AAB05: Benutzer, Gruppen und rechte unter Windows

Fabio Plunser
Betreuer : Walter Mueller

March 27, 2020

Inhaltsverzeichnis

1 Startet die Benutzerverwaltung als Administrator. 1

2 Welche Bentuzer gibt es auf Deinem Rechner? 2
2.1 Welches Benutzerkonto verwendest du derzeit? . . . 2

3 Dokumentiere die Eigenschaften deinens Benutzerkontos. 2
3.1 Läuft dein Kennwort aus? . . . 2
3.2 Zu welchen Gruppen gehört das Konto? . . . 3

4 Welche Gruppen gitb es auf Deinem Rechner? 3
4.1 Beschreibe den Unterschied zwischen den Gruppen "Administratoren", und "Benutzer" . . . 4

5 Dokumentiere die Berechtigung auf dem Ordner C:/Programme 4
5.1 Welche Rechte besitzt die Gruppe der Administratoren, welche die der Benutzer? . . . 4
5.2 Dokumentiere deine Erkenntnisse mit screenshot und beschreibe die Rechte mit Worten. . . . 4
5.3 Warum funktioniert das nur mit einem NTFS-Dateisystem? . . . 5

6 Beschreibe die Rechte auf deinem Heimatverzeichnis (i.A. C:/USer/me.... 6

7 Dokumentiere die effektiven Rechte für den Benutzer Guest auf deinem Heimatverzeichnis. 6

8 Registry: 7
8.1 Starte den Registry-Editor mit regedit (ggf. als Administrator) . . . 7
8.2 Welche Rechte hast du auf den Teilbaum HKEY-Current-User und welche auf HKEY-Local-Machine? 7

9 Wie hilft dieses System von Rechten und Berechtigungen die Systemsicherheit auf einem Windowsrechner zu gewährleisten? 8
9.1 Was kann ein Trojaner oder eine Schadsoftware auf dem Rechner anstellen, wenn du als "normaler" Benutzer arbeitest? . . . 8

10 MS-Active Directory und MS-Domäne (Internetrecherche): 8
10.1 Was passiert, wenn man einen Rechner in eine Domain hängt? . . . 8
10.1.1 Warum ist das sinnvoll? . . . 8

Abbildungsverzeichnis

1 Computerverwaltung/Lokale-Benutzerkonten . . . 1
2 Computerverwaltung/Lokale-Gruppen . . . 1
3 Benutzerkonto-Eigenschaften . . . 2
4 Benutzerkonto-Eigenschaften . . . 3
5 Computerverwaltung/Lokale-Gruppen . . . 3
6 c-Programme-Berechtigungen . . . 4
7 Heimverzeichnis-Berechtigungen . . . 6
8 Gast-Heimatverzeichnis-Berechtigungen . . . 6
9 HKEY-Current-User-Berechtigungen . . . 7
10 HKEY-Loca-Machine-Berechtigungen . . . 7

1 Startet die Benutzerverwaltung als Administrator.

(Explorer /rechte Maustaste auf "DieserPC" - Verwalten (Win-X) /Computerveraltung / System / lokale Benutzer und Gruppen, nur unter min10 educatioanal bzw. professional) bz. bei Win10Home: Start/Suchen/netplwiz (etwas eingeschränkte Oberfläche)

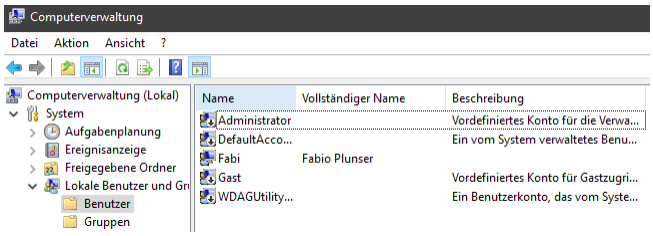


Figure 1: Computerverwaltung/Lokale-Benutzerkonten

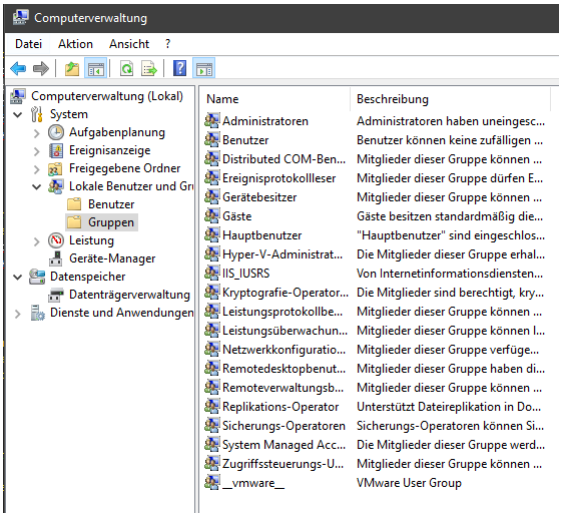


Figure 2: Computerverwaltung/Lokale-Gruppen

2 Welche Bentuzer gibt es auf Deinem Rechner?

Wie bei *Figure*1 zusehen gibt es:

- Administrator
- DefaulAccount
- Fabio
- Gast
- WDAGUtillity

2.1 Welches Benutzerkonto verwendest du derzeit?

Fabio

3 Dokumentiere die Eigenschaften deinens Benutzerkontos.

3.1 Läuft dein Kennwort aus?

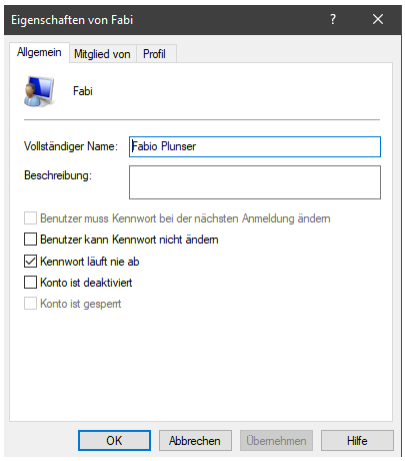


Figure 3: Benutzerkonto-Eigenschaften

Kennwort läuft nie aus.

3.2 Zu welchen Gruppen gehört das Konto?

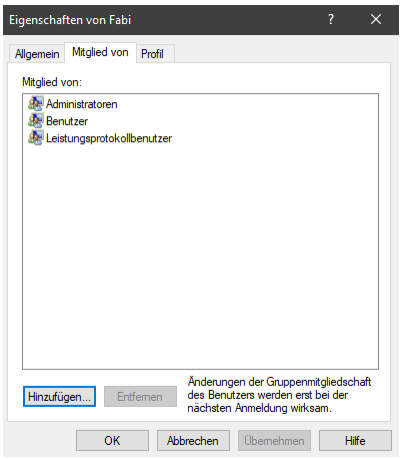


Figure 4: Benutzerkonto-Eigenschaften

- Administrator
- Benutzer
- Leistungsprotokollbenutzer

4 Welche Gruppen gitb es auf Deinem Rechner?

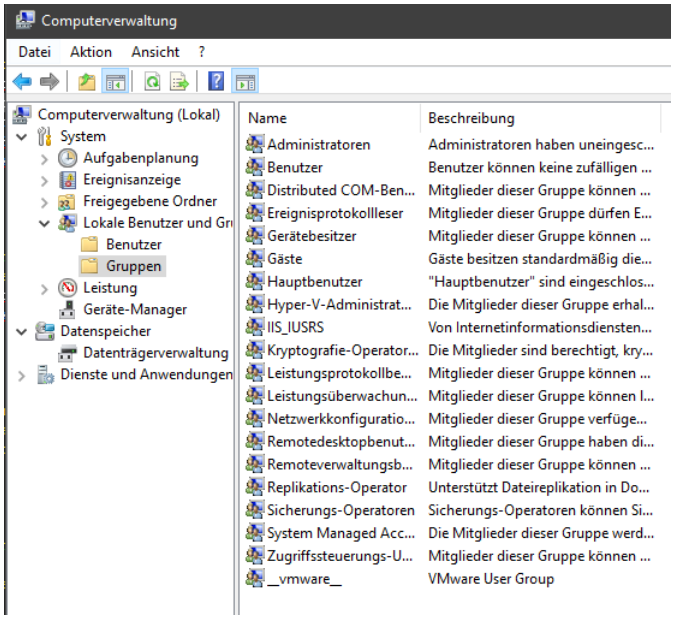


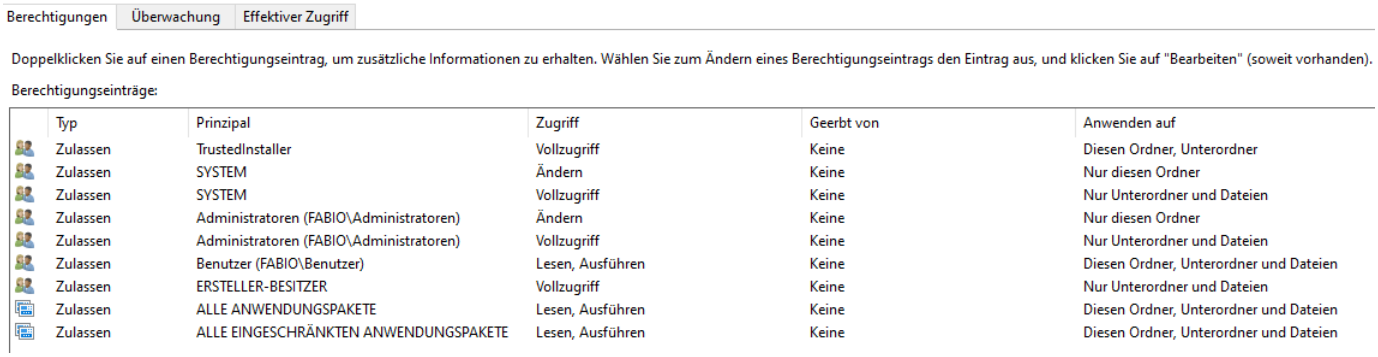
Figure 5: Computerverwaltung/Lokale-Gruppen

4.1 Beschreibe den Unterschied zwischen den Gruppen "Administratoren", und "Benutzer"

Administrator hat das recht auf alle Daten von allen Benutzern zuzugreifen.
Benutzer haben nur die Rechte auf ihren eigenen Daten.

5 Dokumentiere die Berechtigung auf dem Ordner C:/Programme

(Im Explorer: Eigenschaften/Sicherheit/Erweitert ....)



Berechtigungen | Überwachung | Effektiver Zugriff

Doppelklicken Sie auf einen Berechtigungseintrag, um zusätzliche Informationen zu erhalten. Wählen Sie zum Ändern eines Berechtigungseintrags den Eintrag aus, und klicken Sie auf "Bearbeiten" (soweit vorhanden).

Berechtigungseinträge:

Typ	Prinzipal	Zugriff	Geerbt von	Anwenden auf
Zulassen	TrustedInstaller	Vollzugriff	Keine	Diesen Ordner, Unterordner
Zulassen	SYSTEM	Ändern	Keine	Nur diesen Ordner
Zulassen	SYSTEM	Vollzugriff	Keine	Nur Unterordner und Dateien
Zulassen	Administratoren (FABIO\Administratoren)	Ändern	Keine	Nur diesen Ordner
Zulassen	Administratoren (FABIO\Administratoren)	Vollzugriff	Keine	Nur Unterordner und Dateien
Zulassen	Benutzer (FABIO\Benutzer)	Lesen, Ausführen	Keine	Diesen Ordner, Unterordner und Dateien
Zulassen	ERSTELLER-BESITZER	Vollzugriff	Keine	Nur Unterordner und Dateien
Zulassen	ALLE ANWENDUNGSPAKETE	Lesen, Ausführen	Keine	Diesen Ordner, Unterordner und Dateien
Zulassen	ALLE EINGESCHRÄNKTEN ANWENDUNGSPAKETE	Lesen, Ausführen	Keine	Diesen Ordner, Unterordner und Dateien

Figure 6: c-Programme-Berechtigungen

5.1 Welche Rechte besitzt die Gruppe der Administratoren, welche die der Benutzer?

Administrator besitzt Vollzugriff.
Benutzer besitzt Lesen und Ausführen

5.2 Dokumentiere deine Erkenntnisse mit screenshot und beschreibe die Rechte mit Worten.

Siehe *Figure*6 und 5.1

5.3 Warum funktioniert das nur mit einem NTFS-Dateisystem?

Im Gegensatz zu Inode-basierten Dateisystemen, welche bei Unix zum Einsatz kommen (Konzept: alles ist eine Datei), werden bei NTFS alle Informationen zu Dateien in einer Datei (Konzept: alles ist in einer Datei), der Master File Table, kurz MFT gespeichert. In dieser Datei befinden sich die Einträge, welche Blöcke zu welcher Datei gehören, die Zugriffsberechtigungen und die Attribute. Zu den Eigenschaften (Attributen) einer Datei gehören unter NTFS Dateigröße, Datum der Dateierstellung, Datum der letzten Änderung, Freigabe, Dateityp und auch der eigentliche Dateiinhalt.

Quelle: Wikipedia

6 Beschreibe die Rechte auf deinem Heimatverzeichnis (i.A. C:/USer/me....

Figure 7: Heimverzeichnis-Berechtigungen

Berechtigung hat meine PC-Konto FabioPlunser, dass mit meiner alten Mail verlinkt ist, das System und jeder in der Gruppe Administrator. FABIO/Administrator → FABIO ist der Name des PCs

7 Dokumentiere die effektiven Rechte für den Benutzer Guest auf deinem Heimatverzeichnis.

(Sicherheit/Erweitert/Effektive Berechtigungen)

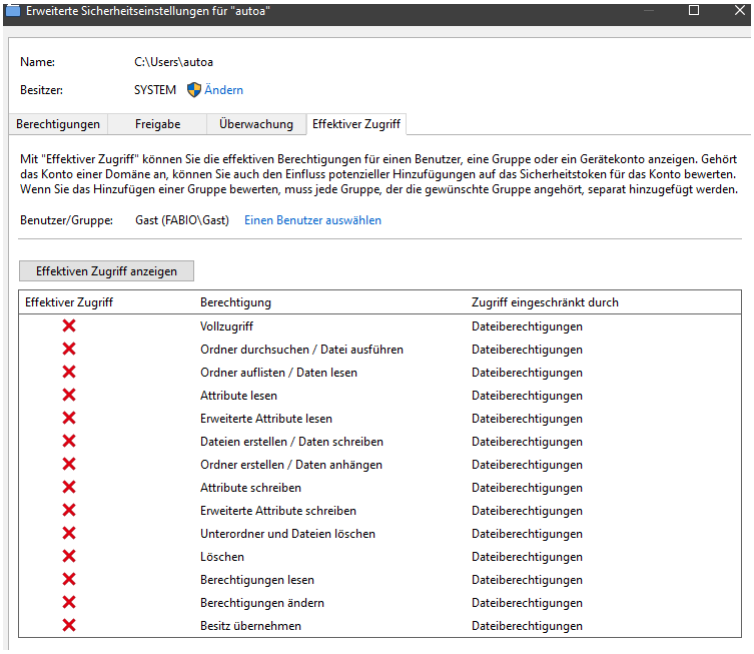


Figure 8: Gast-Heimatverzeichnis-Berechtigungen

8 Registry:

8.1 Starte den Registry-Editor mit regedit (ggf. als Administrator)

8.2 Welche Rechte hast du auf den Teilbaum HKEY-Current-User und welche auf HKEY-Local-Machine?

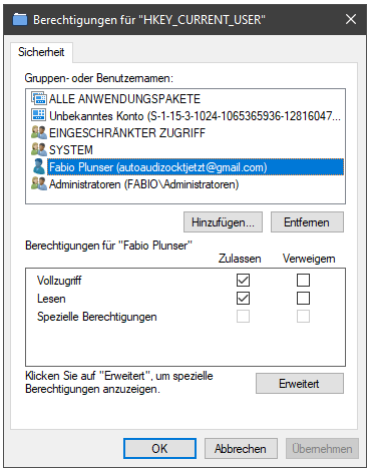


Figure 9: HKEY-Current-User-Berechtigungen

Vollzugriff und Lesen. Mein Konto und die Gruppe Administratoren besitzt diese.

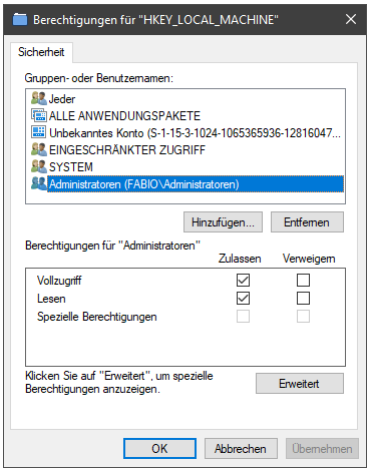


Figure 10: HKEY-Loca-Machine-Berechtigungen

Gruppe Administrator besitzt Vollzugriff und Lesen, somit auch ich.

9 Wie hilft dieses System von Rechten und Berechtigungen die Systemsicherheit auf einem Windowsrechner zu gewährleisten?

Falls es auf meinem PC mehrere Benutzer gäben würde, könnte ich alle Berechtigungen für jede einzelne Datei/Festplatte/Programm genau einstellen.
Da ich der einzige Benutzer dieses PC's bin ist es für mich nur wichtig alle Adminrechte zu haben.

9.1 Was kann ein Trojaner oder eine Schadsoftware auf dem Rechner anstellen, wenn du als "normaler" Benutzer arbeitest?

Er kann alle meine Daten beschädigen, stehlen oder verschlüsseln. Jedoch kann er nicht, falls es noch andere Benutzerkonten auf dem Rechner gibt, auf diese Zugriffe, das geht nur wenn ich als Administrator diese Schadsoftware bzw. Torjaner aufrufe/auslöse.

10 MS-Active Directory und MS-Domäne (Internetrecherche):

10.1 Was passiert, wenn man einen Rechner in eine Domain hängt?

Der Rechner ladet zuerst beim hochfahren die lokalen Benutzer und Gruppen einstellungen sobald sich ein Benutzer in der Domäne anmeldet überschreibt die Domäne diese Berechtigungen. Somit können Berechtigungen einmal auf einem Server festgelegt werden und sie werden dann für alle Benutzer in der Domäne übernommen.

10.1.1 Warum ist das sinnvoll?

Um z.B. in einer großen Schule oder Firma nicht für jeden PC einzeln die Berechtigungen einstellen zu müssen. Weiterhin hat eine Domände den Vorteil, dass alle Benutzer und ihre Daten auf einem Server liegen somit kann sich dieser Benutzer auf den jeden PC in der Firma anmelden und seine Daten bearbeiten (je nach Netzwerk layout).