

## Passwortsicherheit

Kategorie : security

Veröffentlicht von [Bomania](#) am 05.10.2006

Herr Müller öffnet die Internetseite seiner Online-Bank und möchte eine Überweisung veranlassen. Doch der Kontostand zeigt nicht die erwartete Zahl. Starr blickt Herr Müller auf die nackte Null. Seine Hände werden kalt und feucht. Ein kurzer Anruf bei seiner Bank bestätigt, was er schon befürchtet hatte. Sein Konto wurde leer geräumt.

Nie waren persönliche (Zugangs-)Daten so in Gefahr wie heute. In Zeiten von [Phishing](#), Passwortknackern und [Social Engineering](#) muss ein neues Verständnis für den Umgang mit Passwörtern geschaffen werden. Dieser Artikel behandelt nicht die Aspekte von Verschlüsselungsmethoden, sondern widmet sich ganz dem Wesen und der Handhabung von Passwörtern. Der Artikel ist praxisorientiert und soll auch unversierten Anwendern weiterhelfen.

**Erfahren Sie in diesem Artikel, wie Sie starke Passwörter erstellen und sich merken können. Lernen Sie den sicheren Umgang mit Passwörtern indem Sie Gefahrenmomente beseitigen.**

Einleitung



So bitte nicht - keine personenbezogenen Daten, geschweige denn Klartextwörter Was versteht man überhaupt unter Passwortsicherheit? Und wieso ist das heute so wichtig? Die Passwortsicherheit definiert sich nicht nur durch einen sicheren Aufbewahrungsort des Passworts (das Zettelchen unter der Tastatur gehört übrigens definitiv nicht dazu). Vielmehr ist damit auch die Zusammensetzung des Passworts gemeint. Eine Verschlüsselung - sei sie noch so sicher - ist letztlich wertlos, wenn unsichere Passwörter verwendet werden. Und solche werden auch heute noch häufig eingesetzt. Am Arbeitsplatz, am privaten PC, für E-Mail-Konten, Messenger und Online-Shops. Den Datenschutzbeauftragten dreht sich der Kopf bei soviel Naivität. Deshalb muss ein neues Bewusstsein für Passwörter geschaffen werden um seine Daten geschützt zu wissen.

1. Gefahr erkannt, Gefahr gebannt Zum Thema Passwortsicherheit gehört nicht nur die Stärke eines Passworts. Als erstes sollten Gefahrenquellen ausgeschlossen werden. Und Gefahrenmomente lauern an vielen Stellen. Wer um die Risiken weiß, ist schon einen Schritt weiter. Gefahrenmomente, wie sie unten aufgeführt sind, gefährden die Sicherheit Ihrer Daten und sollten von vornherein ausgeschlossen werden können.

### **1.1 Unverschlüsselte Verbindungen im Webbrowser**

Eine mit SSL verschlüsselte Verbindung überträgt die Daten sicher zum Empfänger. Wenn Sie Daten im Webbrowser eingeben, werden diese grundsätzlich unverschlüsselt gesendet. Das heißt, prinzipiell können Ihre Daten - die richtigen Werkzeuge und das notwendige KnowHow vorausgesetzt - "abgehört" werden. Wenn Sie eine per [SSL](#) verschlüsselte Verbindung verwenden, werden die Daten codiert übertragen und sind so vor fremden Augen geschützt. Man erkennt eine solche gesicherte Verbindung an der URL in der Adressleiste des Internetbrowsers. Statt "<http://www...>" steht dort "<https://www...>". Die meisten Internetbrowser zeigen dies zusätzlich durch farbliche Hervorhebung und kleine grafische Symbole an. Auch wenn SSL/TSL keine perfekte Sicherheitslösung darstellt, ist es doch ein erster und wichtiger Schritt.

**Tipp:** Achten Sie darauf, dass das Server-Zertifikat noch gültig ist! Klicken Sie eine Infomeldung des Browsers nicht leichtfertig weg, wenn von einem abgelaufenen Zertifikat die Rede ist. Mit manipulierten Zertifikaten lassen sich Verbindungen abhören. Was Sie tun können: Wo immer nur möglich sollten Sie gesicherte Datenverbindungen bevorzugen. Dies gilt vor allem dann wenn empfindliche Daten im Spiel sind: Online-Shops, Kreditkarten, Auktionshäuser, E-Mail-Zugang, usw. Viele Online-Shops stellen automatisch beim Bezahlvorgang eine gesicherte Verbindung her. Andere Webseiten bieten dies optional an. So kann z.B. der bekannte [Internet Service Provider](#) "[GMX](#)" auch über <https://> aufgerufen werden.

## 1.2 Unverschlüsseltes WLAN-Netz

Ein unverschlüsseltes WLAN-Netz ist ein leichtes Ziel für Hacker. Die Gefahr lauert hier nicht im Internet sondern vor der Haustür. Es genügt ein WLAN-fähiges Notebook und ein entsprechendes Tool welches WLAN-Netze aufspürt und Zugriff verschafft. Solche Programme gibt es kostenlos im Internet. Die meisten sind in einschlägigen Kreisen wohlbekannt und stellen eine nicht zu unterschätzende Gefahr dar. Ein ungeschütztes WLAN-Netz kann angezapft und abgehört werden. Alles was sie unverschlüsselt ins Internet übertragen, würde sofort in die Hände des Hackers geraten: Kreditkartendaten, Zugangsdaten, persönlicher E-Mail-Verkehr - einfach alles. Darüber hinaus kann der Angreifer kostenlos und unbehelligt über das WLAN-Netz im Internet surfen. Illegale Handlungen würden dann auf die IP-Adresse des WLAN-Betreibers zurück fallen.

Was Sie tun können: Verwenden Sie eine WLAN-Verschlüsselung. Den ehemaligen Standard-Verschlüsselungsalgorithmus [WEP](#) sollten Sie jedoch meiden. Dieser bietet keinerlei Schutz mehr. Der Nachfolger [WPA](#) ist besser geeignet, auch wenn er ebenfalls als nicht mehr so sicher gilt. Viele Geräte unterstützen bereits den Nachfolger [WPA2](#). Verwenden Sie wann immer möglich WPA2 zur Verschlüsselung Ihres WLAN-Netzes. Zusätzlich sollten Sie die [SSID](#) im Router/Access-Point ändern und verstecken lassen. Wählen Sie eine möglichst komplizierte Bezeichnung dafür. Die meisten Geräte bieten die Option, die SSID verstecken zu lassen. Nutzen Sie diese weitere Sicherheitsvorkehrung. Außerdem sollten Sie unbedingt das Standard-Passwort des WLAN-Routers ändern. Wählen Sie ein starkes Passwort! Mehr dazu in Kapitel 2. Als letztes sei noch die Möglichkeit einer [MAC](#)-Filtertabelle erwähnt. Sie lässt sich zwar mit entsprechenden Tools umgehen, aber jede zusätzliche Sicherheitsvorkehrung erhöht den Gesamtschutz des Netzes.

## 1.3 Phishing



Professionell aufgemachte E-Mails sollen das Vertrauen des Anwenders erschleichen. Die Trickbetrüger haben im Laufe der Zeit immer bessere Maschen entwickelt, um unbescholtene Anwender zur Ader zu lassen. Der Begriff *Phishing* leitet sich ab aus dem engl. Wort "fishing" (zu deutsch "abfischen"). Im Grunde ist diese Art der Trickbetrügerei nicht neu. Schon in Zeiten in denen E-Mail und Internet keine Rolle spielten, wurden durch *Social Engineering* vertrauliche Informationen oder Bargeld erschwindelt. Der Täter gibt sich als Angestellter, Administrator oder gar naher Verwandter des Opfers aus. Phishing setzt genau hier an. Durch offiziell anmutende und professionell gestaltete E-Mails soll der Anwender dazu gebracht werden, einen Link in der E-Mail anzuklicken. Meist unter dem Vorwand, die Kundendatenbank müsse gewartet werden. Aber auch andere Gründe erzeugen Handlungsdruck bei den Opfern. Die E-Mails sind täuschend echt dem Original nachempfunden und zielen meist auf Kunden von Online-Banking und Bezahlsysteme wie PayPal ab.

Was Sie tun können: Sie werden aufgefordert, einen Link in der E-Mail anzuklicken um sich einzuloggen? Sie sollen Ihre Online-Banking Zugangsdaten und vielleicht sogar noch TAN-Nummern eingeben? Ignorieren Sie solche E-Mails! Geben Sie die Adresse zu Ihrer Online-Bank, PayPal, eBay, oder sonstiges **ausschließlich manuell im Browser** ein. Ebenfalls wird Sie auch niemals ein vermeintlicher Administrator um Ihre Zugangsdaten bitten! Verwenden Sie ein gutes Virenschutz-Programm und aktualisieren Sie regelmäßig die Virendefinitionsdateien. Benutzen Sie die neusten Browserversionen. [Firefox 2](#) sowie [Internet Explorer 7](#) verfügen über einen eingebauten Phishing-Schutz.

#### 1.4 Illegale Software

Damit sind nicht unbedingt Hackertools gemeint, deren Einsatz außerhalb des lokalen Netzes verboten sind. Vielmehr ist hier die Rede von "Vollversionen", [Cracks](#) und gecrackter Software wie sie in einschlägigen Kreisen zu finden sind. Trotz verschärfter Ermittlungen der Polizei und abmahnwütigen Anwaltskanzleien scheinen viele Anwender noch unbedarft mit dem Thema *Filesharing* umzugehen. Dabei drohen einem nicht nur rechtliche Folgen. Einige Cracker machen sich auch einen Spaß daraus, die freigepatchte Software noch mit einer Hintertür (Trojaner) zu versehen. Mit etwas Pech installiert sich so nicht nur eine illegale Softwarekopie sondern auch gleich ein Keylogger, der sämtliche Tastenanschläge und weitere Informationen aufzeichnet und per Internetverbindung an den Hacker schickt.

Was Sie tun können: Verwenden Sie keine Software aus zweifelhafter Herkunft! Meiden Sie Cracks und "Vollversionen" aus Filesharing-Quellen!

#### 1.5 Standard-Passwörter

Viele Programme und Geräte (wie z.B. Netzrouter) haben ein voreingestelltes Standard-Passwort. Wenn Sie das nicht ändern, ist es ein leichtes Ziel für Hacker. Die versuchen natürlich als erstes das Standard-Passwort.

Was Sie tun können: Ändern Sie in Programmen, Zugängen und Geräten das vordefinierte Standard-Passwort!

## 1.6 Unsichere Aufbewahrungsorte

Das sicherste Versteck für ein Passwort wäre immer noch das Gehirn. Mal abgesehen von *Social Engineering* würde es niemanden gelingen, das Passwort von dort heraus zu bekommen. Doch wer kann sich schon so viele Passwörter für E-Mail, Online-Banking, Messenger, usw. merken? Deshalb werden häufig zwei Fehler gemacht: Entweder wird einfach nur *ein einziges* Passwort für *alles* benutzt. Oder aber die Passwörter werden auf ein Zettelchen geschrieben und "gut versteckt". Noch schlimmer aber, Zugangsdaten in eine einfache Textdatei auf die Festplatte zu speichern. Von alledem raten wir Ihnen unbedingt ab.

Was Sie tun können: Benutzen Sie für jeden Zugang, egal welcher Art, ein eigenes Passwort! Die wichtigsten Passwörter, welche Sie vielleicht täglich benötigen, erstellen Sie mit Hilfe der Tipps aus Kapitel 3. Damit lassen sich die Passwörter gut merken und sind trotzdem schwer zu knacken. Um alle Ihre Passwörter und Zugangsdaten sicher und übersichtlich auf Ihrem Computer zu managen, empfehlen wir Ihnen das kostenlose Tool [KeyPass Password Safe](#). Dieses Programm ist OpenSource und wird ständig weiter entwickelt. Es verfügt über viele nützliche Funktionen und verschlüsselt die Datenbank sehr sicher mit den Algorithmen AES und Twofish. Sie benötigen nur noch ein einziges *Master-Passwort* um das Programm zu öffnen. Dieses sollte natürlich entsprechend stark sein. Lesen Sie dazu mehr im folgenden Kapitel.

2. Starke Passwörter Im letzten Kapitel haben wir einige wichtige Gefahrenquellen beseitigt. Jetzt können wir uns dem zweiten wichtigen Teil zuwenden: Die Passwortstärke.



Zufällig generierte Passwörter sind sicher, lassen sich aber schlecht merken **Das Problem:** Viele Anwender meinen immer noch, es reiche aus, den eigenen Namen mit dem Geburtsjahr zu kombinieren. Ebenfalls beliebt sind Namen von Familienmitgliedern, des Liebessängers oder des Haustieres. Vielleicht noch ganz "raffiniert" irgendwelche Zahlen anhängen. Oder aber eine Buchstabenreihe auf der Tastatur zu verwenden, wie "asdfg" oder "qwertz". Diesem Irrglauben zu unterliegen kann fatale Folgen haben. Selbst wenn Sie Wörter verwenden, die nicht im Zusammenhang mit Ihrer Person stehen, sind solche Passwörter ein leichtes Ziel. Klartext- und Wörterbuchattacken finden solche Passwörter in kürzester Zeit heraus. Daneben werden auch Brute-Force-Attacken eingesetzt. Dies ist die Suche nach dem Passwort mittels Brachialgewalt (brute = brutal). Dabei werden alle möglichen Zeichenkombinationen getestet. Je länger und komplizierter das zu knackende Passwort, desto zeitintensiver ist diese Prozedur.

**Tipp:** Verwenden Sie das kostenlose Programm [Bo-PassCreator](#). Es generiert starke Passwörter, wobei Sie den zu verwendenden Zeichensatz selbst wählen können. Das Programm prüft Ihre Passwörter außerdem auf die *Stärke*, sprich, wie gut das Passwort einer Brute-Force-Attacke standhalten könnte. **Die Lösung:** Verwenden Sie nur starke Passwörter mit mindestens acht

Zeichen. Sie dürfen keine Zeichenfolgen beinhalten die im Wörterbuch zu finden sind. Möglichst kompliziert sollte ein Passwort sein, gemischt mit Zahlen und Buchstaben. Sonderzeichen sollten nach Möglichkeit auch verwendet werden. Das Passwort darf nicht dasselbe sein wie der Benutzername. Verwenden Sie niemals ein Passwort zweimal. Halten Sie sich bei der Wahl Ihrer Passwörter möglichst an folgende Richtlinien.

Das Passwort...

->...muss mindestens acht Zeichen lang sein. ->...oder Teile davon dürfen nicht in einem Wörterbuch zu finden sein. ->...darf nicht aus Wörtern oder Zahlen bestehen, die einen persönlichen Bezug haben. -> ->...sollte aus Buchstaben und Zahlen bestehen; nach Möglichkeit auch mit Sonderzeichen. ->...darf nirgends aufgeschrieben werden (z.B. auf Zettelchen). ->...sollte nach sechs Monaten geändert werden. ->...darf nicht ein bereits zuvor verwendetes Passwort sein.

3. EselsbrückenStarke Passwörter sind schön und gut. Aber wie soll man sich die bitteschön merken? Wie schon im Kapitel "Gefahr erkannt, Gefahr gebannt" angesprochen wurde, können Sie zur sicheren Aufbewahrung Ihrer Zugangsdaten ein entsprechendes Tool verwenden. Es gibt allerdings auch Passwörter die man häufiger benötigt, vielleicht auch unterwegs oder am Arbeitsplatz. Dann nützt das Tool auf dem heimischen PC auch nicht viel wenn Sie keinen Zugriff darauf haben. Wir stellen Ihnen hier zwei Möglichkeiten vor für sichere und gleichzeitig gut merkbare Passwörter.

### 3.1 Ein Passwort mit Geschichte

Geben Sie Ihrem Passwort eine Geschichte. Erfinden Sie einen Satz und verwenden Sie jeweils den Anfangsbuchstaben davon. Achten Sie darauf, Groß- und Kleinbuchstaben sowie Zahlen einzubringen. Hier ein Beispiel wie es aussehen könnte:

*Jeden Montag kaufe ich bei Aldi 15 Liter Cola = JMkibA15LC*

Ein Passwort nach diesem Prinzip ist leicht merkbar und bietet zudem hohen Schutz. In diesem Beispiel ist das Passwort 60 Bit stark, was für den normalen Gebrauch schon recht ansehnlich ist. Mit einem aktuellen Computer würde es etwa ein Jahr dauern, dieses Passwort zu knacken. Zum Vergleich, ein Passwort wie "qwertz" ist nur 29 Bit stark und würde nicht einmal eine Stunde überstehen.

### 3.2 1337 1s k3w1

**Tip**: Auf typische Hackerbegriffe wie "h4xX0r", "0wn0rz", "k3w1", "n00b", etc. sollten Sie verzichten. Diese sind bekannt und wären schnell erraten. Die sog. Leetspeak macht sich die optische Ähnlichkeit von Zahlen und Buchstaben zunutze. Leet (1337) ist ursprünglich aus einschlägigen Hackerkreisen bekannt und wird auch heute noch häufig verwendet. Überwiegend in Chats oder zur Verwendung in Nicknamen. Ein Beispiel wie es aussehen könnte:

*MeinPasswortfürMail = M31nP4ssw0rt4M41l*

Hier wurden vor allem die Vokale ausgetauscht. E wird zu 3, A wird zu 4, usw. Das Wort "für" wurde gegen 4 ausgetauscht, da sich im englischen wie auch im deutschen die beiden Wörter beim Aussprechen ähneln. Ein solches Passwort lässt sich ebenfalls leicht merken, optional können auch Sonderzeichen eingesetzt werden.

Das typische Leet-Alphabet:

->A = 4, @ ->B = ß ->C = © ->D = |) ->E = 3, € ->F = f ->G = 6, 9 ->H = # ->I = ! ->J = ¿ ->K = X ->L = 1, | ->M = AA, ^^ ->N = ?, 2 ->O = 0, ° ->P = |², |? ->Q = 0\_ ->R = ®, ? ->S = 5, \$, § ->T = 7, † ->U = μ ->V = /, ' ->W = VV, |/ ->X = >Y = ¥ ->Z = 2

**Fazit**Die Passwortsicherheit spielt nachwievor eine große Rolle. Nicht nur am Arbeitsplatz sondern auch am heimischen PC. Gerade auch, weil das Internet immer mehr Möglichkeiten bietet. Zugangsdaten begleiten jeden Anwender durch den PC-Alltag. Sie sorgen dafür, dass Zugriff auf ein System, Netz oder persönliche Daten nur berechtigten Personen möglich ist. Wer leichtfertig mit Passwörtern umgeht, sie unverschlüsselt auf dem Computer speichert oder auf einem Zettel notiert, riskiert Zugriff durch Fremde. Auch am Arbeitsplatz kann dies weitgehende Folgen haben. Unsichere Passwörter laden dazu ein, geknackt zu werden. Im schlimmsten Fall wird Ihr System kompromittiert oder auf Ihren Namen Bestellungen getätigt.

Mit wenigen Schritten lässt sich die Sicherheit erhöhen. Dieser Artikel soll aufzeigen worauf es ankommt: Ein gesunder Umgang mit Passwörtern. Gefahrenquellen finden und beseitigen. Starke Passwörter benutzen. Damit sind Sie gerüstet für den PC-Alltag und die Welt wird wieder ein Stückchen sicherer. (bba)

#### **Weblinks**

->[KeePass Password Safe](#) ->[Bo-PassCreator](#) ->[Password Generator](#)