


## Sicherheit Lektion 4 Zugriffskontrollen

- ✗ Zugriffskontrollen
- ✗ Benutzername und Passwort
- ✗ Biometrische Zugangskontrollen
  
- ✓ Sie haben in der vergangenen Lektion verschiedene Netzwerktypen und Vorteile von Netzwerken erarbeitet. Wie wird nun gewährleistet, dass der Zugriff nur auf jenen Bereich frei gegeben wird, den ein Mitarbeiter oder eine Mitarbeiterin zur Arbeit braucht? Das wird durch Zugriffskontrollen realisiert.



### Aufgabe

Recherchen:  [www.1pw.de/brute-force.html](http://www.1pw.de/brute-force.html),  
[de.wikipedia.org/wiki/Brute-Force-Methode](https://de.wikipedia.org/wiki/Brute-Force-Methode),  
[www.passwordsafe.de](http://www.passwordsafe.de), [www.7-zip.de](http://www.7-zip.de)

#### 1. Zugriffskontrollen

Netzwerkadministratoren und –administratorinnen vernetzen in Unternehmen die einzelnen Rechner und geben den Mitarbeitenden den für die Arbeit jeweils notwendigen Zugang. Sicherheitseinstellungen fallen ebenfalls in ihren Aufgabenbereich.

##### Authentifizierung und Autorisierung

Zum Anmelden müssen sich die Mitarbeitenden *authentifizieren*. Dazu weisen sie sich durch die Eingabe eines Benutzernamens und eines Kennworts aus. Das bedeutet auch, dass jedem Benutzer / jeder Benutzerin ein eigenes Konto zugewiesen wird.

Nachdem die Authentifizierung erfolgte, wird geprüft, welche Zugriffsrechte erlaubt sind. Dieser Vorgang wird *Autorisierung* genannt.

Selbstverständlich setzt dieses System voraus, dass die Benutzenden verantwortungsvoll mit ihren Passwörtern umgehen.

#### 2. Passwort

Richtlinien zum Erstellen von Passwörtern sind die Geheimhaltung, das regelmäßige Ändern und das Erstellen eines sicheren Passworts.

##### Wann ist ein Passwort sicher?

Ein gutes Passwort ...

- ▶ besteht aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen
- ▶ ist derzeit mindestens 8 Zeichen lang
- ▶ ist kein Wort, das in irgendeinem Wörterbuch dieser Erde zu finden ist
- ▶ hat nie einen persönlichen Bezug (Geburtsdatum, Namen, etc.)
- ▶ wird regelmäßig geändert und nicht zweimal verwendet (jeder Zugang hat also ein eigenes Passwort)

Gute Passwörter werden nicht notiert oder in einer Excel-Tabelle gespeichert. Vielerorts erhält man den Tipp, Passwörter aus den ersten Buchstaben der Wörter eines Satzes zu bilden (*Oeh9wsBL* für *Österreich hat 9 wunderschöne Bundesländer*). Schlechte Passwörter sind *asdf* oder *1234* oder *Lieblingsreiseziele* oder *Kosenamen* oder *Autonummern* oder *Fußballclubs* oder *Geburtsjahre*, etc.

### 3. Biometrische Verfahren

Biometrische Verfahren nutzen unverwechselbare Eigenschaften eines Menschen, zB Fingerabdruck, Augenscanner, Gesichts- oder Stimmerkennung. Gucken Sie sich im Geschäft um: Manche Laptops verfügen über einen Fingerabdruckscanner.

## Sicherheit Schritt vier Passwortstrategie

### Übung und Selbststudium

1. Mit Benutzerkonten legen Sie fest, welcher Nutzende was tun darf. Legen Sie in der Systemsteuerung ein Benutzerkonto an und sehen Sie dabei die verschiedenen Rechte an.
2. Überlegen Sie sich eine Passwortstrategie. Recherchieren Sie auch im WWW beispielsweise unter [www.1pw.de/brute-force.html](http://www.1pw.de/brute-force.html) oder [de.wikipedia.org/wiki/Brute-Force-Methode](http://de.wikipedia.org/wiki/Brute-Force-Methode).
3. Wenn Sie viele Passwörter haben, speichern Sie diese Daten nicht einfach in einem Dokument, sondern nutzen Sie zum Verwalten professionelle Tools. Besuchen Sie unter anderem [www.passwordsafe.de](http://www.passwordsafe.de).
4. Sichern Sie Ihre Dateien mit einem Kennwort. Finden Sie in den Eigenschaften eines Ordners oder einer Datei heraus, wie Sie diese Elemente verschlüsseln können. Komprimierte Dateien kann Windows 7 nicht verschlüsseln. Finden Sie also heraus, wie Sie Zip-Dateien mit einem Passwort schützen können. Besuchen Sie unter anderem [www.7-zip.de](http://www.7-zip.de).

### Testen Sie Ihr Wissen

1. Aus welchen Zeichen besteht ein sicheres Passwort?
2. Was ist eine Authentifizierung?
3. Was ist eine Autorisierung?

### Notizen