Security Lektion 4
Zugriffskontrollen

- Zugriffskontrollen
- Passwort
- Komprimierte Dateien schützen
- Dateien und / oder Festplatten verschlüsseln
- Biometrische Zugangskontrollen

✓ Sie haben in der vergangenen Lektion verschiedene Netzwerktypen und Vorteile von Netzwerken erarbeitet. Wie wird nun gewährleistet, dass der Zugriff nur für autorisierte Personen erlaubt wird? Das wird durch Zugriffskontrollen realisiert.

Aufgabe Recherchen: de.wikipedia.org/wiki/Brute-Force-Methode
www.7-zip.de, www.passwordsafe.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. Meist wird ein Zugriff auch protokolliert.

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. Ein gutes Passwort …

- besteht aus Klein- und Großbuchstaben, Ziffern und Sonderzeichen
- ist derzeit mindestens 8 Zeichen lang, besser länger
- 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

.

Weil Passwörter jeweils nur für einen Zugang verwendet werden sollen, brauchen Sie ein System, das Ihre Passwörter sicher verwaltet. Dazu gibt es *Passwortmanager*[1]. Hier

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

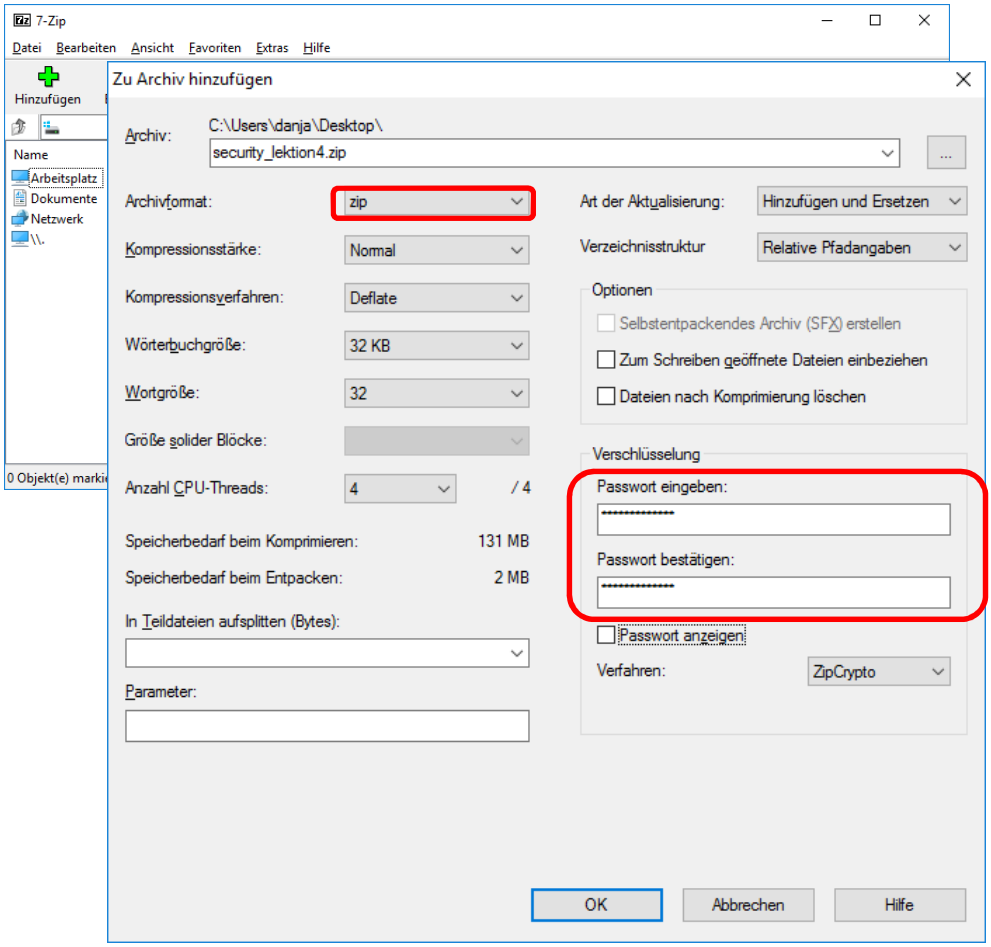
[1] *Informationen dazu finden Sie sicher auch über eine Recherche online. Besuchen Sie beispielsweise http://www.chip.de/news/Passwort-Manager-kostenlos-Alle-Passwoerter-leicht-*

sichern Sie alle Passörter, der Zugang wird ebenfalls durch ein Passwort gesichert. Dieses Passwort halten Sie streng geheim. Lassen Sie Ihren PC oder Ihr mobiles Gerät nicht unbeaufsichtigt. Bei neuen, modernen Systemen wird bereits eine *Multi-Faktor-Authentifizierung* verwendet. Dabei braucht der Nutzende zum Anmelden eine Smart-card und einen PIN-Code.

3. Komprimierte Dateien schützen

Um gezippte Dateien zu schützen, müssen Sie ein zusätzliches Programm installieren. In dieser Übung wird **7-zip** verwendet[2].

- Ziehen sie eine komprimierte Datei in das Anwendungsfenster oder arbeiten Sie über die Navigation auf der linken Seite.
- Im eingeblendeten Dialogfeld ZU ARCHIV HINZUFÜGEN wählen Sie das Archivformat zip (siehe Umrandung oben in der Abbildung).



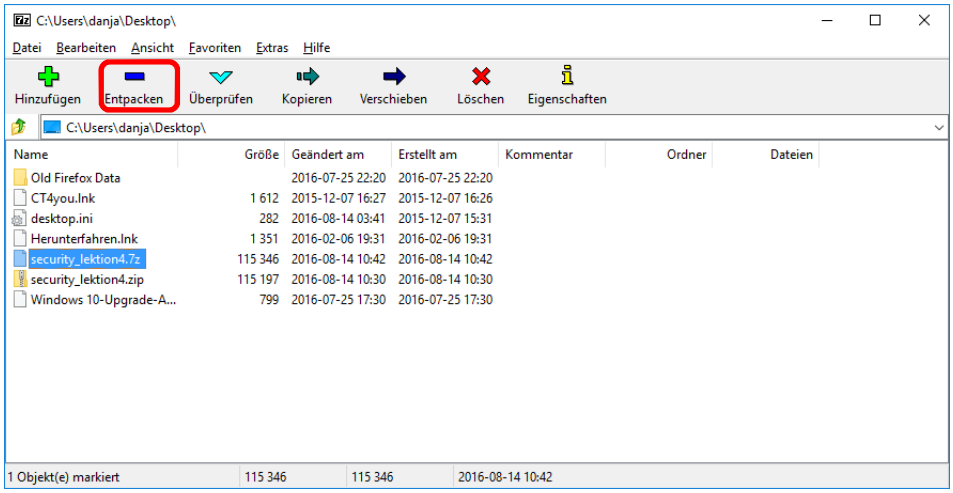
- Geben Sie ein sicheres Passwort ein (siehe Umrandung unten in der Abbildung oben).

---

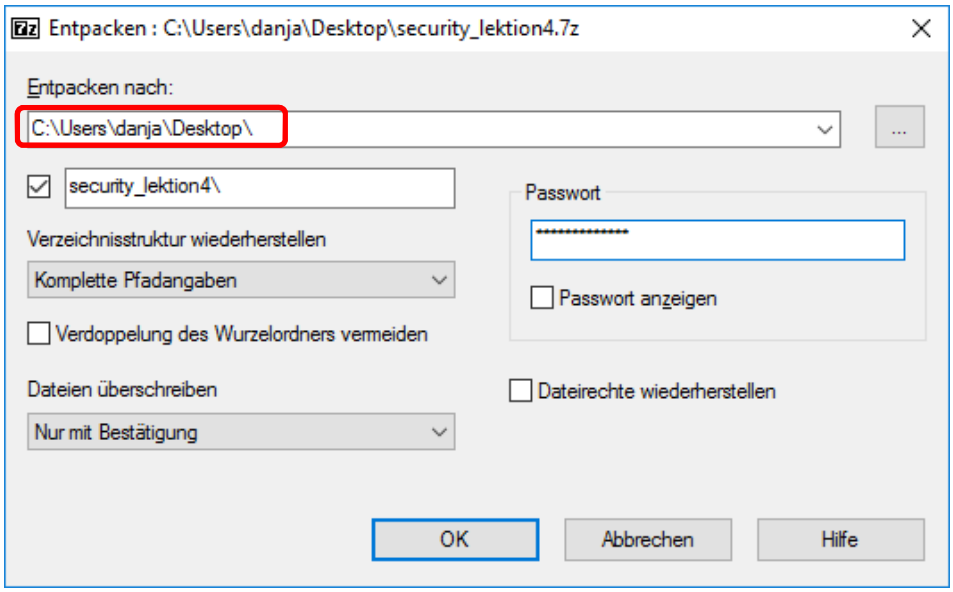
und-sicher-verwalten_76106640.html oder http://www.computerwoche.de/a/die-besten-passwort-manager,2519783.

[2] *Laden Sie diese Software von www.7-zip.de auf Ihren Rechner, installieren Sie es und öffnen Sie die Anwendung.*

- Zum Entpacken wählen Sie im Programm 7-zip die z.zip-Datei aus (siehe Abb.).



- Klicken Sie auf Entpacken (siehe Umrandung in der Abbildung oben).
- Geben Sie das korrekte Passwort ein (siehe Abbildung).

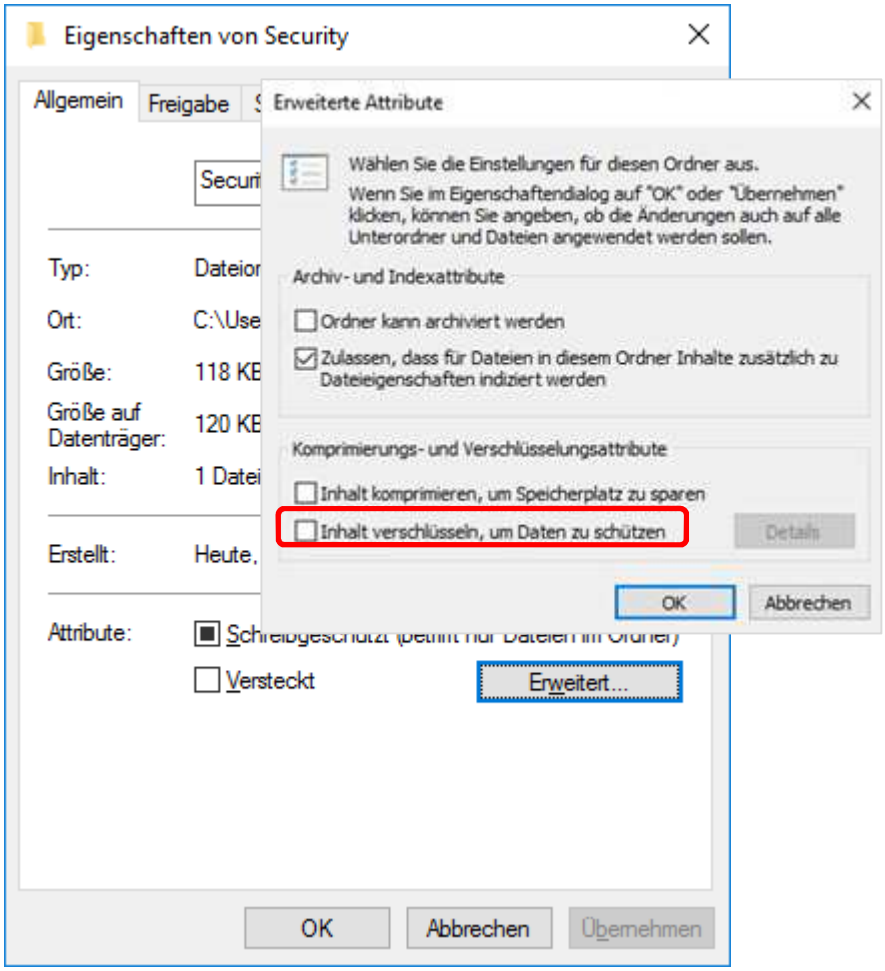


- Sie finden die gezippte Datei in dem angegebenen Ordner, hier also am Desktop (siehe Umrandung in der Abbildung oben).

4. Dateien und / oder Festplatten verschlüsseln

Windows 10 kann in der Version für Unternehmen bereits Dateien ohne weitere Programme verschlüsseln. Bei neuen mobilen Geräte ist ebenfalls eine Verschlüsselung integriert. Mit geeigneten Systemen[3] können sogar Festplatten verschlüsselt werden.

- Klicken Sie im Windows-Explorer eine oder mehrere Dateien oder einen Ordner an und öffnen Sie über das Kontextmenü die **Eigenschaften**.
- Klicken Sie auf **Erweitert** (siehe Abbildung).



- Im eingeblendeten Dialogfeld ERWEITERTE ATTRIBUTE aktivieren Sie das Kontrollfeld INHALT VERSCHLÜSSELN, UM DATEN ZU SCHÜTZEN (siehe Umrandung in der Abbildung).
- Bei Ordnern wird das Dialogfeld ÄNDERUNGEN DER ATTRIBUTE BESTÄTIGEN angezeigt. Wählen Sie eine Option und bestätigen Sie mit **OK**. Bei Dateien

[3] *Unter http://praxistipps.chip.de/windows-10-festplatte-verschluesseln-so-klappts_43269 finden Sie eine übersichtliche Anleitung, wie Sie Festplatten mit dem Programm BitLocker verschlüsseln können. Zu Thema Verschlüsseln unter Windows 10 finden Sie unter anderem auf http://www.computerwoche.de/a/so-schuetzen-sie-ihre-daten,2369354 hilfreiche Informationen. Recherchieren Sie auch selber online zu diesem Thema.*

erhalten Sie ein VERSCHLÜSSELUNGSWARNUNG. Wählen Sie NUR DATEI VERSCHLÜSSELN.

- Bestätigen Sie mit **OK**. Die Datei(en) bzw. der Ordner erhält eine grüne Farbe.

Grenzen einer Verschlüsselung
Zum Verschlüsseln werden komplexe mathematische Algorithmen verwendet. Die Nutzung selber ist für den Anwendenden relativ einfach. Wichtig ist, dass Sie Ihre Passwörter gut verwalten. Geht ein Kennwort nämlich verloren, dann können Sie nicht mehr Auf Ihre Daten zugreifen. Auch die verwendeten Schlüssel dürfen Sie weder verlieren noch an andere Personen weitergeben. Am besten sichern Sie den beim Verschlüsseln erstellten Schlüssel zusätzlich an einem sichern Ort.

5. Biometrische Verfahren

Biometrische Verfahren nutzen unverwechselbare Eigenschaften eines Menschen, zum Beispiel 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 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.
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 nicht verschlüsseln. Finden Sie also heraus, wie Sie Zip-Dateien mit einem Passwort schützen können. Besuchen Sie beispielsweise 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?

Welche Maßnahmen Sie ergreifen können, um im www sicher zu surfen und sicher zu bezahlen, erfahren Sie in der nächsten Lektion.