

L4 1. Chancen und Risiken der Nutzung von Netzwerken: Datensicherheit

1.2 Information:

Zur Datensicherheit zählen technische Maßnahmen, die dem Schutz von allen möglichen Daten dienen. In der Datensicherheit werden unter anderem folgende Ziele verfolgt:

1. Vertraulichkeit: Nur die Personen, die auch berechtigt sind, haben Zugriff auf die jeweiligen Daten.
2. Integrität der Daten: Die Daten werden davor geschützt, von unbefugten Personen z.B. gefälscht oder gelöscht zu werden.

Je nachdem wo Sie Ihre Daten ablegen, ist die Datensicherheit mehr oder auch weniger gefährdet und sie können unterschiedliche Maßnahmen ergreifen, um Ihre Daten zu schützen (vgl. auch vorheriges Thema).

Aufgabe 1

Überlegen Sie, mit welchen Mitteln Sie in Bezug auf Computer und Netzwerke die beiden oben beschriebenen Ziele „Vertraulichkeit“ und „Integrität“ erreichen könnten. Beschreiben Sie 3 oder 4 Maßnahmen, bei Bedarf können Sie dazu auch im Internet recherchieren.

Aufgabe 2

Tauschen Sie sich mit Ihrem Nachbarn und vergleichen Sie Ihre Maßnahmen miteinander. Einigen Sie sich auf 2 oder 3 Maßnahmen, die in Ihrem Umfeld und Alltag umsetzbar sind und die Ihnen helfen können, die Vertraulichkeit und Integrität Ihrer Daten sicherzustellen.

Abschluss:

Stellen Sie die von Ihnen gewählten Maßnahmen in der Klasse kurz vor.

Praktische Anwendung:

Im Umgang mit Computern und Netzwerken ergibt sich immer wieder die Situation, dass man vertrauliche Daten an ungesicherten Stellen abspeichern will (z.B. öffentliche Ordner in Netzwerken, USB-Sticks) oder über ungeschützte Übertragungswege senden möchte (z.B. unverschlüsselte E-Mail). Hier kann eine Lösung darin bestehen, die Daten zu verschlüsseln und bei Bedarf das Kennwort den anderen befugten Personen das Kennwort auf einem anderen sicheren Weg mitzuteilen.

Im folgenden wird Ihnen exemplarisch ein kleines Werkzeug vorgestellt, mit dem sich Daten komprimieren und gleichzeitig sicher verschlüsseln lassen, so dass ein unbefugter Zugriff auf die Daten nicht mehr möglich ist. Dieses Programm ist aber nur eines aus einer größeren Menge an Programmen, die eine Verschlüsselungsmöglichkeit bieten. (Eine andere als sehr sicher angesehene Alternative ist das Programm „VeraCrypt“, das auf der einen Seite zusätzliche Möglichkeiten bietet, dafür aber in der Bedienung komplexer ist.)

Ziel der Einführung ist, dass Sie ein kleines Word-Dokument mit einem geheimen Inhalt schreiben, dieses Dokument verschlüsseln und Ihr Sitznachbar dieses Dokument dann entschlüsseln darf, um zu testen, ob alles geklappt hat.

Schritt 1:

Schauen Sie sich bitte das Video „Verschlüsseln mit 7-zip“ an:

<https://vimeo.com/266398850>

Schritt 2:

Schreiben Sie ein Word-Dokument mit einem kurzen(!) Text, verschlüsseln Sie dieses Dokument und geben Sie es Ihrem Nachbarn (z.B. über das Tauschlaufwerk oder einen USB-stick).

Schritt 3:

Ihr Nachbar erhält von Ihnen das (geheime) Kennwort und versucht, nach Anschauen des Videos „Entschlüsseln mit 7-zip“:

<https://vimeo.com/266405590>

das verschlüsselte Dokument zu entschlüsseln und den Inhalt zu lesen.

Hat es geklappt?

freiwillig:

Testen Sie das Ver- und Entschlüsseln mehrerer Dateien mit 7-zip. Hier ist das Video dazu:

<https://vimeo.com/266408362>