# Modul 305 Teil 6 (Indiviuelle Benutzerrechte in Windows XP)

Individuelle Benutzerrechtevergabe unter Windows XP

Windows XP gilt als Mehrbenutzersystem. Als Administrator kann man sehr vieles kontrollieren. Dennoch gibt es viele Tricks um als Nicht-Administrator einige Dinge zu sichern oder zusperren. Programme und Dateien lassen sich leicht verbergen und versperren.

Benutzer in der Registry

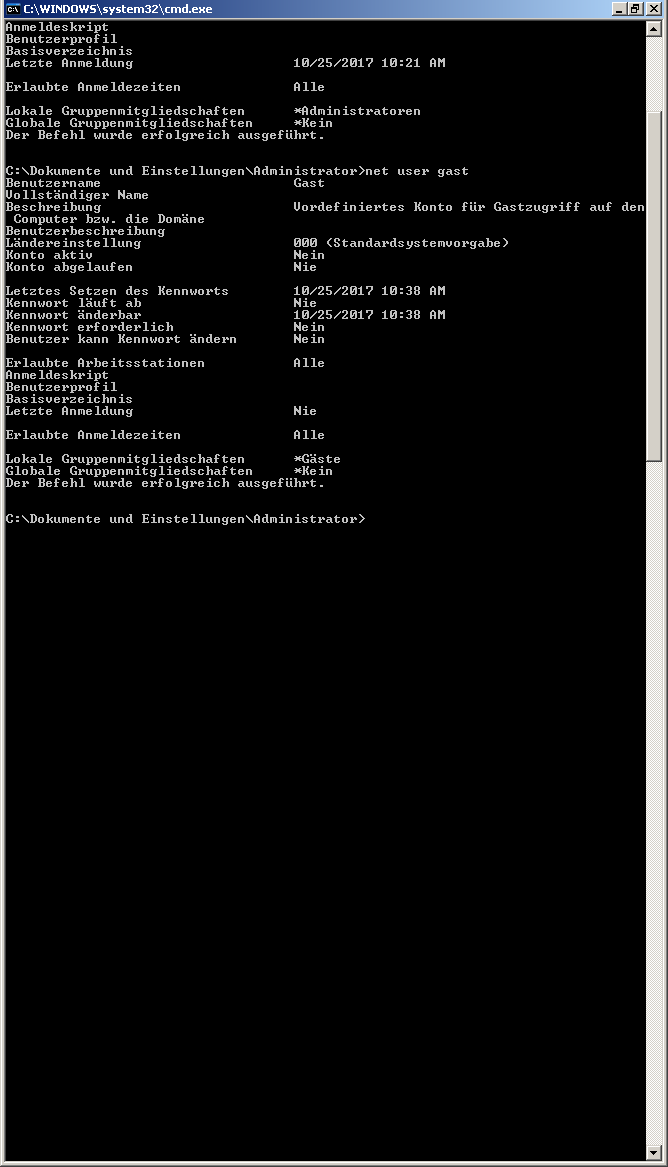
Alle Einstellungen rund um den Benutzer findet man im Registry unter ***„Hkey\_Current\_User“*** und ***„Hkey\_Users“***. Zur Sicherheit ist teilweise ***„Hkey\_Users“*** verschlüsselt.

Eigene Benutzer verwalten

Mit Windows XP kann als Administrator sehr viel kontrollieren. Wenn man Ahnung hat, kann man sehr viele Dinge verbergen. Windows XP hat bei Beginn drei Benutzer. Der ***„Administrator“***, ***„Gast“*** und der ***„erstellte Benutzer“***.

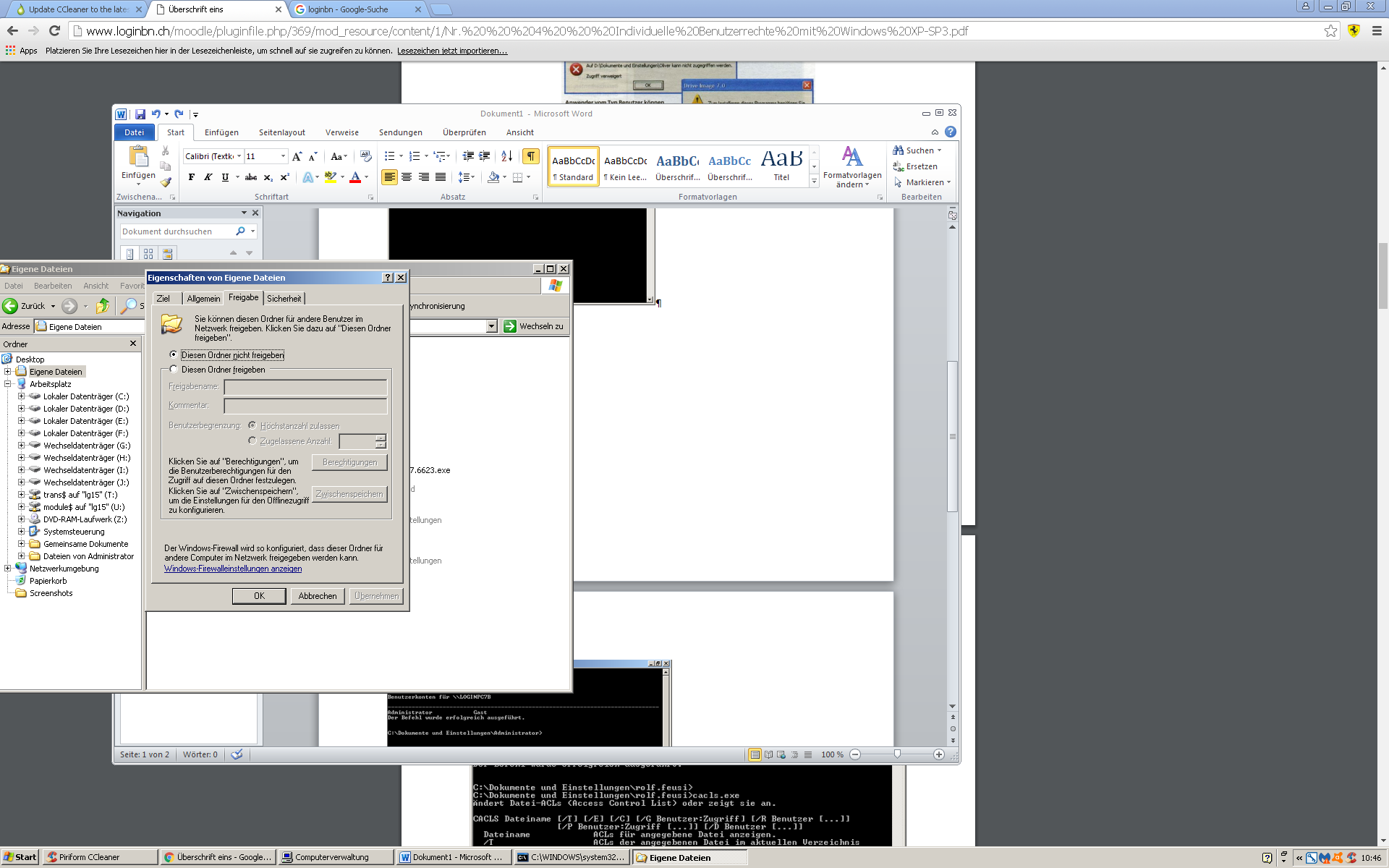
Kontostatus prüfen

Mit dem Befehl ***„net user administrator“*** kann man Informationen zu dem Konto sehen. Der ***„administrator“*** kann auch durch einen anderen Benutzer ersetzt werden um die Information zu dem Profil zu sehen.



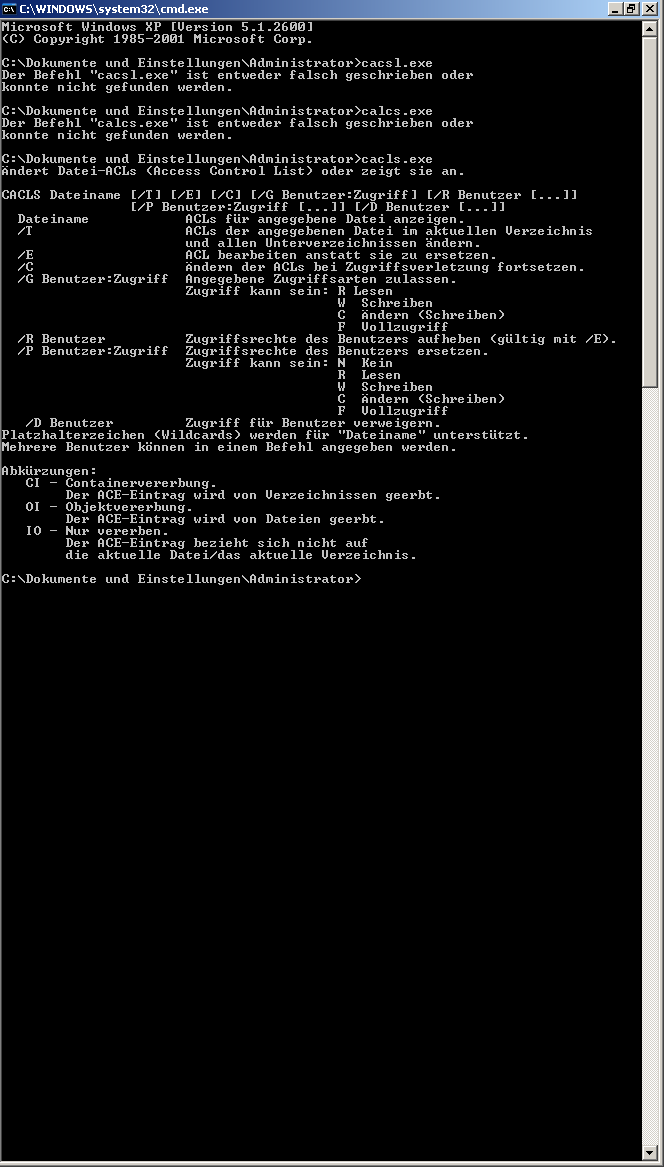
Daten vor Usern schützen

Lokal gespeicherte Daten können von den Administratoren zwar eingesehen werden, allerdings sind sie eingeschränkt. Jeder Benutzer kann private Daten auch von den Administratoren verbergen. Mit dem Befehl „net user“ lassen sich die Benutzerkonten, deren Eigenschaften und die Zugriffszeiten anzeigen lassen. Ganz verborgen bleiben die Daten, welcher der Benutzer in seinem eigenen Profil gespeichert hat. Dies ist aber nur, wenn der Benutzer dies im Ordner so eingestellt hat. Ordner kann man auch für ganz einfach sperren. Für dies muss man nur einen Rechtsklick auf den Ordner machen und dann auf ***„Eigenschaften“*** klicken. Im Register Freigabe muss man nur das Häcken auf ***„Diesen Ordner nicht freigeben“*** machen und schon ist er vor anderen Benutzern geschützt.



Cacls-Trick

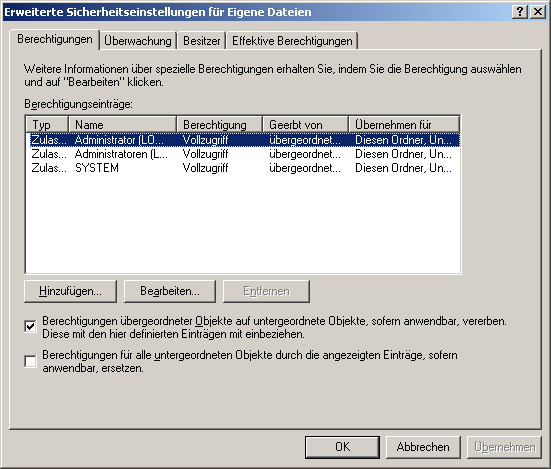
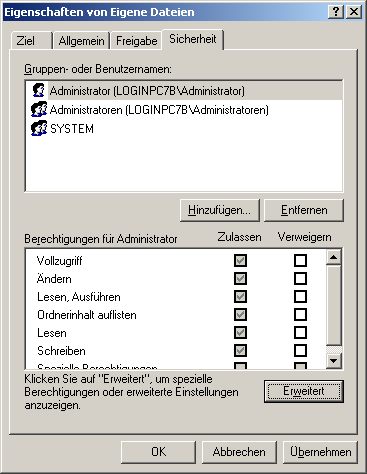
Mit dem Cacls-Trick kann man den Zugriff auf Dateien verbieten selbst wenn diese nicht im eigenen Profil gespeichert sind. Dieses Tool funktioniert aber nur im CMD. Der Vorteil von diesem Tool ist, dass man freigegebene Ordner anpassen kann. Mit diesem Tool kann man jede Datei von jedem Benutzer sperren. Mit Cacls kann man auch die Datei löschen. Mit dem Befehl „cacls.exe. datei.docx /D Benutzer“ werden dem „Benutzer“ alle Zugangsrechte von der Datei weggenommen. Mit cacls /s? werden einige Informationen angezeigt.

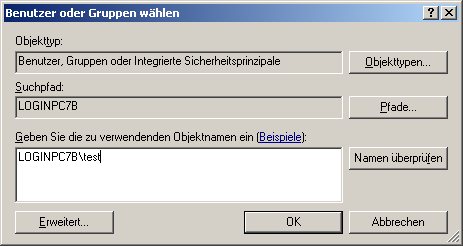




Kontrolle durch Admins

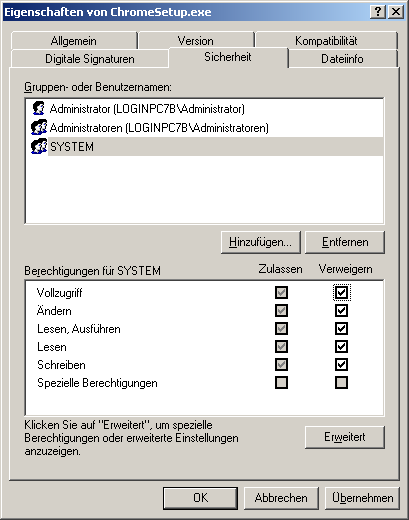
Mit den Sicherheitseinstellungen der Dateieigenschaften können Administratoren einfach Einstellungen machen. Voraussetzung dazu ist, dass man die einfache Dateifreigabe deaktiviert.





Programme selektiv sperren

Der Administrator kann ein Programm für Benutzer sperren. Dazu klickt der Administrator auf die Exe der Andwendung. In den Eigenschaften unter Sicherheit sieht man welche Benutzer Zugriff haben. Meistens ist der Benutzer auf „Jeder“ eingestellt. Der Adminstrator kann jetzt jeden Benutzer entfernen oder hinzufügen. Die neuen Einstellungen, die der Administrator gemacht hat, werden sofort angewendet und gespeichert.



Anwender überwachen

In den erweiterten Sicherheitseinstellungen findet man sogar eine Überwachungsfunktion in den Policies. Der Administrator klickt auf Eigenschaften-Dialog. Danach auf „Erweitert und dann im Register „ Überwachung“. Mit „Hinzufügen“ kann der Administrator auswählen welche Gruppe oder welcher Benutzer überwacht werden soll. Der Anwender soll aber gewarnt sein. Eine falsche Einstellung in der Registry kann im schlimmsten Fall den ganzen Computer lahmlegen. Bei den Überwachungseinstellungen besteht diese Gefahr aber nicht. Die protokollierten Ereignisse werden in den Überwachungsrichtlinien gespeichert. Dazu geht man zuerst in die Gruppenrichtlinien mit dem Befehl ***„gpedit.msc /a“.*** Der Parameter /a führt die Gruppenrichtlinien als Administrator aus. Um in die Überwachungsrichtlinine zu kommen muss man unter Computerkonfiguration/Windowseinstellungen/sicherheitseinstellungen/LokaleRichtlinein/Überwachungsrichtlinien gehen.

Systemänderungen verhindern

Über die Gruppenrichtlininen kann man als Administrator einstellen, dass Systemänderungen nur von berechtigten Usern gemacht werden können. Meistens ist der Zugriff auch nur auf die Administratoren beschränkt.