Lesetext Passwörter

L202

Aufgabe:

Lies den folgenden Text einmal für dich durch. Markiere Stellen, die dir wichtig erscheinen.

Beantworte die Fragen am Ende des Textes möglichst genau.

Zeit: 45‘ **Sozialform:** EA

Immer wieder richten Hacker im Internet Unheil an. Viele Menschen machen ihnen das leicht, denn sie haben unsichere Passwörter. Wie aber sollte ein gutes Passwort aussehen?

Passwörter brauchen Menschen am Computer häufig. Wenn sie zum Beispiel bei Facebook ihre Freunde anschreiben wollen, dann müssen sie sich einloggen. Nur wer die Zugangsdaten hat, kommt auf seine Seite. Passwörter werden aber auch abgefragt, wenn die Menschen im Internet etwas kaufen oder einfach nur eine E-Mail schreiben wollen.

Doch Passwörter müssen möglichst sicher gewählt werden. Denn wenn andere sie zu leicht erraten können, dann können sie Unheil anrichten. Sie können beispielsweise unbemerkt E-Mails versenden oder aber einkaufen gehen. Viele Leute benutzen Passwörter, die oft verwendet werden. Das liegt daran, dass die Menschen sie sich leicht merken können. "123456" ist zum Beispiel so ein Passwort. Oder "abc123". Experten sagen: Solche Passwörter sind nicht sicher. Sie sind einfach zu bekannt.

Und wie finde ich ein sicheres Passwort?

Die Experten sagen: Das Passwort darf nicht zu leicht sein. Diebe haben Programme, die zum Beispiel einfach Wörter abfragen, die im Lexikon stehen. Auch sollten wir nicht den Namen unseres Haustieres oder unser Geburtsdatum wählen. Das lässt sich ebenfalls schnell rausfinden.

Gute Passwörter entstehen, wenn Menschen Buchstaben und Zahlen gleichzeitig wählen. Allerdings lässt sich das Passwort "M34a7IeORx3" nicht gut merken. Daher empfehlen die Experten, dass wir uns einen Satz ausdenken sollen, den wir uns gut behalten können. Er kann zum Beispiel lauten: Ich habe Mama lieb. In dem Satz sollten wir bestimmte Buchstaben streichen, damit er unkenntlich wird. Das "a" und das "i" zum Beispiel kann rausgekürzt werden. Dann entsteht: "chhbeMmleb" - ein Passwort, das recht sicher ist. Die Experten sagen ausserdem: Wir sollten Passwörter nie mehrfach nutzen. Für jede Internetseite sollten wir ein eigenes haben. Denn wer immer dasselbe Passwort nutzt, ist leicht übers Ohr zu hauen.

Passwort knacken

Wirklich unknackbar ist am Ende kaum ein Passwort!

Ebenso wenig Begriffe, die in einem Wörterbuch oder Lexikon stehen (könnten). Programme zum Passwortknacken greifen sehr gern auf Lexika, Duden, Namensbücher oder ähnliche Daten zurück

und probieren einfach alle dort enthalten Begriffe nacheinander aus. Eine solche *Bruteforce-Attacke* wäre für uns Menschen an der Tastatur sicher nicht beherrschbar, aber ein Computer-Programm versucht es einfach tausende Male pro Sekunde – wenn sein muss auch über sehr lange Zeiträume.Mit ausreichend Zeit und einem leistungsfähigen Computer lässt sich jedes Passwort irgendwann herausfinden. Es kommt letztendlich nur darauf an, den Aufwand für das Herausfinden zu maximieren und potentielle Angreifer quasi zum Aufgeben zu bewegen.

Fragen zum Textverständnis

1. Welche dieser Passwörter sind unsicher, sicher oder sehr sicher? Übertrage die folgenden Passwörter in die entsprechende Spalte der Tabelle:

Anna2019 D1g(a%r9Wx; Fluffy23 1234567 passwort OBSEs4c8808Pä
sFr3%//s2QxjW OBS mrcoolman fortnite123 asdfg13579 19Bruno75Bello%

unsicher	sicher und einfach	sehr sicher, aber...

2. Wie gehen Hacker beim Knacken von Passwörtern vor und was ist der beste Schutz dagegen? Suche im Text die folgenden Wörter und bilde daraus zwei bis drei ganze, erklärende Sätze:

Hacker Programme abfragen Lexikon Bruteforce-Attacke tausende Sekunde Aufwand maximieren Aufgeben

3. Erstelle ein persönliches, sicheres Passwort nach dem folgenden Muster:

   Nimm diesen Satz:

   Das ist mein sicheres Passwort, an das kommt niemand ran!

   Schreibe alle Anfangsbuchstaben als neue Buchstabenkombination auf:

   _____

   Achte nun noch auf die Gross- und Kleinschreibungen und füge die enthalten Satzzeichen an der richtigen Stelle ein:

   _____

   Um es nun den potentiellen Hackern noch etwas schwerer zu machen, hängst du einfach eine dir vertraute Zahl ans das Ende. Wie wäre es mit Pi oder deinem Geburtsjahr? Einen deutscher Umlaut, den, wenn überhaupt, nur Angreifer aus dem deutschsprachigen Raum in ihren Hackerprogrammen haben, stellst du zudem noch an den Anfang. Fertig!

   _____

   Das Passwort hat nun 15 Zeichen, sieht äusserst komplex aus und dürfte nur sehr schwer knackbar sein. Merken liesse es sich aber recht gut.
   Experimentiere auf einem Blatt Papier einfach mal ein wenig mit dieser Methode herum. Du wirst sehen, wie schnell du sich eine Handvoll ausgezeichneter Passwörter generiert hast.

   _____

   _____

   _____

   _____

   _____

   _____

   _____

4. Suche im Internet nach einem Passwort-Checker und vergleiche die Sicherheit deiner Passwörter.