Inhalt

Je **geheimhaltungswürdiger** Daten sind, desto höher ist der **Wert** dieser Daten anzusetzen.

Brute Force in der Cloud

Denken Sie an **PIN** und **TAN**, die den Zugriff auf Ihr Konto schützen und denken Sie an eine Liste mit Decknamen von Agenten. Im ersten Fall geht es um **schnöden Mammon**, im zweiten Fall um **Menschenleben**.

> Je höher der Wert der Daten anzusetzen ist, desto höher werden die Anstrengungen ausfallen, um in den Besitz dieser Daten zu gelangen.

Im digitalen Zeitalter kommt zum Schutz brisanter Daten nahezu flächendeckend Verschlüsselung zum Einsatz.

Wir alle assoziieren mit Verschlüsselung den Begriff **Passwort**. Wir nutzen ein Passwort um uns morgens in der Arbeit am Rechner anzumelden, wir nutzen ein Passwort um uns bei Facebook einzuloggen, verwenden eines beim Einkaufen bei Amazon, beim Steigern bei eBay und beim Zugriff auf unser E-Mail Konto. Jeder weiß insgeheim, dass derjenige der unser Passwort kennt, auch Zugriff auf die entsprechenden Dienste hat.

Die Gefahren, denen unser Passwort ausgesetzt ist, sind mannigfaltig. Trojaner, KeyLogger, Phishing Mails und Konsorten zielen darauf ab, uns unsere Passwörter zu entwenden. Zunehmend werden große Internetseiten „gehackt“, werden Daten gestohlen und natürlich missbräuchlich verwendet.

Brute Force in der Cloud droht!

Relativ neu sind jedoch Möglichkeiten, die sich im Zusammenhang mit Cloud Computing ergeben. **Nie war es so einfach, sich zum Brechen von Passwörtern der Rechenleistung von abertausenden leistungsfähigen Computern zu bedienen. Man benötigt „lediglich“ das entsprechende Know-how und eine Kreditkarte.**

- **Entstehen daraus neue Gefahren für unsere Passwörter?**
- **Können wir uns hier wirksam schützen?**
- **Wie können wir uns schützen?**

Parallel Computing – Verteiltes Rechnen in der Wolke *

Parallel Computing (paralleles Rechnen) in der Cloud ist ein Verfahren, mit dem man eine (*Rechen*-)Aufgabe auf mehrere Computer in der Cloud verteilt. Diese **Parallelisierung** funktioniert im Zusammenhang mit Brute Force oder allgemein mit Verschlüsselung ganz wunderbar. Diese Eigenschaft machen sich bereits viele Programme zu Nutze, die auf einem normalen Rechner zum „knacken“ von Passwörtern eingesetzt werden. Moderne Rechner verfügen über Mehrkern-CPUs, einzelne Recheneinheiten, denen man unterschiedliche Aufgaben zuteilen kann. ArchiCrypt Live, die Echtzeitverschlüsselungslösung, verwendet

diese Form der Parallelisierung beim Ver- und Entschlüsseln. Es gibt auch „Passwortknacker“, die sich zusätzlich der Rechenpower des Grafikchips bedienen. All dies ist aber NICHTS im Vergleich zu dem, was man durch Cloud Computing inzwischen realisieren kann. Wer etwas „Kleingeld“ übrig hat und im Besitz einer Kreditkarte ist, kann sich einen ganzen **Verbund von Rechnern stundenweise Mieten** und diesen Verbund mit dem Lösen einer Aufgabe betrauen. Dem Knacken eines Passwortes

Brute Force (Angriff mit Brachialgewalt) *

Brute Force ist ein wenig intelligentes Verfahren, um ein Passwort zu „erraten“. In diversen Artikeln ist dieses Angriffsverfahren Gegenstand der Diskussion. In der Informatik bezeichnet man Verfahren als Bruce-Force Verfahren, die mangels effizienter Alternativen alle in Frage kommenden Lösungen eines Problems auf Korrektheit testen. Brute-Force ist relativ einfach zu realisieren. In Weißt Du wieviel Sternlein stehen? wird anhand der PIN einer EC Karte aufgezeigt, wie viele Möglichkeiten es für eine PIN der Länge 4, bestehend aus den 10 Ziffern, gibt. Im gleichen Artikel wird eine Formel entwickelt, mit der wir uns für ein Passwort der Länge k, gebildet aus dem Zeichenvorrat N, die Anzahl an Möglichkeiten berechnen können. „Alle anderen Kryptosysteme können mit einem ciphertext-only-Angriff gebrochen werden, indem einfach nacheinander alle denkbaren Schlüssel ausprobiert werden und dann nachgesehen wird, ob der entstandene Klartext irgendeinen Sinn ergibt.“ (*Bruce Schneier, Angewandet Kryptografie, Protokolle, Algorithmen und Sourcecode in C, Addison-Wesley 1996, Seite 9*) Mit „…anderen …“ ist das spezielle One-Time-Pad gemeint.

$$Anzahl Moeglichkeiten = N^k$$

> **Kleines Beispiel:**
>
> Frage: Wie viele Möglichkeiten gibt es, aus den 26 Kleinbuchstaben ein Passwort der Länge 3 zu bilden?
>
> Antwort: Unser Zeichenvorrat besteht aus den 26 Kleinbuchstaben. Also N=26. Die Passwortlänge beträgt 3. Eingesetzt in unsere Formel ergibt sich ein Wert von 26^3=26*26*26= 17576 verschiedene Möglichkeiten.

Im **Experiment** wird davon ausgegangen, dass ein Angreifer aus **wirtschaftlichen Gründen** eine Obergrenze für k (*Anzahl Stellen des Passwortes*) festlegen wird, er aber

nicht verlässlich weiß, ob die Länge des Passwortes genau k beträgt.

Konkret: Will ein Angreifer Passwörter bis maximal Länge 6 durchprobieren, muss er zunächst alle Passwörter der Länge 1,2,3,4 und 5 testen. Folglich steigt die Anzahl an Möglichkeiten zu

$$Anzahl Moeglichkeiten = N^1 + N^2 + ... + N^{k-1} + N^k$$

Für unser Beispiel mit Obergrenze k = 6 ergibt sich damit eine Anzahl von

$$26^1 + 26^2 + 26^3 + 26^4 + 26^5 + 26^6 = 321.272.406$$

Rahmenbedingungen des Experiments *

Im Experiment wird Bezug auf Amazon's EC2 Dienst genommen. Zur Anwendung kommen ausschließlich **High-CPU Reserved Instanzen,** die **pro Stunde ca. 0,19 $ (USD)** kosten.

> Jede Instanz kostet 0,19 USD pro Stunde

Das Verfahren ist grundlegend an die von Withfield Diffie und Martin Hellmann im Jahre 1977 vorgeschlagene **DES-Cracking Machine** angelehnt. **Wir wollen ein einfaches Modell zur Veranschaulichung von Prinzipien!**

> Jede Instanz testet 2 Millionen Passwörter pro Sekunde

Die Begrenzung auf 1oo Instanzen, die Amazon für einen Account festgelegt hat, wird nicht berücksichtigt. Man kann bei Amazon größere Mengen beantragen. Zudem ist Amazon's EC2 Verbund nur beispielhaft.

Im Zusammenhang mit unserem **Brute Force Angriff** mittels **Cloud Computing** werden die zu prüfenden Passwörter gleichmäßig auf die verfügbaren Instanzen verteilt. Findet eine Instanz die korrekte Lösung, meldet sie dies und alle Instanzen werden angehalten. Der Verwaltungsaufwand geht gegen Null. Alle Instanzen arbeiten autark. Nur dann, wenn eine Instanz einen Treffer landet, erfolgt eine Rückmeldung.

Angenommen, wir habe eine Million an möglichen Passwörtern. Nur im ungünstigsten Fall wird man erst beim Test des millionsten Passwortes einen Treffer landen. Im besten Fall, landet man bereits beim ersten Versuch einen Treffer. Statistisch gesehen, wird man bei 50% aller zu testenden Passwörter einen Treffer landen.

> Für unser Brute Force Experiment gilt ein Angriff als erfolgreich beendet, wenn 50% der möglichen Schlüssel getestet wurden.

Alle Berechnungen werden für Passwörter mit steigender Komplexität durchgeführt. **Steigende Komplexität bedeutet**, dass mehr Zeichen zur Verfügung stehen, aus denen das Passwort aufgebaut werden kann. Zunächst begrenzen wir den **Zeichenvorrat**, aus dem ein Passwort aufgebaut wird auf **Kleinbuchstaben [a-z]**, gehen dann über zu **Groß- und Kleinbuchstaben [a-z][A-Z]** nehmen anschließend Ziffern hinzu **[a-z][A-Z][0-9]** und schließlich auch Sonderzeichen **[a-z][A-Z][0-9][*#+:-...]**.

Bei [a-z] sind also Passwörter der Art a, z, ab, azda möglich.

Bei [a-z][A-Z] sind also Passwörter der Art a, z, ab, azda, A, BZHSJI, BZhuatfD möglich.

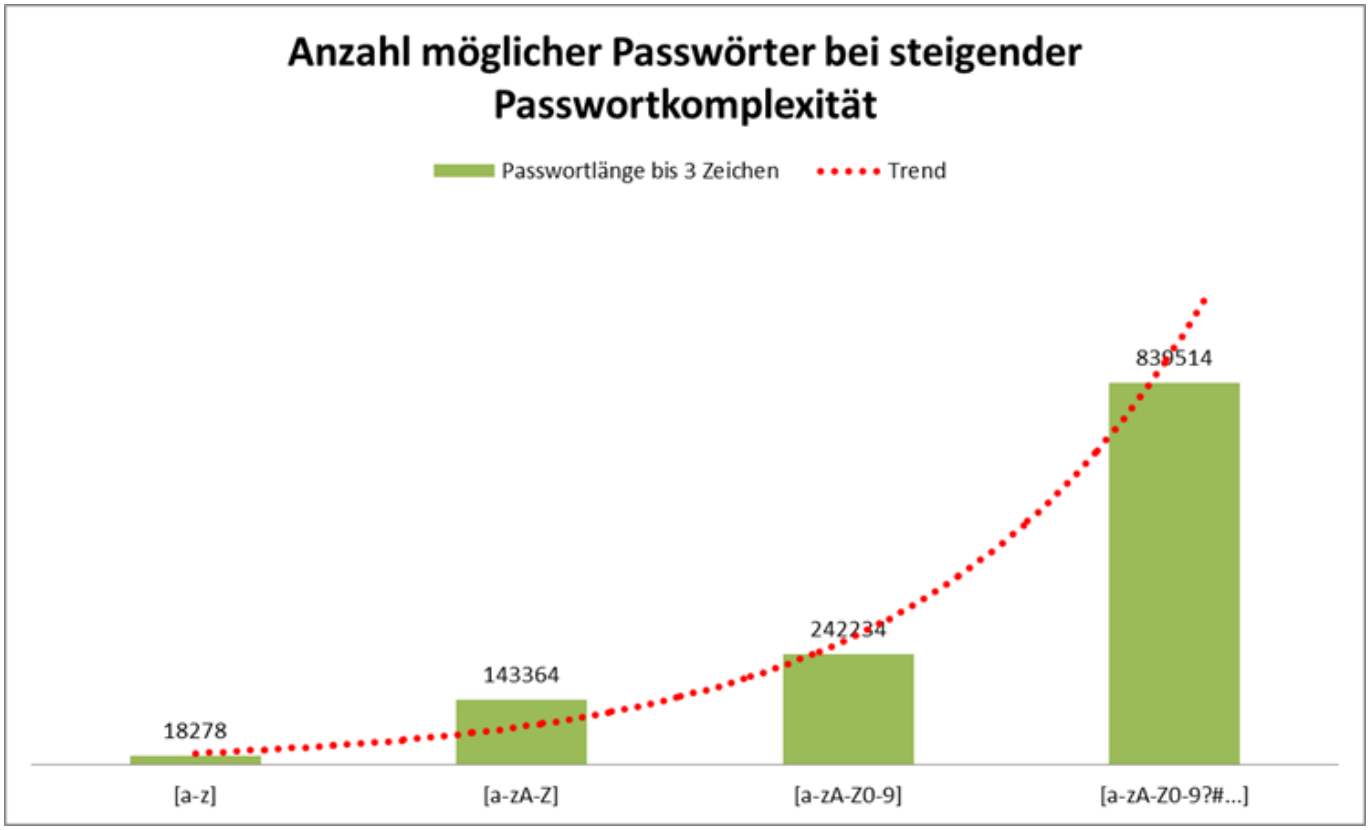
Bei [a-z][A-Z][0-9] sind also Passwörter der Art a, z, ab, 125, aa3zda, A, BZHSJI, BZhua5fD möglich.

Bei [a-z][A-Z][0-9] sind also Passwörter der Art a, z, #, ab, 1+25, aQa3zd!a, A, BZHSJI, BZhua5fD möglich.

Die Anzahl an **Sonderzeichen** wurde mit **32** angenommen.

Anzahl möglicher Passwörter unterschiedlicher Komplexität *

Je größer der Zeichenvorrat aus dem ein Passwort gebildet werden kann, desto höher die Komplexität.

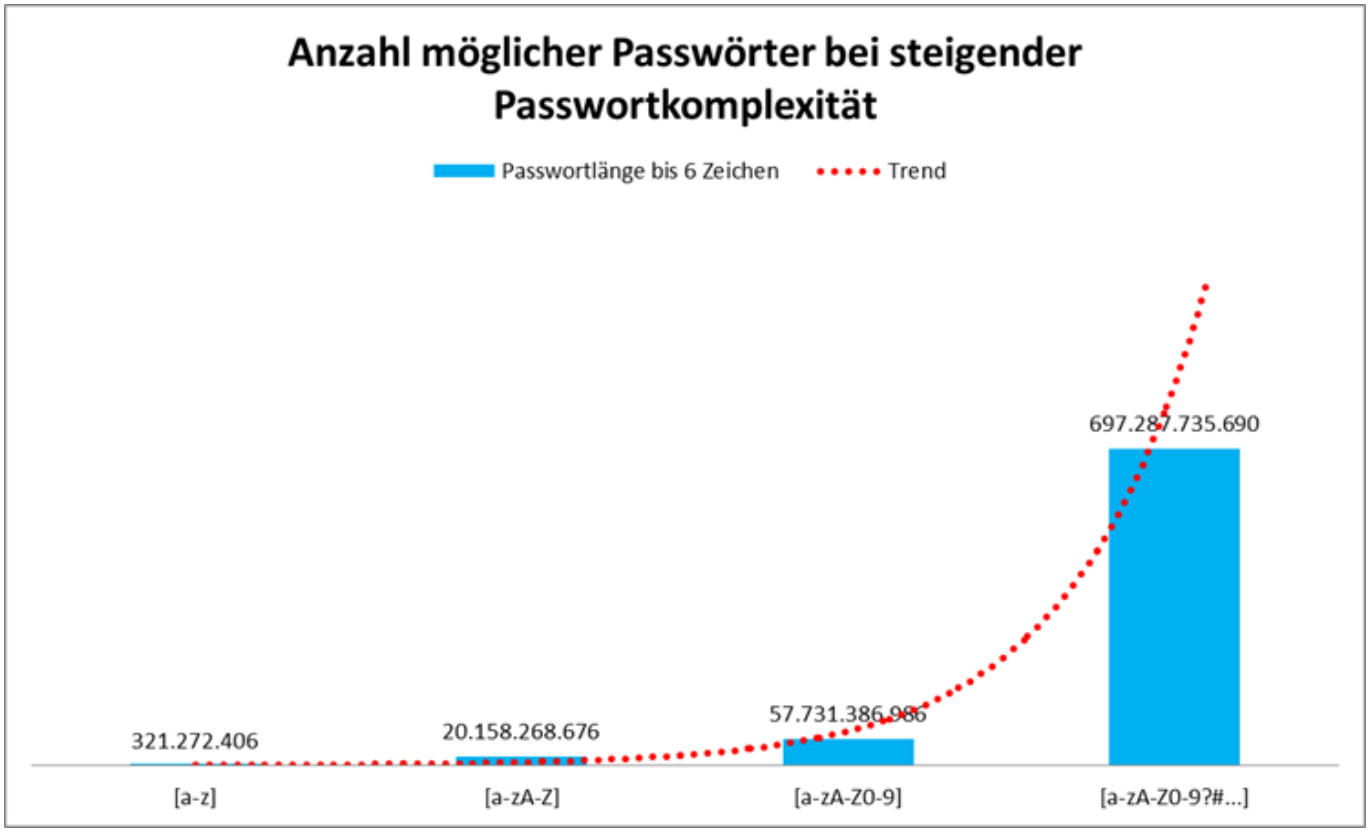


Bemerkenswert, dass bereits bei einer Passwortlänge von nur **3 Zeichen** eine recht hohe Anzahl möglicher Passwörter existiert, sofern man nur den kompletten Zeichenvorrat [a-z][A-Z][0-9][*#+:-...] verwendet. Bereits an dieser Stelle kann man dies als Fazit mitnehmen.

MERKE: Passwörter sollten immer maximal komplex aufgebaut sein.

Gemäß Rahmenbedingen, kann eine Instanz 2 Millionen Schlüsselüberprüfungen pro Sekunde durchführen. Bei einer Passwortlänge von 3 haben wir den Brute Force Angriff noch nicht gestartet, da ist das korrekte Passwort bereits gefunden. In Sekundenbruchteilen! Und das mit einer einzigen Instanz. Das geht leicht noch mit dem Heimcomputer! Wenn Sie jetzt denken, dass Passwörter aus 3 Zeichen unrealistisch sind, würden Sie sich wundern. Die „Passwörter“ „sex“ und „123“ sind nach wie vor extrem beliebt.

Eher wahrscheinlich sind aber sicher Passwörter, die aus **6 Zeichen** bestehen.

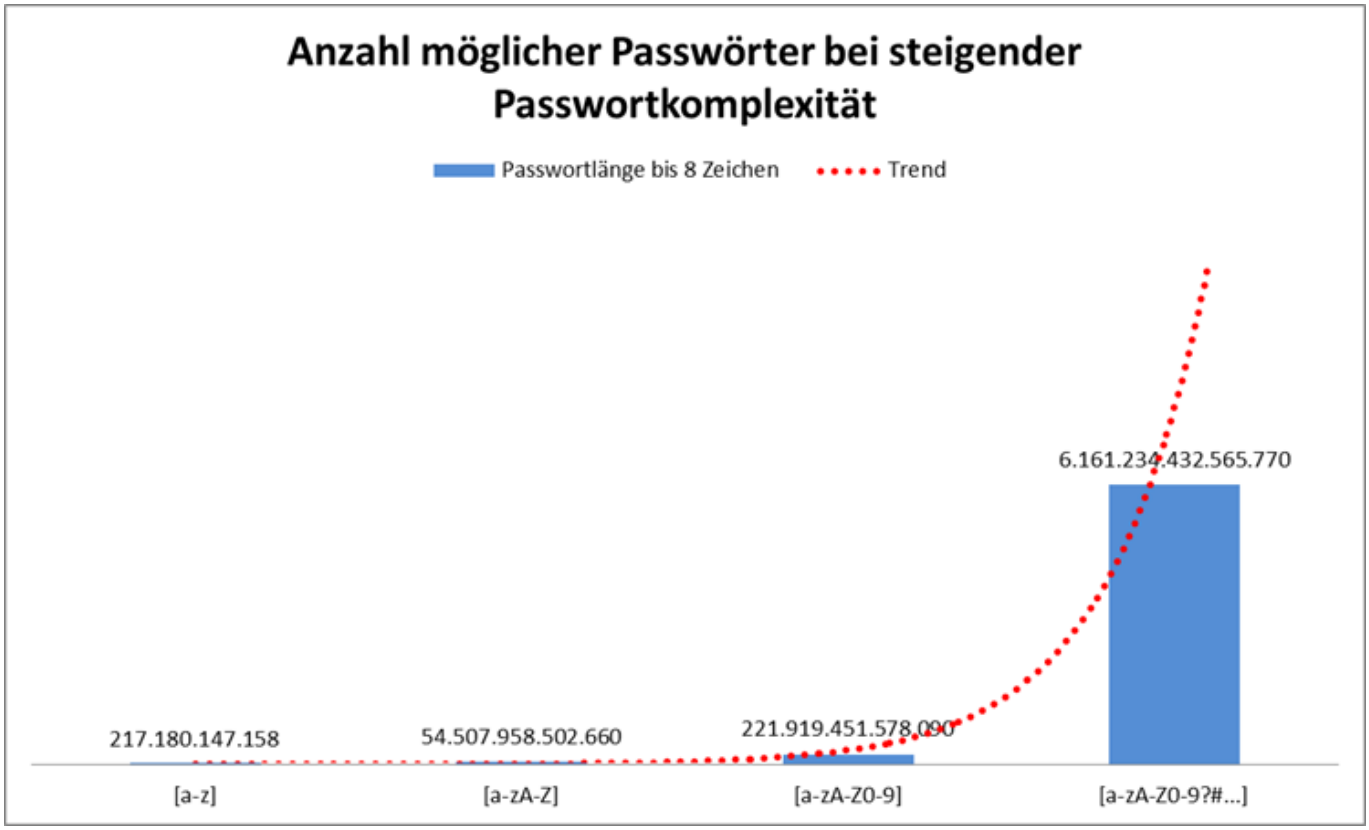


Auch hier beeindruckt der Sprung der Anzahl bei Verwendung aller Zeichen (*maximale Komplexität*).

Sind wir mit einem solchen 6 Zeichen langen Passwort auf der sicheren Seite?

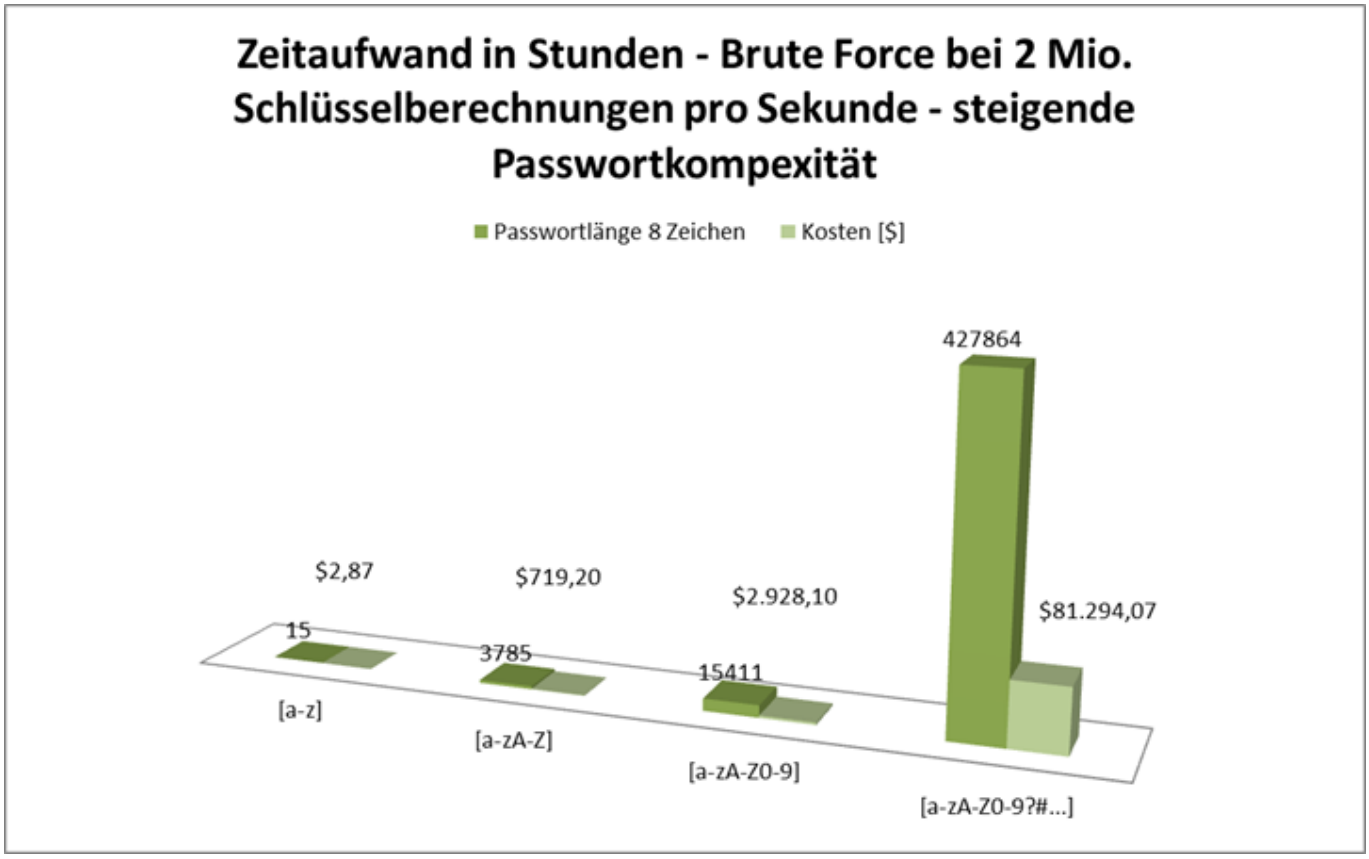
Es gibt **697.287.735.690** mögliche Passwörter. Wie oben erläutert, wird man bereits bei ca. 50% einen Treffer gelandet haben. Also reduziert sich die Zahl auf 348.643.867.845 Tests. Da eine Instanz pro Sekunde 2 Millionen Tests ausführen kann, ergibt sich ein Zeitaufwand von 174.322 Sekunden. Das sind ca. **48 Stunden**. Auch das ganz **ohne** Cloud Computing eine lösbare Aufgabe.

Viele Jahre wurde eine Passwortlänge von 8 Zeichen empfohlen. Ist man damit heute immer noch auf der sicheren Seite? *



Verwendet man *ausschließlich Kleinbuchstaben [a-z]*, sieht man auf den ersten Blick, dass die Länge keinesfalls ausreicht. Ein Vergleich mit den Dimensionen bei einem Passwort der Länge 6 und bei Verwendung des kompletten Zeichenvorrats bringt dies bereits zutage. Man muss nicht rechnen.

Sehen wir uns hierzu eine Grafik an, der wir den **Zeitaufwand** und die **Kosten zur Berechnung** in der Cloud entnehmen können:



Der Zeitaufwand bezieht sich hier immer noch auf **eine einzige Instanz**. Man könnte diese Werte also auch auf dem Heim PC erreichen, wodurch die Kosten natürlich auf Höhe des Stromverbrauchs lägen. Dennoch macht die Angabe der Kosten Sinn. **Die Kosten bleiben (*vereinfacht*) konstant, unabhängig von der Zahl der angemieteten Instanzen.** Ob wir eine Instanz 100 Stunden rechen lassen oder 100 Instanzen für jeweils eine Stunde, die Kosten sind identisch.

Im niedrigen Komplexitätsbereich haben wir überschaubare Kosten. Knapp **3 Dollar** und **15 Stunden** Aufwand bei einem Passwort der Länge 8, bestehend nur aus Kleinbuchstaben. Die Zeiten für die Tests werden bei zunehmender Komplexität zunehmend kritisch. Bei Verwendung von Groß- und Kleinbuchstaben sind bereits **3785 Stunden** (ca. 157 Tage) nötig, um das Passwort zu „knacken“. Hier muss man bereits auf paralleles Berechnen zurückgreifen, um mittels Brute Force in angemessener Zeit zu einem Ergebnis zu kommen. Beauftragt man **100 Instanzen** mit dem Brute-Force Angriff, reduziert sich der Zeitaufwand auf ca. **1 ½ Tage**. Durchaus machbar!

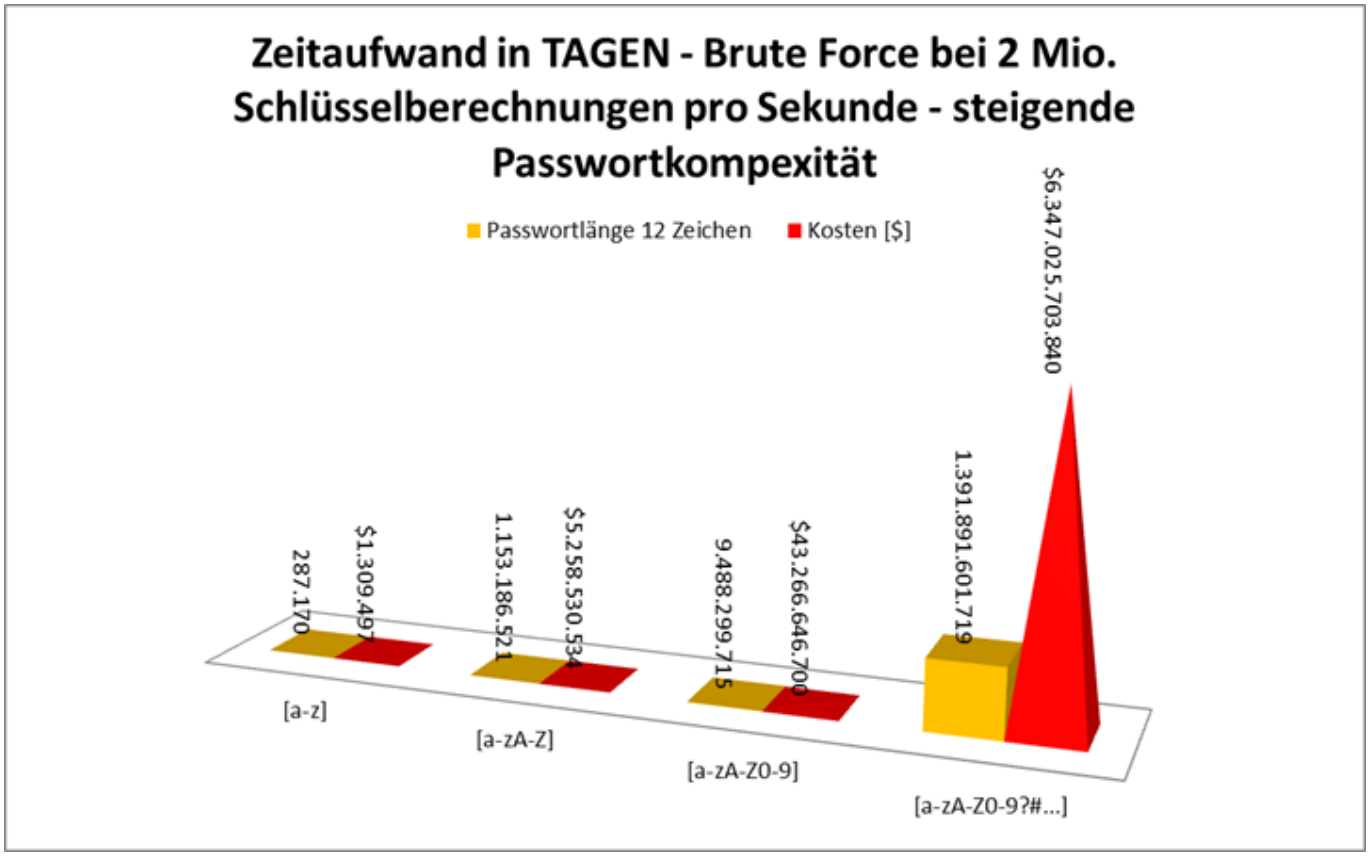
Bei Verwendung des kompletten Zeichenvorrates sieht es so aus, als sei man zurzeit noch auf der sicheren Seite. Brute Force dauert hier bei Verwendung einer Einzelinstanz **48**

JAHRE.

Setzt man **10.000 Instanzen** auf das Passwort an, braucht man jedoch gerade einmal **42 Stunden**. 10.000 Instanzen hören sich unglaublich an und sind sicher eine Hausnummer. Niemand würde diese Ressourcen in das Brechen des Passwortes von Lieschen Müller stecken. Aber es gibt Ziele, bei denen sich dieser hohe Aufwand lohnt. Auch diese enormen Rechenkapazitäten kommen in der Realität bereits vor. Die **National Security Agency** (*NSA*) dürfte über eine Infrastruktur verfügen, die derartige Zahlen weit hinter sich lassen dürfte.

MERKE: Passwörter sollten mindestens die Länge 12 aufweisen und aus dem kompletten Zeichenvorrat aufgebaut sein.

Hier werden dann bei **Zeitaufwand** und **Kosten** Dimensionen erreicht, die in absehbarer Zeit niemand aufbringen wird.



In dieser Grafik ist der **Zeitaufwand in TAGEN** aufgeführt. Nicht in Stunden! Bereits bei Verwendung von **nur Kleinbuchstaben** und dem Einsatz von **10.000 Instanzen**,

benötigen wir **28 Tage** die komplette Rechenpower und, nicht ganz unerheblich, über 1 Mio. US Dollar.

Macht uns das sicher?

Paralleles Rechnen ist nicht nur mit kostenpflichtigen Cloudlösungen realisierbar, sondern auch mit „kostenlosen“ **BOT Netzen**. Dabei gab es BOT Netze, die aus bis zu 30 Millionen Rechnern bestanden. Durchaus denkbar, dass diese Netze nicht nur zum Spammen und für DDoS Attacken verwendet werden, sondern auch zum „Knacken“ von Passwörtern.

Nehmen wir einmal diese 30 Millionen Rechner als Wert und prüfen, ob man einem komplexen 12 Zeichen Passwort gefährlich werden kann.

Der Zeitaufwand für eine Einzelinstanz beträgt **1.391.891.601.719 Tage**. Dies entspricht **3.813.401.648 Jahren**. Setzen wir die **30 Mio. Instanzen** eines Bot Netzes auf dieses Passwort an. Als Ergebnis erhalten wir **127 Jahre**. Wenig aussichtsreich. Hinzu kommt, dass BOT Netzwerke relativ instabil sind. Schließlich hat man es mit befallenen Rechnern von Normalanwendern mit unterschiedlicher Anbindung an das Internet zu tun. Damit steigt der Aufwand für diejenige Instanz die die Abarbeitung der verschiedenen Teilaufgaben koordiniert. Ausgefallene Instanzen wollen ersetzt werden.

Vielen von Ihnen dürfte AES (*Advanced Encryption Standard*) ein Begriff sein. Der Nachfolger des berühmten DES (Data Encryption Standard) Verfahrens. Für dieses DES Verfahren wurden und werden bis zum heutigen Tage Verfahren ersonnen, um mit minimalem Zeit- und Geldaufwand Brute Force Angriffe auszuführen. Das COCACOBANA (*Cost-Optimized Parallel Code Breaker or COCO*) Projekt und das Projekt RIVYERA zeigen, welche Leistungen mit spezialisierter Hardware möglich sind. siehe DES Brute Force Cracking Efforts 1977-2010

Fazit *

Müssen Sie Angst haben?

Sofern Sie sich an die obigen Empfehlungen halten und ein Passwort mit Mindestlänge 12 Zeichen nutzen, welches sich des gesamten Zeichenvorrats bedient, nicht. Zumindest zurzeit nicht, wenn es um Brute Force und Cloud Computing geht. Die Daten, die sie schützen, müssen mindestens den Wert haben, den ein Angreifer investieren muss, um an

sie zu gelangen. Kein Angreifer wird 100.000$ investieren, um Ihren neuen Vertrag mit der Versicherung einsehen zu können.

Diese Aussage gilt heute, im März 2013. Auch für 2014 wird sich vermutlich wenig ändern. Welche Empfehlung man 2015 geben muss, steht auf einem ungeschriebenen Blatt!

Wie einleitend beschrieben, lauern aber an vielen Stellen Gefahren, denen wir nicht mit einer absolut zuverlässigen Methode entgegenwirken können. Auch nicht mit einem „100 Zeichen langen SUPER Passwort“! Diese Verfahren erfordern von den Angreifern viel weniger Aufwand, sind viel erfolgversprechender und daher deutlich wahrscheinlicher.

Im Artikel das beliebteste schlechte Passwort 2012 habe ich einige allgemeine Regeln für den Umgang mit Passwörtern aufgeführt. Um die Gefahren zu minimieren, die von Trojanern, Phishing Seiten und Mails ausgehen, sollten Sie unbedingt einen **Virenscanner** einsetzen. Anscheinend verzichten immer noch unzählige Nutzer auf diesen Schutz. Die Ausrede, man surfe ja nur auf sicheren, namhaften Seiten, zählt LEIDER nicht mehr. Immer häufiger werden solche vertraulichen Seiten „gehackt“ und als Schleuse für Schadsoftware verwendet.

