Zusammenfassend zur Sicherheit bei der Rechnernutzung

Es gibt 11 Schutzmechanismen, die auf einem Rechner wirksam werden können:

1. **Mißtrauen**
   Alles was vom Rechner ausgeschrieben wird genau lesen und bei Zweifel, die Aktion lieber abbrechen und einen Kundigen befragen.
   Günstige Angebote immer kritisch hinterfragen (es verschenkt niemand etwas!).
   Immer wenn an einer Mail von einem mir unbekannten Nutzer ein Anhang hängt, muss man sehr mißtrauisch sein, denn ist in diesem Anhang ein Virus enthalten, ist er auch beim Öffnen schon auf meinem Rechner (so hat sich offensichtlich der Virus im Mai 2015 in das Computernetz des Bundestages geschlichen, weil Einige mit nicht aktuellem Virenscanner und neugierig solche Anhänge geöffnet haben. Welche Folgen das hat, sieht man)

2. **Firewall**
   Dieses Programm wird im System immer installiert und regelt die Ein- und Ausgänge zum Netz. Meckert die Firewall, dann hat das einen Grund, also nicht ausschalten.

3. **Nutzer am Rechner, Passwörter**
   Jeder Nutzer am Rechner (der den Rechner starten) hat grundsätzlich ihm zugewiesene Nutzungsrechte! Die Rechte werden mit **Nutzernamen** und **Passwörter** belegt, jeder Nutzer sollte deshalb immer einen Namen und ein Passwort haben! Hat man das nicht, haben auch Viren ein leichtes Spiel.
   Es gibt **Nutzer mit Administrator-Rechten** und solche mit **eingeschränkten Rechten**.
   Der **Administrator** darf alles am Rechner (so erhält man den Rechner mit vorinstalliertem Betriebssystem), z.B. darf er Programme installieren und löschen, was ein Nutzer mit geringeren Rechten nicht darf.
   Schadsoftware erhält immer die Rechte des jeweiligen Nutzers, ist er nicht Administrator, kann die Schadsoftware nicht installiert werden! Die Schadsoftware sucht nach dem Administrator, heißt er wie standardmäßig „Administrator“ und hat er kein Passwort, kann diese sofort nun doch ohne weitere Nachfragen installiert werden. Hat man ein Passwort und dieses im Rechner gespeichert, kann es durch die Schadsoftware gefunden und genutzt werden! **Also niemals Passwörter speichern und sie sollten für alle notwendigen Aktionen immer anders sein!!!**
   Je länger ein Passwort ist, um so sicherer ist es!
   Man arbeitet also sicherer als **Nicht-Administrator** und meldet sich nur zur Installation neuer Software als Administrator an.
   Fürs **Online-Banking** kann man sich einen **weiteren Nutzer** anlegen, nicht „Banking“ oder „Geld“ sondern z.B. „**Rudi-ratlos**“ und ein irriges Passwort „**-Rru@_Ditlos?**“. Bei diesem Nutzer wird nur die Bank-Software installiert und man greift nicht aufs Internet zu und keine weitere Software, dann sollte der Nutzer sehr sicher sein.

4. **Betriebssystem**
   Betriebssysteme müssen immer durch **Updates** auf den neusten Stand gebracht werden! Auch wenn die Einstellungen dies automatisch tun, sicher aber zu einer Zeit, wenn man den Rechner nicht eingeschaltet hat (3 Uhr Nachts), deshalb sollte man immer nach dem Einschalten sofort nach Updates suchen, d.h. man muss in der Lage sein diesen Vorgang auszulösen. Wenn man Online-Banking machen will, ist diese Aktion lebensnotwendig!
   Für ältere Betriebssysteme (XP und VISTA) werden keine Updates bereitgestellt, somit sind sie anfällig für Schadsoftware (siehe Mai 2017: WannaCry-Virus; befiel im Wesentlichen diese alten Systeme (DB XP-Terminals)).
   Betriebssystem-Updates schließen von Programmierern gefundene Lücken, die die

Schadsoftware nutzt. Durch das Update wird die Angriffsstelle geschlossen, führe ich das Update nicht durch, bleibt diese Angriffsstelle offen!

5. **Update Internetbrowser**
   Internet-Explorer (Windows 7, 8 und 8.1) Edge (Windows 10) werden mit dem Betriebssystem-Updates ebenfalls aktualisiert, alle anderen Browser, wie z.B. „Firefox“ nicht. Diese müssen ebenfalls aktualisiert werden. Auch hier gilt, dass das zumeist automatisch erfolgt, aber man sollte auch in der Lage sein diesen Vorgang selbst auszulösen. Explorer sind ebenfalls beliebte Ziele für Schadsoftware, denn fasst jeder Nutzer des Internets muss diese Software nutzen, da kann man viel Schaden anrichten!

6. **Installation von Software**
   Software kann man kaufen oder aus dem Internet herunterladen.
   Kauft man ein neues Gerät zum Rechner, kauft man auch die Software-Lizenz mit. Das kann in Form von CD‘s sein, aber meist erhält man nur eine Lizenz-Nummer. Verbindet man das Gerät mit dem Rechner, nimmt es Verbindung zu seinem Hersteller auf und läd die entsprechende Software auf den Rechner runter, allerdings nur nach Bekanntgabe der Lizenz-Nummer, diese Verfahren wird auch als „Drag and Drop (D&D / Ziehen und Ablegen) bezeichnet. Manche Software kann man so auch ohne Lizenz-Nummer laden, z.B. „Libre Office“ oder „Acrobat Reader“, die sind generell frei. Will man irgendwelche andere Software aus dem Internet laden, dann sollte das nur über bekannte Firmen erfolgen, wie z.B. „Chip“, „Computer Bild“, „c‘t“ usw. und sollte es die da nicht frei geben, aber nur bei unbekannten Anbietern, dann ist äußerste Vorsicht geboten, es kann Schadsoftware mit übergeben werden! Man sollte sich bei „Google“ informieren.
   Google hat zwei Stellen für eine Eingabe:
   Ziemlich weit oben kann die Adresse einer WWW-Seite eingegeben werden (das ist eigentlich keine Leistung von Google sonder kann auf jeder WWW-Seite eines Internet-Browsers erfolgen):

   Jetzt öffnet man nun doch die Seite der Schadsoftware, das wollte man ja nicht!
   Die zweite Eingabe ist die **Suchanfrage**:

   Da bekommt man die entsprechenden Verweise auf Seiten zu dem Thema, natürlich auch zur Schadsoftware, die brauche ich ja nicht zu öffnen! Man bekommt meist Hinweise von anderen Nutzern, die auch Probleme mit der Seite hatten.

7. **WOT**
   WOT (Web of Trust) ist eine Internetnutzer-Community, die sich dem Kampf gegen Betrug im Internet verschrieben hat. Das sieht dann z.B. so aus:

   Hinter der Adresse der Seite wird dann ein kleiner Kreis geschrieben, der hat die Farben:
   grün, **gelb**, **rot** oder **grau** (hier grün)
   (grün – ok; gelb – Vorsicht; rot – gefährlich; grau – nicht bewertete Seite)
   WOT wird als Add-On in Firefox installiert.
   Leider ist diese Software auch sehr stark das Ziel von Schadsoftware, man möchte nicht als „böse“ erkannt werden und es werden auch Daten abgegriffen, so dass einige WWW-Anbieter diese Software nicht mehr anbieten! Man bekommt aber schnell eine Information, dass man die Seiten besser nicht öffnen sollte, z.B. so:

So kann das aussehen, das ist ein Virus!!! Freundliche Angebote, wie „Gratis-Scan & -Diagnose“, „PC-Reiniger“, „Geld zurück“ usw. führen zu WWW-Seiten mit Viren.
Die Mitteilung:“*...Ihr PC ist gefährdet…, sollen wir eine ganz notwendige Diagnose durchführen?*“ Antwortet man mit **ja**, ist **der Virus auf meinem PC!**

Bitte immer nach dem Motto verfahren: „**wenn ich nicht gespielt habe, kann ich auch keinen Gewinn haben!**“ (es verschenkt niemand etwas)
Nur wenn ich selbst solche Aktionen auslöse, ist das ok. Windows bietet in seinem System schon eine Menge von Ordnungs- und Reinigungs-Funktionen an, die sind garantiert virenfrei!

8. **Anti-Viren-Software/Virenscanner**
Bisher haben wir viel Sicherheit erzeugt ohne eine spezielle Software gegen Viren zu nutzen. Die kann man Gratis im Internet bekommen (aber bitte nur wie oben beschrieben, bei bekannten Anbietern) oder auch kaufen. Die gekauften Systeme bieten meist einen besseren Schutz. Allen ist jedoch eigen, dass auch sie immer aktualisiert werden müssen, also Updates durchgeführt werden. Da gelten die selben Regeln wie allgemein: „sie werden automatisch durchgeführt, aber ich muss in der Lage sein, den Vorgang auch auszulösen!“
Grundsätzlich gibt es immer mindest 2 Aktionen:
Update und
Systemprüfung
Update
Viren setzen grundsätzlich in dem Programm, dass sie befallen haben, eine Kennung ab. Das dient dazu, dass sie dieses Programm nicht wieder angreifen, denn sonst würden sie sich hier festlaufen. Diese Kennung ist aber auch die Möglichkeit, sie zu finden. Damit der Vieren-Scanner auch weiß, nach welcher Kennung er suchen muss, müssen die Muster ständig aktualisiert werden (Update). Da Viren massenhaft pro Minute erscheinen, müsste das eigentlich pausenlos erfolgen, dann kann aber der Rechner nicht mehr arbeiten, also macht man einen Kompromiss, z.B. alle 15 Minuten (oder so). Die Aussage: „*habe ich gestern Abend gerade gemacht!*“ ist sträflich, denn **pro Tag** werden etwa **~390.000 Viren** erzeugt, also
~271 pro Minute (~4/sec). Die müssen alle erst mal gefunden und dem Scanner mitgeteilt (Update) werden.
Systemprüfung
Da werden alle Dateien meines Rechners nach Viren durchsucht. Wenn man ein paar Millionen Dateien auf dem Rechner hat (das ist ganz normal), dann dauert diese Prüfung schon mal eine Stunde und mehr.

9. **Internetzugang**
Eigentlich muss man an den Anfang der Sicherheitskette noch ein weiteres System hinzufügen – das Internet-Modem.
Die Bezeichnung Modem ist zu kurz gefasst, denn dieses Gerät kann weit mehr als nur eine Internetverbindung herzustellen.
Im Sinne der Sicherheit ist hier eine weitere Firewall-Software installiert. Das „Modem“ ist auch ein Rechner, hat natürlich auch ein Betriebssystem mit vielen Teilkomponenten. Das

Betriebssystem wird meist vom Hersteller automatisch aktualisiert, man kann den Vorgang auch selbst auslösen.
Das System hat ein Passwort, was man natürlich auch ändern kann, denn die Standardeinstellung ist wieder leicht zu ermitteln. Vor gar nicht langer Zeit wurde reihenweise auch Modems angegriffen, die Hersteller der Modems mussten neue Firmware liefern. Die Schadsoftware kontrolliert die Datenbewegung und kann sich bei jeder Nutzung in das gesamte private Rechnernetz ausbreiten.
Sofern man kein Internet-Telefon nutzt, kann man natürlich auch bei Nichtnutzung des Internets das Modem abschalten (ausschalten).

10. Software/Daten von anderen übernehmen

Auch wenn es der beste Kumpel ist und er mir sicher keinen Schaden zufügen will, sollte man einen **USB-Stick, SD-Karte oder externe Festplatte** erst nutzen, wenn sie auf Viren untersucht wurde. Man kann einzelne Dateien, Ordner oder Datenträger auf Viren untersuchen. Manchmal weiß der Freund selbst nicht, dass er Viren auf seinem Speicher hat. So hat man wohl auch Schadsoftware in die völlig autonomen Rechner des Iranischen Atom-Programms eingeschleust, man hat einen (oder mehrere) goldig glänzende USB-Sticks auf dem Gelände „verloren“. Irgend ein Mitarbeiter hat dann das Spiel am Rechner gespielt und den Virus ins System gebracht, welcher dann die Zentrifugen zu unerlaubten Drehzahlen gebracht hat, so dass sie dann endlich geborsten sind. Und das zeitlich sehr unterschiedlich, dass man nicht sofort auf einen Virus schließen konnte.
Wir nutzen zwar keine Zentrifugen, man sollte von unbekannter Software Abstand halten, also nicht nutzen!

11. Passwörter speichern

Wie bereits dargestellt, sollte man für **unterschiedliche Aktionen auch unterschiedliche Passwörter** verwenden. Hintergrund ist, ist eines ermittelt worden, dann passt es eben nicht für andere Aktionen. Natürlich braucht man zur Sicherheit eine Kopie in schriftlicher Form, besser ist natürlich das in einem Textsystem auf dem Rechner abzulegen, was aber wieder ganz schlecht ist.
Ich habe folgenden Weg gewählt:
Alle meine Daten werden mit einem von mir geschriebene Programm kodiert und in eine Liste gespeichert (z.B. ein Ausschnitt daraus):

== |qqp|{~€,cA<@b
>=fsmzspm€qz,`,O{y
?<Mz otx wqzz zsF,<<==CEAC<EDB

Auf dem Rechner wurde ein lokaler WWW-Server installiert, der mittels Programm (und das kann nur im lokalen WWW-Server gestartet werden) diese Daten wieder dekodiert und man erhält eine WWW-Seite mit den lesbaren Daten. Die Seite muss mittels Passwort, was wiederum kodiert ist, geöffnet werden. Der lokale Server kann vom Netz nicht genutzt werden, die Firewall unterbindet das.
Von unterwegs kann ich diese Daten deshalb auch nicht lesen!

Was sagen andere zur Computer-Sicherheit?

Der NSA-Hacker empfiehlt sechs Abwehrmaßnahmen

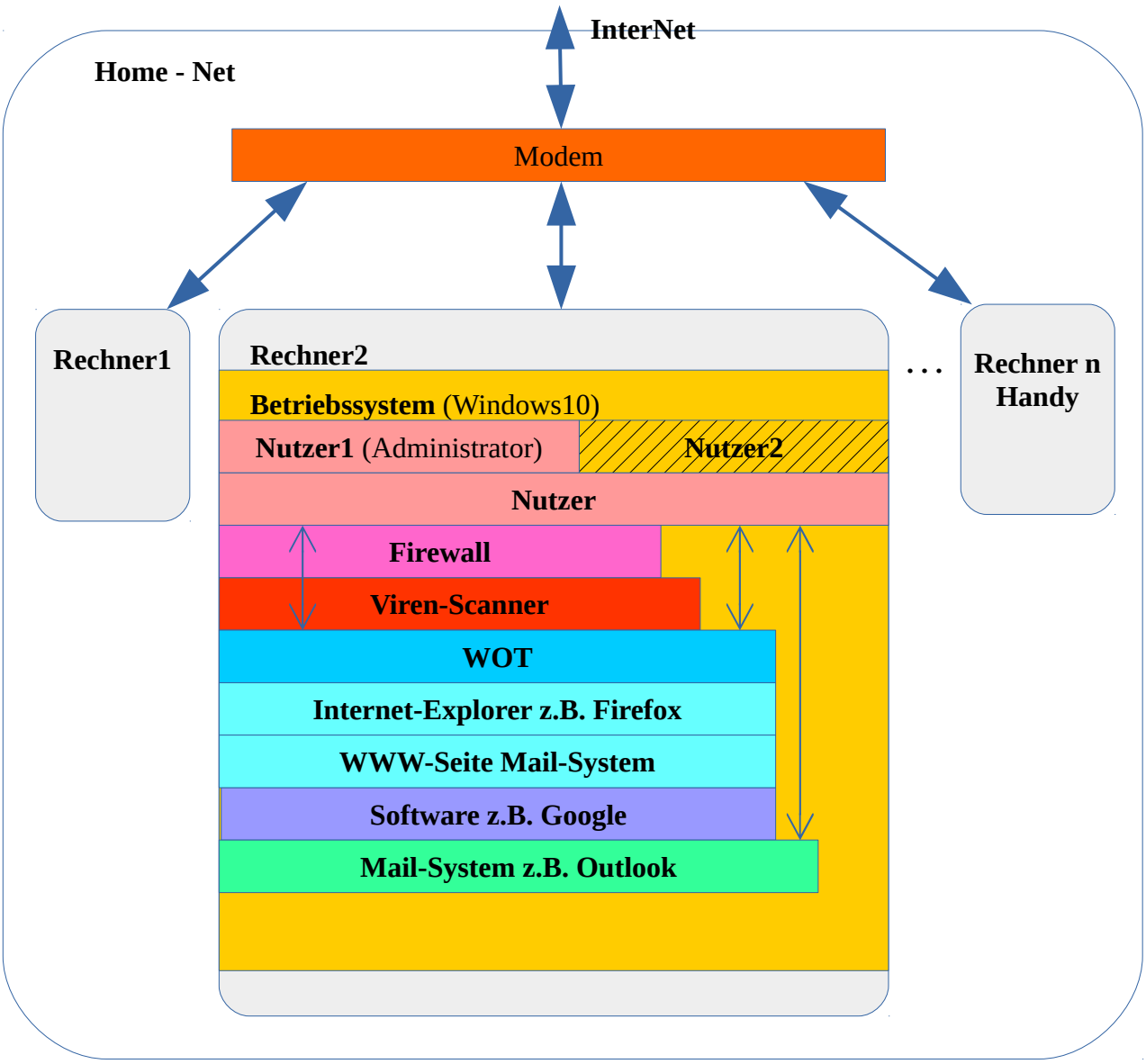
Patrick Beuth
Patrick Beuth ist Redakteur im Ressort Digital bei ZEIT ONLINE.

Der Leiter der NSA-Elitehacker erklärt bei einem seiner seltenen öffentlichen Auftritte, wie man seinem Team das Leben schwer macht.
Was Joyce noch zum Thema Netzwerke sagte, sollte jeden Administrator aufhorchen lassen: "Wenn Sie Ihr Netzwerk wirklich schützen wollen, müssen Sie es kennen, inklusive aller Geräte und Technologien darin. In vielen Fällen kennen wir es besser als die Menschen, die es entworfen haben und betreiben." Der "subtile Unterschied" sei jener zwischen dem, was nach Ansicht eines Admins in seinem Netzwerk laufen sollte, und dem, was wirklich darin läuft.

Sechs Abwehrmaßnahmen empfahl Joyce,
beginnend mit dem Whitelisting von Anwendungen. Das bedeutet, eine nicht explizit freigegebene Software kann auf einem Computer nicht installiert werden.
Zweitens sei eine strikte Rechtevergabe für die Anwender wichtig,
drittens stets aktualisierte Software,
viertens segmentierte, also nicht miteinander verbundene Teilnetze.
Fünftens könne ein sogenanntes Reputationsmanagement dafür sorgen, dass abnormales Verhalten eines Nutzers bemerkt wird – wenn er zum Beispiel plötzlich erstmals versucht, auf bestimmte Daten zuzugreifen.
Der **sechste** Ansatz ist die Überwachung des Netzwerkverkehrs. Ein smarter Admin, der die Netzwerk-Logs liest und auf Anomalien achtet, ist demnach so etwas wie der natürliche Feind der NSA.

Zum Schluss zeigte Joyce seinem Publikum noch eine Folie mit einem QR-Code darauf. "Wer von Ihnen scannt jetzt den QR-Code des NSA-Typen?", fragte er scherzhaft – wohl wissend, dass QR-Codes ein alter Trick sind, um Nutzer auf unbekannte, verseuchte Websites zu leiten. Dieser führe aber auf eine legitime NSA-Seite mit weiterführenden Informationen zum Thema Gefahrenabwehr. "Das ist ein echter Link", sagte er. "Vertrauen Sie mir."

10 goldene Regeln für Computersicherheit **(Universität Bielefeld)**


InterNet
Home - Net
Modem
Rechner1
Rechner2
Betriebssystem (Windows10)
Nutzer1 (Administrator)
Nutzer2
Nutzer
Firewall
Viren-Scanner
WOT
Internet-Explorer z.B. Firefox
WWW-Seite Mail-System
Software z.B. Google
Mail-System z.B. Outlook
. . .
Rechner n
Handy

Noch einmal zu Passwörtern

In welcher Situation ist die Sicherheit des Passwortes notwendig?
Eigentlich gibt es unter vielen 3 wichtige Situationen:
1.
Der Rechner ist ausgeschaltet.
Ein nicht berechtigter Nutzer schaltet den Rechner ein und muss nun mittels probieren das richtige Passwort finden.
Da ist es wichtig, dass das Passwort nicht trivial ist und auch keinen Bezug auf den Nutzer hat. Und es sollte auch keinen Bezug auf die Umgebung haben. Weiterhin lassen sich die Einstellungen am Rechner so wählen, dass ab einer bestimmten Anzahl von Versuchen die Zeiten zum erneuten Versuch ständig vergrößert werden, wenn man bis zum nächsten Versuch Stunden braucht, macht es keinen Sinn mehr.
„Kein Passwort“ würde in dieser Situation jedem Nutzer Zugang gewähren.
2.
Der Rechner ist eingeschaltet und bleibt sehr lange in diesem Zustand, z.B. Server, es erfolgt lange Zeit keine Bedienung über die Tastatur.
Um das Passwort zu finden, muss eine Schadsoftware auf dem Rechner laufen, die pausenlos alle Varianten des Passworts generiert und mit dem gespeicherten, kodierten vergleicht. Hier gilt, je länger das Passwort ist, um so sicherer ist es (siehe unten). Da die Schadsoftware ja auch auf dem Rechner laufen muss gilt, um so langsamer der Rechner ist, um so sicherer ist er. Die Schadsoftware ist schnell zu finden und zu löschen.
3.
Rechner ist eingeschaltet, er wird oft über die Tastatur bedient.
Eine Schadsoftware untersucht ständig den Datentransfer von der Tastatur und könnte so auch das Passwort scannen. Natürlich muss die Schadsoftware auch herausfinden, wann das gesuchte Passwort übertragen wird. Ist das aber der Fall, dann **gibt es keinen Schutz für das Passwort!**
Man kann nur die Schadsoftware so schnell wie möglich finden und dann sofort löschen.

Wie gestaltet man ein Passwort?
Die Aussage „**kompliziert**“ würde ich als nicht ausschlaggebend bezeichnen (nur für den Fall 1), denn lasse ich ein Passwort mit einem Programm suchen, dann ist es egal welches Zeichen da steht, es wird genau wie ein einfaches Zeichen gefunden. Es sollte dennoch nicht „**trivial**“ sein, denn dass würde man als Mensch schon mal probieren, z.B. „12345678“ oder „qwertzui“ (das ist die oberste Reihe der Buchstaben, in gleicher Weise auch die anderen Tasten-Reihen). Besser ist natürlich schon, eine „**nicht triviale**“ Reihe von Zeichen einzugeben. Für ein Programm ist das aber egal, da zählt nur die Anzahl der Zeichen (Fall 2)!
Ein Beispiel:
Es sollen folgende Zeichen verwendet werden (es gibt noch weitere Möglichkeiten)

Zeichen:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z	26
	a b c d e f g h i j k l m n o p q r s t u v w x y z	26
	0 1 2 3 4 5 6 7 8 9	10
	! “ § $ % & / ( ) = ? ; : _ - . , < > * + # ° @ €	25

		87

Das sind somit 87 verschiedene Zeichen, was ist damit möglich?
Jetzt kommt die Mathematik ins Spiel, da kann man die Statistik nutzen, z.B. gilt in unserem Fall die „**Variation**“. **Variation mit oder ohne Wiederholung**, also z.B. das Passwort „Donnerstag“ ist

mit Wiederholung da das Zeichen „n“ 2 mal auftritt, die müssen nicht nebeneinander stehen, z.B. ist „Januar“ auch mit Wiederholung.
Die Variationen **ohne Wiederholung** wird aus: **n! / (n-k)!** berechnet
(n Fakultät geteilt durch (n – k) Fakultät)
(n – Anzahl der vorhandenen Zeichen (87), k – Anzahl der Stellen des Passwortes (z.B. 8))
Die **Variation mit Wiederholung** wird berechnet: **n^k** (n hoch k)

In der folgenden Tabelle sind die Variationen in Abhängigkeit von der Anzahl der Stellen für dieses Beispiel berechnet worden (1 Zeichen bis 13 Zeichen).

Anz. Stellen	Variationen ohne Wiederholung		Variationen mit Wiederholung
1	87		87
2	7.482		7.569
3	635.970		658.503
6	**363**.586.592.880	Milliarden	**433**.626.201.009
8	**2**.356.041.121.862.400	Billiarden	**3**.282.116.715.437.121
9	**186**.127.248.627.129.600	Billiarden	**285**.544.154.243.029.527
10	**14**.517.925.392.916.108.800	Trillionen	**24**.842.341.419.143.568.849
11	**1**.117.880.225.254.540.377.600	Trilliarden	**2**.161.283.703.465.490.489.863
12	**84**.958.899.399.345.068.697.600	Trilliarden	**188**.031.682.201.497.672.618.081
13	**6**.371.917.454.950.880.152.320.000	Quadrillionen	**16**.358.756.351.530.297.517.773.047

Das ist schon beachtlich,
mit **8 Zeichen** gibt es über **3 Milliarden** Möglichkeiten zur Formulierung des Passwortes,
mit **13 Zeichen** sind das über unglaubliche **16 Quadrillionen**.

Man kann nun weiter einmal berechnen, wie lange ein Programm braucht, um das Wort zu knacken. Nehmen wir an, der Rechner kann mit einem Tempo von **2GHz** (2×10^9Hz) arbeiten und er würde pro Takt eine Kombination zum Vergleich erzeugen (was nicht geht, er braucht mehrere Takte zur Lösung des Problems)
16 Quadrillionen sind 16×10^{24} .
Für die Vergleiche sind etwa:

$16 \times 10^{24} / 2 \times 10^9 = 8 \times 10^{15}$ sec notwendig oder
8×10^{15} sec / 60 = 133.333.333.333.333,333… min
133.333.333.333.333,333… min / 60 = 2.222.222.222.222,222… Stunden
2.222.222.222.222,222…Stunden / 24 = 92.592.592.592,592… Tage

also **92 Milliarden Tage** werden mit diesem PC gebraucht, **um ein 13 Stelliges Passwort zu knacken**.
Allerdings ist das die maximale Anzahl, es wird sicher viel eher gefunden, denn die richtige Kombination kann schon am Anfang liegen, das ist dann Pech!
Aber das Programm muss alle möglichen Tasten für ein Passwort berücksichtigen, damit braucht es eben auch noch länger, denn es weiß ja nicht, dass ich bestimmte Tasten gar nicht benutze.

Wie erfolgt der Vergleich des Passwortes?

Wenn man einen Administrator am Rechner vereinbart, muss (sollte) man dazu auch ein Passwort angeben. Der Rechner muss es speichern. Immer wenn ich mich mit meinem Passwort anmelde, vergleicht der Rechner (das Betriebssystem) mein eingegebenes Passwort mit dem gespeicherten – stimmen sie überein, darf ich arbeiten.
Nun wäre es ja ganz einfach dieses Vergleichspasswort vom Knacker suchen zu lassen, man weiß sogar wo es steht, und nutzt es – das funktioniert so aber nicht.
Das Passwort wird bei der Eingabe grundsätzlich kodiert, Knacker kennen auch den Algorithmus, aber das Verfahren zur Kodierung funktioniert nur in einer Richtung ein zurück gibt es nicht, weshalb man ein vergessenes Passwort auch nicht aus dem gespeicherten regenerieren kann. Es gibt unendlich viele andere Möglichkeiten dieses kodierte Passwort auch aus anderen Passwörtern zu erzeugen, es gibt quasi **keine** Möglichkeit aus dem gespeichertem Passwort das unkodierte Passwort zu erzeugen. Deshalb versuchen die Knacker das Passwort aus der Variation aller Tasten zu probieren. Was man jedoch dabei wenigsten herausbekommt, ist die Länge des Passwortes, das ist schon von Vorteil, aber hat es 13 Zeichen, brauche ich mit meinem PC gar nicht versuchen, es zu knacken, denn dass wären mit dem oben gezeigten Beispiel

mehr als 253 Millionen Jahre (im schlimmsten Fall)!

Da scheint offensichtlich ein Passwort bestehend aus **13 a** auch sicher zu sein:

aaaaaaaaaaaaa

Es ist gar nicht so einfach genau 13 a zu schreiben!

An einem Beispiel kann man eine Variante der Passwort-Suche testen.

Es ist jedoch nur mit 3 Zeichen langen Passwörtern sinnvoll (geht auch mit 4 Zeichen)