Was ist ein starkes Passwort?

Je länger ein Passwort, desto schwerer kann es ein Angreifer herausfinden. Deshalb sollte dein Passwort immer so lang wie möglich sein. So ist das Passwort „mecodia rockt das Internet!” mit einem normalen Computer und passender Software schätzungsweise erst nach einer Quintilliarde Jahre berechnet. Es ist also für Software fast unknackbar und auch für andere Menschen nur schwer zu erraten. Auch das Verändern eines Satzes kann schon für mehr Sicherheit sorgen (“Morgenstund hat Bäume im Mund” = 1 Oktillionen Jahre Rechenzeit).

Wie erstellst du ein gutes Passwort?

Satz-Trick
Denke dir einen Satz aus, den du dir leicht merken kannst. Nun nimmst du von den einzelnen Wörtern immer den Anfangsbuchstaben sowie die Zahlen und Sonderzeichen und fügst diese zu einem neuen Wort zusammen.
Ersetzen-Trick (Leet-Speak)
Leetspeak ist eine einfache Möglichkeit ein Wort so zu verändern, dass es als sicheres Passwort eingesetzt werden kann. Dazu werden Buchstaben durch Sonderzeichen und Zahlen ersetzt. So kann zum Beispiel aus einem E eine 3 werden, oder aus einem S wird das Sonderzeichen §.

BEISPIEL
Passwortsicherheit = Pa§sw0rts/ch3rhe1t
Vorteil

Aus einem einfachen Wort lässt sich ein sicheres Passwort zaubern. Gerade auch Menschen aus deinem Umfeld können es dann nicht mehr so einfach erraten.

Nachteil

Es kann eine Weile dauern, bis du das Passwort eingegeben hast. Vertippen kann vorprogrammiert sein. Und wenn dein Passwort zu kurz ist, können Angreifer auch diesen Code einfach knacken.

BEISPIEL

Heute Nachmittag um 16:30 Uhr gehe ich ins Fußballtraining! = HNu16:30giiF!

Vorteil

Einen Satz kannst du dir einfacher merken als viele zufällige Zeichen. Durch den Satztrick hast du trotzdem ein sicheres Passwort. Achte aber immer darauf, dass auch alle Vorraussetzungen erfüllt sind.

Nachteil

Es besteht das Risiko, dass durch den Satztrick ein zu kurzes Passwort entsteht. Achte also immer auf eine ausreichende Zeichenanzahl.

Wort-Trick

Eine weitere Möglichkeit dir ein sicheres Passwort zu erstellen ist das Aneinanderreihen von Wörtern. Nimmst du dir drei Worte, die in keinem logischen Zusammenhang stehen, ergibt das ein sehr langes und sicheres Passwort.

Wie erstellst du ein gutes Passwort?

Passwort variieren

Setze nie überall das gleiche Passwort ein, denn wenn eines geknackt ist, sind alle

anderen Dienste auch nicht mehr sicher. Allerdings verlierst du schnell den Überblick, wenn du für jeden Dienst den Satztrick anwendest oder ein Wort mit Leetspeak aufbesserst. Aber auch dafür gibt es einen einfachen Tipp! Zu deinem sicheren Passwort ergänzt du am Anfang oder Ende noch die ersten drei oder vier Buchstaben des Dienstes, für den du das Passwort benutzen möchtest.

BEISPIEL
Es gibt fast keine einfachere Möglichkeit dir ein langes Passwort zu erstellen. Obwohl du zum Eingeben ein bisschen Zeit benötigst lohnt sich der Aufwand.
Nachteil
Du musst sicherstellen, dass die verschiedenen Worte in keinem logischen Zusammenhang Stehen (z.B. nicht TischFuß oder StuhlBein). Die Worte dürfen sich auch nicht wiederholen.

BEISPIEL
HNu16:30giiF! als Passwort bei Amazon = HNu16:30giiF!Ama
Vorteil
Du hast für jeden Dienst ein eigenes sicheres Passwort, das du dir trotzdem leicht merken kannst. Unser Tipp: Mit dem Satztrick kombinieren!
Nachteil

Vollkommene Sicherheit gibt‘s nicht!
„Fußball“ kann in wenigen Sekunden geknackt werden. An „?Fu55bA77!“ muss ein Angreifer schon länger herumprobieren.

Grundlegend hat ein Angreifer zwei verschiedene herangehenweisen, um dein Passwort zu erhalten. Entweder bricht er auf dem Server eines Dienstanbieters ein oder du lieferst ihm dein Passwort einfach frei Haus. Wie genau das funktioniert kannst du auf den nächsten Seiten nachlesen.
Du darfst nie vergessen, dass jedes Passwort irgendwann geknackt werden kann - egal wie lang es ist. Das dauert vielleicht eine Weile, aber 100% Schutz kann es nie geben.
Check dein Passwort!
Wenn du es testen möchtest, ob dein Passwort wirklich sicher ist, dann schau auf auf der Seite CheckDeinPasswort.de vorbei.

Um zu verstehen, warum du ein sicheres Passwort benötigst und wie du es am besten erstellst, musst du erst einmal verstehen wie ein Angreifer vorgeht, um dein Passwort zu knacken.

Es gilt: Jedes Passwort kann irgendwann geknackt werden. Durch die praktischen Tricks versuchst du also die Zeit zu verlängern, die ein Angreifer zum Knacken benötigt.

Das Passwort Offline-Cracking

Egal ob bei deinem E-Mail-Account, Online-Spielen oder im Facebook-Profil. Bei jedem dieser Dienste legst du dir ein Benutzerkonto zu. Sicherlich hast du schon einmal von Hackerangriffen auf große Unternehmen, z.B. bei Amazon oder Sony, gehört. Hierbei stehlen Angreifer die Benutzerdaten auf dem Server des Anbieters. Dein Benutzername und dein Passwort sind nun in den Händen des Angreifers. Eine Hürde haben die Angreifer noch zu bewältigen. Denn

dein Passwort wird auf den meisten Servern nicht in Klartext gespeichert, sondern als sogenannter Hash verschlüsselt. Ein Hash verschleiert dein Passwort, indem es mithilfe komplizierter mathematischer Funktionen in eine Zahlen-/Buchstabefolge umgerechnet wird.
Der Ablauf einer Anmeldung bei deinem Dienst ist also: Du gibst dein Passwort ein, aus dem eingegebenen Passwort wird ein Hash gebildet und dieser wird mit dem gespeichterten Hash auf dem Server verglichen. Stimmen die Hashs überein, dann wirst du angemeldet. Das Ziel
Wie werden Passwörter geknackt?
des Angreifers ist es also deinen Hash zu berechnen. Das macht der Angreifer jedoch nicht auf dem Server deines Anbieters, sondern auf seinem eigenem Computer oder Mietserver. Deshalb nennt man das „Offline-Attacke".
Hat ein Angreifer deinen Hash erbeutet, dann muss er ihn noch entschlüsseln. Dafür kann er zwei Methoden nutzen.

Brute-Force-Attack

„Attacke der rohen Gewalt"
Die Brute-Force-Attack ist eine Methode, die nach einer gewissen Zeit garantiert zum Erfolg führt. Ein Angreifer lässt von einem Computer dazu möglichst viele Zeichenkombinationen aus Buchstaben, Zahlen und Sonderzeichen berechnen.
Aus diesen erstellten Passwörtern berechnet er dann Hashs, die er mit deinem Hash vergleicht. Ein handelsüblicher Computer kann in einer Sekunde mehrere Millionen solcher Kombinationen durchspielen. Hast du das Passwort „F0ßbA77!", dann muss

der Computer an den acht Stellen des Passworts so lange verschiedene Zeichen einsetzen, bis er das Passwort erraten hat. Das dauert bei einem normalen Computer ungefähr zwölf Jahre.
Durch Zufall kann der Angreifer das Passwort aber auch schon viel schneller erraten. Das ist wie das Suchen der Nadel im Heuhaufen!
Mal findet man sie früher, mal später.

Je länger dein Passwort, desto sicherer ist es!

WIE SIEHT EIN HASH AUS?

Ein SHA-1-Hash für das Wort
F0ßbA77!
ist z.B.
e79e475d0fbc23a10e423c2e0f268a616727f2a8

Wie werden Passwörter geknackt?

dabei möglichst viele Informationen, die dann automatisch ausgewertet werden. Das können auch persönliche Informationen sein (wie dein Wohnort oder Geburtsdatum), die ein Angreifer z.B. in deinem Facebook-Profil finden kann. Mit Kombinationen aus diesen Begriffen starten der Angreifer jetzt eine Dictionary-Attack.
Ein weiteres Problem: 17% der Menschen in Deutschland benutzen reale Namen als Passwort. Viele ergänzen die Namen dann lediglich noch mit einer 01 oder einem Ausrufezeichen. Aus dem Passwort „Berlin” wird dann einfach ein „Berlin01”. Das machen jedoch so viele Menschen, dass viele Angreifer die Informationen, die sie über Spidering

erhalten haben, automatisch ergänzen.
So werden z.B. Name, Wohnort oder ein Produktname einfach noch um bestimmte Zahlen (01,10,123) ergänzt oder es werden Ausrufezeichen angehängt. Durch dieses intelligente Modifizieren von Spidering-Daten haben viele Angreifer einen großen Erfolg.
Passwort ist, desto mehr Möglichkeiten muss der Angreifer berücksichtigen. Er benötigt dann länger, um das Passwort zu knacken.

Dictionary-Attack
„Wörterbuch-Attacke"
Je länger das Passwort, desto schwerer ist für einen Angreifer die Berechnung deines Passworts mit der Brute-Force-Attack. Jedoch machen es viele Menschen den Angreifern unnötig einfach, indem sie simple Wörter benutzen. Passwörter wie „Frankfurt", „Feuerwehr" oder „Passwort" sind keine Seltenheit.
Mit einer Brute-Force-Attacke dauert die Berechnung der Passwörter eine Weile. Daher nimmt sich der Angreifer Wörterbücher, Lexika oder Markenregister zur Hand und probiert alle Begriffe aus, die dort enthalten sind. Nutzt du also ein Wort aus einem Wörterbuch oder zum Beispiel einen Markennamen wie "FC Bayern München", so kann ein Angreifer dein Passwort innerhalb von Minuten Knacken. Wichtig: Viele Namen von Schauspielern, Sängerinnen oder Sportlern sind auch eingetragene Marken!
Eine Dictionary-Attack kann von Angreifern noch effektiver gestaltet werden. Firmenpasswörter haben häufig eine Ähnlichkeit zum Namen oder Produkten der Firma. Deswegen ziehen die Angreifer – wie ein Spinne beim Netzbau ihre Kreise

über Internetseiten und sammeln

Aneignen von Passwörtern

Greift ein Angreifer auf den Server deines Anbieters zu, kannst du daran nichts ändern. Du kannst dich nur durch ein sicheres Passwort schützen, für dessen Berechnung der Angreifer zu lange benötigt. Doch häufig verliert nicht der Anbieter, sondern der Benutzer selbst das Passwort. Durch eigenes Fehlverhalten können andere Menschen von deinem Passwort erfahren und es gegen dich einsetzen!

Soziale Manipulation

Bei dir sollten die Alarmglocken läuten, wenn dir Unbekannte, Unternehmen oder Freunde einen dubiosen Link schicken oder nach deinem Passwort fragen. Absender von E-Mails können leicht gefälscht werden. Über die seriös wirkende E-Mail wirst du auf eine gefälscht Webseite gelockt, die z.B. wie die echte Anmeldeseite deiner Bank aussieht. Hier darfst du niemals deine Anmeldedaten eingeben! Ansonsten bist du ein Phishing-Opfer geworden und auf eine vorgetäuschte Seite hereingefallen.

Besonders dreist ist das Social Engineering. Über Internetdienste können recht einfach Telefonnummern vorgetäuscht werden.

Wenn also im Büro auf einmal das Telefon klingelt und anscheinend die IT-Abteilung am Apparat ist: „Wir bräuchten nur kurz zum Einrichten Ihr Pass-

wort", dann können ein paar kritische Nachfragen nicht schaden! Kurz gesagt: Ob per E-Mail oder am Telefon, traue keinem, der einfach so

nach deinem Passwort fragt!

Malware
Schadprogramme

Unter Schadprogrammen versteht
man ein Programm, welches
dir häufig unbemerkt Schaden zufügen oder
auch Daten stehlen kann. Häufig installieren
sich Schadprogramme durch das blinde Surfen
im Internet.
Lädst du Software von nicht vertrauenswürdigen
Seiten herunter, kann sich sehr schnell
ein Virus, ein Wurm oder ein Trojanisches
Pferd auf deinem Computer oder Smartphone
einnisten. Diese wollen dein Gerät meist nicht
einfach nur kaputt machen. **Heutzutage geht es viel mehr um illegale Datengewinnung!**

So können einige dieser Schadprogramme deine
Passwörter auslesen und sich ungebremst
auf deinen Konten und Geräten bewegen. **Deine Passwörter werden dann an einen Angreifer verschickt – ohne, dass du es bemerkst!**
Lade deshalb Software nur auf vertrauenswürdigen
Seiten, wie z.B. Chip Online herunter!
Aktualisiere laufend deinen Virenschutz auf dem Computer und auf dem Smartphone.

Wie werden Passwörter geknackt?
Shoulder-Surfing
Schulterblick-Methode

Shoulder Surfing ist wohl die einfachste, effektivste und häufigste Methode in deinem Umfeld.
Ein Freund hat dir beim Eingeben deines Passworts über die Schulter geschaut oder kann sonstige Hinweise zu deinem Passwort einsehen.
Hast du dein Passwort zum Beispiel auf einem Notizblatt an den Computer-Bildschirm geklebt, kann jeder Besucher dein Passwort einfach anschauen.
Das Shoulder Surfing hat also nicht mit IT-Wissen zu tun, sondern schlichtweg damit, ob jemand aufpasst während du unaufmerksam bist.
Ähnlich ist das auch mit der Bildschirmsperre auf deinem Smartphone.
Benutzt du dazu ein Muster, dass du nachzeichnen musst, dann ist das oft leicht zu durchschauen.
Durch Fettrückstände deiner Haut auf deinem Display kann jeder dein Muster innerhalb von kürzester Zeit nachfahren, du könntest es ihm also auch gleich zeigen.