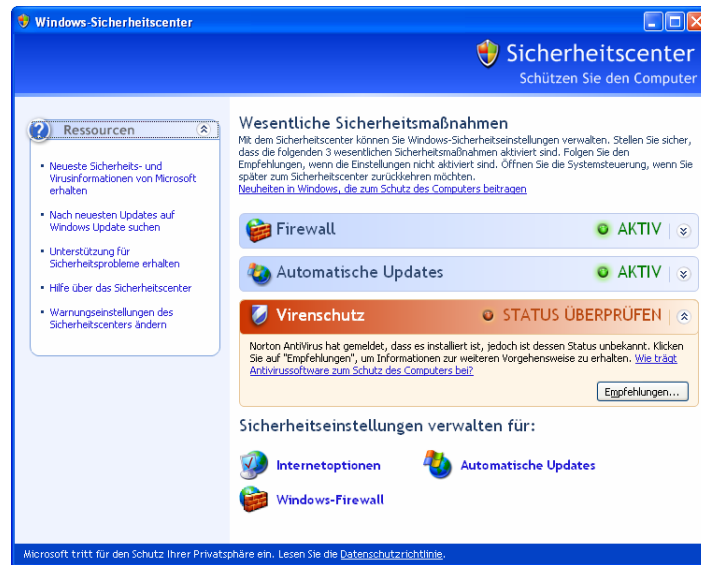


Abbildung 4: Fehlender Virenschutz wird erkannt (rot hervorgehoben)

Besorgen Sie sich in diesem Fall umgehend eine Antiviren-Software und halten Sie diese über die automatische Updatefunktion aktuell. Eine Auswahl solcher Schutzprogramme finden Sie unter folgendem Link:

http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de#sprungmarke0_4

Internetoptionen

Die Internetoptionen sind ebenfalls über das Windows Sicherheitscenter zugänglich (siehe Abbildung 4 unten links). Wählen Sie das Register „Sicherheit“ (siehe Abbildung 5, links):

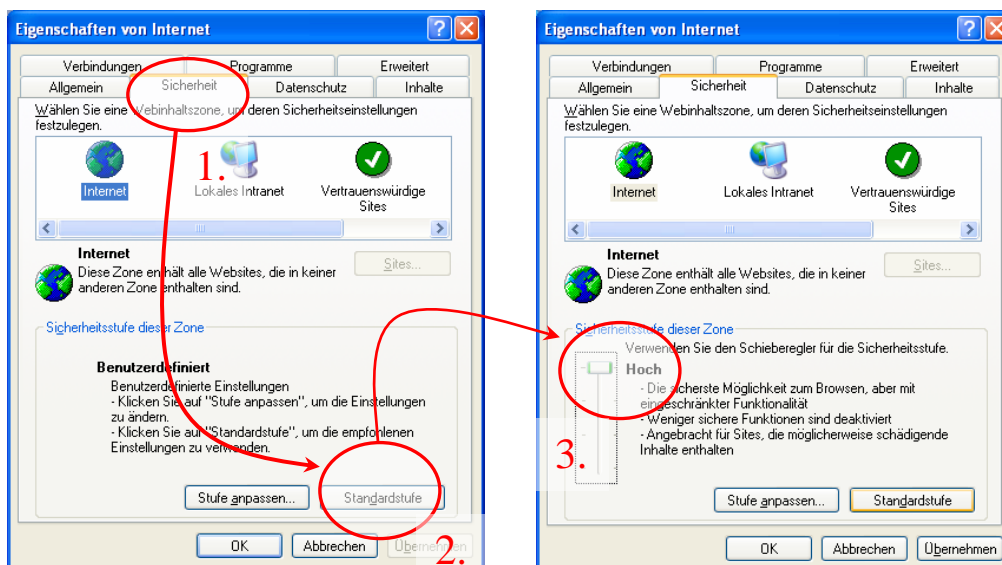


Abbildung 5: Register "Sicherheit"

Wählen Sie für die Zone „Internet“ die Standardstufe „Hoch“. Dies lässt sich unter dem Punkt „Standardstufe“ durch Verschiebung des Reglers erreichen. Wählen Sie anschliessend für die Zone „Vertrauenswürdige Sites“ die Standardstufe „Sehr niedrig“ und klicken Sie auf „Sites...“. Es öffnet sich ein Fenster wie in Abbildung 6.



Abbildung 6: Definieren von vertrauenswürdigen Webseiten

Entfernen Sie das Häkchen bei der Option „Für Sites dieser Zone ist eine Serverüberprüfung erforderlich“. Tragen Sie hier die Homepage Ihrer Online-Bank (z.B. <https://ihreonlinebank.ch>) und die Windows-Update Homepage (*.update.microsoft.com , *.windowsupdate.microsoft.com und *.windowsupdate.com) ein. Geben Sie dazu zuerst im oberen Feld die Adresse ein und klicken Sie anschliessend auf „Hinzufügen“. Achten Sie auf die exakte Schreibweise. Wenn die Übermittlung über eine sichere Verbindung abgewickelt wird, muss der Adresse dementsprechend <https://> vorangestellt werden. Das Zeichen * kann als Platzhalter eingesetzt werden.

Hinweis: Sollten nach diesen Einstellungen gewisse Homepages nicht mehr korrekt angezeigt werden, lässt sich dies durch eine vorübergehende Herabsetzung der Standardsicherheitsstufe für die Zone „Internet“ auf „Mittel“ anpassen. Vergessen Sie nicht, nach dem Besuch der jeweiligen Homepage die Stufe wieder auf „Hoch“ zu stellen.

Verwaltung von Benutzerkonten

Windows XP Home

Während der Installation von Windows XP Home muss ein Benutzerkonto erstellt werden. Dieses und alle später eingerichteten Benutzer besitzen standardmässig Administratoren-Rechte und sind mit keinem Passwort geschützt! Dies ist ein Sicherheitsrisiko, das umgehend behoben werden sollte. Starten Sie die Benutzerverwaltung „Systemsteuerung → Benutzerkonten“; es erscheint ein Fenster wie in Abbildung 7.

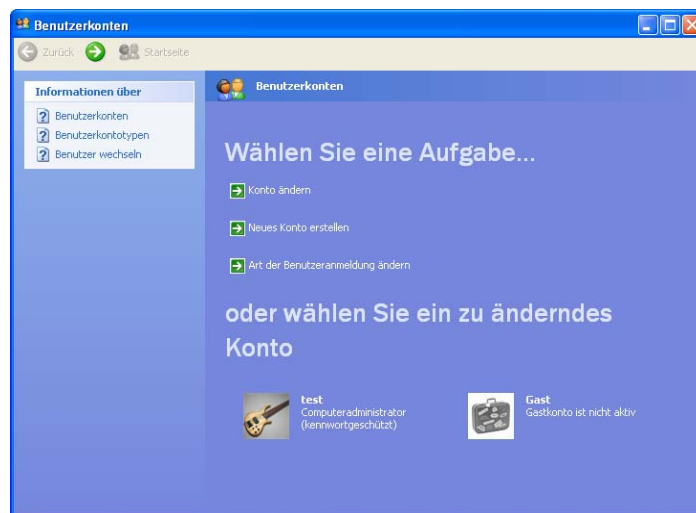


Abbildung 7: Eingerichtete Benutzer

- Kontrollieren sie zuerst, ob das Gastkonto deaktiviert ist. Falls nein, deaktivieren Sie dieses.
- Setzen Sie anschliessend für jeden Benutzer ein Passwort. Klicken Sie dazu auf das entsprechende Konto, worauf sich ein Fenster wie in Abbildung 8 öffnet.
- Klicken Sie auf „Eigene Kennwort ändern“ (siehe Abbildung 9).

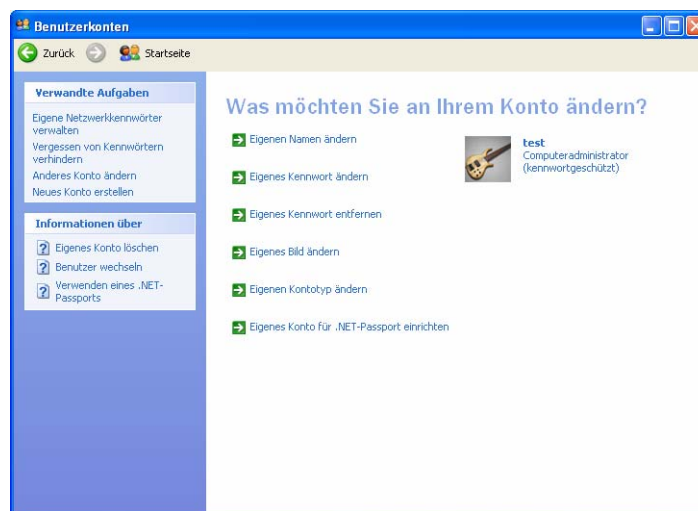


Abbildung 8: Eigenschaften des Benutzerkontos "test"

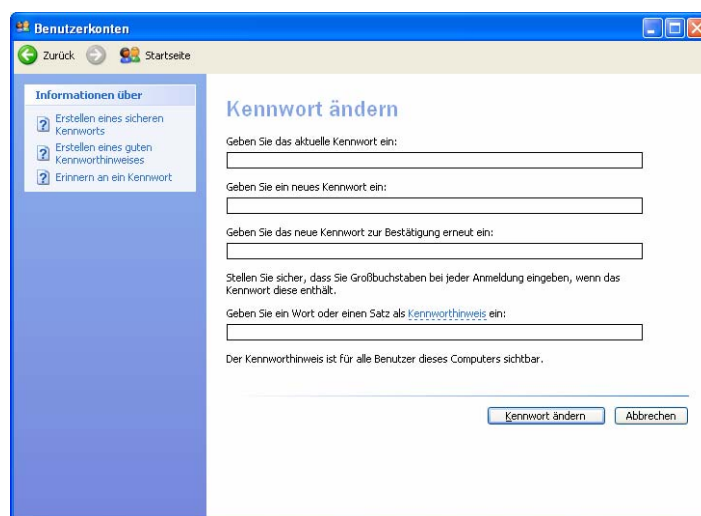


Abbildung 9: Setzen eines Passwortes für das Benutzerkonto "test"

Da standardmässig kein Passwort gesetzt wurde, kann das erste Feld leer gelassen werden. Vergeben Sie für jedes Benutzerkonto ein schwer zu erratendes Passwort und vermeiden Sie es, dieses aufzuschreiben. Beachten Sie bei der Wahl eines Passwortes folgende Grundsätze:

- Passwort sollte aus Buchstaben, Zahlen und Sonderzeichen bestehen
- Mindestlänge sollte 8 Zeichen nicht unterschreiten
- Passwörter sind regelmässig zu wechseln (ca. alle 3 Monate)

Nutzen Sie Eselsbrücken bei der Passwortwahl. Ein Beispiel:

Ausgangswort:	hallihallo
Gross/Kleinschreibung:	HalliHallo
Einbringen von Zahlen :	Hall1Hall0
Einbringen von Sonderzeichen:	H@ll1H@ll0

Nutzen Sie für verschiedene Zwecke (wie z.B. e-Banking, Ihren Rechner, weitere On-line-Dienste) jeweils auch verschiedene Passworte.

Zusätzlich zu den von Ihnen eingerichteten Benutzerkonten befindet sich ein weiteres Konto (Administrator) mit Administratoren-Rechten auf dem System, das in der Ansicht „Benutzerkonten“ (Abbildung 7) jedoch nicht auftaucht. Um das Passwort dieses Benutzers ändern zu können, müssen Sie im Startmenü „Ausführen...“ den Befehl „control userpasswords2“ eingeben. Es erscheint das Fenster wie in Abbildung 10. Hier lässt sich unter dem Punkt „Kennwort zurücksetzen“ ein neues Passwort für das versteckte Benutzerkonto „Administrator“ vergeben.

Achtung: Dieses Passwort dürfen Sie keinesfalls vergessen. Ansonsten wird es bei Verlust der Passwörter der von Ihnen eingerichteten Konten unmöglich, diese wieder zurückzusetzen.



Abbildung 10: Setzen des Passwortes für den versteckten Administrator

Windows XP Professional

Unter Windows XP Professional ist die Benutzerverwaltung ähnlich. Allerdings wird bereits während der Installation die Vergabe eines Passwortes für den „versteckten“ Administrator verlangt.

- Das Setzen von Passwörtern für die von Ihnen eingerichteten Konten erfolgt analog zu Windows XP Home.
- Für die nicht sichtbaren Benutzerkonten kann dies wie bei Windows XP Home mit Hilfe des Befehls „*control userpasswords2*“ erfolgen. Allerdings ist dies ein-facher über die „*Systemsteuerung*“ möglich (siehe Abbildung 11).

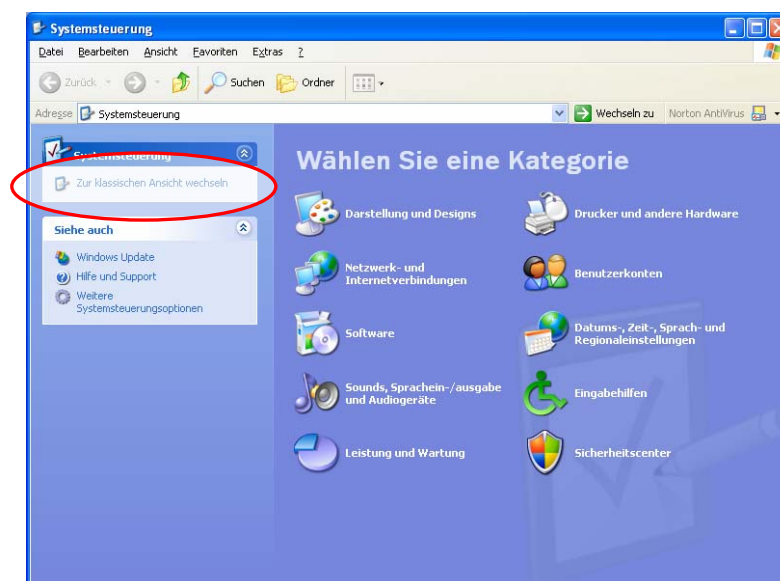


Abbildung 11: Systemsteuerung mit eingeschränkter Auswahl

Wechseln Sie auf die klassische Ansicht, indem Sie oben links auf das entsprechende Feld klicken (rot markierte Stelle in Abbildung 11). Die Darstellung wie auch die Anzahl Kategorien ändert sich damit (siehe Abbildung 12).

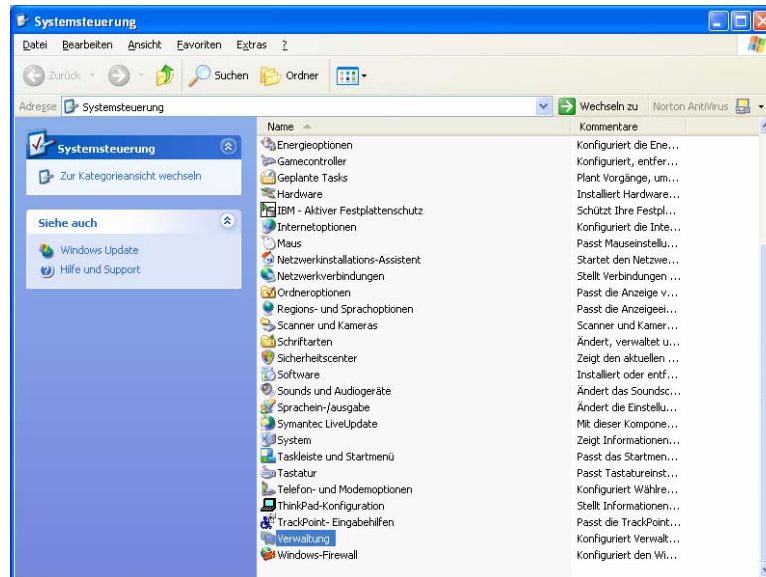


Abbildung 12: Klassische Ansicht der Systemsteuerung

Unter dem Punkt „Systemsteuerung → Verwaltung → Computerverwaltung → Lokale Benutzer und Gruppen → Benutzer“ lassen sich die vorhandenen Benutzerkonten anzeigen. Um ein Passwort zu setzen, gehen Sie auf den gewünschten Benutzernamen und drücken sie die rechte Maustaste. Anschliessend können Sie das Kennwort festlegen.

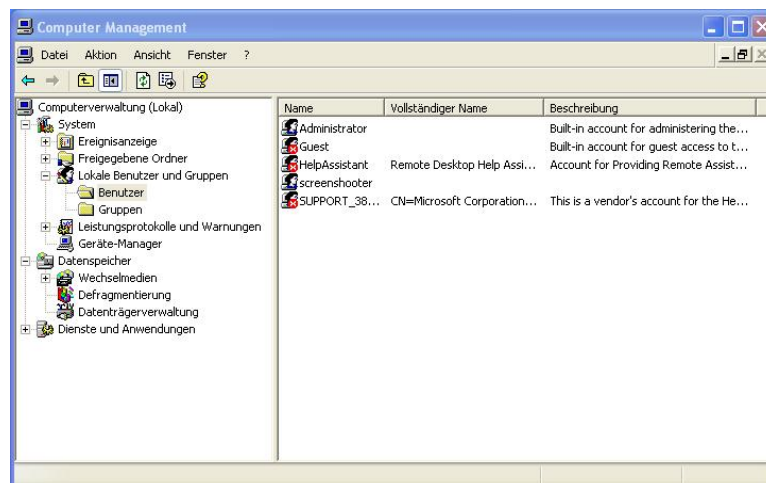


Abbildung 13: Anzeigen sämtlicher Benutzerkonten unter Windows XP Professional

Datensicherung

Trotz aller Vorsichtsmassnahmen können Daten unwiderruflich verloren gehen. Dies muss nicht zwingend durch einen Virus oder einen Angriff geschehen, sondern kann beispielsweise auch die Folge eines technischen Defekts sein. Aus diesem Grund ist es empfehlenswert, regelmässige Datensicherungen (Backups) durchzuführen. Dabei ist unbedingt darauf zu achten, dass die Backups regelmässig auf ihre Wiederherstellbarkeit (d.h. Lesbarkeit und Vollständigkeit) hin kontrolliert werden.

Die gesicherten Daten sind dabei auf ein externes Medium wie z.B. CD-ROM, DVD oder eine externe Festplatte zu kopieren und an einem geschützten Ort aufzubewahren. Weitere Informationen finden Sie unter:

<http://www.melani.admin.ch/themen/00166/00171/index.html?lang=de>

Zusätzliche Sicherheitseinstellungen

Unter Beachtung der im vorangegangenen Kapitel aufgeführten Empfehlungen wird ein solider Grundschutz erreicht. Allerdings lassen sich weitere Verbesserungen der Systemsicherheit erreichen, die im Folgenden besprochen werden. Diese Konfigurationen sind vor allem dann vorzunehmen, wenn mehrere Benutzerkonten auf dem System vorhanden sind, wenn von extern auf das System zugegriffen wird oder ein erhöhter Schutzgrad erforderlich ist.

Wichtige Hinweise:

Die im Folgenden aufgeführten Empfehlungen sollten nur von erfahrenen Windows-Benutzern umgesetzt werden. Vorgängig sind die wichtigsten Daten auf einem externen Datenträger zu sichern.

MELANI kann keinerlei Haftung für Schäden übernehmen, die bei fehlerhafter Konfiguration des Rechners auftreten können!

Anmeldeoptionen

Beim Aufstarten eines Windows XP Systems erscheint die Willkommenseite (Welcome-Screen), auf dem Informationen über vorhandene Benutzerkonten angezeigt sind. Diese können einem Unbefugten unnötige Hinweise liefern und einen unautorisierten Zugang zum System vereinfachen. Um dies zu vermeiden, sollte auf den klassischen Anmeldebildschirm (Loginbildschirm) umgestellt werden. Dies ist über das Menü „Systemsteuerung → Benutzerkonten“ unter dem Punkt „Art der Benutzeranmeldung ändern“ möglich. Entfernen Sie das Häkchen bei „Willkommenseite verwenden“.

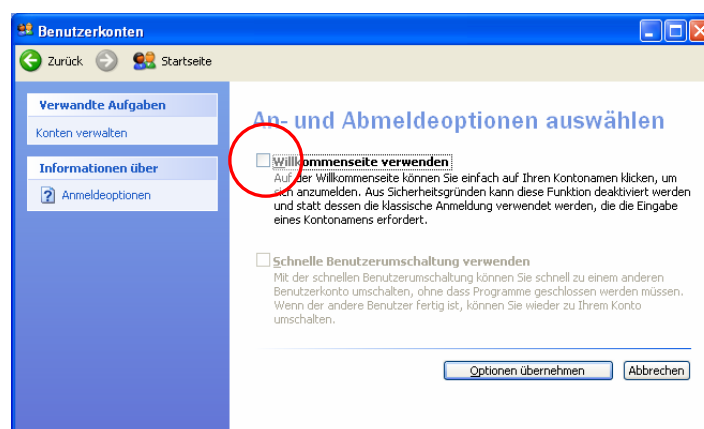


Abbildung 14: Standardanmeldung aktivieren

Standardmässig wird dann der zuletzt eingeloggte Benutzer angezeigt, was sich ebenfalls unterdrücken lässt:

- **Windows XP Home:** Geben Sie unter dem Startmenü „Ausführen...“ den Befehl *regedt32* ein. Setzen Sie den Wert für „*dontdisplaylastusername*“ unter „*HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Windows → CurrentVersion → policies → system*“ auf 1.
- **Windows XP Professional:** „*Systemsteuerung → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitsoptionen*“ und dort im rechten Fenster unter der Richtlinie „*Interaktive Anmeldung: Letzten Benutzernamen nicht anzeigen*“ die Sicherheitseinstellung „*Aktiviert*“ ändern.

Lokale Sicherheitseinstellungen unter Windows XP Professional

Unter dem Menü „*Systemsteuerung → Verwaltung → Lokale Sicherheitsrichtlinie*“ lassen sich diverse Konfigurationen in Bezug auf die Sicherheit vornehmen. Namentlich sind dies die *Kontorichtlinien*, *Kontosperrungsrichtlinien*, *Überwachungsrichtlinien*, *Benutzerrechte* sowie erweiterte Einstellungen unter dem Punkt *Sicherheitsoptionen*. Die Account- und Passwortpolicy lässt sich über die Menüpunkte *Kennwortrichtlinien* und *Kontosperrungsrichtlinien* konfigurieren. Die empfohlenen Werte sind nachfolgend aufgeführt.

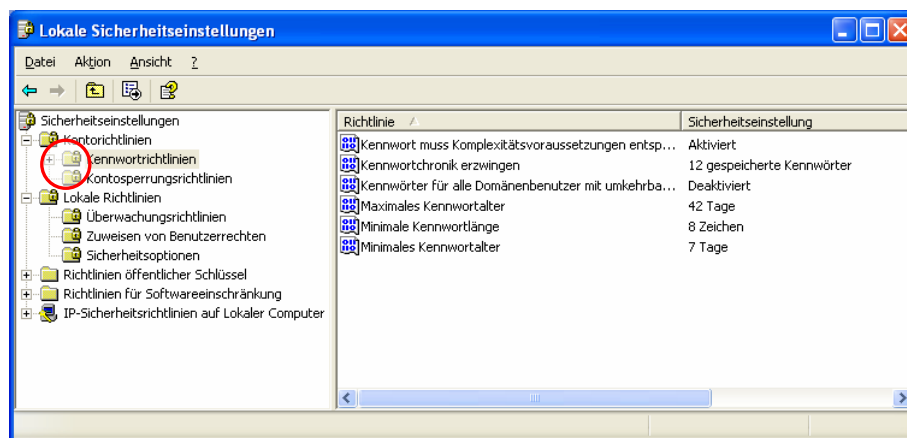


Abbildung 15: Konfiguration der Account- und Passwortpolicy

Kennwortrichtlinien

<p><i>Kennwort muss Komplexitätsvoraussetzungen erfüllen:</i></p>	<p>Mit der Aktivierung dieses Wertes muss ein Passwort sowohl aus Gross- und Kleinbuchstaben, Zahlen wie auch Sonderzeichen bestehen. Diese Einstellung wird allerdings erst beim nächsten Passwortwechsel des Benutzers aktiv. Bereits vergebene Passwörter sind davon nicht betroffen.</p> <p><i>Empfohlene Einstellung:</i> Aktiviert</p>
--	--

<i>Kennwortchronik erzwingen:</i>	<p>Mit dieser Einstellung wird verhindert, dass Benutzer bei einem erzwungenen Passwortwechsel bereits verwendete Passwörter nochmals nutzen können. Der gewählte Wert gibt die Anzahl von Passwörtern an, die sich das System merkt. Ist der Wert beispielsweise auf 12 gesetzt, kann der Benutzer erst beim 13. Passwortwechsel wieder das erstgewählte Passwort eingeben. Der gültige Wertebereich liegt zwischen 0 (Benutzer kann sofort wieder das alte Passwort verwenden) und 24.</p> <p><i>Empfohlene Einstellung: 12</i></p>
<i>Kennwort für alle Domänenbenutzer mit umkehrbarer Verschlüsselung speichern:</i>	<p><i>Empfohlene Einstellung: Deaktiviert</i></p>
<i>Maximales Passwortalter:</i>	<p>Damit wird der Benutzer gezwungen, sein Passwort in regelmässigen Abständen zu wechseln.</p> <p><i>Empfohlene Einstellung: 60 – 90 Tage</i></p>
<i>Minimales Passwortalter:</i>	<p>Um zu verhindern, dass der Benutzer die Einstellungen der „<i>Kennwortchronik erzwingen</i>“ umgeht, sollte dieser Wert ebenfalls gesetzt werden. Ansonsten kann der Benutzer hintereinander x-mal das Passwort wechseln, bis er wieder sein gewohntes Passwort eingeben darf.</p> <p><i>Empfohlene Einstellung: 5 Tage</i></p>
<i>Minimale Kennwortlänge:</i>	<p>Für Konti (Accounts) mit speziellen Privilegien (z.B. Administratoren) empfiehlt sich eine Länge von 12 oder mehr Zeichen. Für normale Benutzerkonten sollte der Wert auf mindestens 8 Zeichen gesetzt werden.</p> <p>Hinweis: Windows XP unterstützt eine Passwortlänge von bis zu 127 Zeichen.</p>

Kontosperrungsrichtlinien

Die Einstellungen bezüglich der Kontosperrung sind unter dem zweiten Punkt der Kontorichtlinien vorzunehmen (siehe Abbildung 16).

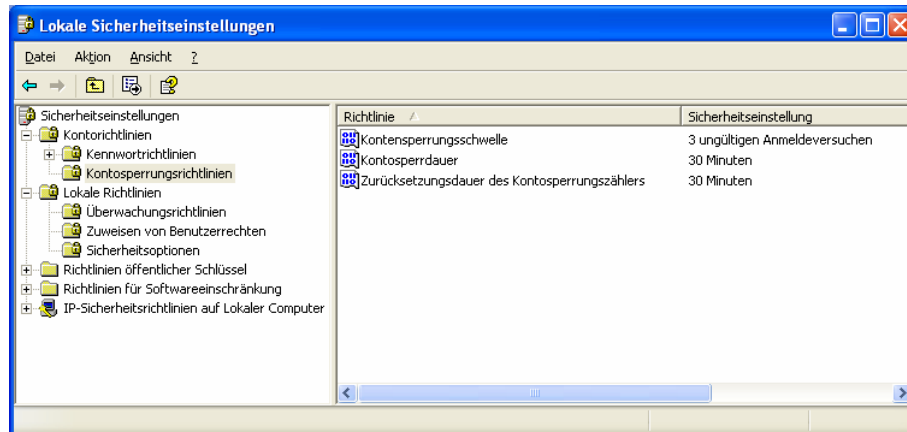


Abbildung 16: Sperrung von Benutzerkonten

Empfohlen werden die folgenden Einstellungen:

<p><i>Kontosperrungsschwelle:</i></p>	<p>Hier wird festgelegt, wie viele ungültige Anmeldeversuche bis zur Sperrung des Kontos möglich sind. So sollen Brute-Force Attacks mittels automatisierter Tools verhindert werden.</p> <p>Empfohlene Einstellung: maximal 3 Versuche</p>
<p><i>Kontosperrdauer:</i></p>	<p>Damit lässt sich in Minuten festlegen, wie lange ein Konto temporär gesperrt wird. Gültige Werte reichen von 0 bis 99999 Minuten.</p> <p><i>Wichtiger Hinweis:</i> Der Wert 0 bedeutet nicht, dass der Account gar nicht gesperrt wird, das Gegenteil trifft zu. In so einem Fall muss der Administrator das Benutzerkonto wieder freigeben. Dies kann somit zu einer Denial-of-Service Attacke führen. Auf den Administratoren-Account kann vom Terminal her immer zugegriffen werden, hier ist also keine Sperrung möglich.</p> <p>Empfohlene Einstellung: 15 – 30 Minuten</p>

<p>Zurücksetzungsdauer des Kontosperrungszählers:</p>	<p>Setzt die Zeit, bis der Wert der Kontosperrungsschwelle wieder zurückgesetzt wird.</p> <p>Empfohlene Einstellung: 15 – 30 Minuten</p>
--	--

Überwachungsrichtlinien

Dieses Menü erlaubt Einstellungen in Bezug auf sicherheitsrelevante Ereignisse wie Systemanmeldungen, Kontoverwaltung, Zugriffe auf Dateien usw. Je nach Anforderung sind unterschiedliche Einstellungen sinnvoll. Unter dem nachfolgenden Link sind entsprechende Empfehlungen aufgeführt:

<http://www.microsoft.com/germany/technet/sicherheit/prodtech/windowsxp/secwinxp/xpsegch03.mspx#EDD>

Zuweisen von Benutzerrechten

Die eingestellten Rechte sind grundsätzlich zweckmässig eingestellt.



Abbildung 17: Einstellungen der Benutzerrechte

Sicherheitsoptionen

Die voreingestellten Optionen bieten auch in diesem Fall bereits eine gute Sicherheit, ermöglichen jedoch individuelle Anpassungen.

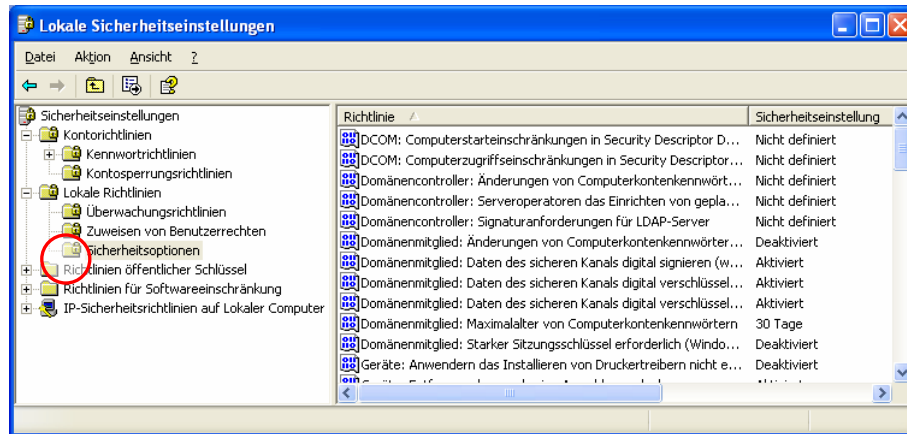


Abbildung 18: Sicherheitsoptionen

Dienste

Auf einem standardmässig aufgesetzten Windows XP System laufen Dienste, die für den täglichen Betrieb nicht zwingend notwendig sind. Für diejenigen, die wissen wollen, welche Dienste welchen Zweck erfüllen, empfiehlt sich der nachfolgend aufgeführte Link (in Englisch):

http://www.theeldergeek.com/services_guide.htm

Dort wird jeder Dienst erklärt sowie eine Empfehlung zu dessen Statuszustand (aktiviert, manuell, deaktiviert) gegeben. Anpassungen bezüglich der Dienste erfolgen unter dem Menü „Systemsteuerung → Verwaltung → Dienste“.

Kontrolle und Einschränken von ausgehenden Verbindungen

Die integrierte Windows-Firewall bietet keine Möglichkeit, ausgehende Verbindungen zu überwachen oder zu blockieren. Falls Malicious Code auf das System gelangt, kann dieser uneingeschränkt Verbindungen nach aussen aufbauen und so allenfalls sensible Daten an einen Angreifer übermitteln.

Dieser Gefahr kann mit der Installation einer Personal Firewall begegnet werden, die auch ausgehende Verbindungen kontrollieren und gegebenenfalls blockieren kann. Solche Produkte sind teilweise kostenlos im Internet verfügbar.

http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de#sprungmarke0_5

Datenverschlüsselung unter Windows XP Professional

Um heikle Daten zusätzlich zu schützen, empfiehlt sich deren Verschlüsselung mittels EFS (Encrypting File System). Gehen Sie dazu wie folgt vor:

- Starten Sie den Windows Explorer
- Wählen Sie den zu verschlüsselnden Ordner an und öffnen Sie das entsprechende Eigenschaftsfenster (rechte Maustaste → Eigenschaften)
- Klicken Sie unter dem Register „Allgemein“ auf die Schaltfläche „Erweitert...“
- Setzen Sie das Häkchen bei „Inhalt verschlüsseln, um Daten zu schützen“ (siehe Abbildung 19)
- Bestätigen Sie mit „OK“

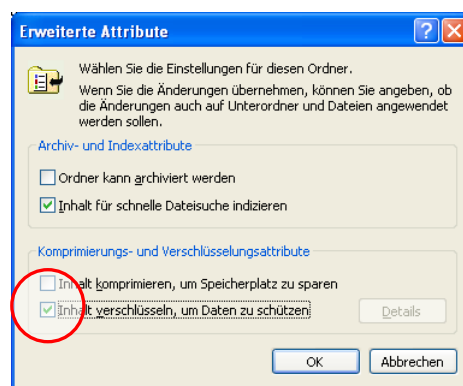


Abbildung 19: Verschlüsselung von Daten

Obwohl die Daten jetzt verschlüsselt sind, werden Sie keinen Unterschied erkennen, da die Entschlüsselung durch Windows automatisch und im Hintergrund erfolgt. Versucht jedoch ein anderer Benutzer auf diese Daten zu zugreifen, wird ihm dies mit der Fehlermeldung „Zugriff verweigert“ verwehrt.

Wichtiger Hinweis: Falls mehrere Personen Daten via EFS verschlüsseln und irgendwann eine Zwangsentschlüsselung notwendig wird, muss beim ersten Gebrauch von EFS ein so genannter Recovery Agent implementiert werden. Dadurch lassen sich im Notfall sämtliche Daten wieder entschlüsseln. Anleitungen dazu sind unter den nachfolgend aufgeführten Links zu finden:

<http://support.microsoft.com/default.aspx?scid=kb;de;307877>

<http://technet.microsoft.com/en-us/library/bb457065.aspx> (englisch)

<http://www.fz-juelich.de/zam/files/docs/tki/tki-0397.pdf>

Achtung: Gehen die Schlüssel verloren, sind die damit verschlüsselten Daten nicht wieder herstellbar!!!

Datei- und Druckerfreigabe deaktivieren

Einer der häufigsten Fehler in Windows ist die unnötige Aktivierung der Datei- und Druckerfreigabe. Viele Angriffe nutzen diese Funktion aus, um unautorisierten Zugriff auf einzelne Daten oder das gesamte System zu erlangen (über die beiden Ports 139 und 445). Obwohl die Windows-Firewall den Zugang zu dieser Funktion grundsätzlich verhindert, empfiehlt sich als zusätzlicher Schutz deren Deaktivierung. Dies kann unter dem Menüpunkt „Systemsteuerung → Netzwerkeinstellungen → LAN-Verbindung“ erfolgen. Über den Punkt „Eigenschaften“ wird das rechte Fenster in Abbildung 20 aufgerufen. Deinstallieren Sie als erstes die beiden Punkte „Client für Microsoft-Netzwerke“ und „Datei- und Druckerfreigabe für Microsoft-Netzwerke“.

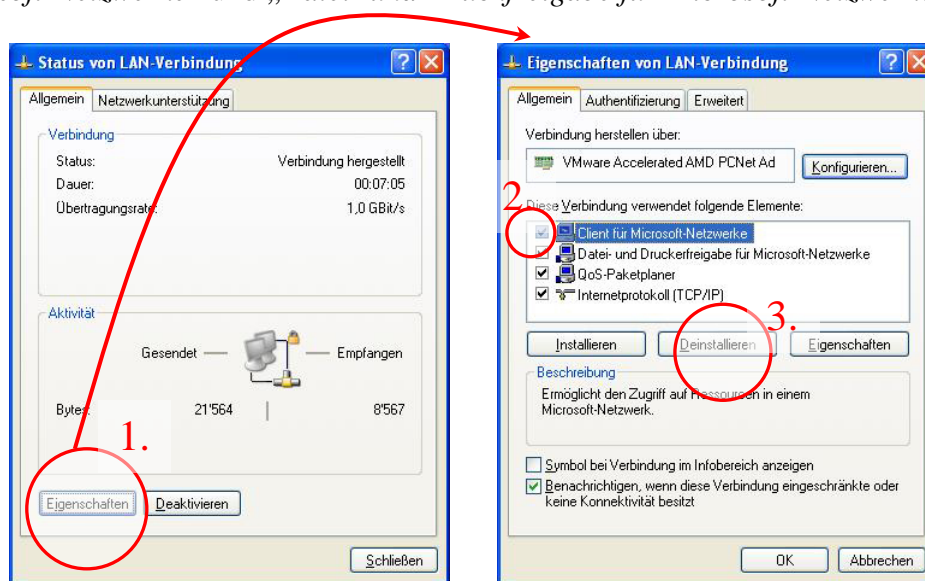


Abbildung 20: Eigenschaften der Netzwerkverbindung

Das rechte Fenster sollte danach demjenigen in Abbildung 21 entsprechen.

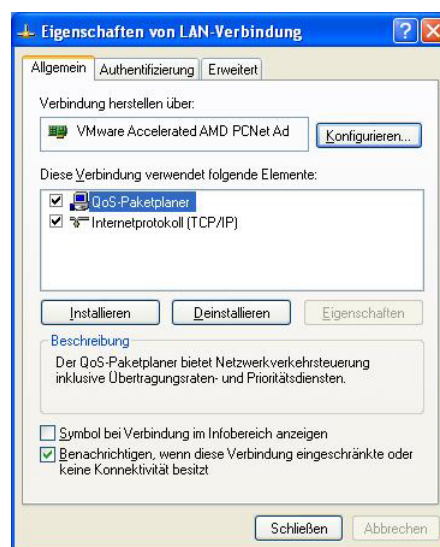
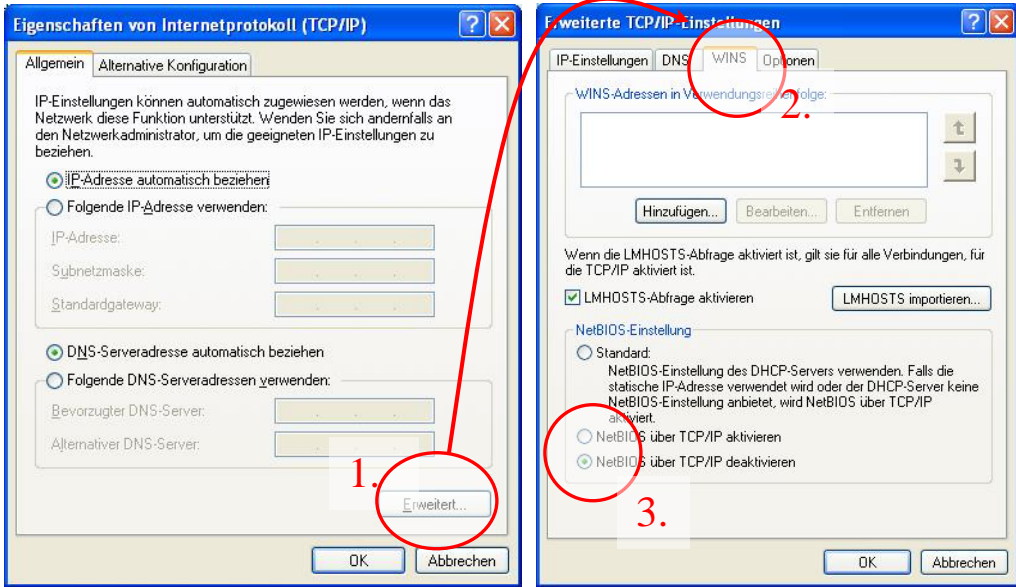


Abbildung 21: Nach der Deinstallation der beiden Netzwerkdienste

Führen Sie einen Doppelklick auf den Punkt „Internetprotokoll (TCP/IP)“ aus, worauf das linke Fenster in  erscheint. Klicken Sie auf „Erweitert...“ und setzen Sie beim Register „WINS“ den Punkt auf „NetBIOS über TCP/IP deaktivieren“.

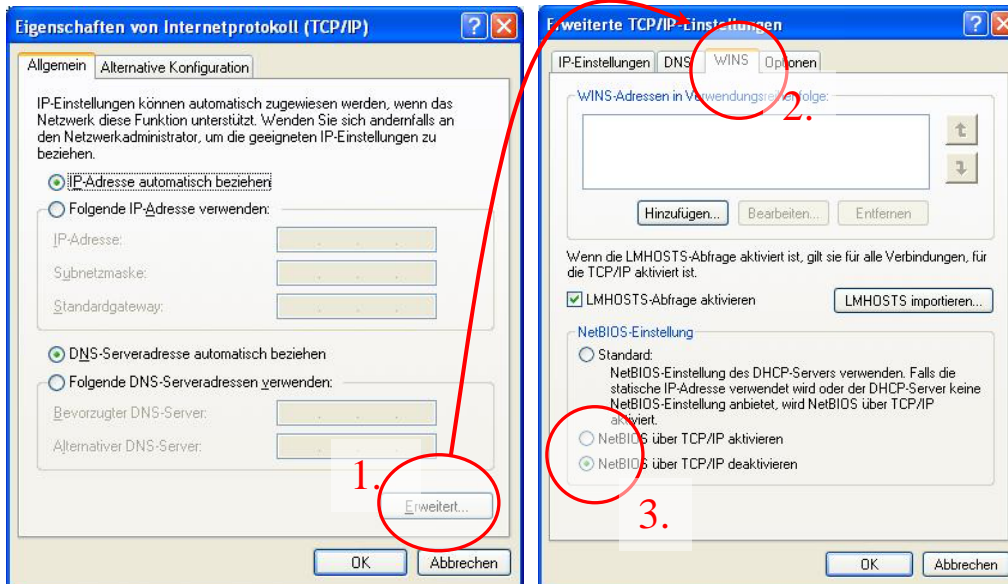


Abbildung 22: Deaktivieren von NetBIOS über TCP/IP

Falls Sie auf Dateifreigaben über das Internet nicht verzichten wollen oder können, sind einige wichtige Punkte zu beachten. Beispielsweise bietet die Home Edition von Windows XP in Bezug auf Datenfreigaben weniger Möglichkeiten als die Professional Edition. Deshalb ist bei Windows XP Home grundsätzlich von Netzfreigaben abzuraten.

Unter Windows XP Professional stehen mehr Optionen für Ordnerfreigaben zur Verfügung, allerdings müssen diese vorgängig im Explorer unter der Option „Ansicht → Ordneroptionen“ freigeschaltet werden.

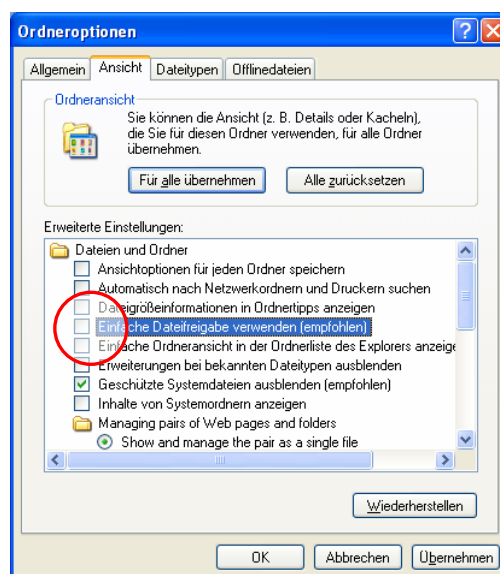


Abbildung 23: Deaktivierung der einfachen Dateifreigabe

Durch Deaktivieren der Checkbox „Einfache Dateifreigabe verwenden“ ist das Register „Sicherheit“ in den Ordner- und Dateieigenschaften zugänglich (siehe Abbildung 24) und lässt damit spezifische Einstellungen wie die Vergabe von Zugriffsberechtigungen zu.

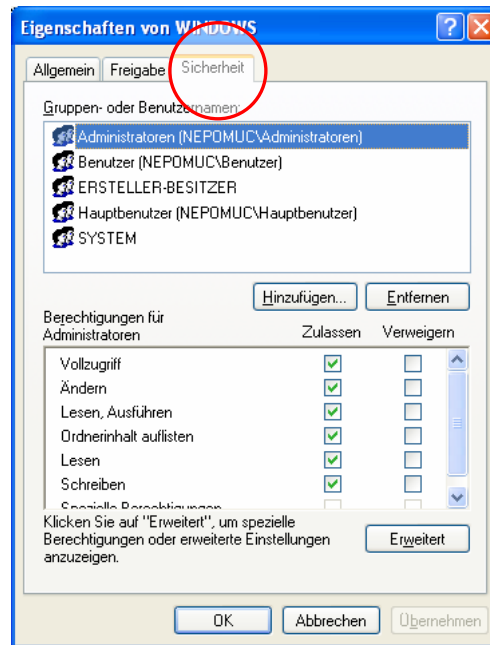


Abbildung 24: Berechtigungen bei Freigaben einstellen

Desktopsperrung und Bildschirmschoner

Wer die bei Windows NT oder Windows 2000 bekannte Tastenkombination Ctrl+Alt+Delete zur Aktivierung der Bildschirmsperre vermisst, kann diese bei Windows XP durch die bereits im Abschnitt „Verwaltung von Benutzerkonten“ diskutierten Einstellungen reaktivieren.

Überprüfung der Systemsicherheit mit Hilfe von Tools

Microsoft Baseline Security Analyzer (MBSA)

Zur Überprüfung der Systemsicherheit im Allgemeinen und der durchgeführten Einstellungen im Besonderen empfiehlt sich Microsofts Baseline Security Analyzer. Das Programm kann sowohl das lokale, d.h. direkt Ihr System, als auch ein entferntes System überprüfen. Informationen zur Verwendung des Tools werden von Microsoft unter dem folgenden Link zur Verfügung gestellt:

<http://support.microsoft.com/default.aspx?scid=kb;de;320454>

Entdecken und Entfernen von Spy- und Adware

Spy- und Adware ist auf vielen Rechnern vorhanden. *Spyware* soll ohne Wissen des Benutzers Informationen über dessen Surfgewohnheiten oder Systemeinstellungen sammeln und diese an eine vordefinierte Adresse übermitteln. Welche Informationen ausgelesen werden, hängt von der jeweiligen Spyware ab und kann von Surfgewohnheiten bis hin zu Passwörtern gehen. Der Begriff *Adware* setzt sich aus den englischen Wörtern *Advertising* (Werbung) und *Software* zusammen. Eine klare Definitionsgrenze zwischen Spyware und Adware ist schwer zu erkennen. Adware wird vielfach für Werbezwecke verwendet, indem die Surfgewohnheiten des Benutzers aufgenommen und dazu benutzt werden, entsprechende Produkte (z.B. durch Links) zu offerieren.

Spyware und Adware gelangt vorwiegend über heruntergeladene Programme auf den Rechner. Tools zu deren Erkennung und Entfernung sind auf der MELANI-Webseite aufgeführt:

http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de#sprungmarke0_12

Allerdings sind diese Tools (Werkzeuge) keine Freikarte für ein unvorsichtiges Surfen im Internet, da selbst die effektivsten Werkzeuge nicht alle Schädlinge identifizieren oder entfernen können.

Referenzen und weiterführende Links

- [1] Updateseite für MS Office
<http://office.microsoft.com/de-de/officeupdate/default.aspx>

- [2] Schutz vor Gefahren und Risiken
<http://www.melani.admin.ch/themen/00103/index.html?lang=de>

- [3] Links zu Antiviren-Software
http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de#sprungmarke0_4

- [4] Datensicherung
<http://www.melani.admin.ch/themen/00166/00171/index.html?lang=de>

- [5] Einstellungen für Überwachungsrichtlinien
<http://www.microsoft.com/germany/technet/sicherheit/prodtech/windowsxp/secwinxp/xpsgch03.mspx#EDD>

- [6] Services Guide for Windows XP
http://www.theeldergeek.com/services_guide.htm

- [7] Links zu Personal Firewalls
http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de#sprungmarke0_5

- [8] Das verschlüsselnde Dateisystem (EFS) verwenden
<http://support.microsoft.com/default.aspx?scid=kb;de;307877>
<http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.mspx> (englisch)

- [9] Verschlüsselung der Festplattendaten unter Windows XP
<http://www.fz-juelich.de/zam/files/docs/tki/tki-0397.pdf>

- [10] Microsoft Baseline Security Analyzer
<http://support.microsoft.com/default.aspx?scid=kb;de;320454>

- [11] Tools zum Thema „Spyware“ und „Adware“
http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de#sprungmarke0_12

- [12] Sicherheitshandbuch für Windows XP (v2)
<http://www.microsoft.com/germany/technet/sicherheit/prodtech/windowsxp/secwinxp/xpsgch01.mspx>

- [13] Windows XP Security Guide (in englisch)
<http://www.microsoft.com/technet/security/prodtech/winclnt/secwinxp/default.mspx>

Anhang A: Ermitteln des installierten Service Packs

Unter „Systemsteuerung → System“ wird das aktuell installierte Service Pack (derzeit SP2) angezeigt.

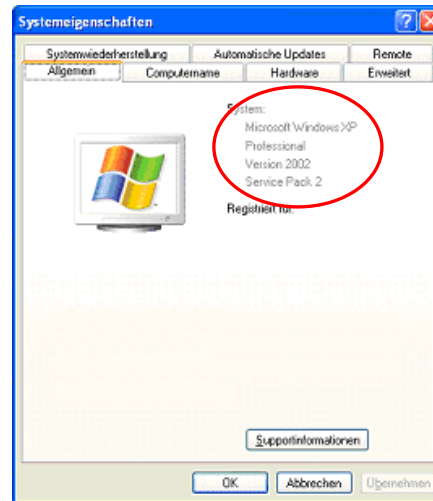


Abbildung 25: Ermitteln des installierten Service Packs

Anhang B: Informationen über das Filesystem anzeigen

Informationen über das Filesystem eines Datenträgers können wie folgt angezeigt werden:

- 1.) Explorer öffnen
- 2.) Den Mauszeiger auf den entsprechenden Datenträger bewegen (z.B. C:)
- 3.) Rechte Maustaste (in den meisten Fällen) drücken und das Menü „Eigenschaften“ auswählen
- 4.) Unter dem Punkt „Allgemein“ ist das verwendete Filesystem ersichtlich (siehe Abbildung 26)

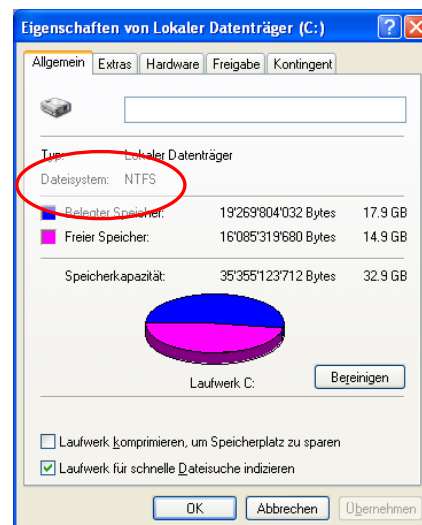


Abbildung 26: Informationen zum Filesystem