

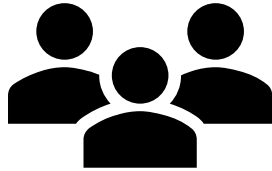
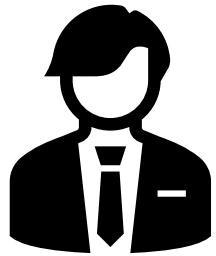
NTFS - Berechtigungen

- ACL, DACL, MACL , RACL
- Grundlegende Berechtigungen
- Erweiterte Berechtigungen
- Hierarchie von Berechtigungen
- Vererbung, Besitz
- Praxis
 - Grafisch
 - Eingabeaufforderung
 - PowerShell

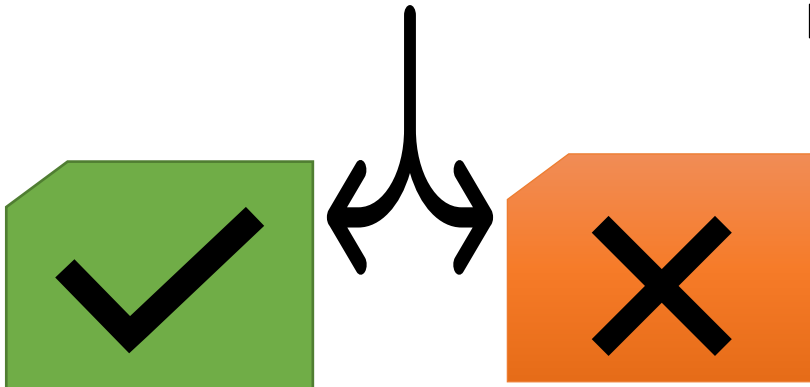
ACL

- **Access Control List (Zugriffssteuerungsliste)**
- Eigenschaft von NTFS
- Gespeichert in MFT
- Berechtigungen für Benutzer und Gruppen
- Sichtbar in Datei-Eigenschaften
- Varianten:
 - Discretionary Access Control (DAC)
 - Mandatory Access Control (MAC)
 - Role Based Access Control (RBAC)

Zugriffsteuerung - DAC

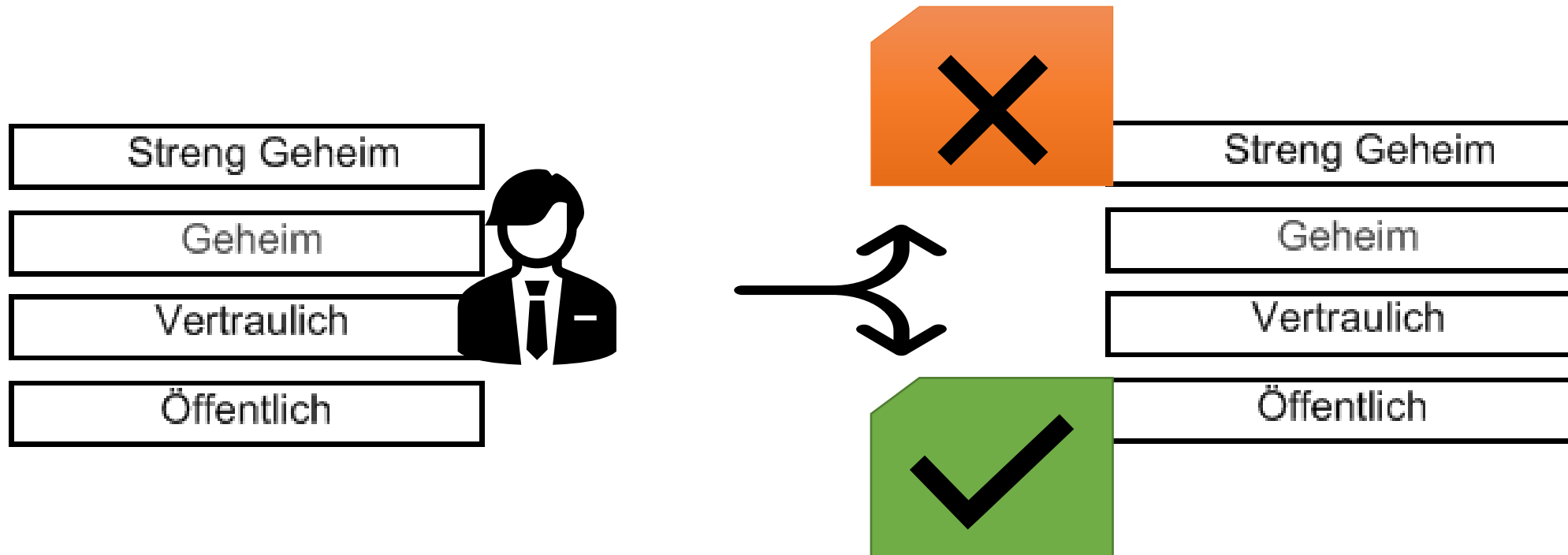


- **Discretionary Access Control**
(Benutzerzentrierte Zugriffskontrolle)
- Zugriffsteuerung auf Basis der Benutzeridentität
- In Windows verwendet, um Zugriff auf Daten im Dateisystem zu regeln



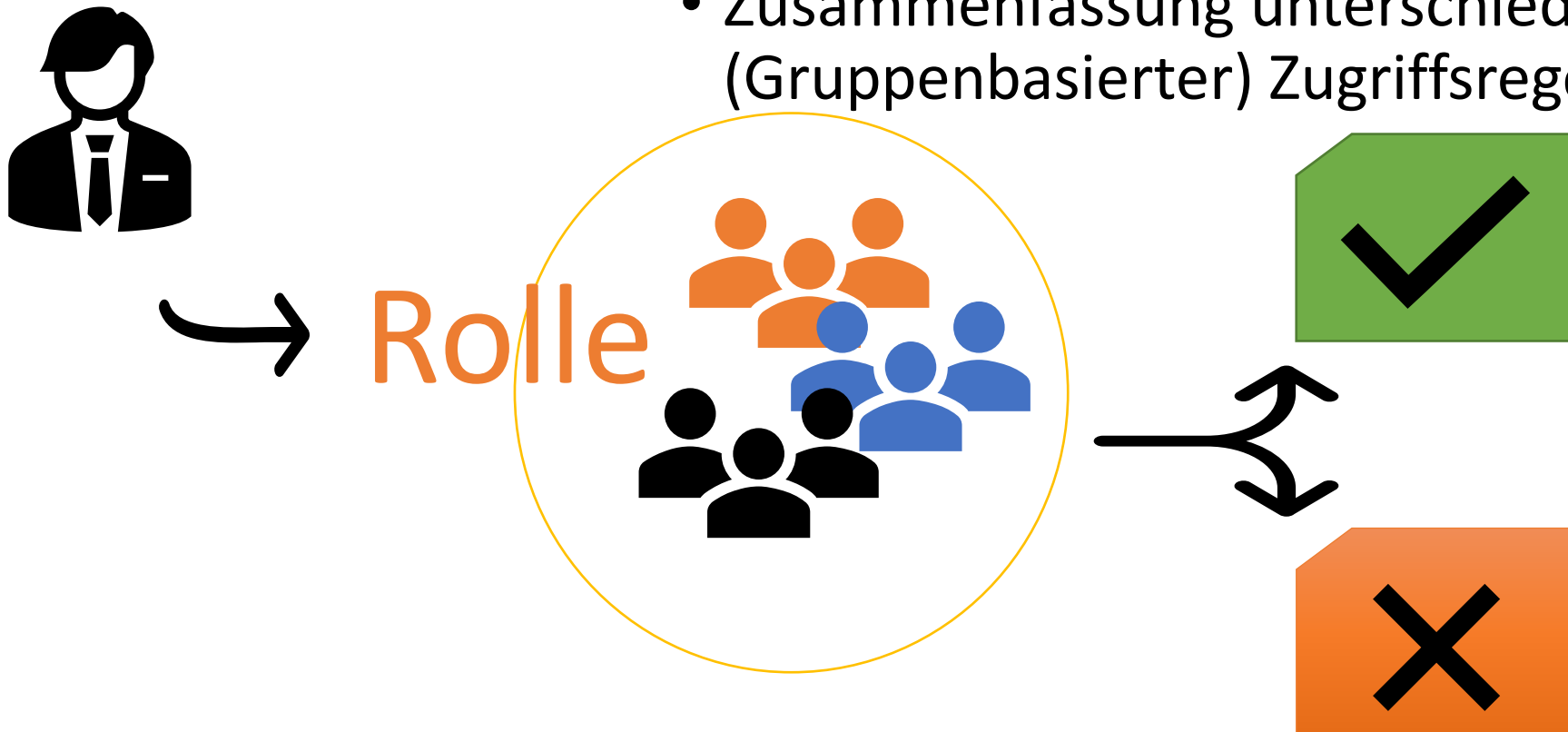
Zugriffsteuerung - MAC

- **Mandatory Access Control** (*zwingend erforderliche Zugriffskontrolle*)
- zusätzliche *Regeln* und *Eigenschaften*



Zugriffsteuerung - RBAC

- **Role Based Access Control** (*Rollenbasierte Zugriffskontrolle*)
- Zusammenfassung unterschiedlicher (Gruppenbasierter) Zugriffsregeln



NTFS - Berechtigungen

- Access Control Lists (ACL) -> DAC
Zugriffsrechte für Benutzer und Gruppen auf
Ordner und Dateien
- vom übergeordneten Verzeichnis vererbt
- Bearbeiten:
 - Datei-Eigenschaften: Reiter Sicherheit
 - cmd: `icacls`
 - Powershell: `get-acl`

Grundlegende Berechtigungen

Vollzugriff: schreiben, löschen, lesen,
Eigenschaften ändern (auch untergeordneter
Elemente)

Ändern: schreiben, löschen, lesen,
Dateieigenschaften ändern

Lesen, Ausführen: Dateien ausführen, lesen
Lesen

Schreiben: Dateien hinzufügen

Grundlegende Berechtigungen

Abhängigkeiten

Vollzugriff: beinhaltet alle anderen Berechtigungen

Ändern: beinhaltet Lesen, Ausführen
Schreiben

Lesen, Ausführen: beinhaltet Lesen

Schreiben. Beinhaltet **NICHT** Lesen, geeignet für Ablageverzeichnisse

Erweiterte Berechtigungen

Erweiterte Berechtigungen:

- | | |
|--|--|
| <input type="checkbox"/> Vollzugriff | <input type="checkbox"/> Attribute schreiben |
| <input checked="" type="checkbox"/> Ordner durchsuchen / Datei ausführen | <input type="checkbox"/> Erweiterte Attribute schreiben |
| <input checked="" type="checkbox"/> Ordner auflisten / Daten lesen | <input type="checkbox"/> Löschen |
| <input checked="" type="checkbox"/> Attribute lesen | <input checked="" type="checkbox"/> Berechtigungen lesen |
| <input checked="" type="checkbox"/> Erweiterte Attribute lesen | <input type="checkbox"/> Berechtigungen ändern |
| <input type="checkbox"/> Dateien erstellen / Daten schreiben | <input type="checkbox"/> Besitz übernehmen |
| <input type="checkbox"/> Ordner erstellen / Daten anhängen | |

Erweiterte Berechtigungen

Ordner durchsuchen/Datei ausführen:

Navigation möglich ohne Berechtigung für
einzelne Ordner oder Dateien

Erweiterte Berechtigungen

Ordner auflisten/Daten lesen:
Inhalte und Dateien eines Ordners ansehen.

Erweiterte Berechtigungen

Attribute lesen:

Attribute einer Datei oder eines Ordners
ansehen

(schreibgeschützt, versteckt, ...)

Erweiterte Berechtigungen

Erweiterte Attribute lesen:

erweiterte Attribute einer Datei oder eines Ordners ansehen.

(verschlüsselt, komprimiert, ...)

Erweiterte Berechtigungen

Dateien erstellen/Daten schreiben:

- Dateien innerhalb eines Ordners erstellen.
(gilt nur für Ordner)
- Datei ändern
(gilt nur für Dateien, nur gemeinsam mit
Leseberechtigung)

Erweiterte Berechtigungen

Ordner erstellen/Daten anhängen:

- Ordner innerhalb eines Ordners erstellen. (gilt nur für Ordner.)
- Änderungen am Ende der Datei vornehmen, (gilt nur für Dateien, nur gemeinsam mit Leseberechtigung)

Erweiterte Berechtigungen

Attribute schreiben

- Attribute von Datei / Ordner ändern
(schreibgeschützt, versteckt, ...)

Erweiterte Berechtigungen

Erweiterte Attribute schreiben

- Attribute von Datei / Ordner ändern
(verschlüsselt, komprimiert, ...)

Erweiterte Berechtigungen

Löschen

- Datei / Ordner löschen
(auch möglich, bei übergeordneter
Berechtigung „Unterordner und Dateien
löschen“)

Erweiterte Berechtigungen

Berechtigungen Lesen

- Lesen der Berechtigungen von Datei / Ordner

Erweiterte Berechtigungen

Berechtigungen Ändern

- Ändern der Berechtigungen einer Datei / eines Ordners
- Besitzer hat immer diese Berechtigung (Besitzübernahme ermöglicht Admin-Zugriff)

Erweiterte Berechtigungen

Besitz übernehmen

- Besitz einer Datei / eines Ordners übernehmen.

Betriebssysteme

Windows-Praxis

Grundlegende Berechtigungen	Vollzugriff	Ändern	Lesen, Ausführen	Lesen	Schreiben
Erweiterte Berechtigungen					
Vollzugriff	✓				
Ordner durchsuchen / Datei ausführen	✓	✓	✓		
Ordner auflisten / Daten lesen	✓	✓	✓	✓	
Attribute lesen	✓	✓	✓	✓	
Erweiterte Attribute lesen	✓	✓	✓	✓	
Dateien erstellen / Daten schreiben	✓	✓			✓
Ordner erstellen / Daten anhängen	✓	✓			✓
Attribute schreiben	✓	✓			✓
Erweiterte Attribute schreiben	✓	✓			✓
Unterordner und Dateien löschen	✓				
Löschen	✓	✓			
Berechtigungen lesen	✓	✓	✓	✓	
Berechtigungen ändern	✓				
Besitz übernehmen	✓				

Vererbung

- Neu erstellte Dateien / Ordner erben Berechtigungen von übergeordnetem Ordner
- kann ausgeschaltet werden
- Umwandlung in explizite Berechtigungen möglich


Verweigern vs. Erlauben

Verweigern hat Vorrang

The image shows a Windows Security dialog box overlaid on a file permissions window. The dialog box contains a warning icon and text explaining that denying permissions takes precedence over allowing them. The background window shows a table of permissions for a file, with columns for 'Zulassen' (Allow) and 'Verweigern' (Deny). The 'Verweigern' column has checkmarks for all listed permissions, while the 'Zulassen' column has checkmarks for all listed permissions. The 'Verweigern' column is highlighted in blue.

Berechtigungen für	Zulassen	Verweigern
Vollzugriff	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ändern	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Lesen, Ausführen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Lesen	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Schreiben	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Windows-Sicherheit

 Sie sind im Begriff einen Zugriffsverweigerungseintrag zu setzen. Zugriffsverweigerungen haben Vorrang vor Zugriffsgenehmigungen. Falls ein Benutzer Mitglied in zwei Gruppen ist, und einer Gruppe der Zugriff genehmigt und der anderen Gruppe der Zugriff verweigert wird, wird dem Benutzer der Zugriff verweigert. Möchten Sie den Vorgang fortsetzen?

Ja Nein

Verweigern vs. Erlauben

Hierarchie der Berechtigungen:

- . Explizit verweigern
- . Explizit erlauben
- . Ererbt verweigern
- . Ererbt erlauben