Das Passwort A-Z

Das 4Ws Netdesign Nachschlagewerk für den sicheren Umgang mit Passwörtern

von Thomas Winterhalter

2. überarbeitete Auflage, Januar 2019

Vorwort:

Es hat natürlich einiges an Arbeit gemacht, dieses Essay zusammenzustellen .

Trotzdem stellen wir es **kostenlos** zur freien Verfügung. Sie können dieses Essay beliebig verwenden, ausdrucken und auch gerne an Freunde, Bekannte, Verwandte, Kollegen etc. weitergeben und weiterschicken.

Wir hoffen, es hilft Ihre Sicherheit im Internet weiter zu erhöhen!

Über eine kleine Spende als Anerkennung unserer Arbeit freuen wir uns aber natürlich sehr.

Über Paypal:
paypal@webinside.de

Inhaltsverzeichnis

1. Einleitung

2013 und 2014 wurden viele Nutzer im Internet erstmals aufgeschreckt:

Zig Millionen Passwörter – insbesondere von eMail-Adressen - wurden geknackt und auch für kriminelle Zwecke missbraucht!

Sogar das Bundeskriminalamt warnte, als Anfang 2014 ein kriminelles Netzwerk entdeckt wurde, in dem sich über 16 Millionen Zugangsdaten fanden. Anfang April 2014 wurden weitere 18 Millionen Zugangsdaten gefunden. In den Folgejahren wurden durch Hacker hunderte Millionen Passwörter teilweise von großen Anbietern geknackt.

Das war aber leider nur der Anfang – es kam immer wieder zu sogenannten Leaks und gipfelte aktuell im Januar 2019, als über 2,4 Milliarden eMail-Adressen mit zugehörigen Passwörtern im Internet auftauchten.

Wer Ihr Passwort kennt, kann nicht nur Schabernack treiben: er kann unter Umständen Ihr Bankkonto leer räumen, er kann Ihren Ruf komplett ruinieren, er kann in Ihrem Namen einkaufen, Verträge abschließen und vieles mehr!

All zu lange vernachlässigten viele Nutzer das wirklich wichtige Thema Passwort-Sicherheit. Mit diesem Essay möchten wir Ihnen helfen, Ihren Internet-Alltag wieder ein großes Stück sicherer zu machen!

Sichern Sie sich ab! Ein paar einfache Grundregeln helfen bereits entscheidend weiter!

In diesem kleinen Essay finden Sie die wichtigsten Informationen, was Sie tun und was Sie auf keinen Fall machen sollten, Tricks und Kniffe und mehr!

Wir können Ihnen nur empfehlen, die Ratschläge zu beherzigen, bevor eines Tages die dicke Rechnung folgt. Schon ein paar einfache Kniffe machen Ihre tagtägliche Arbeit mit Passwörtern im Internet deutlich sicherer, im Idealfall befolgen Sie alle erwähnten Möglichkeiten und bleiben immer wachsam und misstrauisch, dann werden Sie hoffentlich nie Opfer einer Attacke!

2. Die häufigsten Fehler

2.1. Problem: Unsichere Passwörter

Das Hauptproblem sind bis heute nicht raffinierte Hacker, sondern einfach Nutzer, die aus Unwissenheit oder Bequemlichkeit zu einfache Passwörter verwenden! Anbei ein Auszug, was bis heute leider nur allzu gerne als Passwort verwendet wird:

- **passwort**
- **passwort1**
- **1234567**
- **abcdefg**
- **iloveyou**
- **jesus**
- **hallo**
- **sex**
- **ficken** (nun ja, das findet sich wirklich unter den Top 10 der aufgetauchten Passwörter)
- **qwertz** (diese und alle anderen Buchstabenfolgen, die auf der Tastatur direkt nebeneinander liegen)
- **schatz**
- **schalke04**
- **test**

Tun Sie es bitte nicht! Das sind keine sicheren Passwörter!

Sie sollten auch niemals Ihren Benutzernamen als Passwort verwenden!

Genauso schlecht sind Namen jeglicher Art, normale Wörter, Geburtstage und Jahrestage jeglicher Art etc.

- ✖ **christian**
- ✖ **johanna**
- ✖ **hans**
- ✖ **09.05.1965**
- ✖ **09051975**
- ✖ **stuttgart**
- ✖ **berlin**

Der Rat kann nur lauten: Finger weg von Namen und Vornamen und Datums jeglicher Art – das ist so unsicher, da können Sie auch direkt kein Passwort verwenden!
Auch wenn Sie versuchen, Namen durch Anhängen beispielsweise von Geburtsjahren oder sonstigen Zahlen oder einzelnen Sonderzeichen sicher zu machen: auch das sind keine sicheren Passwörter!

- ✖ **klaus1965**
- ✖ **nadine1990**
- ✖ **michael%**
- ✖ **martina$**

Und insbesondere alles, was Sie in Ihrem Wörterbuch finden, sind keine guten Passwörter, egal ob auf Deutsch, Englisch oder in anderen Sprachen!:

- ✖ **hund**
- ✖ **katze**
- ✖ **maus**
- ✖ **mercedes**
- ✖ **monkey**

Vermeiden Sie solche Passwörter und Sie haben den ersten und wichtigsten Schritt für Ihre eigene Sicherheit getan! Unsichere Passwörter sind tatsächlich bis heute das Hauptproblem in Punkto Sicherheit! Accounts, die solche Passwörter verwenden, werden mit schönster Regelmäßigkeit geknackt.

Was stattdessen wirklich sichere Passwörter sind, erfahren Sie im Kapitel 3.1

2.2. Problem: Passwort-Verlust durch Phishing-eMails

Ganoven und Gauner versuchen aber auch auf anderen Wege an Ihre Zugangsdaten zu gelangen. Das zweitgrößte Problem in diesem Bereich sind sogenannte Phising-eMails.

Dabei wird versucht, Sie per eMail zu überzeugen, *irgendwo* Ihre Zugangsdaten einzugeben.

Wann immer Sie eine eMail erhalten, in der Sie aufgefordert werden, dass Sie wegen eines Systemupdates/ einer Umstellung/ eines Fehlers oder weil Ihr Konto gehackt wurde oder was auch immer einen Link in der Mail zu klicken und dann irgendwo Ihr Passwort einzugeben:

Tun Sie es nicht!

Dies sind sogenannt Phising-eMails. Gemeiner weise sehen diese eMails oft täuschend echt aus und sind perfekt den anderen eMails von Anbietern nachempfunden. Aber egal, ob die Mail scheinbar von Ihrer Sparkasse, von Amazon, der Telekom, Hotel.de, 1&1 oder wem auch immer kommt: werden Sie aufgefordert, Ihre Zugangsdaten einzugeben:

T**un Sie es nicht!**

Es handelt sich hierbei um Versuche, Ihre Zugangsdaten auszuspähen!

Oft enthalten diese Mails einen Link. Wenn Sie hier klicken, landen Sie auf einer Seite, die oft ebenfalls perfekt genauso wie beispielsweise die Startseite Ihrer Bank aussieht. Aber es ist nicht Ihre Bank! Für einen Profi ist es keinerlei Problem, jede x-beliebige Internetseite optisch in kürzester Zeit 1:1 nachzubauen!

Glauben Sie nicht, was Sie sehen – seien Sie auf der Hut!

Kein seriöser Anbieter wird Sie jemals auffordern, auf diese Art und Weise Ihre Zugangsdaten preiszugeben. Wenn Sie unsicher sind, greifen Sie zum Telefon, rufen Sie an und fragen nach! Verwenden Sie hierfür aber nicht eine Telefonnummer, die evtl. in der eMail selbst aufgeführt ist – auch diese Nummer könnte gefälscht sein und Sie eher zu einem Kunden-Veruntreuer als zu einem Kunden-Betreuer führen!

2.2.1. Problem: Phising auch am Telefon

"Guten Tag, hier ist Herr Müller von der Sparkasse. Leider gab es ein Problem mit Ihrem Konto. Wir konnten zum Glück reagieren und das schlimmste verhindern, benötigen nun aber Ihren Benutzernamen und Ihre Zugangsdaten, um alles wieder einzurichten."

Auch per Telefon versuchen Kriminelle mittlerweile an Zugangsdaten zu gelangen! Auch hier gilt: keine Bank und auch sonst kein seriöser Anbieter wird Sie jemals telefonisch nach Ihren Zugangsdaten fragen! Legen Sie in dem Fall gleich wieder auf und informieren Sie gegebenenfalls durchaus auch die Polizei und die betroffene Bank!

2.3. Problem: Passwort-Verlust durch Computerviren und Trojaner

Subtiler sind bestimmte Computerviren, die sich unbemerkt auf Ihrem Computer einnisten und all Ihre Eingaben ab sofort überwachen.

Kleine spezielle Programme, sogenannte Trojaner benannt nach dem berühmten trojanischen Pferd, überwachen Sie fortan aus dem Hintergrund und schicken all Ihre Daten und eingegebenen Passwörter und Zugangsdaten an Kriminelle im Internet.

Seien Sie besonders vorsichtig, wenn Sie Dateien aus dem Internet erhalten oder downloaden oder eMails mit Anhang öffnen möchten: hier verbergen sich leider all zu oft Computer-Viren.

Installieren Sie unbedingt einen aktuellen Virenscanner auf Ihrem Rechner und aktivieren Sie die Firewall – das ist zwar kein 100%iger Schutz, aber er wird sehr, sehr viel übles verhindern. Ansonsten gilt auch hier: seien Sie wachsam und misstrauisch – ein Patentrezept, sich vollständig zu schützen gibt es leider nicht!

Computerviren finden übrigens nicht nur ihren Weg über Internet und eMail auf Ihren Rechner, auch USB-Sticks, CDs und DVDs sind beliebte Verteilungswege.

Stecken Sie also nicht jeden USB-Stick ohne Nachdenken an Ihren Rechner!

Wichtig! Trauen Sie keinem e-Mail Absender

Einen eMail-Absender zu fälschen ist leider kinderleicht.

Auch wenn eine eMail scheinbar von einem Bekannten oder Geschäftspartner kommt, schauen Sie lieber zweimal hin, bevor Sie einen Anhang öffnen.

Fragen Sie im Zweifelsfall lieber nach.

Leider verbreiten sich mittlerweile nicht nur Computerviren und Trojaner auf diesem Wege sondern auch sehr gefährliche Ransomware.

Hierbei handelt es sich um Schädlinge, die alle Daten auf Ihrem Rechner verschlüsseln und – wenn überhaupt – nur gegen Zahlung eines hohen Lösegelds wieder freigeben.

2.4. Problem: veraltete Systeme

Es gibt einen Grund, warum Ihr Smartphone, Ihr Tablet, aber auch Programme wie der AdobeReader, der Flashplayer, Windows und viele Programme mehr ständig Updates möchten: es geht nicht selten um Ihre Sicherheit!

Leider gibt es oft sogenannte Sicherheitslücken durch Fehler in Computer-Programmen. Sollte nicht so sein, ist es in der Realität aber leider ständig der Fall! Auch deswegen veröffentlichen Anbieter fortlaufend neue Versionen ihrer Programme. Sie sollten diese Updates unbedingt immer installieren, damit Sie nicht Opfer eines Angriffs über ein veraltetes System werden und sich dann evtl. auf diesem Wege ein Trojanisches Pferd auf Ihrem Rechner einschleusen kann.

2.5. Problem: Verwendung des immergleichen Passworts

Verwenden Sie möglichst für jeden Anbieter ein eigenes Passwort! Warum? Wird beispielsweise durch ein Sicherheitsproblem bei einem Anbieter Ihr Passwort bekannt, sind Ihre anderen Online-Shops, Online-Banking und vieles mehr trotzdem sicher! Je mehr unterschiedliche Passwörter Sie verwenden, umso besser! Mehr zu diesem Punkt ebenfalls in Kapitel 3.

2.6. Problem: Einsatz von Passwörtern in offenen WLANs

Was leider kaum jemand weiß oder beachtet: wenn Sie in einem offenen, d.h. unverschlüsselten WLAN drahtlos surfen und Passwörter unverschlüsselt eingeben, ist es sehr einfach, Ihre Passwörter abzufangen.

Es gibt sogar kostenlose Tools im Internet, mit denen sich bespielsweise in öffentlichen Cafés mit einigen wenigen Mouseclicks die Facebook-Zugangsdaten von anderen Leuten ausspähen lassen.

Also achten Sie im Urlaub unbedingt auch darauf, dass das Surfen in WLANs gefährlich sein kann! Wie man es besser machen kann, erfahren Sie ebenfalls im Kapitel 3!

2.7. Problem: Notierte Passwörter

Leider sieht man nur allzu oft kleine Zettel neben Computern liegen, auf denen fein säuberlich die wichtigsten Zugangsdaten notiert sind.

Dass dies im Fall des Falles natürlich nicht gerade sicher ist, insbesondere, wenn der Computer auch für andere Personen zugänglich ist, sagt schon der gesunde Menschenverstand!

2.8. Problem: Verwendung von voreingestellten Passwörtern

An bestimmten Stellen wie beispielsweise in Ihrem DSL-Router sind oft bestimmte Passwörter voreingestellt. Sie sollten diese Passwörter unbedingt möglichst umgehend gegen ein sicheres Passwort austauschen!

Je nach System sind die voreingestellten Passwörter mal mehr mal weniger sicher und theoretisch können natürlich auch bereits andere Menschen diese voreingestellten Passwörter gelesen haben!

3. Empfehlungen

Nachdem wir nun viel gehört haben, was man falsch machen kann, wie macht man es denn nun richtig?

3.1. Wie sieht ein sicheres Passwort aus?

Als erstes gilt: wählen Sie sichere Passwörter! Ein sicheres Passwort hat mindestens 8 besser 12 Zeichen, enthält Klein -und Großbuchstaben, Zahlen und Sonderzeichen und ist im Idealfall völlig zufällig!

✔ **Qs,b-[7DbgEhxxc1**

Autsch! Und das soll ich mir merken? Ja! Es ist leider nicht einfach, aber Sie können es sich z.B. etwas einfacher machen, indem Sie sich Merksätze bilden und dann immer den ersten Buchstaben für das Passwort verwenden, bestimmte Buchstaben durch Zahlen oder Sonderzeichen austauschen.
Auf der Seite des Bundesamts für Sicherheit in der Informationstechnik finden Sie beispielsweise folgenden Tipp:

Wie merkt man sich ein solches Passwort? Auch dafür gibt es Tricks. Eine beliebte Methode funktioniert so: Man denkt sich einen Satz aus und benutzt von jedem Wort nur den 1. Buchstaben (oder nur den 2. oder letzten, etc.). Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen. Hier ein Beispiel:

"**M**orgens **s**tehe **i**ch **a**uf **u**nd **p**utze **m**ir **m**eine **Z**ähne **d**rei **M**inuten **l**ang."

Nur die 1. Buchstaben: "**MsiaupmmZdMl**". "i und l" sieht aus wie "1", "&" ersetzt das "und" – so wird aus dem Merksatz folgendes Passwort:

Ms1a&pmmZ3M1

Auf diese Weise hat man sich eine gute "Eselsbrücke" gebaut. Natürlich gibt es viele andere Tricks und Methoden, die genauso gut funktionieren.
Wichtig ist hierbei, dass sich der Benutzer des Passwortes den Satz **selbst ausgedacht** hat. Werden zum Beispiel die Anfangsbuchstaben eines Literaturzitates als Passwort gewählt, dann ist prinzipiell die Möglichkeit einer sogenannten Wörterbuchattacke nicht viel unrealistischer, als wenn direkt ein Wort verwendet würde. Dies trifft natürlich insbesondere für weithin bekannte Zitate zu.[1]

3.2. Das 4 Stufen-Konzept

Im Idealfall verwenden Sie für jeden Anbieter ein eigenes Passwort!

Aber seien wir ehrlich: das macht niemand! Es ist schwierig und aufwändig und im Alltag wenig praktikabel, hunderte verschiedene Passwörter im Kopf zu behalten. Aber es wäre tatsächlich der Idealfall! In der Praxis hilft Ihnen aber vielleicht die Strategie, Ihre Passwörter in 4 verschiedene Sicherheitsstufen einzuteilen. D.h. Sie verwenden 4 verschiedene und wirklich sichere Passwörter für verschiedene Bereiche. Natürlich steht es Ihnen auch frei 5 oder 6 oder mehr verschiedene Passwörter zu verwenden - je mehr desto besser!

Dies ist nur eine Anregung, um das Arbeiten mit Passwörtern praktikabel zu machen!

Im folgenden finden Sie aufgeschlüsselt, wie Sie beispielsweise ein 4 Stufen-Passwort-Konzept für sich sinnvoll einsetzen können und auf was Sie besonderen Augenmerk legen sollten.

1 Quelle: https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html – Stand 6.4.2014

3.2.1. Besonders sichern: das eMail-Passwort

Ein besonderes Augenmerk sollten Sie Ihrem eMail-Passwort widmen. Warum? Wenn Sie irgendwo registriert sind und ein Passwort vergessen, können Sie in der Regel per eMail das Passwort zurücksetzen lassen und neu vergeben!

Auf fast jeder Seite findet sich ein Punkt

> Passwort vergessen?

Wenn Sie hier klicken und Ihre eMail-Adresse angeben, erhalten Sie oft eine Anleitung, wie Sie Ihr Passwort nun ändern können oder sogar direkt ein neues Passwort.

Kennt jemand also Ihr eMail-Passwort, hat er prinzipiell die Möglichkeit, mit wenig Aufwand auch andere Zugangsdaten von Ihnen zu kapern, was natürlich sehr unangenehm wäre.

Ihr eMail-Passwort sollte daher wirklich einmalig und besonders kompliziert und zufällig sein.

3.2.2. Besonders sichern: Online-Banking

Besonders wichtig ist auch, dass Sie für Ihre Online-Konten besonders sichere und einmalige Passwörter verwenden! Warum liegt nahe! Jemand der die Zugangsdaten zu Ihrem Online-Konto kennt, hat schon den halben Weg beschritten, um Ihr Konto zu plündern!

Wenn möglich, verwenden Sie statt TAN-Verfahren lieber HBCI. Sie erhalten hierfür ein kleines Gerät von Ihrer Bank, das Sie an Ihren Computer anschließen können. Dieses Gerät verschlüsselt die Kommunikation mit der Bank. Sie müssen hierfür jedes Mal ähnlich wie an einem Geldautomat eine PIN eingeben.

Der Vorteil: selbst, wenn Ihr Computer von einem Virus oder Trojaner infiziert ist: das HBCI-Gerät läuft rein technisch "außerhalb" des Computers und der Virus hat keinen Zugriff darauf. Außerdem müssen Sie nicht mehr mit langen TAN-Listen arbeiten. Alternativen sind auch das mobileTAN Verfahren, bei dem Smartphones zum Einsatz kommen, oder sogenannte TAN-Generatoren.

3.2.3. Besonders sichern: Shopping

Ähnliche Überlegungen gelten, wenn Sie gerne in Online-Shops wie Amazon und Co. einkaufen. Wenn Sie hier Benutzerkonten mit Benutzername und Passwort anlegen, ist Ihr nächster Einkauf natürlich komfortabler, aber wenn diese Zugangsdaten in falsche Hände geraten, besteht die große Gefahr, dass auf Ihre Rechnung munter eingekauft wird!

Für Online-Shopping sollten Sie also eine dritte sichere Stufe an Passwörter einsetzen.

3.2.4. Weitere Passwörter

Auf der vierten Stufe siedeln wir nun mal alle weiteren Passwörter an, beispielsweise zu Facebook, Twitter und anderen sozialen Medien. Natürlich sollten alle Passwörter sicher sein, aber man kann auch realistisch überlegen: was kann im schlimmsten Fall passieren?

Wenn jemand Ihren Facebook-Account kapert, kann dies lästig sein, aber Ihr Online-Konto wäre in unserem vier Stufen Model beispielsweise dank anderem Passwort trotzdem perfekt geschützt.

Seien Sie einfach ehrlich und überlegen Sie: wie sehr Sie der Verlust eines Passworts schmerzen würde. Wenn Sie dabei kein Bauchweh bekommen, verwenden sie hierfür das Passwort der vierten Stufe.

3.3. In Online-Shops als Gast bestellen

Wenn Sie in Online-Shops bestellen, können Sie oft auch ohne Anmeldung, also **ohne einen Benutzernamen und Passwort anzulegen, bestellen**. Insbesondere, wenn Sie nur selten in einem bestimmten Shop bestellen, sollten Sie das auch machen – wenn der Shop diese Möglichkeit anbietet.

Letztendlich wissen Sie nie, was in dem Shop mit Ihren Zugangsdaten passiert. Und je weniger Stellen Ihre Zugangsdaten kennen, umso besser ist es!

Wenn Sie einem Shop nicht trauen, bestellen Sie auch besser auf Rechnung, mit Nachnahme oder mit Vorkasse. Vermeiden Sie es, Kreditkarten-Nummern und Kontodaten einzugeben, wenn Sie sich unsicher fühlen!

3.4. Passwörter nicht speichern!

Ihr Internetprogramm und auch andere Programme bieten es Ihnen fortlaufend an: "Möchten Sie dieses Passwort speichern?"

Wenn Sie ganz sicher gehen wollen, antworten Sie konsequent mit "Nein"!

Wenn Ihr Passwort gespeichert ist, besteht natürlich immer eine größere Gefahr, dass es in falsche Hände gerät, denn nun ist es nicht mehr nur in Ihrem Kopf, sondern schon in Ihrem Computer. Und ganz ehrlich: wissen Sie wo und wie genau? Wohl eher nicht ;-)

Um wieder auf das 4-Stufen-Modell zurückzukommen wäre die Empfehlung: speichern Sie auf keinen Fall Passwörter der ersten 3 Stufen, bei der vierten Stufe können Sie es des Komforts halber in Erwägung ziehen.

Um nochmals Missverständnisse auszuschließen: das sicherste ist, jedes Mal ein anderes Passwort zu verwenden und es nie zu speichern! Aber wir versuchen in diesem Essay einfach auch etwas die Realität und die Machbarkeit im Auge zu behalten.

3.5. Virenscanner verwenden

Installieren Sie auf Ihrem Rechner unbedingt immer einen aktuellen Virenscanner! Dieser verhindert von vorneherein, dass sich Viren und Trohaner bei Ihnen einnisten und verhindert auf diese Art und Weise, dass Ihre Passwörter in falsche Hände geraten. Computerviren und Trojaner sind mit der häufigste Weg, wie Ihre Passwörter und Zugangsdaten in die falschen Hände gelangen!

Aktuelle Virenscanner erhalten Sie beispielsweise unter:

- https://www.avira.com/de/
- https://www.mcafee.com/de-de/
- https://de.norton.com/

Virenscanner gibt es oft werbefinanziert kostenlos, aber es lohnt sich durchaus eine Vollversion, die in der Regel ca. 20-50 EUR pro Jahr kostet, zu erwerben und sein System damit abzusichern.

3.6. Softwareupdates einspielen

Wie unter 2.4 beschrieben, sollten Sie unbedingt darauf achten, immer die aktuellste Software-Version einzuspielen. In vielen Programmen finden Sie im Hilfe-Menue einen Punkt

"Auf Updates prüfen"

oder ähnlich. Viele Programme weisen Sie auch automatisch darauf hin, wenn es neue Versionen gibt.

3.6.1. Windows XP und Windows Vista

Sie sollten Windows XP und Windows Vista **nicht mehr verwenden**, da bereits im April 2014 bzw. April 2017 der Support hierfür von Microsoft eingestellt wurde. Das bedeutet: Sie erhalten insbesondere keine Sicherheits-Aktualisierungen mehr und sind gegen neu auftauchende Bedrohungen nicht mehr geschützt

3.6.2. Windows 7

Noch wird Windows 7 aktualisiert, allerdings endet hier auch der Support im April 2020 – wenn Sie Windows 7 noch verwenden sollten Sie also überlegen, bald auf das aktuelle Windows 10 umzusteigen.

3.6.3. Windows 8 und 8.1

Auch Windows 8 wird von Microsoft noch unterstützt, aber auch diese Windows-Versionen werden auslaufen. Je früher Sie umsteigen, desto weniger Probleme werden Sie eines Tages haben.

3.6.4. Windows 10

Dies ist das aktuelle Windows, das auch mit dem Windows Defender einen sehr guten eingebauten Anti-Viren-Schutz bietet und auch fortlaufend mit aktuellen (Sicherheits-)Updates versorgt werden.

3.6.5. Firefox Internetprogramm ("Mozilla Firefox")

Wenn Sie im Firefox im Bereich "Hilfe" auf "Über Firefox" klicken öffnet sich ein kleines Fenster, indem Sie auch direkt überprüfen können, ob Ihr Firefox aktuell ist.

3.6.6. Firefox Plugins

Unter

https://www.mozilla.org/de/plugincheck/

können Sie überprüfen, ob andere Programme, die im Rahmen von Firefox für Sie beim Internetsurfen verwendet werden aktuell und auf neustem, sicheren Stand sind.

3.6.7. Thunderbird eMail-Programm

Hier finden Sie ähnlich wie im Firefox im Menue "Hilfe" / "Über Thunderbird" Informationen, ob Ihr eMail-Programm auf aktuellstem Stand sind

3.7. Vorsicht bei Verwendung von Passwörtern auf Notebooks, Tablets und Smartphones!

Ihr Computer steht erst einmal zu Hause. Natürlich gibt es auch Einbrecher und Diebe, aber zum Glück ist das wirklich relativ selten. Ein stationäres Gerät – und damit die darauf gespeicherten Passwörter! - ist in der Regel also erstmal nur für Sie zugänglich. Mobile Geräte wie Notebooks, Tablets oder Smartphones hingegen bergen ein deutlich höheres Risiko!

Leider passiert es nur allzu oft, dass Smartphones verloren gehen oder gestohlen werden, Tablets oder Notebooks unbeachtet liegengelassen werden.

Die hier gespeicherten Passwörter sind also in deutlich größerer Gefahr!

Theoretisch kann es reichen, in ein laufendes Notebook für ein paar wenige Sekunden einen infizierten USB-Stick zu stecken. Ist das System nicht ideal konfiguriert, haben Sie so direkt einen Computervirus auf Ihrem Rechner.

Ebenfalls gleichen viele mobile Geräte automatisch die auf Ihnen gespeicherten Daten mit Cloud-Speichern im Internet ab ("Synchronisierung"). Je nach System wird hierbei leider auch sehr lax mit Zugangsdaten umgegangen, so dass später Ihre Zugangsdaten dann nicht mehr nur auf Ihrem Handy gespeichert sind, sondern an ganz anderen Stellen, die Ihnen gar nicht bewusst sind.

Insbesondere von komplettem Online-Banking auf Handys raten wir Ihnen daher unbedingt ab!

Achten Sie auch unterwegs darauf, wer Ihren Bildschirm sehen kann

Wenn Sie in der Bahn oder an anderen öffentlichen Plätzen sitzen, ist es oft sehr einfach Ihren Bildschirm und Ihre Tastatur einzusehen. Jedes gängige Smartphone kann schnell mitfilmen, was auf einer Tastatur eingegeben wird. Auch wenn ein Passwort auf dem Bildschirm in der Regel nicht angezeigt wird, kann es so sehr schnell von Unbefugten abgegriffen werden.

3.8. Nur verschlüsselte WLANs verwenden

Sobald Sie in einem WLAN aktiv sind, achten Sie darauf, ob Sie für das WLAN ein Passwort eingeben mussten. Wenn Sie ein Passwort eingeben mussten (für das natürlich wieder alles in Punkto Sicherheit gilt, was hier bereits für sichere Passwörter gesagt wurde!), ist der Datenverkehr immerhin schon einmal innerhalb des WLANs verschlüsselt. D.h. für Außenstehende ist es nun deutlich schwieriger, Daten abzufangen, die Sie evtl. eingeben.

Wichtig ist hierbei, dass als Verschlüsselungsmethode **WPA2** verwendet wird. Andere Verschlüsselungsmethoden sind nicht sicher!

Wenn Sie für ein WLAN *kein* Passwort eingeben mussten, können Sie dieses Drahtlosnetzwerk natürlich trotzdem nutzen – Sie sollten dann aber darauf achten, dass Sie in der Zeit möglichst keine sensiblen Daten und Passwörter verwenden oder sich irgendwo im Internet anmelden!

Achten Sie insbesondere im Urlaub darauf, sichere WLAN-Netze zu verwenden!

3.9. Auf SSL-Verschlüsselung achten!

Ihr Internetprogramm kann Daten auch verschlüsselt übertragen. D.h. Ihr Internetprogramm verschlüsselt in einem ersten Schritt Ihre eingegebenen Daten, z.B. Ihre Zugangsdaten und damit auch Ihr Passwort, überträgt diese komplett verschlüsselt zum Server und erst dort werden die Daten wieder entschlüsselt.

Alle Stationen dazwischen (auch unsichere WLANs) haben dann keine Chance mehr, Ihre Daten abzufangen (oder sagen wir mal, es wird wirklich sehr sehr schwierig).

Sie erkennen sichere Verbindungen daran, dass sie mit **https://** statt http:// beginnen. Oftmals kennzeichnen die Internetprogramme solche sicheren Verbindungen auch durch ein Schloss-Symbol.

Wenn Sie Benutzerdaten aber auch vor allem Kontodaten oder Kreditkartennummern etc. eingeben, sollten Sie nach Möglichkeit darauf achten, dass Sie eine verschlüsselte Verbindung verwenden.

Beispiel für einen verschlüsselten Aufruf in Google Chrome

3.10. Passwort-Manager verwenden

Es gibt auch Programme, die anbieten, Ihre Passwörter sicher zu verschlüsseln und zu speichern. Der Vorteil: Sie müssen sich nur noch ein sogenanntes Master-Passwort merken. Die anderen Passwörter sind dann mit diesem Master-Passwort zugänglich.

Wenn Sie ein wirklich sicheres System hierfür verwenden, ist prinzipiell dagegen nur wenig einzuwenden. Natürlich ist es aber immer sicherer, Passwörter nur im Kopf zu behalten.

Beispiele für entsprechende Programme finden Sie unter:

https://www.pcwelt.de/ratgeber/Datenschutz-Gratis-Tools-verschluesseln-alle-Ihre-Dateien-307316.html

Oder Sie verwenden das folgende Programm, mit dem Sie übrigens auch jede beliebige Datei auf Ihrem Rechner sicher verschlüsseln können:

https://www.gpg4win.de/

https://www.gnupg.org/

3.11. 2-Wege Authentifizierung verwenden

Viele große Anbieter bieten mittlerweile eine sogenannte 2-Wege Authentifizierung an. Was steckt dahinter?

Zusätzlich zu Ihren Zugangsdaten müssen Sie in der Regel Ihre Telefonnummer hinterlegen. Erfolgt nun beispielsweise ein Zugriff von einem neuen Gerät oder soll das Passwort geändert werden, wird zusätzlich eine SMS mit einem Bestätigungscode an Ihre Telefonnummer geschickt. Nur mit diesem Code geht es weiter.

Wenn Ihr Anbieter diese 2-Wege Authentifizierung bietet, sollten Sie diese nutzen. Eine hundertprozentige Sicherheit bietet dies auch nicht, aber ein Angreifer müsste nun auch zusätzlich Ihr Handy stehlen oder abhören und auch Ihr Handy genau dem Account zuordnen – dies ist sicher dem einen oder anderen Geheimdienst möglich, einem normalen Hacker aber nur sehr schwerlich.

3.12. Benachrichtigungen nicht deaktivieren

Viele Anbieter informieren Sie z.B. wenn Ihr Passwort geändert wurde oder wenn ein Login von einem neuen Gerät erfolgt.

Auch wenn es vielleicht lästig ist:

Sie sollten diese Benachrichtigungen nicht abschalten!

So können Sie schnell erkennen, falls Ihr Konto missbräuchlich genutzt wird.

3.13. Muss ich wirklich alle drei Monate mein Passwort ändern?

Oftmals liest man die Empfehlung, dass man sein Passwort alle 2-3 Monate ändern sollte. Ganz können wir dieser Empfehlung nicht folgen. Wenn ein Passwort nicht geknackt wurde und es auch keinerlei Anzeichen dafür gibt, wird es nicht sicherer dadurch, dass man es austauscht!

Es spielen natürlich statistische Erwägungen eine Rolle: je länger man ein Passwort verwendet, desto wahrscheinlicher ist es, dass es in irgendeiner Art und Weise geknackt wurde. Das ist irgendwie klar.

Aber trotzdem ist diese Empfehlung sicher nicht die vordringlichste Lösung, wenn Sie darum bemüht sind, Ihre Passwörter zu sichern! Es schadet natürlich aber nicht ;-)

3.14. Vorsicht bei Sicherheitsfragen

Viele Anbieter verlangen von Ihnen, Sicherheitsfragen zu wählen und die zugehörigen Antworten zu hinterlegen.

Die Sicherheitsfragen sind allerdings oft sehr simpel, wie beispielsweise:

- **Ihr Geburtsort**
- **Mädchenname der Mutter**
- **Name des Haustieres**

Natürlich erschweren diese Fragen den Zugang, wer aber wirklich an Ihre Daten möchte, kann in der Regel mit etwas Recherche eine Vielzahl dieser Fragen beantworten.

Wir empfehlen daher, Sicherheitsfragen nicht ehrlich auszufüllen. Ein einfacher Trick ist, bei Sicherheitsfragen absurde Antworten zu geben. Wenn Sie als Geburtsort immer den Mars und als Mädchenname der Mutter immer Julius Caesar verwenden, wird dies niemand durch Recherche knacken können.

3.15. Ist mein Computer bedroht?

Einen Schnellcheck für Ihre Systemsicherheit können Sie beispielsweise auf der folgenden Seite des Verbands der deutschen Internetwirtschaft e.V. durchführen:

https://www.heise.de/security/dienste/Netzwerkcheck-2114.html

Achtung! Dies sind nur Schnellchecks! Es werden hier nur die häufigsten und auffälligsten Bedrohungen überprüft – trotzdem ist dies schon hilfreich und sollte unbedingt regelmäßig durchgeführt werden.

3.16. Wenn doch mal was passiert ist……

Wenn bei Ihnen ein Computervirus oder Trojaner gefunden wurde, ist es am sichersten das ganze System komplett zu löschen und neu zu installieren. Viele Computerviren installieren nämlich fortlaufend andere Virenprogramme nach, so dass Sie in einem solchen Fall oft nicht nur einen sondern gleich zig Schadprogramme auf Ihrem Rechner haben und es sehr schwierig ist, einzuschätzen, ob Ihr System erfolgreich gesäubert wurde oder nicht.

Das einzig sichere – auch wenn es sehr aufwändig ist – ist, in einem solchen Fall von null anzufangen, das Betriebssystem und alle Programme neu zu installieren.

Wenn eines Ihrer Passwörter in falsche Hände geraten ist, sollten Sie unbedingt alle Ihre Zugangsdaten ändern – insbesondere wenn Ihr eMail-Passwort in falsche Hände geraten ist.

Wenn ein unbefugter Zugriff auf Ihre Bankkonten erfolgte, informieren Sie bitte umgehend Ihre Bank und lassen Sie Konto und damit verbundene EC- und Kreditkarten umgehend sperren!

EC- und Kredit-Karten können Sie telefonisch über den einheitlichen Sperr-Notruf

116 116

oder aus dem Ausland:

+49 - 116 116

jederzeit sperren lassen.

3.17. Aktuelle Informationen

Wenn Sie auf dem Laufenden bleiben möchten, finden Sie unter folgenden Adressen im Internet immer Informationen über aktuelle Bedrohungen:

3.17.1. Bundesamt für Sicherheit in der Informationstechnik

https://www.bsi.bund.de/

3.17.2. Heise security

https://www.heise.de/security/

3.17.3. Golem

https://www.golem.de/

4. Exkurs: eMail und Passwörter

Ganz kurz streifen wir an dieser Stelle auch das Thema eMail-Sicherheit. Wirklich nur kurz, da dies eigentlich ein anderes Thema ist.

4.1. Grundproblem 1: eMails werden nicht verschlüsselt!

Ohne in Details zu gehen, beachten Sie bitte immer eins:

eMails sind unsicher! eMails sind nicht sicherer als eine Postkarte! Der Inhalt einer eMail wird immer unsicher und unverschlüsselt übertragen (außer Sie haben ihn im Vorfeld händisch verschlüsselt, was leider nach momentanem Stand der Technik recht aufwändig ist und eine gewisse Erfahrung benötigt).

D.h. Sie sollten immer gut überlegen, was Sie einer eMail anvertrauen und was nicht! eMails haben leider in vielerlei Hinsicht noch mehr Sicherheitsprobleme, dies werden wir aber in einem anderen Essay behandeln. Bitte beherzigen Sie bis dahin einfach folgenden Leitspruch: **eMails sind per se unsicher!**

4.2. Was oft falsch verstanden wird: SSL-Verschlüsselung von eMail-Zugangsdaten

In der Regel wird heute der Zugang zum eigenen eMail-Konto verschlüsselt. D.h. Im eigenen eMail-Programm aktiviert man eine SSL bzw. TLS-Verschlüsselung. Das ist auch wichtig und gut so, da so das Risiko minimiert wird, dass die eigenen Zugangsdaten abgefangen werden können.

Es ist allerdings ein gefährliches Missverständnis, dass die eMails selbst auf diesem Wege verschlüsselt und damit sicher würden!

Es wird lediglich der kurze Weg von Ihrem Rechner zur eigenen Mailbox verschlüsselt, danach sind die eMails wieder völlig unverschlüsselt unterwegs und können in der Regel ohne großen Aufwand abgefangen und gelesen werden.

4.3. Sicheres eMail-Passwort wählen

Wie unter 3.2. beschrieben sollten Sie für Ihre eMail-Adresse ein besonders sicheres, einmaliges Passwort verwenden, das Sie wirklich nur für die eMail verwenden.

4.4. Möglichst über SSL zum Mailserver verbinden

In den Einstellungen Ihres eMail-Programms gibt es in der Regel die Möglichkeit auszuwählen, dass Sie sich per SSL-Verschlüsselung verbinden können. Achtung! Auch das macht eine eMail nicht sicher, auch wenn viele das glauben! Aber immerhin wird der Weg von Ihrem Computer zum eMail-Server verschlüsselt und damit insbesondere auch Ihr eMail-Passwort sicher übertragen!

4.5. Vorsicht im Urlaub und unterwegs!

Achten Sie beim eMail-Abruf im Urlaub darauf, dass Sie sich nicht in öffentlich zugänglichen sondern in verschlüsselten WLANs bewegen und dass die Verbindung zum eMail-Server über SSL verschlüsselt ist oder Sie Ihren Webmailer ebenfalls über SSL verwenden.

Auch zu diesem Thema werden wir Sie an anderer Stelle noch ausführlich informieren.

5. Was passiert mit meinen Passwörtern bei den Anbietern?

Die Kurz-Zusammenfassung: Sie wissen es nie!

Daher sollten Sie auch immer überlegen, welchem Anbieter Sie welches Passwort anvertrauen und welchem nicht.

Manche Anbieter speichern auch heute noch Ihre Zugangsdaten unverschlüsselt. D.h. wenn jemand bei diesem Anbieter einbricht, hat er sofort Zugriff auf Ihre Daten und kennt ab diesem Moment Ihr Passwort.

Auch wenn die Daten nicht unverschlüsselt gespeichert werden, gibt es leider eine breite Spanne an sicheren aber auch nicht sicheren Verfahren.

Manche sind in kürzestes Zeit zu knacken, manche nur schwer.

Letztendlich wissen Sie aber nie, was der Anbieter, bei dem Sie Benutzername und Passwort hinterlegen, intern verwendet und wie Ihre Daten geschützt werden.

Überlegen Sie daher wirklich immer, wem Sie was anvertrauen! Gesundes Misstrauen ist hier einfach von Vorteil!

6. Wie werden Passwörter gehackt?

Dies ist nur ein kleiner Exkurs ohne in die Tiefen zu gehen, wie Kriminelle versuchen, an Ihre Passwörter zu gelangen!

6.1. Brute-Force Attacken

Tagtäglich können wir auf den Internetservern, die wir für unsere Kunden betreuen, live verfolgen, wie rund um die Uhr versucht wird, die Systeme zu knacken. Dies ist mittlerweile leider trauriger Alltag.

Der einfachste Weg, der immer wieder versucht wird, sind simple sogenannte Brute-Force-Attacken. D.h. die Angreifer versuchen die gängigsten Passwörter einfach eines nach dem anderen durch und hoffen, dass sie damit Erfolg haben.

Umso wichtiger ist es, wie ausgeführt, sichere Passwörter zu verwenden. Dies ist die häufigste und einfachste Angriffsmethode.

6.2. Password Sniffer, Viren und Trojaner

Passwort Sniffer sind Systeme, die auf Ihrem Rechner (also z.B. als Computervirus) aber auch in Netzwerken (also z.B. auf dem Weg von Ihrem Rechner zum Server) versuchen, Passwörter zu entdecken und zu entwenden. Hier helfen am besten Verschlüsselungstechniken.

6.3. Phishing

Bei dieser auch in den vorherigen Kapiteln bereits beschriebenen Angriffsmethode spielt der Mensch selbst die wichtigste Rolle als Schwachpunkt und es wird versucht, ihn zu überlisten.

6.4. Rainbow-Tables

Werden bei einem Anbieter gespeicherte Passwörter gestohlen, die zwar verschlüsselt sind, aber nicht nach aktuellstem Stand der Sicherheits-Technik, versuchen Angreifer oft mit sogenannten Rainbow-Tables das originale Passwort zu entschlüsseln.

Je nach vom Anbieter gewählten Verfahren kann dies leider recht schnell erfolgreich sein.

Für weitere technische Details verweisen wir hier auf das Internet, da es hier nun wirklich sehr komplex werden würde.

6.5. Klassisch: Überwachung

Auch die Überwachung mit versteckten Kamera, Mikrofonen oder sogar mit einfachen Ferngläsern können Zugriff auf Ihre Passwörter gewähren.

Versteckte Kameras werden beispielsweise gerne über Geldautomaten angebracht, um auf diesem Wege die PIN des Bankkunden in Erfahrung zu bekommen (die PIN ist letztendlich auch nur ein einfaches Passwort!)

Insbesondere bei Bankautomaten und in sehr sensiblen Geschäftsbereichen sollten Sie durchaus auch das im Hinterkopf behalten.

6.6. Exotisch: Handy-Überwachung der anderen Art

In der Welt der Geheimdienste stehen leider noch ganz andere Techniken zur Verfügung. Natürlich können Handy-Verbindungen überwacht und ausgespäht werden. Dies ist nicht erst seit dem NSA-Skandal 2013 und 2014 schmerzhaft ins Bewusstsein geraten.

Es gibt aber auch technische Tools, die Überwachung der ganz anderen Art ermöglichen, beispielsweise das Anzapfen der Kamera Ihres Smartphones oder Überwachungsmöglichkeiten, mit denen Sie vermutlich in keinster Weise gerechnet haben:

Wissenschaftlern ist es beispielsweise gelungen, ein Programm zu entwickeln, dass die sehr genauen Sensoren eines Smartphones dazu nutzt, um die Tastaturanschläge einer Tastatur neben (!) dem Handy auszuwerten.

D.h. das Handy lag unauffällig auf dem Tisch neben einem Rechner und wertete so alle Tastatur-Eingaben aus. Ein normales gängiges Smartphone ohne besondere Technik war hierfür ausreichend, um mit einer sehr hohen Wahrscheinlichkeit auszuwerten, was getippt wurde.

6.7. Exotisch: Geräuschanalyse

Wem das schon nach zu viel James Bond klingt, für den gibt es leider noch viel mehr Möglichkeiten, wie heutzutage Computer, Smartphones und Co. überwacht werden können.

Wissenschaftlern gelang es beispielsweise aus den Arbeitsgeräuschen des Computer-Prozessors mit feinsten Mikrofonen zu entschlüsseln, was auf dem Gerät gerade berechnet wurde.

Erschreckend, aber die voranschreitende Technik bietet leider viel Möglichkeiten, leider auch für Verbrecher oder gewissenlos agierende Geheimdienste.

Einen kompletten Schutz wird es nie geben, man wird immer auf dem Laufenden bleiben und sich ständig informieren und weiterentwickeln müssen.

Aber gegen die gängigsten Angriffsmethoden können Sie sich wirklich recht einfach schützen! Bitte nutzen Sie diese Möglichkeiten auch und verwenden Sie sichere Passwörter und Zugangsdaten!