Immer mehr Seiten im Internet erwarten, dass man sich registriert. Dabei muss mindestens ein Benutzername (*meist E-Mail Adresse*) und ein Passwort festgelegt werden. Unsere Merkfähigkeit ist begrenzt und wir neigen zur Bequemlichkeit. Was liegt näher, als die Verwendung eines Passwortes, das wir uns leicht merken können. Am besten nehmen wir den Namen der Katze oder des Hundes. Um es für andere kompliziert zu machen hängen wir noch das Geburtsdatum der Oma an. Mit „Waldi190354“ haben wir unseren eBay Zugang perfekt abgesichert.

Wenn Sie nicht zu denjenigen gehören, die Passwörter in der oben aufgeführten Variante nutzen, lassen Sie sich versichern, dass solche Passwörter wirklich keine Seltenheit sind. Immer wieder komme ich im Rahmen meiner Tätigkeit mit Menschen in Kontakt, die ihre Daten mit **Waldis** absichern. Nach meinem subjektiven Empfinden dürfte es sich dabei sogar um die überwiegende Mehrheit handeln.

Zu der Kategorie „der bessere Mensch“ zählen sich Computernutzer, die sich ein einziges hochkomplexes Passwort erzeugt und gemerkt haben und dieses dann bei jeder Gelegenheit verwenden. Das Passwort wird für den Zugang zu *Aktuelles aus Hintertupfingen* ebenso verwendet, wie für den Zugang zum *Nutzerkonto bei Amazon*. Vergessen wird dabei, dass der Server in Hintertupfingen eventuell nicht sehr gut abgesichert ist. Unbefugte nutzen immer wieder Lücken solcher Server aus, um an Daten argloser Anwender zu gelangen. Was nützt hier ein Passwort, dass zwar an sich gut aufgebaut ist, jedoch einfach ausgelesen werden kann.

Jetzt denken Sie sich sicher, wie sich der Datenklau in Hintertupfingen auf Ihr Amazon Konto auswirken soll. Woher soll der Datendieb denn wissen, dass Sie ein Konto bei Amazon oder eBay haben?

Dazu muss man wissen, wie Angreifer arbeiten.

Glauben Sie bitte nicht, dass Datendiebe im Computerzeitalter mit Hammer und Meißel ans Werk gehen. Der Betreffende wird sich kaum an seinen Rechner setzen, den Browser starten, Amazon aufrufen und dort die Daten eingeben. Er macht sich natürlich die Vorzüge eines Computers zu Nutze, mit dem man bekanntlich stupide Arbeiten automatisieren kann. So finden sich Ihre Daten dann plötzlich in einer Datenbank mit Millionen von anderen Einträgen wieder. Automatisiert werden diese Daten jetzt auf Seiten getestet, die für den Datendieb lukrativ sind. Dazu zählen auf jeden Fall Seiten wie eBay, Amazon und Co.

Ja gut, aber wenn ich jetzt meinen **Waldi** nur bei eBay verwende, wie soll so ein Krimineller dann mein eBay nutzen können?

Auch hier muss man wissen, wie Digitalpiraten ihre Arbeit verrichten.

Im Falle der Waldi-Absicherung gibt es zwei Angriffspunkte:

1. Sie sind für den Kriminellen derart interessant, dass ein s.g. Social Engineering Angriff (*unter anderem forscht man in Ihrem privaten Umfeld, wertet Müll aus etc.*) interessant ist. Dabei erzeugt man dann eine Liste mit potentiellen Zeichenfolgen (*Namen, Geburtsdaten, Wohn-, Geburtsorte, Telefonnummern, Straßen, Büchernamen, Strom-/Telefonanbieter etc.*). Diese Liste wird dann, wie unter Punkt 2 erläutert, genutzt.

2. Im Internet kursieren zahlreiche Wörterbücher in verschiedenen Sprachen. In diesen Wörterbüchern sind unzählige Begriffe, Zahlen, Daten, Fakten, Sprüche etc. aufgelistet. Mit einem Computerprogramm wird die Liste jetzt je nach Angriffsszenario noch erweitert. Zum Beispiel kann man Groß-/Kleinschreibung variieren,

Buchstaben verdrehen oder Begriffe kombinieren.

Mit diesen sich daraus ergebenden Zeichenfolgen greift der Kriminelle jetzt das Objekt seiner Begierde an. Meist hat man bereits mit sehr kleinen Wörterbüchern, die aus häufig verwendeten Passwörtern bestehen, Erfolg. Moderne Analysewerkzeuge können bis zu 100 MILLIONEN Passwörter pro Sekunde testen.

Bei einem Datendiebstahl bei MySpace wurden 2007 ca. 34.000 bis 60.000 Datensätze erbeutet. Herr Bruce Schneier, ein anerkannter Fachmann im Bereich Datensicherheit analysierte die ihm vorliegenden Passwortdaten und gelangte zu interessanten Ergebnissen.

Statistische Verteilung der Passwortlänge
==========
Anzahl Zeichen Anteil [%]

1-4 0.82%
5 1.1%
6 15%
7 23%
8 25%
9 17%
10 13%
11 2.7%
12 0.93%
13-32 0.93%

Hier die TOP 20 der verwendeten Passwörter

password1, abc123, myspace1, password, blink182, qwerty1, fuckyou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, superman1, iloveyou1 und monkey

Die Schlussfolgerungen liegen auf der Hand:

1. Ein Passwort muss eine bestimmte Länge haben.
Es besteht ein Konflikt zwischen der Länge eines Passwortes, welches der Nutzer noch bereitwillig lernt und der Länge eines Passwortes, welches mit den angesprochenen Analysewerkzeugen ermittelt werden kann.
Diese magische Passwortlänge liegt zur Zeit bei etwa 8-9 Zeichen

Ergebnis: *Ein Passwort sollte aus mindestens 8 Zeichen (besser 12 und mehr) bestehen. Das Passwort sollte sich aus Ziffern, Groß-/Kleinbuchstaben und Sonderzeichen zusammensetzen.*

2. Keine lexikalischen Begriffe
Keine Begriffe/Zeichenfolgen verwenden, die aus einem (Wörter)Buch stammen. Dazu zählen auch Namen, Daten und Fakten.

Ergebnis: *Nutzen Sie zur Erzeugung des Passwortes den kompletten Zeichenvorrat – Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen*

3. Einmalige Verwendung
Nutzen Sie ein bestimmtes Passwort ausschließlich zur Absicherung eines einzigen Zugangs oder Kontos etc.

Ergebnis: *Erzeugen Sie sich für jeden neuen Fall in dem Sie ein Passwort benötigen ein eigenes sicheres Passwort.*

Beispiel für ein solches Passwort:
Zh8(Dx23_%k6s

„***Tolle Tipps, aber nicht praxistauglich***“ werden Sie sich jetzt denken! Da haben Sie Recht. Auch ich habe nicht die Muße, mir ständig neue sichere Passwörter zu erzeugen und mir diese dann auch noch dauerhaft einzuprägen! Allerdings wäre ArchiCrypt nicht ArchiCrypt, wenn es keine Lösung für dieses Problem gäbe.

Die Antwort lautet ArchiCrypt Passwort Safe! Sie müssen sich nur noch **ein** sicheres Passwort erzeugen und merken. Das Passwort nämlich, mit dem der Passwort Safe geschützt wird. Den Rest erledigt der Passwort Safe für Sie. Er generiert sichere Passwörter für jede beliebige Internetseite und überträgt diese per Tastendruck in die Eingabefelder. Man spart sich also sogar das Eintippen des Passwortes.

Neben diesen Basisfunktionen setzt der Passwort Safe viele weitere innovative Ideen um. Er schützt vor **Key-Loggern** (*Programme, die Ihre Eingaben auf der Tastatur mitschneiden*), er **analysiert und bewertet bestehende Passwörter** und bietet mit **PassOnPaper** sogar einen **Passwort Safe in Papierform**, der Ihnen dann zur Seite steht, wenn Sie vor dem Fahrradschloss stehen und die Kombination partout nicht einfallen will J