Sicher im Internet

Herr Johannes bei den Furzen

https://krawutzi.wordpress.com/
https://krawutzi.wordpress.com/sicher-im-internet/

Version: 1.9.0, Dezember 2020

Inhaltsverzeichnis

Kapitel 00: Einleitung

Willkommen bei "Sicher im Internet"!

Hier möchte ich mein Wissen über IT-Sicherheit mit euch teilen und versuchen in leicht verständlichen Anleitungen euren Computer für die Verwendung mit dem Internet etwas sicherer zu gestalten.
Gleich mal vorweg, **eine hundertprozentige Sicherheit gibt es nicht!** Das muss mal gesagt werden.
Jedoch kann man mit relativ einfachen Schritten einen Computer zumindest so sicher machen, dass nicht jeder Bedrohung Tür und Tor geöffnet sind.

Ich werde auch allgemein über das Verhalten im Internet referieren und was beim Herunterladen und installieren von Software zu bedenken ist.

Bei meinen Anleitungen werde ich ausschließlich zur Verwendung von freier, bzw. für den Privatanwender kostenlose Software raten, da es meistens nicht notwendig ist, Geld für Sicherheit auszugeben.

Natürlich ist die verwendete Software ein recht kontroverses Thema, da wie üblich in der IT-Welt, bei einer Frage vier verschiedene Antworten möglich, bzw. auch richtig sind. Ich beschränke mich bei meinen Vorschlägen auf Programme, die ich entweder selbst verwende, oder aus beruflicher Erfahrung gut kenne.
Diese werden **immer für das Microsoft Windows Betriebssystem** sein, weil das die meisten Leute benutzen

Weiters schlage ich nur Dinge vor, die ich auch meinen Freunden (die mich ja jederzeit persönlich quälen können) empfehlen würde.

Was noch zu erwähnen wäre ist, dass ich zugunsten der Lesbarkeit bewusst auf das Gendern (Binnen-I) verzichtet habe. Natürlich sind bei der Nennung der männlichen Formen auch immer die jeweiligen Damen gemeint...

Ich hoffe, dieses Skriptum wird euch ein wenig helfen und trägt so ein wenig zu einem sicheren Internet bei!

Kapitel 01: Warum der Internet Explorer schlecht ist

Hände hoch, wer weiß, was ein Browser ist?
Der Internet Explorer zum Beispiel ist einer. Browser kommt vom englische Wort "to browse", was auf gut deutsch umsehen, stöbern, abweiden usw. heißt.
Auf alle Fälle ist das Internet für die meisten Menschen mit dem Internet Explorer gleichzusetzen.

Grundsätzlich kann man gegen den Internet Explorer, kurz IE genannt, auch nicht viel sagen. Er ist bestimmt nicht sicherer oder unsicherer als andere Browser. Das Problem ist seine Verbreitung, denn bei fast jeder Windowsinstallation ist zumeist der IE der Standardbrowser, was ihn zu einem potenziellen Angriffsziel macht.

Warum?
Na weil böse Hacker auch nur Menschen sind. D.h. sie sind grundsätzlich faul und schreiben ihren Schadcode fast immer nur passend für die meistverwendeten Browser. Wohlgemerkt, ausnutzbare Lücken gibt es in JEDER Software.
Deshalb möchte ich euch eine alternative vorschlagen, nämlich den **Mozilla Firefox!**

Natürlich gäbe es auch noch andere Alternativen, wie z.B. Google Chrome oder Opera. Ich aber bevorzuge den Firefox, da es recht **viele nützliche Erweiterungen** dafür gibt, auf die ich in weiteren Kapiteln Bezug nehmen werde!

Also öffne zum Letzten Mal den IE, und gehe auf die Seite **https://www.mozilla.org/de/firefox/new/** und lade das Installationspaket herunter.
Du kannst bei der Installation alle Voreinstellungen lassen, dann werden auch deine ganzen Lesezeichen importiert, falls du welche gespeichert hast.
Eine genaue Anleitung, wie du Firefox installierst, findest du hier:
https://support.mozilla.org/de/kb/Firefox-unter-Windows-installieren
Beim ersten Start kannst du noch festlegen, dass der Firefox dein Standardbrowser ist. D.h. wo immer du auf eine Internetadresse drauf klickst, wird die Seite fortan mit dem Firefox geöffnet.

Gratuliere, du hast schon den ersten Schritt für ein sicheres Internet gemacht!

Kapitel 02: Sichere Passworte und der Passwortsafe

Jetzt mal ehrlich: **Wie viele Zeichen haben deine Passwörter?**
Vier?
Sechs?
Acht?
Na, ich will euch nicht demoralisieren, aber mit derzeitigen technischen Mitteln und da rede ich nicht von einer CIA Serverfarm, sondern von einem halbwegs vernünftigen PC, ist ein achtstelliges Passwort, sofern es halbwegs komplex ist, in **drei Stunden bis zu drei Tagen** geknackt. Wenn es ein einfaches Passwort ist, wie z.B. "12345678" oder "qwerasdf" sofort!
In dunklen Ecken des Internets gibt es nämlich Listen von bekannten, oft verwendeten Passwörtern, die bei Attacken erst mal ausprobiert werden. Leider verwenden ca. 80% der Leute solche Passwörter und zwar überall.
Und das ist die traurige Wahrheit!

Wie also soll ein gutes Passwort aussehen?
Ich würde sagen so: **j2DUt6XeN7E9**
Oder so: **8M@57d2CeL4w**
Momentan würde es mit einem PC **344000 Jahre** dauern, dieses Passwort zu knacken.
Na freilich! Und wer soll sich den Blödsinn merken?

Der Passwort-Tresor
Hier kommt jetzt der Passwort-Tresor ins Spiel, wie ich es auch im Freundeskreis schon lange und gebetsmühlenartig vortrage.
Der Vorteil eines Passwort-Tresors liegt auf der Hand: Ich muss mir nur das Passwort für den Tresor merken, die richtig komplexen Passwörter kennt dann der Tresor.
An dieser Stelle empfehle ich **KeePass** http://keepass.info/
Keepass kann installiert werden, oder auch in einer mobilen Version von einem USB-Stick aus gestartet werden.
Das Programm unterstützt auch **Autotype**, d.h. du öffnest eine Webseite mit Passwortaufforderung und KeePass gibt die Daten selbst ein und du brauchst maximal nur mehr "weiter" klicken!

Doch auch hier sollte man beachten: Das Passwort für Keepass, bzw. auch für deine Anmeldung auf deinen Rechner solltest du **ein recht komplexes Passwort** verwenden, welches du dir aber trotzdem leicht merken kannst!
Und das funktioniert so: Denke dir einen **Merksatz** aus, dieser muss auch nicht viel

Sinn ergeben, aber merkbar sein, z.B.:
Franzi **u**nd **H**ugo, **d**ie **2** **b**ösen **s**chmieren **Q**uargel **a**uf **d**umme **K**atzen**!**
Das Passwort lautet: FuH,d2bsQadK!
Dieses Passwort würde erst in **465 Millionen(!!!!) Jahren** geknackt sein.
Der Merksatz ist lustig und blöd und deswegen leicht zu merken!

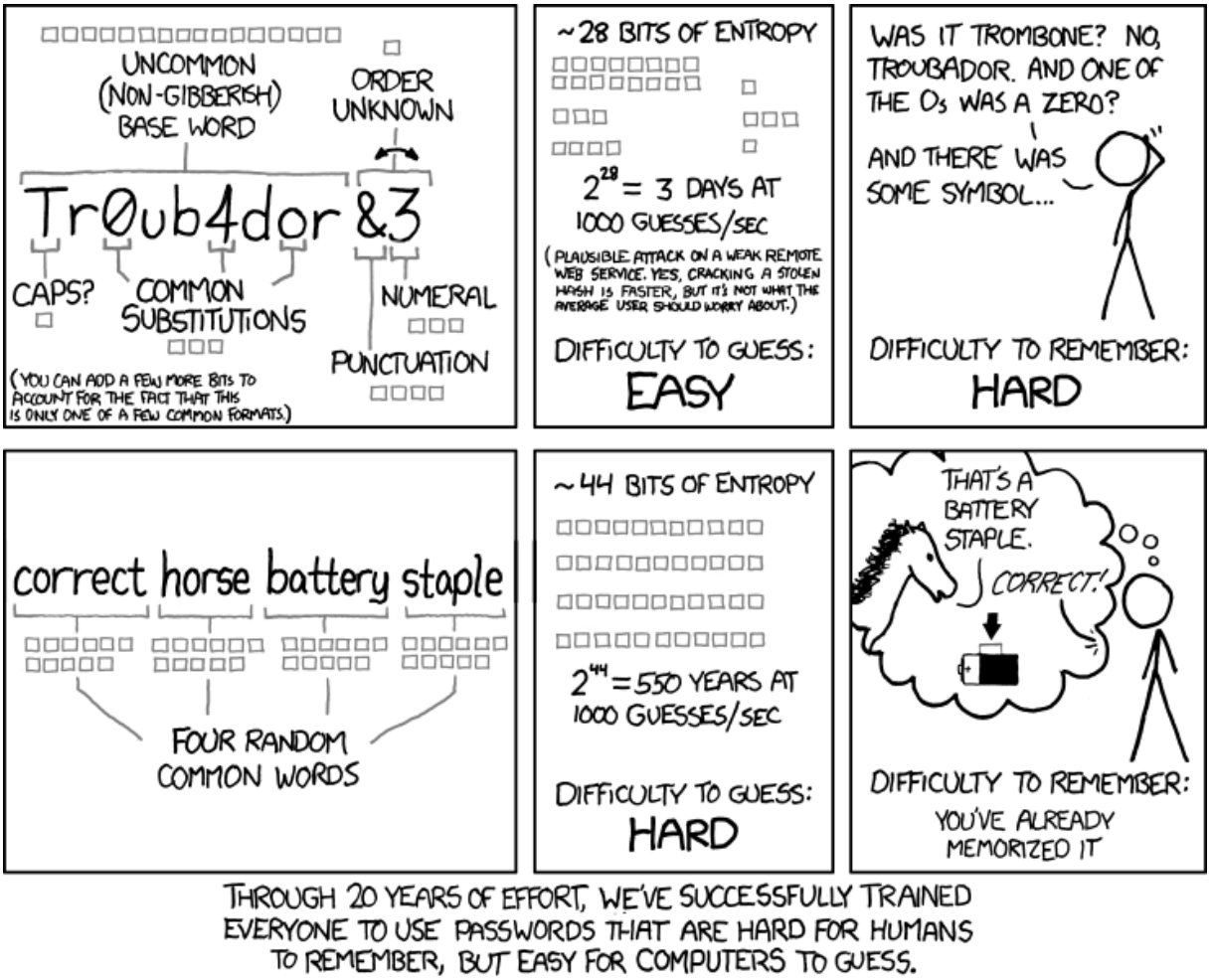
Nun zur Mehrfachverwendung von Passwörtern:
AUF KEINEN FALL EIN PASSWORT MEHRMALS VERWENDEN! NIEMALS!
Dafür hast du jetzt einen Passwort-Tresor! Der ist ja dafür da, viele Passwörter zu speichern.
Dies funktioniert auch besser als ein Zettel, da man im Tresor eine Suchfunktion hat.

Apropos Zettel:
Viele schlaue Leute haben Passwörter auf Haftnotizzetteln auf ihren Monitor kleben. Ich brauche ja nicht erläutern, wie blöd das ist. Auch unter die Tatstatur geklebt, ist ein Klebezettel nicht sicher. Das ist der erste Ort, an dem böse Menschen nachsehen.

Noch was Lästiges: Der Passwortwechsel!
Ein Passwort ist nur sicher, wenn es auch oft genug gewechselt wird.
Da muss ich mich auch selbst an der Nase nehmen. Es ist echt eine Pest, aber Passwörter sollten zumindest alle drei Monate gewechselt werden. Und zwar durch ein ganz anderes. Die häufigste Art der Passwort-Spionage ist nämlich immer noch das gute alte abschauen!

Was traurig ist
Manche Webseiten können möglicherweise mit sehr langen bzw. sehr komplexen Passwörtern nicht umgehen, weil sie eine Längenbeschränkung verwenden bzw. keine Sonderzeichen enthalten sein dürfen. In diesem Fall einfach das längst mögliche Passwort mit Groß, Kleinbuchstaben und Zahlen verwenden. Sollte das auch nicht funktionieren, sollte man vielleicht von einer Anmeldung dort absehen…

Vier zufällige Wörter
Einen sehr guten Ansatz um sich ein leicht merkbares, jedoch aber langes und schwierig zu knackendes Passwort zu gestalten, habe ich auf dem Nerdblog **xkcd** gefunden:



Quelle: http://xkcd.com/936/

Diese Methode würde sich hervorragend dazu eignen, sich ein **gutes, aber leicht merkbares Passwort für unseren Passworttresor** auszudenken und ist eine gute Alternative zur Merksatzmethode!

Nachschlag

Auf folgender Seite kannst du nachsehen, wie lange es dauern würde, ein Passwort zu knacken. Aber bitte dann dieses Passwort nicht verwenden, eh klar, oder?
https://howsecureismypassword.net/

Hier kannst du dir komplexe Passwörter generieren lassen:
https://www.passwort-generator.com/

Kapitel 03: Werbung? Mir doch egal

Also, ich find das voll super: Du kommst auf eine Internetseite und möchtest anfangen zu lesen und plötzlich - ein RIESIGES ROSA IRGENDWAS legt sich über die Internetseite und verkündet, dass du jetzt gefälligst zum Mobilfunkbetreiber mit dem ROSA Logo wechseln sollst.
Wurscht, ob du dich gerade für einen unkündbaren zweijährigen Vertrag beim Betreiber XY verpflichtet hast, weil du unbedingt das neue EiPhone 27 wolltest.
Außerdem ist es der Werbung wurscht, ob du vielleicht eh schon Kunde des Mobilfunkbetreibers mit dem Rosa Logo bist.
Du musst die Werbung erdulden oder wegdrücken. Die Älteren werden sich vielleicht noch an die unsäglichen **Pop-ups** https://de.wikipedia.org/wiki/Pop-up von früher erinnern, die auf fast jeder Internetseite die Leser terrorisiert haben und mittlerweile fast Geschichte sind…

Gewohnheit
Viele Leute, die ich kenne, ignorieren das einfach und drücken gekonnt auf JEDER SEITE die Werbung weg.
Es ist ihnen außerdem auch wurscht, wie sie immer beteuern.
Doch das Problem ist meist nicht die Werbung selbst.
Ich verstehe ja, dass die Webseitenbetreiber Geld verdienen möchten. Es soll ja sogar Blogger geben, die beinahe ihren gesamten Lebensunterhalt durch das Betreiben ihrer Internetseite mit Werbung und bezahlten Beiträgen verdienen.
Ignorieren wir hier gleich mal die Objektivität von bezahlten Beiträgen zu Produkten, die der Leser gleich per Klick kaufen kann.

Ad-Farmen
Das wahre Problem sind die Anbieter der Werbung und ihr riesiger Datenhunger.
Denn es reicht nicht, dem Konsumenten Werbung unterzujubeln, nein, man versucht alle Daten die es über dich herauszufinden gibt zu speichern und das ist gar nicht so wenig.
Jeder Browser kann einem Webserver gewisse Daten mitteilen, normalerweise um die Internetseite für den Browser optimiert auszugeben. Dabei handelt es sich um Daten wie den verwendeten Browser, das Betriebssystem, die zuletzt aufgerufene Internetseite bis zu deiner gesamten Historie der aufgerufenen Internetseiten, die Größe deines Bildschirmes, und ganz wichtig, deine IP Adresse https://de.wikipedia.org/wiki/IP-Adresse (stark vereinfacht die Telefonnummer deines Rechners im Internet). Meistens hinterlässt die Werbung noch ein sogenanntes Cookie https://de.wikipedia.org/wiki/Cookie (eine kleine Textdatei), die bei einem weiteren Besuch der Internetseite abgerufen wird.
Durch diese Daten sind die sogenannten Ad-Farmen irgendwann in der Lage, dein

Surfverhalten, Produkte die du gut oder schlecht findest, deinen Namen, deinen Wohnort, deine Vorlieben, dein Geschlecht, möglicherweise auch deine sexuellen Vorlieben, deinen richtigen Namen und dein Aussehen zu speichern, sprich du bist der berühmt-berüchtigte gläserne Mensch.

Verschwörungstheorie
Vielleicht wirst du jetzt denken, das ist alles nur Spinnerei und Verschwörungstheorie.
Aber lass es mich kurz **anhand von Facebook** erklären:
Facebook (sowie Google, Apple, Microsoft und jeder weitere Betreiber einer Ad-Farm) speichert oben genannte Daten über dich und kann aufgrund von dem, was du auf Facebook schreibst, liest und likest jede Menge weitere Daten über dich generieren.
Facebook ist überhaupt das Paradebeispiel, denn die Server wissen alles über dich und über deine Freunde und Verwandten auf Facebook, manchmal sogar über Leute, die du kennst und nicht einmal bei Facebook sind.
Du bekommst aufgrund der ganzen generierten sogenannten Meta-Daten auf dich zugeschnittene Werbung präsentiert, bei der die Chance, dass du das beworbene auch kaufst, am größten ist.
Ich werde dieser Problematik sogar ein eigenes Kapitel widmen.

Nun, bei sozialen Medien hinterlässt du ja meist gewollt jede Menge Spuren im Internet durch das, was du von dir gibst, aber auf gewöhnlichen Internetseiten kannst du sogar über einen aktiven Facebook-Login (das Cookie von Facebook) persönlich identifiziert werden und dadurch verdienen die Betreiber der Ad-Farmen Milliarden. Mit DEINEN DATEN. Auch wenn du nicht gleich gehst und was kaufst.

Deshalb verwende ich einen Adblocker!
Im Firefox kannst du ihn ganz leicht installieren, indem du auf die Seite https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/ gehst und **uBlock Origin** installierst.
Diese kleine Erweiterung befreit dich von einem großen Teil der Werbung im Internet und schützt dich recht gut gegen das Ausspionieren deiner Daten und vor bösartiger Werbung. Ja auch sowas gibt es, diese überzeugt dich, Schadsoftware auf deinem Rechner zu installieren, weil dein Rechner angeblich eine Sicherheitslücke hat (die du danach ganz bestimmt hast).
uBlock Origin ist übrigens eine Alternative zum recht bekannten Adblock Plus, welches ich aber lieber nicht verwende, weil der Betreiber eine **Liste mit "nicht aufdringlicher Werbung"** pflegt und diese in die Browser-Erweiterung einbindet. Diese Liste gibt es, weil der Hersteller der Erweiterung sich dafür von Ad-Server Betreibern gut bezahlen lässt, und damit meine ich wirklich, wirklich gut…

Man kann sich zwar entscheiden, diese "nicht aufdringliche Werbungen" trotzdem zu blockieren, jedoch finde ich das Vorgehen unethisch.

Adblock oder nicht Adblock

Momentan gibt es einige Internetseiten, die die Benutzer von Adblocker aufmerksam machen, wie arm sie jetzt sind, weil sie ja nichts mehr verdienen und dich dazu überreden wollen, den Adblocker auf ihrer Seite auszuschalten.
Neuerdings gehen Betreiber von Internetseiten sogar so weit, dass sie Benutzern von Adblocker das Anzeigen der Seite ganz verweigern und du entweder für den Inhalt zahlen bzw. den Adblocker deaktivieren sollst.
Der Axel Springer Verlag (Bild Zeitung, Die Welt) nennt Adblock Benutzer sogar "**die Diebe des Internets**"!
Dies sind psychologisch mehr oder weniger ausgefeilte Aussagen, die von beinharten Geschäftsleuten kommen, die den Rachen einfach nicht voll genug bekommen können und eben nicht einsehen wollen, wieso jetzt die Einnahmen ohne Gegenleistung nicht stetig weiter steigen...
Wie seriös das jetzt ist, lassen wir dahingestellt und man sollte den Besuch von Seiten, die zu solchen Mitteln greifen, vielleicht überdenken und ich schlage euch vor, diese negativen Bemerkungen über Adblock-Benutzer einfach zu ignorieren.

Nachschlag

Was dein Browser über dich verrät:
http://www.zendas.de/service/browserdaten.html
http://www.gurusheaven.de/security/anonymitaets_test.shtml

Kapitel 04: Betriebssystem aktuell halten

Wissen alle, was ein Betriebssystem ist?
Wenn du deinen Computer einschaltest, dann startet es. Meistens mehr oder weniger schnell. Es ist die Benutzeroberfläche, die es dir ermöglicht Dateien zu verwalten und Programme zu starten.
Microsoft Windows, Linux, und MacOS sind solche für Personal Computer, Windows Phone, Android und iOS sind die bekanntesten Systeme für Smartphones. Wenn du dich dafür genauer interessierst, siehe https://de.wikipedia.org/wiki/Betriebssystem

Gar nicht so unwichtig
Ein Betriebssystem ist eine irrsinnig komplexe Ansammlung von einer Vielzahl von Programmen, die dafür sorgt, dass der Computer das tut, was er soll.
Früher waren die PC Systeme recht einfach, es gab nur eine Kommandozeile, auf der du dem Betriebssystem Befehle erteilen musstest. Es gab keine Maus, keine hochauflösenden Monitore und kein Internet, das Arbeiten war teilweise recht mühsam.
In diesen "guten alten Zeiten" passten die meisten Betriebssysteme noch auf eine Diskette (wer erinnert sich noch?) mit **1440 Kilobyte**, moderne Betriebssysteme benötigen den gigantischen Speicherplatz von **10 Gigabyte** was ungefähr dem 7300 fachen Speicherplatz einer Diskette entspricht. Milliarden Zeilen von Maschinencode sind dafür erforderlich, Programmierer arbeiten weltweit und rund um die Uhr an neueren Version und Verbesserungen.

Kein System ohne Fehler
Es ist angesichts der Größe eigentlich unmöglich alles vollständig zu testen, daher befinden sich in allen (auch in den aktuellen) Betriebssystemen oft tausende mehr oder weniger gefährliche Fehler, die vom simplen "wieso geht das nicht" bis hin zum Totalabsturz mit Datenverlust führen können.
Früher einmal musste man sich die so genannten **Bugfix-Releases**, also die ausgebesserten Versionen des Systems oder Programmes, noch selbst im Fachgeschäft kaufen, denn schließlich kosteten ja zumindest die Datenträger etwas. Wenn man sein System nicht aktuell hielt, weil man die Fehler nicht bemerkte, oder sie einem einfach nicht betrafen, konnte man auch getrost darauf verzichten. Viren gab es nur wenige und deren Verbreitung war auch auf Disketten angewiesen und ging daher recht langsam vonstatten.

Heute sieht es etwas anders aus, denn fast jeder Computer ist, sobald er eingeschalten ist, **mit dem Internet verbunden**. Eine große Anzahl von Computerviren funktionieren erst dadurch, indem eine oft alte Lücke in den Systemen ausgenutzt wird.

Je komplexer das System...
...umso mehr Fehler hat es. Dies ist eine Tatsache. Darum haben auch wichtige Computer sehr einfache Betriebssysteme, die auf die fundamentalen Funktionen beschränkt sind. Die Raumsonden **Voyager 1 und 2** https://de.wikipedia.org/wiki/Voyager-Programm wurden im Jahr 1977 gestartet und einige Systeme arbeiten immer noch. Und dies trotz Kälte und Strahlung des Weltraumes und der langen Betriebsdauer.
Fast unvorstellbar, oder? Mit Fehlern, die gemacht wurden, musste man sich abfinden, oder sie mussten recht aufwendig per Funk ausgebessert werden. Dies war natürlich recht gefährlich, denn ein Fehler und die Sonde wäre hoffnungslos verloren…

Paranoia
Der häufigste Grund, warum manche ihr Betriebssystem nicht aktuell halten, ist die Paranoia, dass der Hersteller zwar das Betriebssystem aktualisiert, aber auch gleichzeitig Daten vom Rechner abzieht.
Was auch teilweise stimmt, denn fast alle Rechner halten statistische Daten für den Hersteller bereit, um eine Ahnung zu bekommen, was die Kunden oft brauchen und was weniger, wie oft der Rechner benutzt wird und wie lange, wie viele Programme installiert sind und welche, außerdem natürlich Informationen über die Hardware, also das PC Kastl, welches ja von unterschiedlichsten Herstellern kommen kann.
JEDES Betriebssystem sammelt solche Daten und schickt sie an den Hersteller, dies ist nicht geheim und auch keine Verschwörung, man wird bei der Installation darauf hingewiesen und man kann sich aussuchen, ob man das will oder nicht.
Es ist ein gewisses Vertrauen notwendig, wenn man sich ein Produkt kauft, man muss darauf vertrauen, dass einem der Hersteller nicht "übers Haxl haut"...
Wenn man ständig das Gefühl hat, abgehört zu werden und einem ständig Daten fehlen, und DIE haben sie gestohlen, dann sollte man ärztliche Hilfe suchen und keine Computer mehr verwenden.
Wer diese Probleme hat und Mitglied bei Facebook ist, gehört sowieso entmündigt!
Oder man kann auch sein eigenes Betriebssystem schreiben, siehe Nachschlag!

Die Angst erwischt zu werden
Ein anderer Grund, warum manche nicht aktualisieren, ist dass sie eine "nicht ganz legale Kopien" von Programmen und Betriebssystemen verwenden, die sie von "Freunden aus dem Internet" haben.
Sprich fast alles auf dem Rechner ist aus dem "**dunklen Internet**" heruntergeladen und man hegt insgeheim die Angst, vom Hersteller dabei erwischt zu werden.

Warum das vielen so geht ist leicht erklärt: Man kauft sich einen PC. Man packt ihn aus, schließt ihn an und wirft als erster alle Beschreibungen und Datenträger, die dabei sind weg, oder legt sie wo hin, wo man sie garantiert nie wieder findet. Wer braucht das schon?
Dann nach einiger Zeit hat man dem Rechner in einen, sagen wir mal untoten Zustand gebracht, wo nichts mehr richtig funktioniert. Nun ruft man um Hilfe.
Natürlich kennt fast jeder jemanden, der sich mit sowas auskennt...
Dieser Jemand fragt dann nach den CDs und Zetteln mit Lizenzen, die beim Computer dabei waren. Ach, die hab ich schon lange nicht mehr!
Was tun? Ein Betriebssystem kaufen kostet meist so um die €100.- und das ist vielen zu teuer.
Also besorgen sich viele Hilfe von anderen, meist weniger professionellen Freunden, die sich auch auskennen, aber den Betroffenen einfach eine vom Internet heruntergeladene illegale Kopie installieren. Mit dem Zusatz "...tu lieber nicht aktualisieren, sonst funktioniert das vielleicht nicht mehr..." oder "...damit der Hersteller nicht merkt, dass du eine illegale Kopie verwendest..."
Ich könnte ganze Bücher nur über diese Problematik schreiben…

Zu wenig Datenvolumen
Was auch immer wieder vorkommt ist, dass manche nicht aktualisieren, weil dies das monatliche Datenvolumen des Internetanbieters übersteigt.
Leute, wer so wenig Datenvolumen hat, sollte sich einen anderen Internetanbieter suchen.

Was tun?
Wenn ihr einen Internetanschluss habt, haltet auch das Betriebssystem aktuell. Unbedingt.
Ich weiß, das ist lästig, und kommt immer, wenn es gerade nicht passt und dauert viel zu lange. Aber es ist einfach notwendig, denn unbehandelte Schwachstellen führen zu weniger Sicherheit, weniger Sicherheit führt zu Schäden und Datenverlust!

Nachschlag:
Ein sehr religiöser Programmierer hat selbst ein Betriebssystem geschrieben, zur Ehre Gottes und in HolyC!
http://www.templeos.org/
und
http://www.golem.de/news/templeos-goettlicher-hardcore-1508-115081.html

Liste von Betriebssystemen:
https://de.wikipedia.org/wiki/Liste_von_Betriebssystemen

Kapitel 05: Immer einen aktuellen Virenschutz verwenden

Virenschutz ist ein sehr heikles Thema. Jeder weiß, dass es Computerviren, Trojaner, Malware, Spyware, Adware usw. gibt, aber trotzdem gibt es Leute, die sich trauen, ungeschützt ins Internet zu gehen.
Ich glaube, ich brauche nicht extra zu betonen, dass das eine eher schlechte Strategie ist. So ähnlich wie ständiges Rudelbumsen mit Fremden und das ohne Gummiüberzieher und gleichzeitig sich alles in die Nase ziehen, was so an weißem Pulver unbekannter Herkunft herumliegt, während man russisches Roulette spielt…

Na, na, so schlimm ist es nun auch wieder nicht...
Zumindest für deine Daten kann es relativ schlimm ausgehen. Es gibt Viren, die alle Fotos und Dokumente auf deiner Festplatte verschlüsseln, damit du sie nicht mehr öffnen kannst. Der Autor des Virus bietet dir dann an, gegen Bezahlung die Daten wieder zu entschlüsseln. Bezahlt man nicht, bleibt einem nur mehr eine **Neuinstallation** mit totalem Datenverlust als "Option". Das ist vor allem für Leute ohne Backup ein Problem...
Ich habe schon von so genannten "Profis" gehört, die angeblich schon immer ohne Virenschutz unterwegs sind und noch niiiiie einen Virus hatten. Wers glaubt, wird selig. Zumindest keinen, den sie bemerkt hätten, denn nicht alle Viren sind so geschaffen, dass sie sofort Schaden anrichten. Manche warten viele Monate.
So lange, bis sie Befehle erhalten und aktiv werden. D.h. man kann von etwas befallen sein und auch andere gefährden ohne es zu merken. Wenn man was merkt, ist es schon zu spät...
So funktioniert beispielsweise ein **Botnet**, wie du hier https://de.wikipedia.org/wiki/Botnet nachlesen kannst.
Übrigens: Versuche im Labor haben gezeigt, dass ein durchschnittlicher PC mit Breitband-Internetverbindung bei "normaler" Benutzung in nur zehn Minuten total verseucht werden kann.

Welchen Virenschutz soll man verwenden
Das ist schwierig. Manche schwören auf Kaufware von Symantec oder Kaspersky, andere verwenden gerne Freeware von Avast, Avira oder ähnliches.
Ich habe schon so ziemlich alles ausprobiert, teils beruflich, teils privat, ich bin selber unschlüssig. Gekaufte Lösungen haben auch Schwachstellen und erkennen auch nicht alle Bedrohungen, ebenso wie gratis Virenscanner.
Ein Problem von einigen gratis Virenscannern ist die **eingebaute Werbung** für die Kauflösung des Produktes, die man dann bei jeder Gelegenheit wegklicken muss. Das ist auch lästig.

Kommerzielle Produkte will ich an dieser Stelle nicht bewerten, da gibt es jede Menge Tests im Internet zu finden und fast alle kommen auf ein anderes Ergebnis. Ich glaube es ist Geschmackssache und eine Frage des Budgets, welchen Virenscanner man sich kauft.
Wenn es um freie Lösungen geht, empfehle ich schon länger den Virenscanner **Security Essentials** http://windows.microsoft.com/de-AT/windows/security-essentials-download von Microsoft.
Denen, die jetzt sagen, dass Microsoft ja kein Virenschutz-Hersteller ist, sei folgendes gesagt: Stimmt, aber sie haben sich irgendwann einfach einen Virenschutz-Hersteller gekauft...
Microsoft bewirbt Security Essentials relativ wenig, trotzdem ist der Virenschutz in Kombination mit der eingebauten Windows Firewall und dem Tool zum Entfernen bösartiger Software ausreichend geschützt und der Vorteil liegt auf der Hand. Alles wird von Windows Update automatisch aktualisiert. Weiters ist er sehr gut ins Betriebssystem integriert und man bemerkt fast nicht, dass er da ist.

Ich verwende meinen Computer gar nicht im Internet
Ja, wenn man mit seinen Rechner nie und zwar wirklich nie ins Internet geht, und auch keine USB Sticks, Disketten, CDs, DVDs, Speicherkarten von Kameras, MP3 Player, E-Book Reader, USB Ventilatoren und Tassenwärmer, und alles was ich vergessen habe, an oder in seinen Computer steckt, nur dann ist vielleicht kein Virenschutz notwendig.
Ich spreche hier vom **absoluten Inselbetrieb**, d.h. der Rechner ist total gegen alle Netzwerke und auch von externen Datenträgern isoliert, so dass nichts hinaus und nichts hinein kommt. Dies ist aber meiner Meinung nach eher unrealistisch. Ich kenne niemanden, der so einen Rechner hat.
Ich empfehle ausdrücklich, unbedingt **IMMER einen Virenschutz** zu verwenden!

Jetzt holt sich der schon wieder ein Update, oder ein alter Virenschutz ist besser als keiner!
Angesichts der ständig wachsenden Anzahl von Bedrohungen, sollte man seinen Virenschutz mindestens täglich aktualisieren, wenn man von der Software nach einem Intervall gefragt wird. Manche prüfen sogar stündlich automatisch, ob es eine neue Version der Virensignaturen gibt.
Hat man seinen Computer länger nicht eingeschaltet, sollte man **zuerst warten, bis sich der Virenschutz aktualisiert hat**.
Eine reine Vorsichtsmaßnahme, denn wie gesagt, es gibt täglich neue Bedrohungen und manche überrollen das Internet wie eine Welle...

Löscht euren Virenschutz (lieber doch nicht)!
In einem Artikel auf Heise Security vom 30.1.2017 habe ich gelesen, dass der ehemalige Firefox Entwickler Robert O'Callahan dazu rät, Virenschutz-Software von seinem Rechner zu deinstallieren, da diese mehr Schaden anrichten würden, als sie nutzen:
https://www.heise.de/security/artikel/Ex-Firefox-Entwickler-raet-zur-De-Installation-von-AV-Software-3609009.html

Stimmt das wirklich?
Nun, ich will nicht abstreiten, dass sicherlich auch Antivirensoftware fehlerhaft sein kann und es tatsächlich Bedrohungen gibt, die genau darauf abzielen.
Aber was soll Virenschutzsoftware eigentlich können?
Diese Software soll eigentlich dem Benutzer die Gewissheit geben, einen wirksamen Schutz vor Viren und auch vor den Gefahren des Internets zu haben. Aber ist denn das überhaupt möglich?
Ich würde mal kühn behaupten, **NEIN**.
Kein Schutz kann 100% Sicherheit geben. Niemand kann euch das Denken abnehmen. Auch kein gekaufter, teurer Virenschutz kann das.
Denn euch muss schon klar sein, dass die Bedrohungen aus dem Internet (bösartige Webseiten und Werbung, Malware, Trojaner, Spam und Scam und so weiter und so fort) und mittlerweile auch schon durch verseuchte Hardware (USB Gadgets mit Rootkit, usw.) überhand nehmen. Die Bedrohungsszenarios haben sich in den letzten Jahren stark verschlimmert und dadurch werden auch die Anforderungen für Antiviren-Software immer größer. Aber je größer der Programmier-Aufwand ist, umso größer ist natürlich auch der Fehleranteil.
Ihr wisst schon, je komplizierter der Mechanismus, umso leichter kann er gestört werden.

Soll ich jetzt meinen Virenschutz deinstallieren?
Ich würde **wirklich niemanden raten, einen Virenschutz du deaktivieren oder gar zu deinstallieren**. Selbst dann nicht, wenn ihr euch wirklich gut mit Computer auskennen würdet.
Aber wer kennt sich schon wirklich gut aus? Wer ist perfekt?
Ein kleiner Schnitzer reicht schon aus, eine Fehlentscheidung und euer Rechner ist verseucht. Ein aktiver Virenschutz bietet vielleicht nicht Schutz vor allen Bedrohungen, aber zumindest vor den meisten.
Natürlich ist es wahr, dass auch Sicherheits-Software ein Risiko für einen Rechner darstellen kann, aber ein komplett ungesicherter Rechner stellt ebenso ein großes Risiko dar.

Die Virenschutz-Branche muss umdenken
Leider leben wir in einer Zeit, wo es nur so vor Gefahren wimmelt und die Anzahl der Gefahren exponentiell ansteigt. Möglicherweise müssen die Hersteller von alten Pfaden abweichen und sich neue Konzepte überlegen, um den neuen Gefahren gegenüber stehen zu können.
Aber bis dahin müssen wir uns mit dem Schutz begnügen, den wir haben. Klingt blöd, ist aber so.

Verantwortung wird gerne ausgelagert
Leider müssen auch wir selbst umdenken, denn unsere Welt ist immer stärker von Computern bzw. rechnergestützten Systemen bestimmt. Kein Haushalt ist ohne Computer, ja sogar in den Hosentaschen und Handgelenken tragen wir welche. Jedoch muss uns aber bewusst sein, dass diese Systeme auch viele Risiken bergen und wir sollten darum umso besser Bescheid wissen, was diese Systeme tun!
Ein Virenschutzprogramm zu kaufen alleine reicht nicht aus, denn es benötigt noch zusätzlich ein umfangreiches Hintergrundwissen über die drohenden Gefahren und Risiken um diesen nicht in die Falle zu gehen...

Nachschlag:
Hier kannst du verdächtige Dateien oder Webseiten gegen eine Vielzahl von Virenscannern laufen lassen, falls du bei einer Webseite oder heruntergeladenen Datei unsicher bist:
https://www.virustotal.com/

Weil ich gerade Tassenwärmer und USB Ventilatoren erwähnt habe:
http://www.pcwelt.de/news/E-Zigarette_hat_Computervirus_im_Gepaeck-Kurios-9006386.html

Kapitel 06: Wir benutzen Ghostery

Im usprünglichen Dokument habe ich die Benutzung von Ghostery vorgeschlagen. Dies muss ich nun revidieren, da sich Ghostery wegen einer Firmenübernahme zu einem neuen Geschäftsmodell hingewandt hat und **liefert nun seinerseits selbst Werbung aus**, allerdings ohne Tracker, wie man betont.

Bei einer Neuinstallation ist diese Option standardmässig akiviert, kann aber deaktiviert werden.
Nun, ein Werkzeug, welches eigentlich zur Blockierung von Werbung und deren Schattenseiten entwickelt wurde, nun aber selbst Werbung ausliefert, stellt sich meiner Meinung nach selbst ad absurdum.
Da ich diese Vorgehensweise nicht gutheisse, kann ich dieses Werkzeug nicht mehr guten Gewissens weiterempfehlen.

Ich würde sogar vorschlagen, die Browser-Erweiterung Ghostery zu entfernen. Keine Angst, die Erweiterung **uBlock Origin** reicht als Schutz vor Trackern vollständig aus, da diese auch hier blockiert werden.

Nachschlag:
https://www.golem.de/news/ghostery-rewards-werbeblocker-ghostery-liefert-werbung-aus-1807-135431.html

Noch einige passende Wikipedia Artikel:
https://de.wikipedia.org/wiki/Besucherz%C3%A4hler
https://de.wikipedia.org/wiki/Web_Analytics

Kapitel 07: Wer lesen kann, ist klar im Vorteil!

Heute geht es um ein scheinbar recht einfaches Thema, nämlich dem Lesen.
Für die meisten Menschen sind Computer ein Werkzeug, oder zumindest ein Spielzeug. Lesen tut man aber auf einem Computer weniger gerne. Schon gar nicht irgendwelche komischen Meldungen, die mit einem großen roten X oder einem ! gekennzeichnet sind.
Es handelt sich dabei oft um **wichtige Meldungen des Betriebssystems**, wenn es Probleme gibt, oder der Benutzer um eine Entscheidung gefragt wird.
Oftmals werden alle Warnversuche des Rechners in den Wind geschlagen und einfach ignoriert, weil sie halt nerven.
Dies kann im schlimmsten Fall dazu führen, dass man den PC komplett neu installieren muss und alle deine Daten weg sind.

Ich hab keine Ahnung, ich habe einfach auf "OK" gedrückt!
Natürlich wäre es auch super, wenn man verstehen würde, was der Blechtrottel eigentlich will, oder?
Denn das OK drücken bedeutet, dass man als Benutzer mit der vom Computer beschriebenen Vorgangsweise einverstanden ist.
Es ist mir vollkommen klar, dass nicht jeder das technische Verständnis hat, um alle Meldungen restlos verstehen zu können.
Auch Profis wissen nicht immer, was bestimmte Meldungen bedeuten. Aber man könnte vielleicht **das Internet befragen**!
Das geht aber nur, wenn man auch die Frage kennt...
Also, wenn ihr vom Computer Dinge gefragt werdet, die euch ratlos machen, dann merkt euch bitte den **Wortlaut der Meldung**.
Einfacher geht es, wenn man einen Screenshot der Meldung macht. Mit der **Tastenkombination "Alt - Druck"** speichert der Computer den Inhalt des aktuellen Fensters als Bild. Danach musst du nur mehr das Bild in ein Textdokument oder eine E-Mail einfügen (**Tastenkombination "Strg - v"**).
So musst du dir nichts merken und man kann im Nachhinein Rückschlüsse ziehen, was die Ursache für ein gewisses Verhalten war, bzw. warum etwas schief gegangen ist.

Also, ich hab das sicher nicht installiert
Ein sehr häufiges Problem ist das Installieren von unerwünschten Programmen. Das hört sich jetzt vielleicht komisch an, denn wenn ich mir ein Programm herunterlade, installiere ich ja nur dieses eine Programm, oder?
Leider nein, denn viele Programme versuchen **lustige Toolbars**

https://de.wikipedia.org/wiki/Symbolleiste auf deinem Rechner zu installieren, **verstellen die Suchseite** deines Browsers, oder installieren **Testversionen von anderen Programmen**, die dann nach einiger Zeit recht häufig vermelden, dass sie gerne gekauft werden wollen.
Auch unschön ist, wenn eine so genannte **Scareware** mit installiert wird. Wie der Name sagt, sollen solche Programme den Benutzer überzeugen, dass sein Rechner unsicher und potentiell gefährdet ist und gegen Bezahlung wären all diese Lücken ganz leicht zu schließen.
Mein Ratschlag wäre von einer "weiter - weiter - weiter - weiter - fertig" Installation abzusehen und wirklich bei jedem Installationsschritt **genau zu lesen, was da steht**. Denn mittlerweile muss der Benutzer einer Installation von zusätzlichen Programmen explizit zustimmen. **Es ist wie mit Vampiren, man muss sie selbst herein bitten!** Ist ein PC mit zig Toolbars und unseriösen "Sicherheitsprogrammen" verunziert, ist man meist selbst schuld.
Oft ist gratis Software halt doch nicht ganz gratis. **Man bezahlt mit seinen Daten**, indem man Werbung angezeigt bekommt, oder man wird letztendlich vielleicht sogar erpresst.
Dieser Problematik werde ich noch ein eigenes Kapitel widmen.

Wer lesen kann ist klar im Vorteil
Ich kann es leider nicht oft genug sagen. Bitte immer lesen was da steht. Auch wenn du es nicht verstehst, bitte unbedingt speichern und jemanden fragen, der wirklich was von Computern versteht. Am besten sofort.
Es ist echt total schwer, auch für Profis, die Lösung für Probleme herauszufinden, wenn die Ursache nicht bekannt ist.
Das nicht lesen von Warnungen, Hinweisen und Fehlermeldungen des Computers ist zu vergleichen mit dem wegschmeißen von Zahlungserinnerungen. Man darf sich halt dann nicht wundern, wenn eines Tages der Exekutor kommt und auf deine Wertgegenstände den Kuckuck klebt…

UTFSF
Fortgeschrittene Benutzer kennen das schon und sind schon einen Schritt weiter. Sie suchen sich im Internet selbst Hilfe, sind vielleicht sogar bei diversen Foren und Netzwerken registriert und stellen dort ihre Fragen.
Leider, wurden die meisten Fragen schon einmal beantwortet und die Verwendung der Suchfunktion hätte das Problem viel schneller gelöst als die erneute Fragestellung, das Aufregen über die mangelnde Hilfsbereitschaft anderer Benutzer, das Hinweisen auf die Suchfunktion und schließlich die Beendigung des Beitrages durch den Moderator…

LMGTFY

Bitte nervt keine Spezialisten mit trivialen Fragen, wie z.B. "Wie mache ich einen Text fett".
So etwas kann man recht einfach herausfinden in dem man die Suchmaschine seines Vertrauens fragt.
Häufig bekommt man von bösen Spezialisten Antworten dieser Art zugeschickt:
http://lmgtfy.com/?q=wie+mache+ich+einen+Text+fett

Nachschlag:

https://de.wikipedia.org/wiki/Screenshot#Erstellung
https://de.wikipedia.org/wiki/Schadprogramm
https://de.wiktionary.org/wiki/UTFSF

Kapitel 08: Vorsicht beim Installieren von heruntergeladenen Programmen

Wie im letzten Kapitel erwähnt, geht es heute um die Installation von Programmen, die man aus dem Internet heruntergeladen hat. Oft spricht man mit Freunden oder Bekannten und zufällig kommt es zum Thema "was für ein Programm verwendest du eigentlich für [Sachen, die du gerne mit dem Computer machen würdest]"?
Die Antwort laute dann "Ja, ich verwende da [voll superes Programm was das alles kann und noch viel mehr]"!

Ja, so stellt sich der kleine Johannes die große Welt vor und befragt mal die Suchmaschine seines Vertrauens.
Siehe da, gleich das erste Ergebnis ein Treffer! Juhu, geh auf die Seite [Lustige Downloadseite] und lade das herunter. So, Werbung, Werbung, Werbung, noch mal "Weiter zum Downloadlink", wieder Werbung, Werbung, Werbung, jetzt nur mehr fünf Sekunden bis zum Download, ja, jetzt geht endlich der Download auf und das Glumpert wird endlich heruntergeladen.
Nun brauchst du nur mehr den Installer ausführen und nach gefühlten 100 Seiten Blabla und 100 mal "Weiter" klicken ist das Programm installiert. Und ein neuer voll toller Browser. Und eine neue Suchmaschine. Sicherheitshalber für alle Browser, die du installiert hast. Und eine Testversion eines Programmes, welches deinen Rechner garantiert schneller macht. Und die Testversion einer brandneuen Internet Security Suite, die ganz sicher alle deine Daten weitergibt. Und so weiter und so fort.

Drive-by-Installation
Du meinst das wäre übertrieben? Ich habe schon oft selbst Programminstallationen durchgeführt, die genau das beschriebene einfach mitinstallieren wollten, wenn ich es nicht extra abgewählt hätte. Diese Programme werden **PUP (Potentiell unerwünschte Programme)** genannt und sind mittlerweile eine große Gefahr für Nicht-Profis, wobei es auch Profis ab und zu gelingt, sowas unabsichtlich zu installieren :(

Bitte deaktivieren sie den Virenschutz während der Installation
Die Höhe sind Installationsprogramme, die gleich vorweg warnen, dass man den Virenschutz kurz deaktivieren soll, damit die Installation "erfolgreich" ist.
Dazu kann ich nur sagen: **BLOSS NICHT!**
Ein halbwegs vernünftiger Virenschutz würde nämlich erkennen, wenn gewisse Dinge auf deinem Rechner manipuliert werden, z.B. Hosts Datei, DNS Server, Standard Browser, Suchmaschinen, Proxyserver usw. Der Virenscanner würde bei der Installation solcher Programme permanent Fehlermeldungen bringen und den Benutzer misstrauisch machen...

Übrigens würde ich mir generell von **NIEMANDEN einreden lassen, Virenschutz, Firewall, Malwareschutz und dgl. zu deaktivieren**, auch nicht kurz. Finger weg von Programmen, die das wollen und von "Freunden" die einem das einreden wollen!

Wer macht denn sowas?
Gratis Software ist nicht immer gratis. Irgendwie wollen die Download-Seiten Geld verdienen, und mit der Methode ist es ganz leicht, viel Geld zu verdienen. Wie das geht, erkläre ich im Nachschlag, leider wird es da etwas technisch und es gibt jede Menge weiterführende Informationen ;)
Sogar früher recht seriöse Download-Portale wie Cnet, oder Download(dot)com sind schon zu dieser Praktik übergegangen. Lädt man sich dort etwas herunter, kommen auch viele unerwünschte Programme mit. In diesem Artikel http://www.howtogeek.com/198622/heres-what-happens-when-you-install-the-top-10-download.com-apps/ auf How to Geek wird beschrieben, was alles passiert, wenn man sich die Top 10 Downloads bei Download(dot)com herunterlädt und installiert…

Wo soll ich dann was herunterladen?
Zum Installieren von den am häufigsten benötigten Programmen empfehle ich **Ninite** https://ninite.com/
Dieses Portal bietet eine Reihe von **oft benötigten Freeware-Programmen** an. Man hakt einfach an, was man braucht und anschließend kann man sich ein sehr kleines Installationspaket herunterladen. Dieses Paket beinhaltet aber nicht die Programme selbst, sondern lädt immer die neueste Version aus dem Internet herunter und installiert sie danach. Dieser Dienst ist für private Benutzer kostenlos.
Natürlich gibt es bei Ninite auch nicht jedes beliebige Programm und man muss natürlich auch hin und wieder bloß so was herunterladen.
Dafür gibt es zwei recht gute Anlaufstellen für Freeware und Open Source. Es sind die Portale **Fosshub** http://www.fosshub.com/ und **SourceForge** https://sourceforge.net/ wo sehr viele Hersteller ihre Programme zum Download anbieten.

Weiters empfehle ich die gewünschte Software einfach **beim Hersteller direkt herunterzuladen**. Eine kleine Suche mit der Suchmaschine deines Vertrauens verrät dir, wer der Hersteller des gewünschten Programmes ist und wie die Webseite lautet. Das erspart meistens viel Zeit und Ärger.
Eine Suche im Internet nach "Programm was dies und jenes kann herunterladen", die ja durchaus legitim ist, führt (meist bei den ersten paar Treffern) übrigens auch fast immer zu dubiosen Seiten.
Leider ist das Internet so dermaßen mit schlitzohrigen Downloadseiten übersät, dass die Suche nach guten Programmen einer Sisyphus-Arbeit gleicht. Man bekommt **erst im Laufe der Jahre** einen guten Überblick, was man probieren kann und was nicht. **Oft mit leidlichen Erfahrungen**.
Wenn du also nach Software suchst, frage einen Profi und nicht jemanden, der selbst

alle 3 Monate seinen Rechner wegen Viren und sonstigen Blödsinn neu aufsetzten muss…

Nachschlag:
Hier sind nun die oben versprochenen Informationen! (es wurde viel mehr als ich gedacht habe…)

Die **Hosts Datei** wird verwendet um auf einem Computer Hostnamen (Name von Rechnern im Netzwerk) in für die Netzwerkkarte verständliche IP Adressen zu übersetzten. Normalerweise werden Hostnamen von einem DNS Server übersetzt, jedoch wird der Inhalt der Hosts Datei bei der Namensauflösung bevorzugt. Dieses Verhalten wird oft von bösartiger Software verwendet, um den Benutzer auf andere Server im Internet umzuleiten. Man kann auf diese Weise einen Rechner statt auf www.google.at auf eine Seite umleiten, die der Google Seite ähnlich ist, aber jemanden anderen gehört. Dort werden dann Benutzerdaten abgegriffen und verkauft, und mit Werbung Geld verdient.
Dies funktioniert auch natürlich recht gut mit eBanking-Seiten, wobei man es dort auf deine Login-Daten und TANs abgesehen hat.
Weitere Informationen zur Hosts Datei: https://de.wikipedia.org/wiki/Hosts-Datei

DNS Server werden genau wie die Hosts Datei dazu verwendet, um Namensauflösung zu machen, wobei ein DNS Server im Netzwerk befragt wird. Dieser DNS Server wird meistens von deinem Internet Betreiber zur Verfügung gestellt.
Bösartige Software kann nun die DNS Server umstellen und alle deine Anfragen über Namensauflösung (einige hundert pro Stunde) wandern nun zu einem DNS Server, über den Betrüger die Gewalt haben und dort schalten und walten, wie es ihnen passt. Außerdem kann man damit Geld verdienen, wenn man Werbung anzeigt, wenn du dich z.B. in der Adressleiste des Browsers vertippst. Ansonsten sind die Auswirkungen gleich wie bei der Hosts Datei.
Weitere Informationen zu DNS: https://de.wikipedia.org/wiki/DomainNameSystem

Fremde Browser werden auch oft mitinstalliert. Ich habe das einmal bei einem Freund gesehen. Ich habe meinen Augen nicht getraut, denn so einen komischen Browser habe ich noch nie gesehen, und den Namen noch nie gehört. Dieses Ding hat nicht einmal versucht, einem bekannten Browser ähnlich zu sehen, doch Nicht-Nerds fällt so etwas scheinbar nicht auf...
Wenn du so ein Ding mal auf deinem Rechner hast, ist es aus mit der Sicherheit im Internet. Alles was du suchst, eingibst (natürlich auch Passwörter) und siehst, wird ziemlich sicher aufgezeichnet und die gewonnenen Daten verkauft. Die Werbung von den Seiten die du besuchst wird ausgetauscht durch Werbung des Betreibers des fremden Browsers. Wenn man einen fremden Browser auf seinem Rechner hat, kann man sich echt gratulieren…

Suchmaschinen Rochade ist auch recht beliebt. Dabei wird bei allen installierten Browsern eine neue Suchmaschine eingestellt. Dies geschieht um Benutzerdaten abzugreifen und Werbung zu platzieren. Natürlich ist es auch möglich, dass einem gefälschte Suchergebnisse präsentiert werden, die zu weiteren dubiosen Seiten mit noch mehr Werbung führen. Dies wird oft mit kleinen Programmen erreicht, die sobald du wieder auf deine gewöhnte Suchseite zurückstellst, die falsche Suchmaschine erneut einstellt. Diese Programme werden natürlich beim Systemstart mit gestartet um sicher zu gehen, dass du immer die gefälschte Suchseite verwenden musst. Diese Dinger sind echt sehr schwer wegzukriegen…

Proxyserver werden auch recht häufig eingestellt. Eigentlich werden heute Proxyserver (im Privatbereich) fast nicht mehr verwendet. Früher dienten sie dazu, um oft besuchte Internetseiten quasi zwischen zu speichern um dadurch den Internetverkehr zu verringern. Fast jeder Internet-Provider bot diesen Dienst an. Früher waren nämlich die Bandbreiten noch viel geringer und das Internet dementsprechend langsam... Heute werden Proxys meistens in Firmen verwendet, damit die Benutzer nicht direkt ins Internet kommen und nicht jede beliebige Seite besucht werden kann. Die Verringerung der Netzwerklast ist nun eher zweitrangig. Wird dir ein Proxyserver untergejubelt, kann auch dein gesamtes Surfverhalten und alle Eingaben, die du im Browser machst, mitprotokolliert werden. Werbung des Proxy-Betreibers natürlich inklusive.

Weitere Informationen zu Proxyserver: https://de.wikipedia.org/wiki/Proxy_%28Rechnernetz%29

Kapitel 09: E-Mail

So ziemlich alle, die einen Computer haben, kennen und verwenden E-Mail. Dies ist zwar heutzutage nicht mehr die häufigste Kommunikationsform im Internet, wird aber immer noch gerne für unschöne Dinge missbraucht, vor denen man gewappnet sein sollte.

Werbung, meist unerwünscht, auch Spam genannt
Jeder kennt Spam, denn **bis zu 80% der weltweit versandten E-Mails** sind Spam. Eine Mail zu versenden kostet quasi nichts, riesige Herden von infizierten Zombie PCs, die unter fremder Kontrolle stehen, verschicken täglich abertausende Mails. Wenn nur ein Promille der Adressaten etwas kauft oder auf den Link in der Mail klickt, ist die Rechnung schon aufgegangen. Beworben werden häufig Medikamente aus zweifelhafter Herkunft (meist Potenz und Haarwuchsmittel), billige Luxuswaren, ebenfalls aus zweifelhafter Herkunft, Versicherungen, Aktienpakete, und vieles mehr.
Man sollte **niemals irgendwelche Anhänge in Spams öffnen**, so harmlos sie auch aussehen. Auch auf Internet-Links zu klicken ist keine gute Idee.
Auch sollte man nie die beworbenen Produkte kaufen, egal welcher Art sie sind.

Vorschussbetrug, auch Scam genannt
Von rührenden Geschichten bis hin zu offensichtlichem Betrug, es ist immer die gleiche Masche: Jemand (angeblich Anwalt oder ähnliches) im Ausland (meist in Afrika) sitzt auf einem Riesenhaufen Geld, **NUR DU** kannst helfen, es außer Landes zu schaffen und mit einen Vorschuss von sagen wir mal €100 um gewisse Behörden zu schmieren, bist du dabei und kannst dabei einen Haufen Geld verdienen.
Leider tauchen dann immer wieder Probleme auf, du wirst hingehalten und vertröstet. Dann wirst du gebeten, einen weiteren Vorschuss zu leisten, und so weiter und so fort.
Es hat schon Fälle gegeben, wo eigentlich ganz vernünftige Menschen **tausende Euro** bezahlt haben, bevor sie den Fall der Polizei übergeben haben, die meistens auch nicht viel tun kann. Abgesehen davon, dass man (wenn die Geschichte wahr wäre) selbst zum Betrüger wurde.
Die Versender von Scams sind meistens **arme Menschen ohne Arbeit**, die sich ihren Lebensunterhalt auf diese Weise verdienen, aber auch raffinierte Trickbetrüger wenden solche Mittel an, um Leuten Geld aus der Tasche zu ziehen.
Es sollte eigentlich jedem klar sein, dass solche Geschichten nicht wahr sein können, aber bei der Aussicht auf viel Geld schalten manche Menschen leider ihr Hirn aus...

Phishing Mails
Du bekommst ein Mail von einer Bank und wirst gebeten z.B. deine Kontodaten zu überprüfen.
Oder die vermeintliche Bank meldet einen Datenverlust und du sollst dich einloggen und sehen, ob eh alles passt.
Ein Internet Link führt dich direkt zur Seite der Bank. Oder ist es nur eine Seite, die so aussieht wie die deiner Bank? Wer dort seine Daten (inklusive Tan natürlich) eingibt, verliert gleich einmal die Kontrolle über sein Konto.
Das alles funktioniert natürlich auch für andere Bezahldienste wie Paypal und auch Internet Dienste wie Amazon, Ebay, usw. wurden schon gephisht.

Schicke diese Nachricht an alle deine Freunde
Kettenbriefe, ich hasse sie. Sie sind das Arschgeschwür des Internets.
Bill Gates spendet für jedes weitergeleitete Mail einen Dollar für krebskranke Kinder. Natürlich! Freilich!
Schicke dieses Mail an sieben Freunde oder du wirst sieben Jahre schlechten Sex haben. Sowieso! Eh klar!
Ganz ehrlich, wer solche Dinge glaubt, dem kann ich nur **Credulitas 10 Dragees** https://krawutzi.wordpress.com/2015/09/24/credulitas-10/ empfehlen.

Ein tragisches Beispiel gab es übrigens vor einigen Jahren, wo ein Ketten-Mail mit den Daten eines jungen Mannes mit Leukämie im Internet unterwegs war. Der oder die Versender erzählten von einer tragischen Geschichte und dass ein passender Knochenmarkspender gesucht wurde. Im Kettenbrief war Name, Adresse und Telefonnummer des jungen Mannes, der fortan Tag und Nacht Besuch und Anrufe von Menschen bekam, die unbedingt Knochenmark spenden wollten.
Nur, dass das alles nicht wahr war und der junge Mann seinen Namen ändern und wegziehen musste.

Ein Kettenbrief, der über Jahre hinweg immer wieder auftaucht ist, dass in Schulen nicht mehr mit "Grüß Gott" gegrüßt werden darf, und zwar um Rücksicht auf die anderen Religionen von Migrantenkindern zu nehmen.
Dieser Brief existierte in verschiedenen Varianten, mal war es das Kreuz in den Klassen, manchmal war es in einem anderen Bundesland. Natürlich stimmt das nicht, rechtsradikale Gruppen machen sowas ganz gerne um die Menschen aufzuhetzen.

Es mögen vielleicht ein paar Geschichten aus Kettenbriefen stimmen, aber in der Mehrheit sind die Informationen einfach falsch und werden auch **Hoax** genannt. Im Nachschlag kommt ein Link, wo du nachsehen kannst ob solche Sachen richtig sind, oder nicht.

Übrigens: Der sicherste Weg, keine Kettenmails mehr zu erhalten, ist dem Absender mit Kündigung der Freundschaft zu drohen. Das klingt zwar recht drastisch, hat aber bei mir geholfen.
Echte Freunde müllen einem nicht den Posteingang voll.

Wie kommen die eigentlich zu meiner E-Mail Adresse?
Da gibt es einige Möglichkeiten.
Einige probieren ganz einfach mit Namensdatenbanken und verschicken dann Millionen Mails nach diesem Schema: **vorname.nachname@einefirma.com**.
In der Nachricht befindet sich ein Link zu einer kleinen, meist unsichtbaren Bilddatei, die auf einem Webserver liegt. Die ist mit einem eindeutigen Namen versehen, der der Mail-Adresse zugeordnet ist. Wenn du die Nachricht öffnest, wird das auf dem Webserver mitprotokolliert und man hat den Beweis, dass die Mail-Adresse echt ist. Dies ist der Grund, warum ein Mail-Programm warnt, wenn Teile der Nachricht auf einem Webserver liegen.
Andere durchsuchen mit sogenannten **Harvestern** (Ein automatisches Script, das Links auf Webseiten verfolgt) das ganze Internet nach dem @-Zeichen, um Adressen zu "ernten".
Wenn du einen Trojaner auf deinem Rechner hast, werden natürlich auch alle deine Kontakte verwendet um an gültige Mail-Adressen zu gelangen, weiters wird dein Rechner, wie oben beschrieben, als Mail versendendes Zombie verwendet. Weiters sollte man auf keine Links klicken, die in Spam-Mails sind, dies dient auch meist dem Spammer und die Echtheit einer Adresse bestätigt zu bekommen.

Die so gewonnenen Mail-Adressen werden dann in den dunklen Ecken des Internets verkauft und dienen dann für zielgerichtete Angriffe, bzw. für Werbung, da man mit Namen, Mail-Adressen, und dgl. weitere Daten verknüpfen (ich sage nur Facebook) kann, die zu noch mehr Daten führen, usw.

Sie müssen sich registrieren, um den Download zu starten
Manchmal ist es notwendig, sich mit einer Mail-Adresse zu registrieren, um was herunterladen zu können. Oder du musst deine Mail-Adresse angeben, nur weil du in einem Forum eine Frage stellen willst. Wenn du das Gefühl hast, nach dem Download oder wenn deine Frage beantwortet wurde, nie mehr wieder zurück zu kehren, solltest du vielleicht nicht deine echte Mail-Adresse verwenden. Es besteht die Gefahr, ab sofort Werbung zu bekommen, weil die ja deine Mail-Adresse haben.

Ich verwende für diesen Fall **http://mailinator.com/**. **Mailinator** ist quasi eine Instant-Wegwerf-Mail-Adresse, mit der du Mails empfangen kannst, aber nicht musst. Ich nehme bei solchen Registrierungen z.B. seppi@mailinator.com, danach gehe ich auf die Seite und sehe in das Postfach von Seppi. Ich kann mir die Mail weiterleiten, wenn ich möchte, oder einfach den Registrierungscode heraus kopieren, oder die Anmeldung mit dem Link in der Mail abschließen.

Danach interessiert mich das Ganze nicht mehr.
Jede weitere Mail, ob Werbung oder nicht, kommt nicht in mein richtiges Postfach

Was ist eigentlich BCC
Wenn du eine Nachricht an mehrere Personen gleichzeitig verschicken willst, diese sich aber nicht kennen, solltest du die Adressen nicht im "An:" Feld eingeben sondern im "BCC:" Feld. BCC bedeutet Blind Carbon Copy, was so viel heißt wie, Durchschlag an alle, aber ohne Sicht auf die Adressen.
Dadurch verhinderst du, dass jemand gültige Mail-Adressen sammeln kann. Auch wenn du das niemanden zutraust, aber Mail-Konten werden öfter gehackt, als man denkt. Nämlich mit Phishing Mails…

Weiterleiten von Mails
Bedenke folgendes, wenn du ein Mail weiterleitest: Es ist so, als ob du einen Brief samt Umschlag in einen neuen Brief steckst und dann diesen verschickst.
Der neue Brief enthält nicht nur deine Adresse, sondern auch die auf dem anderen Brief, den du hineingesteckt hast. Dies ist in den meisten Mail-Programmen nicht ersichtlich, kann aber angezeigt werden.
Jetzt komme ich wieder zurück zum Kettenbrief: Ich habe vor einigen Jahren ca. **500 Mail-Adressen** aus einem Kettenmail extrahiert, alle gültig. Die sind oft Monate oder Jahre unterwegs und werden von allen immer weitergeleitet. Auch das wird von den bösen Buben verwendet, um Mail-Adressen zu gewinnen.
Wenn du das verhindern willst, kopiere nur den Inhalt der Nachricht und füge ihn in eine neue Nachricht ein.

Mir doch egal.
Viele Verbrechen beginnen mit Spams, Scams und Hoaxes. Solltest du solche Mails erhalten, lösche sie einfach.
Auf keinen Fall klicke auf irgendwelche Links. Schicke keinen Spam oder Hoax weiter. Glaube nichts, was dir irgendwer mit Mail sendet.
Du unterstützt dadurch nur die bösen Buben des Internets!

Nachschlag:
https://de.wikipedia.org/wiki/Spam
https://de.wikipedia.org/wiki/Vorschussbetrug
https://de.wikipedia.org/wiki/Phishing

Anti Kettenbrief:
http://www.fun-mix.de/funtexte/kettenbrief2.html

Hoax Info:
http://hoax-info.tubit.tu-berlin.de/

Scambaiter schlagen zurück! Siehe "The Trophy Room" auf der Seite
http://www.419eater.com/

Kapitel 10: Facebook und Co

Ein recht großer Prozentsatz aller Internetbenutzer ist auf Facebook, oder ähnlichen sozialen Netzen vertreten. Manche etwas mehr, manche weniger. Allerdings bin ich mir nicht ganz sicher, ob auch alle wissen, was das für sie bedeutet. Datenschützer auf der ganzen Welt schlagen die Hände zusammen, wenn sie die Datenschutzerklärung von Facebook lesen, und das nicht ohne Grund.
Ganz ehrlich, hast du dir das schon einmal komplett durchgelesen?
https://www.facebook.com/about/privacy/
OK, nächste Frage, hast du auch wirklich verstanden, was das eigentlich bedeutet?

Ich will ehrlich sein, es hat sich schon gebessert. Die oben verlinkte Datenschutzerklärung ist sogar recht kurz und leicht verständlich. Vor einiger Zeit war es zu lesen, wie ein kleingedruckter, schmieriger hundertseitiger Knebelvertrag, der wahrscheinlich sogar für die meisten Juristen schlecht verständlich und auf mannigfaltigste Weise interpretierbar war.

Was machst du gerade?
Was ich recht bedenklich finde ist der soziale Striptease, den manche da hinlegen. Niemand wäre vor 20 Jahren auf die Idee gekommen, die Fotos vom Buffet des Urlaubs-Ghetto sofort an alle Freunde und Verwandte zu schicken. Oder die Fotos seiner Kinder. Oder Fotos von einer Party, auf der man sich, sagen wir mal daneben, benommen hat. Niemand hätte das, was er sich gerade denkt oder fühlt sofort auf der ganzen Welt verlautbaren lassen.
Mir ist klar, dass wir in modernen und interessanten Zeiten leben, jedoch ist es so, dass uns soziale Medien dazu verleiten, mehr von uns Preis zu geben, als uns eigentlich lieb ist.
Es gibt **keine Geheimnisse mehr** und keine Grenzen. Manche Menschen sind sogar auf Schritt und Tritt verfolgbar, da ihre Facebook-App auf dem Smartphone ständig die GPS Koordinaten im Internet veröffentlicht.
Der gläserne Mensch ist keine Utopie mehr.

Alles für die Werbung
Facebook und seine Partner verdienen Geld mit Werbung. Genauer gesagt, mit zielgerichteter Werbung. Aufgrund der Daten, die Facebook zur Verfügung hat, kann ziemlich genau vorhergesagt werden, was du am wahrscheinlichsten kaufen würdest. Das steigert den Werbewert erheblich und deshalb verdienen sich solche Plattformen eine goldene Nase.

Pakt mit dem Teufel
Mit der Teilnahme bei sozialen Medien bestätigst du, dass alle Daten, die du eingibst, alle Bilder und Videos, die du hochlädst zwar grundsätzlich dir gehören, jedoch der Betreiber des sozialen Mediums das Nutzungsrecht der Daten hat.
D.h. deine Daten werden verkauft und jede Menge Geld wird damit verdient. Unglaublich viel Geld.
Facebook und Co. bieten zwar **gratis eine Kommunikationsplattform** und ein paar **primitive Spiele** für dich und deine Freunde, verdienen damit aber wesentlich mehr Geld, als zum Betreiben der Plattform und etwas Gewinn notwendig wäre. Man sehe sich den Börsenwert solcher Unternehmen an und staune. Facebook ist angeblich **mehr als 200 Milliarden Euro** wert. Tendenz steigend.
Und ihr beschenkt diese Unternehmen reichlich mit all euren Daten!

Es ist eigentlich unglaublich, dass eine Firma mehr über dich weiß, als du selbst. Theoretisch kann Facebook sogar vorhersagen, wann du dich von deinem Partner/deiner Partnerin trennen wirst und könnte dir gleich passende Wohnungsinserate zeigen und einen Anwalt in deiner Nähe empfehlen.
Besser als jeder Hausarzt könnte dir dein soziales Netz Medikamente verordnen.
Man könnte dir Werbung für einen Kurz-Urlaub in Steinhof https://de.wikipedia.org/wiki/Steinhof_%28Wien%29 anzeigen, aufgrund der Einträge und Fotos vom letzten Wochenende.
Das würdest du aber nicht so lustig finden und daher lässt man das lieber. Man schlachtet ja nicht die Gans, die goldenen Eier legt…

Weiters ist unklar, wer noch aller mitliest...
Eine Weitergabe der Daten an Geheimdienste oder Polizei ist nicht nur im konkreten Anlassfall (ein Verbrechen) möglich, was ja normal wäre. Angeblich wird der gesamte Datenstrom, der von Facebook und auch anderen Internet-Riesen weltweit erzeugt wird, direkt zur Analyse an Geheimdienste gesendet. Was die dann mit den Daten machen und wie lange sie diese speichern ist weitgehend unbekannt.
Diese Praktik ist seit einigen Jahren sogar öffentlich bekannt und ging durch alle Medien. Der Aufschrei war groß.
Doch zu groß ist die Abhängigkeit der Benutzer. Zu groß die Bequemlichkeit.
Und so dauerte es nicht lange, bis alles wieder gut war und keiner mehr davon redete. Soziale Medien verzeichneten nur einen kurzen Einbruch bei Neuregistrierungen und einige wenige gingen endgültig.
Mittlerweile ist wieder **alles beim Alten**.

Auch einschneidende Geschehnisse der letzten Jahre tragen dazu bei, dass immer mehr Menschen der Meinung sind, dass wir eigentlich noch viel mehr überwacht werden müssen. Dies dient ja schließlich nur dem Schutz vor Terroranschlägen, oder?
Aber ganz ehrlich, welche Terroristen planen ihre Anschläge ausschließlich per Internet, wo jedes Datenpaket genau verfolgt werden kann und wird? Und das vielleicht noch im Klartext? Na klar.

Ich habe ja nichts zu verbergen!
Wenn ich jemanden mit Datenschutz und Privatsphäre komme, höre ich recht häufig "ich habe ja nichts zu verbergen". Das interessante ist, niemand hat was zu verbergen, solange ihm nichts passiert.
Spätestens, wenn man einmal einen Nachteil dadurch hat, fragt man sich, wie sowas nur passieren konnte.
Wer seine Datenschutzeinstellung nicht richtig trifft, postet für die ganze Welt sichtbar.
Es gab schon etliche Fälle, wo Angestellte gekündigt wurden, bzw. Bewerber auf Arbeitssuche aufgrund ihrer Postings abgelehnt wurden.
Dies ist zwar nicht so ganz legal, jedoch ist diese Praktik weithin bekannt und wird auch angewendet.
Es ist halt nicht dasselbe, wenn ich einem Freund erzähle, dass mein Chef ein Trottel ist, oder ob ich das auf Facebook, für das ganze Internet sichtbar, poste.
Auch vergessen manche gerne, wer eigentlich aller in der Freundesliste ist und mitlesen kann.
Aber bei 500 "Freunden" verliert man schon mal den Überblick…

Was, du bist gar nicht bei Facebook?
Nein, ich bin nicht bei Facebook. Meine Identität im Internet ist verschleiert. In meinen Internetauftritten befindet sich keinerlei Information über meine Person. Ich habe **ein Recht auf Privatsphäre** und nutze es auch.
Nicht alles was ich esse, muss öffentlich dokumentiert werden, nicht alles was ich denke müssen sofort alle wissen und zu guter Letzt: Niemanden geht es etwas an, wer meine Freunde sind.
Ich möchte auch nicht, dass Freunde in sozialen Netzwerken über mich schreiben oder Bilder von mir posten.
Dies stößt zwar meistens auf Unverständnis, jedoch in Zeiten der Gesichtserkennung könnte man ganz leicht erkannt und getaggt werden. Dann ist es aus mit meiner Privatsphäre und das **ohne dass ich selbst Mitglied bin**!
Mich hat schon vor Jahren stutzig gemacht, dass mir Facebook E-Mails geschickt hat, mit Leuten, die ich (möglicherweise) kenne und auch auf Facebook sind. Ich möge nur Mitglied werden und kann dann mit allen kommunizieren!

Das Problem war, ich kannte wirklich alle.
Möglich macht das die Facebook-App auf dem Handy, die praktischerweise auch gleich deine ganzen Kontakte und alle E-Mails hoch lädt.

Cybermobbing und Cyberbullying
Mobbing gab es immer schon. Früher sagte man halt anders dazu.
Wenn man früher von einem Mitschüler/Mitarbeiter gemobbt wurde, wusste das im schlechtesten Fall die ganze Schule/Arbeit.
Wenn man heute von einem Mitschüler/Mitarbeiter gemobbt wird, kann dies weltweit von JEDEM mitverfolgt werden.
Manchmal sogar per Video.
Die Schmach und der Druck für die Betroffenen ist dadurch noch viel größer und hat schon manche in den Selbstmord getrieben.

Na gut, und wenn ich aussteige?
Ja, das ist eine gute Frage. Was passiert dann mit meinen Daten? Daten kann man nicht angreifen, man kann sie dir nicht mehr zurückgeben. Man könnte sie löschen, aber wie willst du wissen, ob jemand deine Daten tatsächlich löscht, nur weil er das behauptet? Es gibt keine Beweise, oder denkst du, dass Facebook dich in sein weltweit verteiltes unglaublich riesiges, Datencenter sehen lässt?
Weiters wird natürlich nur das gelöscht, was keine Konversation mit jemand anderen war. Hmmm. Eigentlich ist aber fast alles auf sozialen Medien eine Konversation mit anderen...
Auf jeden Fall kannst du es getrost vergessen, Präsidentschaftskandidat zu werden, denn bei den Partyfotos von vor 3 Jahren, also wirklich!

Was kann ich also tun?
Grundsätzlich kann man im Internet alles von sich geben, was man auch mittels Flugblatt in der Öffentlichkeit an Fremde verteilen würde.
Das Internet ist öffentlich und alles was du schreibst, kann relativ sicher weltweit gelesen werden.
Bzw. es gibt welche, die das können, egal was du einstellst.
Denke über folgendes Beispiel nach:
Wenn ich aus dem Fenster zehnmal "Ich bin so dumm und weiß nicht warum!" schreie, dann werden das vielleicht ein paar Passanten und meine Nachbarn hören. In einigen Tagen kümmert das keinen Menschen mehr.
Wenn ich das selbe im Internet mache, dann kann das theoretisch weltweit von jedem gelesen werden.
Der Unterschied jedoch ist, dass es recht wahrscheinlich nie mehr verschwindet und in zehn Jahren immer noch gelesen werden kann.

Bitte respektiere auch die Privatsphäre von Menschen die nicht in sozialen Netzwerken sind.
Und bedenke, nicht alle Menschen interessieren sich für deinen Stuhlgang oder deine abartigen Sexualpraktiken ;)

Nachschlag:
https://de.wikipedia.org/wiki/Kritik_an_Facebook
https://de.wikipedia.org/wiki/Globale_%C3%9Cberwachungs-_und_Spionageaff%C3%A4re
https://de.wikipedia.org/wiki/Cyber-Mobbing
http://www.zeit.de/digital/datenschutz/2010-02/facebook-sammelt-emailadressen/komplettansicht

Kapitel 11: Der Herunter-Laden

Ganz ehrlich, wer hat eine illegale Kopie eines Programmes oder Spieles auf seinem Rechner?
Niemand? Natürlich nicht, alles ganz ehrliche Menschen hier...
Viele wissen vielleicht gar nicht, dass sie was illegales aus dem Internet auf ihrem Rechner haben, weil "Freunde", die sich halt mit so Computer ein wenig auskennen, das für sie installiert haben.
Doch seid gewarnt, wenn man keine Ahnung von den Bedrohungen des Internets hat, sollte man lieber die Finger davon lassen…

Ach, das hab ich aus dem Herunterladen
Musik und Filme sind die beliebtesten Ziele, denn bei der Qualität der heutigen Filme und Musik ist man meistens nicht geneigt, Geld dafür auszugeben. Man hat gehört, das bekommt man alles im Internet, also los, her damit!

Weitere beliebte Objekte aus dem Herunterladen sind Programme, die normalerweise **abartig viel Geld kosten**. Drei der am meisten illegal heruntergeladene Softwarepakete sind Adobe Photoshop Creative Suite, Microsoft Office und Symantec Antivirus.
Und ich kann überhaupt nicht verstehen, warum.
Ich kenne eigentlich niemanden, der den vollen Umfang der Bildbearbeitungsprogramme von Adobe braucht. Aber jeder kennt Photoshop vom Hörensagen und ich glaube "**gephotoshopt**" steht sogar im Duden.
Darum braucht man unbedingt Adobe Photoshop, auch wenn man nur Bilder zurecht schneidet und einen schnell mit der Maus gekritzelten Text hinzufügen möchte. Eine Privat-Lizenz für Photoshop kostete einmal €1000.- und mittlerweile kann man sich nur mehr ein Abonnement für €12.- Pro Monat kaufen.

Die Nummer zwei ist dann schon Microsoft Office. Bei fast jedem PC ist eine Demo-Version von MS Office dabei. Das ist recht lustig, bis nach 2 Monate die Testperiode vorbei ist und Office seinen Dienst versagt. Kaufen oder stehlen ist angesagt, eine Vollversion von Office kostet für Normalsterbliche €149.- oder man nimmt ein Abo um €10.- pro Monat.
Ich kenne auch niemanden (weder privat, noch von der Arbeit), der den vollen Umfang von Microsoft Office braucht oder nutzt.

Nummer drei ist dann schon namhafte Antivirus Software von Symantec. Ob es eine gute Idee ist, eine illegale Kopie einer gestohlenen Sicherheits-Software zu verwenden?

Woher kommen die illegalen Angebote
Sie kommen von der dunklen Seite des Internets. Wo Musik und Videos gerippt,

gepackt und zerteilt und zum Download angeboten werden.
Cracker knacken die meist voll funktionsfähigen Demo-Programme, sodass sie funktionieren, als wären sie gekauft und registriert worden. Alles wird dann auf meist dubiosen Download-Portalen als **Torrents** oder **Direct-Downloads** angeboten, worauf ich aber nicht näher eingehen möchte. Im Nachschlag gibts dann ein paar Infos.
Wer sich auf der dunklen Seite des Internets was herunterladen möchte sollte schon zumindest ein Internet-Jedi sein und kein Internet-Ewok.

Sag mir doch, wo ich was herunterladen kann!
Leider gibt es da nicht DIE Seite, wo man alles bekommt. Die Szene ist ein ziemlicher Affenzirkus in einem Narrenhaus namens Internet. Gewürzt mit einer Prise Wahnsinn, verfeinert mit einer Portion Aaaaaah und einer Priese NEINN!
Die Szene ist immer in Bewegung, die Seiten ändern ständig ihren Standort, mal macht eine zu, dafür gibt es morgen wieder zehn neue. Die glorreichen Zeiten von **ThePiratebay** sind längst vorbei, es gibt eigentlich keine vernünftigen Torrent Seiten mehr. Wie es scheint hat die Content-Industrie diese Schlacht gewonnen, aber ganz bestimmt nicht den Krieg!
Wenn man trotzdem vernünftig downloaden will, muss man letztendlich immer zahlen, da die Sharehoster ihre Direct-Downloads nur für zahlende Mitglieder richtig schnell machen. Ansonsten kann ein Download auf halber Strecke abbrechen und komplett versiegen, und man bekommt gar nichts. Oder es ist nicht das drinnen, was draufsteht. Oder man hat nur ein verseuchtes Stück Datenmüll heruntergeladen und der Virenscanner leuchtet auf, wie ein Christbaum.

Um es kurz zu machen, man kann es nicht schnell mal so erklären. Man muss seine **eigenen Erfahrungen** machen, mit allen Risiken und Niederlagen. Entweder man schafft es irgendwann sich auszukennen, oder man ist der Probleme überdrüssig und gibt auf.
Meistens ist das zweite der Fall.

Was kann mir passieren?
Ich glaube, ich muss euch nicht weiter erklären, dass man nur mit gewissem Rüstzeug auf solche Seiten gehen kann. Natürlich haben alle diese Seiten ihre Tücken, denn schließlich machen die Betreiber das nicht umsonst. Werbung ist noch das harmloseste, womit auf solchen Seiten Geld verdient werden soll. Meistens befinden sich noch viele andere kleine Fallen, auf die Max Mustermann hereinfallen kann und soll.

Das erste sind gleich mal **Abo-Fallen**, denn du kannst bei einem dir unbekannten Anbieter monatlich zahlen um dir das herunter zu laden, weswegen du eigentlich hergekommen bist, um es gratis runter zu laden. Allerdings ist das nur die Werbung eines weiteren Anbieters, der dafür zahlt, auf der von dir besuchten Seite angezeigt zu werden. **Kennst du dich eh noch aus?**

Auf den meisten Herunterladen-Seiten befinden sich Beschreibungen und Einblendungen, die einem suggerieren, man müsste sich unbedingt DIESES Programm installieren, damit man in den vollen Download-Genuss kommt.
Diese sind nicht zu übersehen und sehen auch recht vertrauenswürdig aus. Also klicken wir auf installieren!
Ojeh, zu spät, denn du bist gerade gratis Mitglied im Zombie-Netzwerk irgendeines lustigen Hackers geworden. Dieser verwendet nun deinen PC für seine dunklen Machenschaften und verdient so sein Geld.

Falls du es doch schaffst, einen Download zu starten, ohne auf diese Fallen hereingefallen zu sein, gibt es natürlich noch weitere Hürden. Denn du musst ja erst das Programm installieren und dann den Crack ausführen, der im Download war. Der funktioniert natürlich nur dann richtig, wenn du deinen Virenschutz ausschaltest! Sagt der Crack zumindest. Ojeh, schon fast am Ziel, aber du bist jetzt trotzdem gerade gratis Mitglied im Zombie-Netzwerk irgendeines lustigen Hackers geworden.

Falls du auch darauf nicht hereingefallen bist, öffnet sich nun vielleicht dein Browser und auf einer lustigen Seite wird dir mitgeteilt, dass der Crack nur dann funktioniert, wenn du genau DIESES Programm dazu installierst. Na gut, dann klick ich halt auf...
Ojeh, knapp daneben ist auch vorbei und rate mal: Du bist jetzt gerade gratis Mitglied im Zombie-Netzwerk irgendeines lustigen Hackers geworden.

Sagen wir mal, du warst doch misstrauisch und hast das alles ohne Schaden überstanden, das Programm wurde geknackt und funktioniert auch, dann geht noch zu guter Letzt eine Seite auf, auf der du für die Gruppe der Cracker voten kannst. Na gut, voten tut ja nicht weh und ojeh, schon wieder bist du gratis Mitglied im Zombie-Netzwerk deiner Wahl geworden.

Vielleicht habe ich dich unterschätzt und du bist doch ein ganz Schlauer. Hast alles richtig gemacht und nichts ist passiert. Dann gibt es immer noch ein Problem. Das Programm selbst. Das Programm meldet sich nämlich ziemlich sicher in regelmäßigen Abständen bei seinem Hersteller um entweder Updates zu suchen (schlecht, weil es nach einem Update ziemlich sicher nicht mehr funktioniert) oder einfach um mal Hallo zu sagen und einige Daten deines Rechners, die gefälschte Registrierung, deine IP Adresse, deine Mail-Adresse, möglicherweise deinen richtigen Name usw. an den Hersteller zu senden, der dann genau weiß, wie oft und von wem sein Produkt illegal verwendet wird (auch schlecht).
Dies kann man ganz einfach verhindern, indem man eine **Application-Firewall** verwendet, die die Kommunikation des Programmes mit seinem Schöpfer verhindert. Eh klar, oder?

Alternativen
Das alles kannst du dir getrost sparen.
Wenn du neue Filme gleich sehen willst, dann gehe ins Kino. Oder warte, bis sie

nach ein paar Monaten ins Fernsehen kommen.
Wenn du alte Filme sehen willst, frag deine Freunde und Verwandten, vielleicht haben die welche.
Wenn deine Freunde und Verwandte den Film nicht haben, leihe ihn dir in der Videothek.
Wenn du Musik hören willst, höre Radio. Oder Webradio. Oder Podcasts. Oder musiziere selbst.
Wenn du Programme brauchst, verwende Open Source Programme oder Freeware. Ihr erinnert euch noch an **Ninite, Fosshub und SourceForge**?

Dies erspart dir viele Probleme wie Viren, Trojanische Pferde und andere Quälgeister, Datenverlust und Neuinstallation deines Rechners. Möglicherweise auch Anwaltskosten. Es wurden zwar in Österreich noch nicht so viele Menschen wegen raubkopierter Musik, Filmen oder Programmen verklagt, aber der Teufel schläft nicht. Eine Gesetzesänderung im EU Parlament und schon kann alles ganz anders sein. Das Internet vergisst nicht. Es weiß, was du letzten Sommer heruntergeladen hast!

Apropos Raubkopie:
Der Ausdruck Raubkopie ist per se falsch, weil nämlich für einen Raub die Androhung oder die Anwendung von Gewalt notwendig ist.
Ich habe noch nie gehört, dass jemand etwas mit Gewalt oder per Androhung von Gewalt heruntergeladen hat. Aber ist ja Wurst.

Nachschlag:
BitTorrent
https://de.wikipedia.org/wiki/BitTorrent

Direct Download
https://de.wikipedia.org/wiki/Direct_Downloads

Musik
http://www.radio.at/
http://freebies.about.com/od/computerfreebies/tp/free-music-online.htm

Alternative zu Adobe Photoshop
http://www.gimp.org/

Alternative zu Microsoft Office
http://www.libreoffice.org/

Kapitel 12: Sprachsteuerungen

In diesem Kapitel möchte ich auf die Gefahren von Sprachsteuerungen hinweisen. Sprachsteuerung von Computern ist in Science Fiction Serien und Filmen schon seit den 50er Jahren des vorigen Jahrhunderts Gang und Gäbe, funktioniert aber bis heute noch nicht wirklich einwandfrei.

Sprachsteuerungen gibt es schon recht lange. Ende der 90er Jahre war bei einem Office-Softwarepaket eine Demoversion einer Spracherkennungssoftware dabei, mit dem man Spracherkennung für das Textverarbeitungsprogramm aktivieren konnte. Die Software war riesengroß und bedurfte langer Übung auf beiden Seiten, denn die Software musste erst lernen, wie ich spreche und andererseits musste ich selbst lernen, wie man dem Rechner Sprachbefehle erteilen konnte.
Außerdem war der Korrekturbedarf relativ hoch, da recht häufig Wörter falsch erkannt wurden.
Da ich damals nicht viel geschrieben habe, habe ich das nicht mehr wirklich weiter verfolgt.

Viele Mobiltelefone konnten schon **Voice-Dial**. Man drückte die grüne Taste länger und nach einem Signalton konnte man den Namen der Person sagen, die man anrufen wollte. Dies war aber im eigentlichen Sinn gar keine Spracherkennung, weil nur ein Sprachmuster verglichen wurde, welches mit einem Telefonbucheintrag verknüpft war.

Bei all diesen Systemen wurden **alle Daten lokal verarbeitet** und gespeichert und nichts wurde ins Internet (meist mangels Internet) gesendet.

Siri, wo ist meine Unterhose?
Heute schaut es schon ein wenig anders aus. Sprach-Assistenten überall. Im Auto, im Navi, im Handy im Fernseher und auch schon in Spielzeug.
Ich bin kein Gegner des Fortschrittes, ich fände es auch recht schön, wenn man mit verbalen Befehlen gewisse Dinge steuern könnte.
Nur es gibt ein kleines Problem, denn **die Spracherkennung findet nicht länger im Gerät** statt.
Es wird lediglich aufgezeichnet, was man sagt, per Internet zum Hersteller gesendet, dort analysiert ein gigantisches Spracherkennungsnetzwerk das gesprochene, danach wird eine Befehlssequenz zurückgesendet und das Gerät führt diese dann aus.
Dies hat verschiedene Gründe.
Einerseits wäre die Spracherkennung **zu groß und zu komplex**, um auf dem Gerät sinnvoll zu funktionieren. Es sind wahrscheinlich Terabytes an Sprachmustern notwendig und eine recht gigantische Rechnerleistung, um dementsprechend schnell

aus der Frage ein passendes Ergebnis zu bekommen.
Andererseits möchte sich auch natürlich kein Hersteller **in die Karten sehen** lassen, wie seine Software funktioniert. Wäre die Spracherkennung unmittelbar auf dem Gerät, würde man die Software mittels **Reverse-Engineering** auf seine Funktionsweise analysieren können.
Da es sich bei Spracherkennung um eine recht komplexe Art von Software handelt, die Intelligenz vortäuschen soll, kann man sich vorstellen, dass nicht jeder Hersteller das Wissen um die selbe teilen möchte.
Wie also kann der Sprachassistent wissen, wo meine Unterhosen schon wieder versteckt sind?
Nun, der Sprachassistent weiß gar nichts, deswegen benötigt er **unbegrenzten Zugriff auf dein Gerät**, um richtig gut funktionieren zu können, das heißt, GPS Daten (Bewegungsprofil), Adressbuch, Mails, Sprachnotizen, Textnotizen, Fotos zur Bilderkennung, kurz gesagt: alle Daten auf deinen Gerät.
Findet er dann immer noch keine Lösung, wird eine Trivial-Antwort gegeben, z.b: "Deine Unterhosen sind in deinem Kleiderschrank!" oder "du hast sie hoffentlich an!" um Intelligenz bzw. einen echten Assistenten vorzutäuschen.
Erkennst du schon den Pferdefuß? **Alle deine Daten sind einem Konzern (welchen auch immer) zugängig**. Und du hast keine Ahnung, was dieser damit macht. Im besten Fall nichts schlimmes, aber das ist nur guter Glaube. Den auf alle Fälle werden deine Daten längerfristig gespeichert, damit die Software weiter verbessert werden kann. Datenschutzrechtlich ist das eigentlich schwer bedenklich, aber weil du ja die AGBs und Nutzungsbedingungen sorgfältig gelesen und verstanden hast, ist das alles kein Problem, oder?
Kommt denn das überhaupt niemandem seltsam vor?

Fernseher, Programm 25
Letztes Jahr (2015) gab es einen kleinen Skandal, denn der Hersteller eines Smart TVs hatte irrtümlich in der Sprach und Gesten-Erkennung seiner Fernseher die permanente Versendung von Bild und Ton im Wohnzimmer des Besitzers eingestellt.
Eigentlich sollten die Daten nur dann versendet werden, wenn man dem Fernseher mit einem Befehl die Spracherkennung aktiviert.
Ja, Fernseher können heute auch zurück sehen! Denk mal nach, warst du schon mal nackt vor deinem Fernseher?
Kommt denn das überhaupt niemandem seltsam vor?

Hallo Barbie, machen wir eine Tee Party?
Das i-Tüpfelchen ist nun, was dem Hersteller der Barbie eingefallen ist. Mit "Hello Barbie" können Kinder aus aller Welt nun mit ihrer Puppe plaudern.
Eine liebe Idee, oder?
Dafür hat ein Großkonzern seine riesigen Ohren in den Kinderzimmern der Welt. Gespräche, Geheimnisse und Wünsche von Kindern.

Zum Glück gibt es auch einen Nutzen für die Eltern, denn man bekommt ein Protokoll über die Gespräche, welche die Kinder mit ihrer Barbie führen, per Mail zugesandt.
Auch mal was neues, Spionage statt Erziehung...
Kommt denn das überhaupt niemandem seltsam vor?

Siri: sende alle Nacktfotos an alle Kontakte
Problematisch wird es, wenn der falsche Benutzer die Befehle gibt, denn eine Stimmerkennung gibt es normalerweise (noch) nicht. Wenn also die Sicherheitseinstellungen zu lasch sind (Gerät reagiert auf Spracheingaben, obwohl es gesperrt ist) oder du dein Gerät unversperrt und unbeobachtet liegen lässt, kann das schon einmal problematisch werden.
Was wäre, wenn deine Partyfotos, auf denen du, sagen wir mal im Saufkoma bist, per Sprachbefehl an deinen Chef gesendet werden?
Oder jemand befiehlt deinem Handy, deine gespeicherten Nacktfotos (von dir oder sonst jemanden?) auf deiner Facebook-Wall zu posten und alle deine Freunde (inklusive Chef) können das dann im Internet betrachten.
Es könnte auch Schaden angerichtet werden, wenn jemand deinem Handy befiehlt, z.B. alle deine Kontakte oder Mails zu löschen.
Kommt denn das überhaupt niemandem seltsam vor?

Aber es ist die Zukunft!
Ja, aber nur teilweise. Wie man auch in den Science Fiction Filmen und Serien sieht, gibt es immer noch Menschen, die Knöpfe drücken müssen.
Schließlich macht es ja keinen Sinn, einem Computer lang und breit zu erklären, dass man den überkochenden Warp-Kern seines Raumschiffes doch endlich abstoßen soll, wenn man das auch mit einem einzigen Knopfdruck machen könnte.
Für die, die keine Science Fiction Fans sind: Es wäre höchst unerfreulich, wenn ein Atomkraftwerk einen Super GAU hätte, bloß weil man mit dem Computer erst diskutieren muss, ob man den Reaktor herunterfahren möchte oder nicht, obwohl man das drohende Unheil mit einem einzigen Knopfdruck abwenden könnte.

Keine Frage, gewisse Dinge kann man sicherlich per Sprache erledigen. Zum Beispiel E-Mails oder sonstige Nachrichten diktieren.
Vor allem **behinderte Personen** können durch die Spracheingabe von Geräten extrem profitieren.
Aber alles was den Vorgang durch Sprachbefehl komplexer machen würde, ist halt nicht notwendig. Licht einschalten zum Beispiel. Und vor allem ist es nicht notwendig, dass ein ganzer Konzern weiß, dass ich mein Licht eingeschaltet habe.
Die Zukunft wird zeigen, in wie weit die Sprachsteuerung unser Leben verbessert (oder nicht).

Was kann ich dagegen tun?
Wenn man auf seinem Gerät die Spracherkennung aktiviert, nimmt man automatisch am Überwachungsprogramm der Geheimdienste teil.
Denn wie der letzte Überwachungsskandal https://de.wikipedia.org/wiki/Globale_Überwachungs-_und_Spionageaffäre gezeigt hat, haben die Geheimdienste ihre Fangarme in den Datenspeicher aller Internet-Riesen.
Und bedenke folgendes: Wäre jeder Mensch gezwungen, einen Peilsender, der gleichzeitig eine Wanze ist, mit sich zu tragen, wäre der Aufschrei groß.
Wenn es ein stylisches €800,- Smartphone ist, hat man **überhaupt kein Problem** damit, nein, es ist sogar noch erstrebenswert!

Wenn dich sowas nicht stört, weil du eh nichts zu verbergen hast, kannst du ja getrost die Spracherkennung aktivieren, oder aktiviert lassen.
Ansonsten gibt es eigentlich nur eine Möglichkeit:
Spracherkennung aus.

Nachschlag:
Wikipedia über Siri
https://de.wikipedia.org/wiki/Siri_%28Software%29

Wikipedia über Cortana
https://de.wikipedia.org/wiki/Cortana_%28Software%29

Smart TV
http://www.zeit.de/digital/datenschutz/2015-02/samsung-smart-tv-private-gespraeche

Hello Barbie und der Big Brother Award
https://bigbrotherawards.de/2015/technik-hello-barbie

Wer einen Film sehen will, der zeigt warum Sprachsteuerung und in deren Folge künstliche Intelligenz mit Vorsicht zu genießen ist, sehe sich den Filmklassiker **Dark Star** https://de.wikipedia.org/wiki/Dark_Star an. Eine durch einen Kurzschluss fälschlicherweise aktivierte, intelligente Bombe (die zur Vernichtung von Planeten und Sternen, die im Weg sind, benutzt wird), muss irgendwie überredet werden, doch nicht zu detonieren...
Sehr alte, aber recht lustige Science Fiction-Parodie von John Carpenter.
Hier ein Ausschnitt (in Englisch):
https://www.youtube.com/watch?v=qjGRySVyTDk

Kapitel 13: E-Banking

Lieber Leser!
Wenn du das liest, hast du hoffentlich auch bereits meine 12 vorherigen Kapitel von **Sicher im Internet** gelesen!

In diesem Kapitel behandle ich das Thema E-Banking, wobei die "Unglückszahl 13" meiner Meinung dafür recht gut geeignet ist, denn nirgends ist das Risikopotential grösser, als bei E-Banking!
Eigentlich setzt E-Banking die Kenntnis von so ziemlich allen bisherigen Kapitel voraus...
Da es beim E-Banking **um dein Geld** geht, ist grundsätzlich Vorsicht angebracht, also den **Hausverstand einschalten** bitte nicht vergessen!

Der Computer
Klarer Fall, der Rechner sollte über alle Sicherheitsupdates des Herstellers verfügen und auch über einen Virenschutz. Schon gar nicht sollte man sich von einem Rechner der ohnehin schon seltsame, verdächtige Dinge macht, in das E-Banking einloggen.

Ich kann es gar nicht oft genug sagen, wie wichtig dieser Punkt ist. Wenn du das Gefühl hast, dass mit deinem Computer etwas nicht in Ordnung ist oder er irgendwie anders reagiert als sonst, sich scheinbar bei allem total schwer tut und für alles ewig braucht, obwohl der Rechner eigentlich noch neu ist, dann ist Vorsicht geboten!
Lass das unbedingt abklären, denn mit einem verseuchten PC ins Internet zu gehen ist schon ziemlich schlecht, E-Banking ist natürlich noch schlechter!
Wenn mit deinem Rechner etwas nicht in Ordnung ist, solltest du unbedingt die Finger von E-Banking lassen!
Hier geht es tatsächlich **um DEIN GELD!**

Kontrollblick in die URL Leiste
Wenn du, wie gewohnt auf die E-Banking-Seite gehst, solltest du, bevor du dich einloggst, immer in der Adressleiste nachsehen, ob du auch da angekommen bist, wo du hinwolltest. Vor allem dann, wenn etwas anders aussieht als sonst. Dies kann einerseits daran liegen, dass die Bank das Webdesign geändert hat, andererseits, weil du vielleicht woanders hin umgeleitet wurdest.
https://deinebank.at/ebanking ist nicht dasselbe wie
http://deinebank.komischerserver.ru
Die Kommunikation mit deinem Bank-Server findet ausschließlich mit https Verschlüsselung statt, erkennbar am Schloss-Symbol in der Adressleiste und am https:// Präfix!
Diese Praktik solltest du dir im allgemeinen angewöhnen, denn es ist auch bei

anderen Seiten ratsam nachzusehen, ob du wirklich dort bist, wo du hin wolltest. Nämlich bei allen Webseiten, die durch Benutzername und Passwort geschützt sind. Bevor du einen Link verfolgst, solltest du auch unbedingt nachsehen, ob der auch dort hinführt, wo du hin möchtest. Der Mozilla Firefox, den du ja hoffentlich mittlerweile verwendest, zeigt dir, wenn du den Mauszeiger auf einen Link bewegst (ohne darauf zu klicken!!) in der linken unteren Ecke, wohin er wirklich führt. So bist du vor der so genannten URL Maskierung geschützt! Siehe folgenden Link: https://de.wikipedia.org/

Das Kennwort
Gerade hier sollte dir klar sein, dass ein gutes Kennwort gefragt ist. Die meisten E-Banking Portale lassen wahrscheinlich ohnehin keine schwachen Kennwörter zu. Wobei meine Bank ein zufällig generiertes Passwort mit einer Länge von 24 Zeichen nicht akzeptiert hat, weil hier eine ganz komische Richtlinie herrscht, die nur einige wenige Sonderzeichen zulässt...
Natürlich solltest du das Passwort niemanden verraten, nirgends aufschreiben und schon gar nicht wo hin kleben.
Das Passwort im Browser zu speichern ist auch keine so glorreiche Idee, weil Schadprogramme diese vielleicht auslesen und im schlimmsten Fall sogar nach außen (ins Internet) verraten könnten.
Ein **Passworttresor** wäre ratsam und nützlich!

Transaktionsnummern oder TANs
Normalerweise bekommst du eine Liste von TANs von deiner Bank per Post zugestellt. Bei einer Überweisung musst du dann eine dieser Nummern eingeben, als zusätzliches Sicherheitskriterium. Daher versuchen ja auch viele böse Menschen solche TANs zu ergattern, denn mit Benutzername und Passwort alleine kann man noch keine Überweisung machen.
Natürlich solltest du auch die TANs sicher aufbewahren, am besten in den Passworttresor übertragen (ja, ich weiß, es sind viele) und das Zetterl dann verbrennen und / oder aufessen.
Ein wenig besser ist schon ein "One Time Password" per SMS anstatt TANs.

Übrigens lassen sich beide dieser zusätzlichen Sicherheitsmechanismen aushebeln, wenn dein Computer einen Trojaner hat und der Feind schon auf deinem Rechner ist. Dabei glaubst du eine Überweisung durchzuführen, in Wirklichkeit bekommst du nur das zu sehen, was du sehen sollst. Der böse Hacker führt dann die tatsächliche Überweisung durch, mit deinem TAN oder One Time Password. Man nennt dies "**Man in the middle Angriff**" (siehe Nachschlag).

Korrespondenz mit deiner Bank
Keine Bank der Welt schickt einem Kunden in schlechter Sprache formulierte E-Mails, in denen du gebeten wirst, irgendwelche Daten zu aktualisieren, TANs einzugeben oder sonst irgendeinen Schwachsinn zu machen.

Üblicherweise weiß deine Bank, wo du wohnst und schreibt dir einfach einen Brief, wenn es wichtig ist.
Du solltest solche Mails unbedingt löschen, nicht darauf antworten und auf keinen Fall irgendwelche Links darin anklicken.
Heutzutage wird auch die E-Banking-Seite selbst als Kommunikationsplattform verwendet, indem du auf Neuigkeiten hingewiesen wirst, wenn du erfolgreich eingeloggt bist.

E-Banking mit App am Smartphone
Ich bin kein besonderer Fan von E-Banking am Handy. Besonders deswegen, weil die meisten Telefone nicht über genügend Schutz verfügen. Aus Bequemlichkeit werden viele Telefone nicht automatisch gesperrt und viele Passwörter sind im Gerät permanent gespeichert. Sicherheitstechnisch sind sowieso viele Handys ein Problem, da die Hersteller zu wenige oder gar keine Sicherheitsupdates zur Verfügung stellen. Dies macht die Geräte natürlich leichter angreifbar und für bösartige Hacker zu einem Ziel.
Da die meisten Leute alle Schnittstellen ihres Mobiltelefons eingeschaltet haben (WLAN, Bluetooth, NFC und dgl.) könnte ein Telefon sogar kompromittiert werden, nur weil man zufällig im Autobus mit einem Hacker mitfährt...
Man muss sein Mobiltelefon nicht erst verlieren, um nicht mehr Herr über das Gerät zu sein.

Muss das immer alles so kompliziert sein?
Ja, mit der Sicherheit ist das leider nicht immer so einfach, glaube mir. Ich arbeite jetzt schon bald 20 Jahre in der Branche und auch ich muss täglich dazu lernen, lesen, lesen und lesen. Und noch mehr lesen.
Aber wie du hier sicherlich schon gelesen hast: wer lesen kann ist klar im Vorteil!
Immerhin geht es hier um dein (wahrscheinlich hart verdientes) Geld, abzüglich dem, was Vater Staat für angemessen hält, dir davon weg zu nehmen.
Lass dir nicht auch noch was von zwielichtigen Gestalten weg nehmen!

Nachschlag:
Als du dich für E-Banking angemeldet hast, hast du sicher von deiner Bank eine Beschreibung und Sicherheitshinweise bekommen.
Lies das mal durch!

Sicherheit beim Onlinebanking
https://de.wikipedia.org/wiki/Electronic_Banking#Sicherheit_beim_Onlinebanking

Man in the Middle Angriff:
https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff

Mobile Banking
https://de.wikipedia.org/wiki/Mobile-Banking

Kapitel 14: Hilfe, ich werde gehackt!

In diesem Kapitel geht es darum, was man tun kann, wenn man gehackt wird, bzw. wurde.

Gleich mal vor weg, es sieht nicht so wie im Film aus, wo in einem dunklen Keller ein paar junge Männer mit hunderten Rechnern, tausenden Kabeln und fettigen Pizzakartons sitzen und in Bildschirme glotzen in denen permanent grüne Textzeilen ablaufen und scheinbar wahllos auf eine oder mehrere Tastaturen einhämmern (hacken) und dabei seinen Mithackern zurufen, wo er jetzt gerade drin ist, ständig wartend auf die Polizei, die dann die Tür aufbricht und den Keller stürmt.
Dies ist die glorifizierte Vorstellung von Filmstudios, wie das auszusehen hat, wenn Hacker arbeiten.

Die Realität sieht meist komplett anders aus.
In einem dunklen Keller sitzen einige pickelige Buben mit hunderten Rechnern, tausenden Kabeln und fettigen Pizzakartons und warten bis ihre Scripts (die sie aus dem dunklen Internet zusammengesucht haben) einige Opfer gefunden haben und rühmen sich dann auf irgendwelchen Foren oder gehackten Internetseiten mit ihren Taten, bis die Mutti in den Keller schreit, dass der Bub jetzt schlafen gehen muss und seine Freunde jetzt gefälligst heim gehen sollen.

Warum werde ich überhaupt gehackt?
Meistens wird man gar nicht wirklich gehackt. Echte Angriffe von echten Hackern erfolgen gezielt auf eine spezielle Gruppe von Menschen die dort arbeiten, wo die Hacker hinein wollen.
Diese Angriffe sind von langer Hand geplant und dienen meistens einem Ziel, nämlich in vermeintlich besonders gut geschützte Systeme einzubrechen ohne viele Spuren zu hinterlassen, dort geheime Informationen abzugreifen und unentdeckt wieder zu verschwinden. Private Rechner werden normalerweise nicht angegriffen, solange man kein potentielles Ziel ist, z.B. weil man eben in einer Firma arbeitet, die ein Ziel der Hacker ist.

Wenn ein privater Rechner angegriffen wird, ist dies meistens eine breitgestreute Aktion quer über einen Adressbereich des Internets und dient meistens der Geldbeschaffung in irgendeiner Form:
* Du bist Mitglied in einem Zombie-Netzwerk welches zum massenhaften Versenden von Mails oder für **Distributed Denial of Service** Attacken verwendet wird
* Du hast einen Trojaner erwischt, und es wird versucht, Kreditkarten, und oder Bankinformationen zu stehlen
* Ein paar Buben (oder Mädels) versuchen sich in Computerkriminalität und tun es einfach, weil sie es können

Die meisten so genannten "Hacks" sind in Wirklichkeit nur die Folge von **zu einfachen Passwörtern**.
Ich schildere am besten einen Fall, der einer Freundin passiert ist.
Sie hat mich ganz aufgeregt angerufen, denn sie bekommt dauernd komische Mails, und auf Facebook stehen Kommentare, die sie nicht geschrieben hat.
Ich habe mir das ganze mal angesehen, um festzustellen, ob wirklich jemand auf ihrem Rechner war.
Doch dieser war eigentlich sauber.
Passiert war folgendes: Ihr Mailkonto bei GMX wurde geknackt (eigentlich wurde nur das Passwort erraten) und weil sie überall das gleiche Passwort verwendet hat, war natürlich auch gleich Facebook, Willhaben, Ebay, usw. betroffen.
Der Angreifer hat dann einfach überall die Mailadresse zur Kennwortrücksetzung geändert.
Als die Freundin versucht hat, sich ein neues Kennwort zu setzen, ging das einfach nicht, weil dies normalerweise mit einer E-Mail geschieht, die sie aber natürlich nie bekam…

Daher solltest du bei deinem Mailkonto ein besonders sicheres Kennwort haben, denn meistens ist die E-Mail Adresse der Schlüssel zum Entsperren von anderen Zugängen aller Art, auch wenn du dort ein komplett anderes Passwort hättest!

Solche Aktionen laufen üblicherweise vollkommen automatisch (per Script) ab und bedürfen üblicherweise nur der "Ernte" der Daten, bzw. geknackten Konten. Der Angreifer tut dann damit, was ihm so einfällt, d.h. er verwendet die ergaunerten Daten entweder selbst, oder verkauft sie dann im dunklen Internet weiter.

Was kann man in so einem Fall tun?
In so einem Fall kann man außer Schadensbegrenzung überhaupt nichts mehr tun.
Ich habe der Freundin geraten sich ein neues Mail-Konto bei einem anderen Betreiber anzulegen.
Mit einem **wirklich sicheren Passwort**.
Danach muss man nur mehr alle betroffenen Betreiber über die kompromittierten Kontos informieren, was recht aufwendig ist, denn die Kontakte, an die man sich in so einem Fall wenden kann, nicht immer ganz leicht zu finden sind.
Einmal informiert, sperren die Firmen die betroffenen Logins dann meistens relativ schnell und der Spuk sollte ein Ende haben.
Theoretisch.

Die Folgen so eines Vorfalles sind, dass man nun allen seinen Kontakten die neue Mail-Adresse und den neuen Facebook-Namen bekanntgeben muss, und alle anderen betroffenen Konten müssen natürlich auch wieder neu angelegt werden.
Ein weiterer Aspekt mit unangenehmen Beigeschmack ist das **Eindringen in die Privatsphäre**. Das Wissen, dass jemand Zugriff auf alle deine Mails hatte ist zumeist

recht beklemmend. Der Einbrecher weiß nun recht wahrscheinlich, wer deine Familie, Freunde und Bekannte sind und ziemlich sicher auch, wo du wohnst…

Mir passiert das sicher nie!
Die meisten Menschen glauben ja, dass ihnen das niemals passieren kann, weil ihnen bisher auch noch nie was passiert ist.
Die ernüchternde Wahrheit sieht ein wenig anders aus, denn eigentlich kann es jedem, jederzeit passieren.

Man muss sich nur einmal falsch entscheiden!
Ein unüberlegter Klick in einem Spam-Mail genügt.
Oder der Plugin einer Webseite, die eigentlich lustige Katzenvideos anzeigen soll, ist in Wirklichkeit ein Trojaner.
Schon ist man unwissentlich Mitglied einer Zombie Herde, die auf Befehle ihres neuen Meisters wartet.
In so einem Fall hilft meist nur mehr eine Neuinstallation des Rechners.

Eine weitere Möglichkeit ist, dass man in einer Firma arbeitet, die in den Fokus eines Hackers oder eines Hackerkollektives gerät. Jeder Mitarbeiter so einer Firma könnte ein Ziel sein, möglicherweise kommt der Hacker sogar zu dir persönlich ins Büro um dein Vertrauen zu gewinnen und sich so Zugang irgend einer Art zu erschleichen.
Diese Technik nennt man **Social Engineering** und ist meist die Vorbereitungsphase auf einen großen Hacking-Angriff.

Wie kann ich sowas verhindern?
Mit Vorsicht, Hausverstand, und einer gesunden Portion Misstrauen!

Hinterfrage immer, egal ob Büro oder zuhause, wenn unangemeldet z.B. ein Techniker bei dir auftaucht um irgendeine Wartung durchzuführen. Im Zweifelsfall wegschicken, wenn derjenige trotzdem hartnäckig darauf besteht, dass er aber unbedingt rein muss, sofort die Polizei rufen.
Normalerweise wirst du im Vorhinein schriftlich informiert, wenn eine Firma zu dir kommt, um irgendeine Wartung durchzuführen.
Und selbst dann **kann dich eigentlich niemand zwingen, jemanden in deine Wohnung zu lassen, wenn du das nicht möchtest**.

Wenn du plötzlich einen Anruf bekommst, und aufgefordert wirst, bei einer Umfrage mitzumachen und scheinbar unwichtige Daten deiner Firma preis zu geben, solltest du keine Antworten geben. Auch nicht, wenn der/die Anrufer(in) freundlich, sehr kompetent und glaubwürdig wirkt.

Wenn du plötzlich einen Anruf bekommst, und aufgefordert wirst, irgendwelche komischen Befehle in deinen Rechner einzugeben, solltest du das auf keinen Fall tun. Auch nicht, wenn der/die Anrufer(in) freundlich, sehr kompetent und glaubwürdig wirkt.

Lasse niemals eine(n) Fremde(n) an deinen Rechner (egal ob Firma oder Privat) um mal schnell was nachzusehen. Auch nicht (oder schon gar nicht), wenn er/sie nett ist und Geschenke bringt.

Lasse niemals eine(n) Fremde(n) dein Smartphone (egal ob Firma oder Privat) benutzen. Auch nicht (oder schon gar nicht), wenn er/sie nett ist und Geschenke bringt.

Wenn du irgendwo einen USB Stick (oder irgend ein anderes USB Dingsbums) herumliegen siehst, dann solltest du das nicht als Einladung sehen, ihn sofort an deinem Computer (egal ob Firma oder Privat) anzustecken. Der Stick könnte einen Trojaner enthalten!
Am besten wäre es, den unbekannten USB Stick sofort zu vernichten, denn es sind relativ umfangreiche Sicherheitsmaßnahmen notwendig, um ohne Gefahr einer Verseuchung nachzusehen, was auf einem USB Stick ist!

Ja, aber das ist schon irgendwie paranoid, oder?
Ich gebe zu, diese Vorsichtsmaßnahmen klingen schon recht übertrieben.
Aber meine Erfahrung sagt mir, dass die Vorsicht die Mutter aller Elefanten in der Morgenstund´ ist...
Die angeführten Vorsichtsmaßnahmen sollten eigentlich jedem, der mit einem Computer arbeitet, und zwar ganz egal wo, bewusst sein.
Bei diesem Bewusstsein handelt es sich um den Grundschutz eines Systems, in welchem du aufgrund des Internetanschlusses Mitglied bist.

Viele Menschen brauchen normalerweise erst eine schlechte Erfahrung, damit sie in Zukunft vorsichtiger sind.
Ich hoffe aber, es geht auch mit dem Bewusstsein, dass es solche Bedrohungen gibt, oder wie es im Renn-Englisch heißt, **Awareness**!

Nachschlag:
Der Begriff Hacker wird eigentlich sehr vielseitig verwendet und heißt nicht automatisch, dass es sich dabei um böse Menschen handelt.
Normalerweise handeln Hacker nach einem Kodex, der es verbietet, Schaden zuzufügen, ganz in Gegenteil; Sie versuchen sogar die Welt zu verbessern. Diese Hacker nennt man auch "**White Hats**".

Natürlich gibt es auch solche, die sich um irgendwelche moralischen Statuten nicht scheren und einfach ohne Rücksicht auf Verluste Menschen absichtlich Schaden zufügen, meist des schnöden Mammons wegen. Diese Hacker nennet man "**Black Hats**".

Netzvandalen, auch Scriptkiddies genannt
https://de.wikipedia.org/wiki/Scriptkiddie

Hacker
https://de.wikipedia.org/wiki/Hacker

Social Engineering
https://de.wikipedia.org/wiki/Social_Engineering_%28Sicherheit%29

Zombie Netzwerk
https://de.wikipedia.org/wiki/Zombie_%28Internet%29

Denial of Service
https://de.wikipedia.org/wiki/Denial_of_Service

Kapitel 15: Hilfe, ich werde überwacht!

In diesem Kapitel geht es um Überwachung sämtlicher Kommunikation im Internet durch Geheimdienste.
Wir leben in einer Zeit, in der der Ruf nach noch mehr Überwachung immer lauter wird.
Schuld daran sind sämtliche terroristischen Akte seit dem 11. September 2001.
Die Geheimdienste der USA erhielten dadurch immer mehr Befugnisse um in anderen Ländern (zu spionieren), aber auch die eigene Bevölkerung zu überwachen.
Natürlich konnten das die europäischen Geheimdienste nicht auf sich sitzen lassen, und haben natürlich auch nach immer mehr Befugnissen getrachtet. Da der Terrorismus auch natürlich vor Europa keinen Halt machte, bekamen auch die europäischen Geheimdienste, was sie wollten.

Was wird alles überwacht?
Kurz gesagt, so ziemlich alles was es an Daten zu speichern gibt. Seit dem Ende des kalten Krieges meinten ja Verschwörungstheoretiker, dass sämtliche Telefongespräche überwacht, bzw. sogar deren Inhalte aufgezeichnet und ausgewertet werden konnten.
Nun, bei Berücksichtigung der damaligen technischen Mittel war eine totale Überwachung des globalen Telefonsystems eher unwahrscheinlich, aber eine gezielte Überwachung von ausgewählten interessanten Zielen aus Politik, Wirtschaft und organisierten Verbrechen aber sehr wohl!
Wer in den Verdacht kam, in irgendwelche Machenschaften verwickelt zu sein, bzw. mit einer dieser Personen in Verbindung war, konnte dann recht rigoros abgehört werden.

Heute sieht die Sache ein wenig anders aus. Der Fortschritt der Technik (die immer ansteigenden Rechenleistungen und die ständig ansteigenden Speicherkapazitäten) hat sämtliche damalige Befürchtungen nicht nur wahr gemacht, sondern sogar noch bei weitem übertroffen.
Wer da an **George Orwells Roman 1984** denkt, ist sogar noch weit gefehlt, denn in Wirklichkeit ist es schon schlimmer wie in dem Roman.
Die Geheimdienste machen sich gar nicht einmal mehr die Mühe, einzelne Personen zu überwachen.
Heute wird einfach der gesamte Datenstrom an den Netzknoten des Internets abgezweigt, analysiert, geordnet, katalogisiert und dann gespeichert. Die einzige Grenze, die es noch gibt ist "mangelnde" Speicherkapazität, denn man ist ja schließlich nur in der Lage diese unglaubliche Datenansammlung einige Monate zu speichern...
Mit der von der EU auferlegten Vorratsdatenspeicherung werden auch sämtliche

Verbindungsdaten (wer mit wem wann telefoniert) der Telekommunikationsanbieter gespeichert. Die Höhe ist eigentlich, dass wir als Kunden das auch noch **selbst gezahlt** haben. Ich sage nur SIM-Pauschale, Service-Entgelt, und so weiter.
Natürlich kann man auch davon ausgehen, dass diese national gesammelten Daten auch im Rahmen der Terrorismus-Prävention mit den Geheimdiensten in voreilendem Gehorsam "geteilt" wurden.

Was bringt diese totale Überwachung?
Nun, Terroristen und Verbrecher wissen, dass alle "normalen" Kommunikationswege überwacht werden können und kommunizieren daher mittels ganz altmodischer Mitteln wie z.B. der persönlichen Mitteilung. Die Älteren unter euch werden das vielleicht noch kennen.
Daher kann ich mir nicht vorstellen, dass mittels Telekommunikationsüberwachung wirklich irgendwelche Anschläge und Verbrechen verhindert oder gelöst werden können.
Die totale Überwachung bringt nur denjenigen etwas, die die dazu benötigten Apparaturen (und Software) herstellen und verkaufen, bzw. den Aktionären solcher Unternehmen.
Kurz und gut, es geht ziemlich sicher nur um Geld, so wie immer.
Ansonsten dient die totale Überwachung nur dazu, um die Menschen in weiterer Folge zu unterdrücken und vielleicht ein paar Eierdiebe zu fangen.

Es kann ruhig noch mehr überwacht werden!
Viele Leute sind der Meinung, dass ihnen die momentane Überwachung noch viel zu wenig weit geht. Man könnte schließlich jeden zwingen, ein DNA Profil abzugeben, um bei schweren Verbrechen schneller den oder die Schuldigen zu finden. Oder man bekommt einfach einen Chip implantiert, um die Identität kontaktlos über kurze Distanzen feststellen zu können.
Ja, das wäre bequem! Echte Polizeiarbeit braucht man dann nicht mehr, denn immerhin muss man dann nur mehr Beweise sammeln, diese dem Computer übergeben und dieser wirft dann eine praktische Verhaftungsliste aus, die einfach jeden Menschen beinhaltet, die in der Nähe eines Tatortes waren.

Das macht mir überhaupt nichts, ich habe ja nichts zu verbergen!
Die totale Überwachung geht mit Pauschalverdächtigung und Polizeiwillkür Hand in Hand.
Jeder Mensch war schon einmal zur falschen Zeit am falschen Ort oder wird früher oder später einmal zur falschen Zeit am falschen Ort sein.
Ein angeschnäuztes Taschentuch neben einem Mistkübel in der Nähe eines Tatortes genügt und kann dann als Beweis dienen, dass du dort warst.
Weil du ja nichts zu verbergen hast, wirst du natürlich gerne mit der Polizei kooperieren, mitkommen und viele unangenehme Fragen beantworten. Natürlich ist es auch kein Problem, wenn du von der Polizei (vielleicht mehrfach) vom Arbeitsplatz

zu einer Befragung abgeholt wirst. Das sieht jeder Arbeitgeber gerne!
Nun wird natürlich alles was über dich zu finden ist ausgewertet und als weitere Beweise bewertet.
OK, im Mordfall warst du doch nicht verwickelt, aber dafür hat man dich beim Falschparken und bei einer Umweltverschmutzung erwischt!
Auch wenn sich alle "Beschuldigungen" als haltlos erwiesen haben, bleibt trotzdem immer ein Makel übrig.
Dies kann das ganze Leben eines Menschen verändern, denke also darüber nach, bevor du das nächste Mal laut sagst, dass du ja eh nichts zu verbergen hast!

Wie kann ich mich vor Überwachung schützen
Ja, das ist das schönste daran, das geht nämlich gar nicht, weil du heutzutage fast ständig mit dem Internet verbunden bist.
Alles was deinen Rechner verlässt, egal ob E-Mail oder Facebook Posting, geht hinaus ins Internet und wird mit ziemlicher Sicherheit ausgewertet und bei Bedarf gespeichert.
Mit deinem Smartphone hast du sowieso quasi immer **eine Wanze mitsamt Ortungsgerät** in deiner Tasche, du musst erst gar nicht kommunizieren um gefunden zu werden, das erledigt das Telefon automatisch für dich.
Dein ganzes Leben lang produzierst du eine Unmenge an Daten, die möglicherweise nicht nur unmittelbar gut für dich sind.
Das tolle daran ist, dass wir auch noch eine Menge Geld für den Kauf der Smartphones und für deren Internetanschluss zahlen!

Wer soll sich das alles ansehen?
Ein weiteres Problem sehe ich darin, dass die gigantischen Datenmengen, die da angesammelt werden, von **Menschen gar nicht mehr gesichtet und ausgewertet werden können**. Nur mehr mit automatischen Algorithmen kann die unglaubliche Datenmenge bezwungen werden. Das heißt, die Daten werden automatisiert nach Schlüsselworten durchsucht und so quasi eine Liste der Verdächtigen erstellt. Mit anderen Worten: **Ein Computer entscheidet**, ob du Verdächtig bist, oder nicht.

Verschlüsseln! Das könnte helfen!
Natürlich könnte man einen großen Teil der Kommunikation verschlüsselt führen um den Überwachern das Leben schwer zu machen. Meiner Meinung nach bringt das aber auch nicht viel, da es doch recht kompliziert ist, verschlüsselt zu kommunizieren. Dies schränkt auch den Personenkreis, mit dem eine verschlüsselte Kommunikation überhaupt möglich ist, total ein.
Weiters kann man **durch die Verschlüsselung erst recht in den Kreis der Verdächtigen aufgenommen werden**, denn schließlich muss man ja böse Dinge vorhaben, wenn man verschlüsselt kommuniziert!
Weiters kann man relativ leicht zur Herausgabe des Verschlüsselungs-Passwortes gezwungen werden.

Zum einen durch Androhung von Strafen (oder Gewalt) und außerdem, weil man ja sowieso nichts zu verbergen hat, oder?

Werde einfach Agent, Verbrecher oder Terrorist!
Möchte man, dass eine Unterhaltung wirklich vertraulich ist, ohne dass die halbe Welt mithören oder lesen kann, sollte man von sämtlichen elektronischen Kommunikationskanälen absehen.
Man wird sich wohl auf verschwörerische, altmodische und vor allem hinterlistige Weise im Kaffee - oder Gasthaus treffen müssen und dort mit abgeschaltetem Smartphone von Angesicht zu Angesicht mit seinen Freunden (Komplizen) plaudern, bei Kaffee, Bier, Wein und sonstigen verschwörerischen Getränken!
Genauso, wie es die Agenten im Film tun. Oder Verbrecher. Oder Terroristen halt.

Nachschlag:
Du denkst jetzt sicher, das hier geschriebene wäre übertrieben!
Doch leider werden alle möglichen technischen Errungenschaften zum Teil nur dazu verwendet, um die Menschen zu überwachen, bzw. um mit deren Daten Profit zu machen.
Vielleicht kann sich auch noch jemand an die **DDR** erinnern. Es ist noch nicht allzu lange her. Dort hat ein System dazu geführt, dass die eine Hälfte der Bevölkerung die andere Hälfte ausspioniert hat. Dies geschah noch fast ohne technische Hilfsmittel.
Was glaubt ihr, könnte so ein Regime mit der heutigen Technik erreichen?
Die Stasi wäre blass vor Neid gewesen…

https://de.wikipedia.org/wiki/Ministerium_f%C3%BCr_Staatssicherheit
https://de.wikipedia.org/wiki/1984_%28Roman%29
https://de.wikipedia.org/wiki/Globale_%C3%9Cberwachungs-_und_Spionageaff%C3%A4re

Kapitel 16: Hilfe, Mein PC ist verseucht

In diesem Kapitel verrate ich euch, was zu tun ist, wenn ein Rechner von einem **Virus / Trojaner / sonstiger Malware** infiziert wurde.
Trotz aller Vorsichtsmaßnahmen kann es passieren, auf einmal macht der PC eigenartige Dinge und reagiert recht ungewohnt. Je nach Malware können sich die Probleme unterschiedlich darstellen.

Wie finde ich heraus, ob ich verseucht bin?
Nun, im Idealfall schlägt der Virenscanner an und berichtet über seinen Fund.
Dies ist der Optimalfall.
Wenn das passiert, kann man noch von Glück sprechen, sofern der Virus auch entfernt werden kann.
Manche Virenscanner können nicht jeden Schädling auch entfernen, sagen aber zumindest wo man die Medizin bekommen kann.
Trotzdem sollte man den Rechner mit **speziellen Werkzeugen** ansehen, denn möglicherweise hat **ein Schädling einen weiteren im Gepäck**, den der Virenschutz nicht erkannt hat.
Wie jeder Schutz ist auch ein Virenscanner **kein hundertprozentiger Schutz** und außerdem ist es immer gut, eine zweite Meinung einzuholen!
Ich empfehle dazu momentan das Programm "**Malwarebytes Anti-Malware**“ https://www.malwarebytes.org/mwb-intercept/
Es ist für den Privatgebrauch gratis und entfernt eine recht breite Palette an Schädlingen und sonstigen Quälgeistern.
Es schadet nicht, ab und zu einmal einen Suchlauf auf dem Rechner zu starten!

Wenn man einen Rechner länger hat, bekommt man ein Gefühl für die Reaktionsgeschwindigkeit und die Leistung des Gerätes. Ein neuer PC ist wahrscheinlich schneller, als ein betagtes Gerät, aber ein **plötzlicher Leistungsverlust** ist immer mit Vorsicht zu genießen!
Wenn nun der **Virenschutz versagt** hat, kann sich das durch folgende, meist **plötzlich auftretende Warnsignale** äußern:
* der Rechner benötigt ungewöhnlich lange zum Starten, funktioniert aber dann recht normal
* die CPU / Speicher- Auslastung ist recht hoch, ohne dass ein Programm gestartet wurde (Dies ist meist auch hörbar, weil der PC dabei meistens heiß wird und die Lüftung hoch dreht; Mit dem Taskmanager https://de.wikipedia.org/wiki/Taskmanager kannst du nachsehen, wie hoch die CPU / Speicher- Auslastung des Rechners ist)
* das Internet funktioniert nur ganz schlecht
* der "Sanduhr" Mauszeiger wird öfter angezeigt, ohne dass du was tust
* du machst eine Texteingabe, der Text erscheint aber erst viel später

* du kannst von dir erstellte Dateien nicht mehr öffnen und du bekommst eine Art Erpresser-Brief, welches die Freigabe deiner Dateien nach Bezahlung einer gewissen Summe verspricht
* der schlimmste Fall: Dein PC wird ferngesteuert und du hast überhaupt keine Kontrolle mehr

Was kann ich jetzt tun?
Das allererste was du tun solltest, ist den Rechner **vom Netzwerk (Internet / WLAN / LAN) zu trennen**.
Dies ist sehr wichtig!
Jeder Virus trachtet nach Verbreitung und dies geschieht heute fast immer per Netzwerk.
Du solltest **auf keinen Fall den Rechner weiter benutzen**, da sich die Verseuchung meistens noch verschlimmert!
Die meisten Viren holen sich nämlich noch ein paar "Freunde" dazu, damit es lustiger wird!

Wenn du **beschreibbare Medien** wie Disketten, USB Sticks, Speicherkarten von Kameras, MP3 Player, Mobiltelefone, externe Festplatten u.dgl. angesteckt hast, solltest du sie **unbedingt trennen und als verseucht betrachten!**
Stecke diese also niemals auf anderen Rechner an!
Wenn der Speicher so eines Gerätes betroffen ist, könntest du so den Virus auf andere Rechner verbreiten.

Ist das Gerät vom Netzwerk getrennt, solltest du es nun ausschalten und vorerst nicht mehr starten.

Und was dann?
Nun benötigst du ein so genanntes **Antivirus Boot-Medium**. Etliche Antiviren Hersteller bieten so etwas gratis zum Download an. Es handelt sich dabei um ein Mini-Betriebssystem mit einem Virenscanner an Bord, mit dem du deinen Rechner starten kannst.

Falls du einen zweiten, **unversehrten Rechner** hast, kannst du es mit diesem herunterladen, wobei dieser eigentlich auch als verseucht angesehen werden sollte, sofern du sie **gemeinsam in einem Netzwerk** betreibst, oder du bereits Dateien per USB Stick u.dgl. seit der Verseuchung ausgetauscht hast!
In diesem Fall solltest du einen Freund bitten, das Antivirus Boot-Medium für dich herunterzuladen und zu brennen, bzw. auf einem USB Stick zu installieren.
Anmerkung: Eine CD zu brennen wäre besser weil sie nach dem Brennen nicht beschreibbar ist und sich so kein weiterer Virus auf dem Boot Medium einschleichen kann! Wenn du überhaupt kein CD / DVD Laufwerk auf deinem Rechner hast, bleibt dir sowieso nichts anderes über, als einen USB Stick oder eine Speicherkarte zu verwenden…

Mit diesem Bootmedium kannst du nun deinen PC einschalten, ohne dass das eigentlich installierte Betriebssystem geladen wird.
Dies ist notwendig, weil das laufende Betriebssystem sich gegen Veränderungen wehrt und die meisten hartnäckigen Viren genau diese Mechanismen nutzen, um nicht selbst gelöscht zu werden.

Ich würde die **Kaspersky Rescue Disk 10** http://support.kaspersky.com/de/8093 empfehlen, da diese bei Tests bisher recht gut abgeschnitten hat.
Es wird auf der Seite auch sehr gut beschrieben, was alles zu tun ist, um überhaupt von der CD starten zu können und was die weiteren Schritte sind.

Im Prinzip läuft es so ab: Du startest von der CD / dem Stick.
Wenn das Mini Betriebssystem gestartet ist, kannst du wieder eine Netzwerkverbindung herstellen, damit sich der Virenscanner aktualisieren kann.
Dann lässt du alle internen Laufwerke des PC überprüfen bzw. säubern.
Danach kannst du alle anderen Speichermedien wie Disketten, USB Sticks, Speicherkarten von Kameras, MP3 Player, Mobiltelefone, externe Festplatten die du vorher abgesteckt hast ebenfalls untersuchen und ggf. säubern.
Diese Prozedur kann **mehrere Stunden oder sogar Tage** (es kommt auf die Datenmenge an) dauern.

Was tun, wenn das alles nichts hilft?
In manchen Fällen kann es vorkommen, dass sich der Rechner entweder nicht mit einem Antivirus Boot-Medium starten lässt, oder dass er so derart verseucht war, dass er nach Entfernung aller Schädlinge nicht mehr starten kann.
Dies ist leider recht häufig der Fall.
Dann gibt es meistens keine weiteren Optionen mehr, als eine Neuinstallation des Betriebssystems, was oft auch **kompletten Datenverlust** mit sich bringt.
Mit dem Antivirus Boot-Medium lassen sich zwar meist auch die eigenen Dateien wegsichern, jedoch könnten diese auch das Entseuchen "nicht überlebt" haben…

Nun sind diejenigen die Glücklichen, die ein Backup haben!
Im Prinzip ist **jede Rettungsaktion unnötig**, wenn man ein aktuelles **Backup** seiner Daten hat.
Der Zeitaufwand einer Rettungsaktion ist meist um ein vielfaches höher, als eine Neuinstallation mit einer Rücksicherung der Daten.
Weiters ist eine Neuinstallation quasi eine **Verjüngungskur für den Rechner**, da jeglicher Ballast von unnötig installierten Programmen und sonstiger Datenmüll, der sich im Laufe der Zeit ansammelt hat, wegfällt.

Ich würde jedem empfehlen, eine regelmäßige Sicherung seiner selbst erstellten Dokumente und Fotos zu haben.
Fast alle Betriebssysteme bieten eine automatisierte Sicherung der Dateien an, man benötigt eigentlich nur eine externe Festplatte.

Mit einem Beispiel möchte ich euch nahe legen, wie wichtig Backups sind:
Ein Kollege hat einen Bekannten, der von Beruf Fotograf ist.
Dieser speichert natürlich alle seine Fotografien auf seinem Laptop ab, um diese nachbearbeiten zu können.
Bis zur Auslieferung befinden sich oft tausende Fotos auf dem Rechner.
Nun lässt aber der Bekannte meines Kollegen auch seine Kinder an sein berufliches Gerät. Diese installieren dann öfters Spiele aus dem Internet und sonstigen Blödsinn auf Vaters Notebook.
Und natürlich ab und zu auch einen Schädling, denn wie schon beschrieben, ist oft nur ein falscher Mausklick nötig, um sich einen Virus einzufangen.

Natürlich hat der Bekannte meines Kollegen **KEIN BACKUP**, denn wozu soll das gut sein? Das dauert ja sicherlich voll lange und ist außerdem voll kompliziert. Überhaupt kann man ja die Fotos jederzeit wieder machen, oder?
Die **"Es wird schon nichts passieren" Lebensart** ist zwar grundsätzlich O.K., aber wenn ich von einem Gerät beruflich abhängig bin, dann lasse ich erstens niemand anderen darauf herumfingern, installiere zweitens darauf keine Spiele und habe drittens **immer ein Backup**.
Mein Kollege hat sich schon mehrfach erbarmt, diesen Laptop wieder von den Toten auferstehen zu lassen, was oft einige Tage und **einmal sogar zwei Wochen** gedauert hat. Dieser Mensch ist echt lernresistent!

Nachschlag:
https://de.wikipedia.org/wiki/Live-System
http://www.netzwelt.de/news/131181_2-anleitung-backup-windows-7-bordmitteln.html

Profi-Tipp: Das Entseuchen eines PCs ist ein recht kompliziertes und langwieriges Unterfangen. Es wäre ratsam, diesen Vorgang als Übung einmal zu "proben" um im Ernstfall besser agieren zu können.
Wenn du überhaupt keine Ahnung hast, wie du sowas angehen könntest, solltest du vielleicht einen Bekannten, der sich wirklich gut auskennt, um Rat fragen.
Professionelle Hilfe von diversen PC Kliniken ist meistens sehr teuer (weil langwierig) und der Erfolg nicht garantiert!
Eine regelmäßige Sicherung deiner wichtigen Daten kann dir all diese Probleme ersparen!

Kapitel 17: Vorsicht vor gefälschten Updates

Wie ich schon öfter erklärt habe, ist es total wichtig das Betriebssystem, den Virenschutz und auch die Programme des alltäglichen Gebrauches immer **auf einem aktuellen Stand zu halten**. Vor allem, wenn diese mit dem Internet kommunizieren, was heute fast jedes Programm tut.
Das gehört zum **Grundschutz eines jeden Computers**, denn alle Programme ohne Ausnahme haben mehr oder weniger gravierende Fehler, die dem **Betriebssystem schaden** könnten, bzw. ein **Schlupfloch für Viren und dgl.** sein können.

Viele Programme haben heute bereits eine so genannte **Auto-Update Funktion** und sehen selbständig auf der Herstellerseite nach, ob es eine neuere Version gibt.
Sofern der Rechner noch "richtig tickt" wird das auch recht gut funktionieren.
Wenn der Rechner aber einmal verseucht ist, kann man auch davon ausgehen, dass die Updates nicht mehr dort herkommen, wo sie sollten…

Was recht häufig vorkommt ist, dass dem User von **irgendeiner Webseite** vorgegaukelt wird, dass ein Programm auf deinem PC dringend eine Aktualisierung benötigt.
Wenn du dieses gefälschte Update dann installierst, hast du dann im besten Fall "nur" irgendein Programm, welches Werbung (Adware) für ein supertolles Windows-Beschleunigungs-Dings macht.
Oder es ist irgendeine "Sicherheits-Software" die dir ständig von angeblichen Fehlern und Sicherheitslücken auf deinem PC berichtet (Scareware), die dann bei Kauf der Vollversion des Programmes angeblich bereinigt werden.
Aber im schlimmsten Fall bekommst du einen **Trojaner**.
Leider sind die Installationsprogramme der "gefälschten Updates" **den Originalen sehr ähnlich**, nur der Weg, wie es überhaupt dazu kommt ist anders.

Woher wissen die überhaupt, was bei mir installiert ist?
Nun, entweder wird einfach per **Javascript** abgefragt, was du installiert hast. Im Nachschlag findest du eine Seite, die dir zeigt, wie leicht das geht!
Diese Methode funktioniert aber nicht immer zuverlässig, denn wenn du kein Java Installiert hast, oder Javascript deaktiviert ist, geht das freilich nicht.
Deswegen machen viele Seiten, die dir sowas andrehen wollen, einfach einen **Schuss ins Blaue**, und präsentieren dir einfach irgendeinen **gut klingenden Namen** von Programmen, die recht viele Benutzer kennen.

Dies ist eigentlich eine recht **plumpe Methode**, die aber scheinbar sehr gut funktioniert.
Internet Explorer, Windows Mediaplayer oder MS Word sind einige der Windows-typischen Programme, jedoch auch **bekannte Browser** wie Firefox, Chrome, Opera u.v.a. können betroffen sein, da eine Identifizierung des Browsers bei jedem Besuch einer Webseite stattfindet.

Ja, soll ich jetzt Updates installieren oder lieber doch nicht?
Dies soll auf keinen Fall ein Argument für Update-Verweigerer sein, weil sie ja schon immer wussten, dass aktualisieren gefährlich ist...
Man sollte sich auf alle Fälle mit den Aktualisierungsmechanismen des Betriebssystem und der Programme vertraut machen, damit man ein Gefühl dafür bekommt, wie sowas aussieht, wenn alles in Ordnung ist. Denn dadurch ist man gewappnet, wenn irgendeine dahergelaufene Internetseite einem ein Update aufs Auge drücken will.

Woher kann ich wissen, ob ein Update echt ist?
Eine Möglichkeit wie die Echtheit eines Programmes gewährleistet werden kann ist, wenn die Programme mit Sicherheitszertifikaten signiert sind. Das Betriebssystem überprüft die Gültigkeit des Zertifikates automatisch und gibt dann die Installation frei.
Jedoch wurde dieses eigentlich gute System schon oft unterwandert.
Außerdem ist nicht jeder Hersteller von Software verpflichtet, seine Programme zu signieren. Du als Benutzer kannst entscheiden, ob du nicht signierter Software vertrauen willst, oder nicht.
Zertifikate sind daher meiner Meinung nach nicht der Weisheit letzter Schluss, siehe im Nachschlag.

Ein weiterer Ansatz sind **App-Stores**, wo nur "vertrauenswürdige" (sprich Mitgliedsbeitrag zahlende) Hersteller ihre Software hochladen dürfen und die Programme selbst auch einen Kontrollprozess durchlaufen müssen. Auch hier wird fleißig signiert und Gauner haben auch hier schon sämtliche Sicherheitsmaßnahmen unterwandert.
Auch eine **verpflichtende Teilnahme an App-Stores** für Hersteller und Konsumenten wurde bereits aus Sicherheitsgründen angedacht, was jedoch durch Proteste auf beiden Seiten (Hersteller und User) nicht durchgesetzt wurde.
Man soll immer frei entscheiden können, wo man mitmachen möchte, und nicht zu einer Teilnahme gezwungen werden…

Ob Updates nun echt sind, oder nicht, kann man nur dann wissen, wenn man schon einmal Programme aktualisiert hat.
Dies sollte eigentlich zu einer Routine werden, so wie man in der Wohnung ab und zu Ordnung schafft, oder einen Großreinigungstag ausruft.
Bei Programmen, die man häufig benutzt, sollte man einfach ab und zu den

Menüpunkt "**nach Aktualisierung suchen**" anklicken bzw. einfach die Funktion "**automatisch nach Aktualisierung suchen**" aktivieren.

Man darf es nicht als Bürde empfinden, wenn sich Programme aktualisieren wollen, denn dies dient der Sicherheit des Systems und oftmals wird man ja auch mit **neuen oder verbesserten Funktionen** belohnt!
Diese "Salami-Taktik" vieler Hersteller birgt dadurch sogar einen Vorteil ;)
Doch leider empfinden das viele Menschen als lästig und neigen deswegen dazu, unachtsam einfach irgendwo drauflos zu klicken, nur weil da schon wieder ein Update ist, oder deaktivieren sämtliche Updates komplett!

Merke: Wenn ein Programm ein Update machen möchte, sagt dir das fast immer das Programm selbst wenn du es öffnest, und nicht irgendeine Webseite im finsteren Internet, wo du grade zufällig eine abgefilmte Version eines aktuellen Kinofilmes herunterladen willst!
Wichtig ist nur, **den Unterschied zu erkennen…**

Was tun, wenn ich mir nicht sicher bin?
Nun, der Besuch der Internetseite des Herstellers ist immer eine gute Idee, denn wenn es eine Aktualisierung gibt, ist das meistens gleich auf der Startseite zu lesen.
Wenn du keine Ahnung hast, wie die Herstellerseite lautet, kannst du das meistens im Menüpunkt "**Hilfe**" oder auch manchmal nur "**?**" nachsehen, denn dort befindet sich fast bei jedem Programm ein Untermenüpunkt "**über [Name des Programmes]**" wo dies Informationen gelüftet werden und manchmal sogar gleich ein Internetlink zu finden ist!
Leider gibt es da keine fixe Regel, wo in einem Programm diese Informationen versteckt sind, es bleibt dem Programmierer überlassen, wie er die Menüstruktur oder die Oberfläche seines Programmes gestaltet.

Weiters kann man, wenn man über eine Aktualisierungsmeldung unsicher ist, einfach auf **nein drücken** und bei dem betroffenen Programm selbst nach Updates suchen.
Dann kann man recht sicher sein, dass es kein "gefälschtes Update" ist.
Was man vielleicht auch tun kann, ist einfach den **Browser komplett zu schließen**, wenn eine Update-Meldung kommt (außer diese kam vom Browser für den Browser), um festzustellen, ob tatsächlich ein Programm das Update verlautbart hat, oder ob eine Webseite nur so tut als ob!
Man muss sich einfach einmal damit auseinandersetzen, nur das bringt das notwendige Wissen, um nicht gleich einem Betrug aufzusitzen.

Nachschlag:
Was dein Browser über dich verrät
http://www.zendas.de/service/browserdaten.html

Sie verwenden [diesen veralteten Browser], verwenden sie doch [den superneuen Browser]
Früher war es mal Gang und Gäbe, wenn man gewisse Internetseiten angesurft hat, eine Werbung eingeblendet zu bekommen, die darauf hinwies, man solle seinen Browser entweder auf eine neue Version aktualisieren, oder vielleicht gleich gänzlich austauschen. Diese teilweise gut gemeinte Ratschläge führten dazu, dass viele leichtgläubige Menschen darauf trainiert wurden, alles aus dem Internet (Internet = Qualitätsbeweis) zu installieren, nur weil einem das vorgeschlagen wurde.
Diese Vorgehensweise stellte sich recht bald als kontraproduktiv heraus und wird heutzutage eher nicht mehr verwendet, außer von zwielichtigen Seiten, die einem einen gefälschten Browser oder andere Malware unterjubeln wollen.

Sicherheit durch Zertifikate
Heute werden ja die meisten Programme mit Zertifikaten signiert, um die Authentizität des Herstellers zu gewährleisten. Für mehr Info über Zertifikate und Signaturen hier der Wiki Artikel: https://de.wikipedia.org/wiki/Digitales_Zertifikat
Das Problem ist, dass es Lieferanten von Schadcode immer wieder schaffen, sich ein gültiges Zertifikat zu ergaunern um damit ihre Malware zu signieren. Das Betriebssystem überprüft dann bei der Installation die digitale Signatur und käme daher nie auf die Idee, dass es sich um ein schädliches Programm handelt.
Der einzige Weg um das zu unterbinden ist nun das besagte Zertifikat als ungültig zu erklären, was meistens weitere Kreise zieht, da dadurch auch die Signatur von anderen Programmen und Herstellern ungültig werden können.

Kapitel 18: Wir verwenden eine Sandbox

In den vorherigen Kapiteln habe ich ausgiebig über die Gefahren, die einem Rechner im Internet drohen, geschrieben.
Einerseits durch das Surfen in den finsteren Ecken des Internets, andererseits durch die Installation von heruntergeladenen Programmen.
Wie ich betont habe, ist es trotzdem notwendig **Erfahrungen zu sammeln**, um zwischen guten und bösen Webseiten oder guten und bösen Programmen unterscheiden zu können.
Auf die Erfahrung von Freunden und Bekannten kann man sich meist nicht allzu sehr verlassen, da diese möglicherweise selbst die Gefahren nicht (er)kennen und einem **unwissentlich schlechte Ratschläge** geben...
Da du aber bis jetzt alle Kapitel durchgehalten hast, gehe ich davon aus, dass dich die Thematik etwas mehr interessiert als andere!

Was kann ich tun, um mich abzusichern?
Eine recht gute Möglichkeit ist die **Virtualisierung**. Darunter versteht man die Installation eines zusätzlichen Betriebssystems, welches in einer eigenen, gesicherten Umgebung läuft.
Diese **Virtuellen Maschinen (kurz VMs)** können im laufenden Betrieb deines Rechners eingeschaltet werden (im Gegensatz zu einer Parallelinstallation, siehe Nachschlag) und sind quasi ein **zusätzlicher Rechner in deinem Rechner**.
Auch andere Betriebssysteme (DOS, ältere Windows Versionen, Linuxe, MacOS, Android u.d.gl.) können in dieser virtuellen Umgebung installiert werden und man kann darin, bis auf **gewisse Leistungseinbußen** (das virtualisierte System benötigt natürlich auch Systemressourcen wie Speicher, CPU Leistung und Festplattenzugriffe), ganz normal arbeiten.
Diese VMs werden meist verwendet, um **Programme laufen zu lassen, die für ein älteres oder gar anderes Betriebssystem** programmiert sind.
Aber auch für **Testumgebungen** werden VMs gerne verwendet, da es möglich ist, den **Zustand der VM "einzufrieren"**.
D.h. ich kann theoretisch herum werken wie ich will, alles umbauen, ruinieren, verstellen, verseuchen usw. und wenn ich genug habe, kann ich wieder zum vorigen Zustand zurückkehren.

Aber das kling recht kompliziert!
Ich muss gestehen, es ist wirklich nicht ganz einfach, denn der Umgang mit VMs bringt selbst hartgesottene Profis manchmal auf die Palme!
Weiters sind auch gewisse Lizenzbedingungen zu bedenken, denn wenn man einen

PC kauft, erwirbt man nur die **Lizenz für EINE Installation**. Wenn ich also in einer VM mein Betriebssystem ein weiteres Mal installieren möchte, muss ich mir eigentlich eine Lizenz erwerben, abgesehen davon, dass man heute in der Regel gar keinen Installationsdatenträger mehr hat und diesen erst kaufen oder herunterladen muss...
Dann musst du mal die Eckdaten deiner VM bestimmen (Speicher, Festplattenbelegung, usw.) und den ganzen Installationsprozess des Betriebssystems durchlaufen und alle notwendigen Programme installieren.
Falls dich das immer noch nicht abgeschreckt hat und du dich für VMs im Detail interessierst, findest du dazu Informationen im Nachschlag!

Hier kommt nun die Sandbox ins Spiel!
Sandboxing ist eine **Form der Virtualisierung** innerhalb deines Betriebssystems, ohne Installation eines weiteren kompletten Betriebssystems. Ein gewisser Speicherbereich im Hauptspeicher deines Computers wird für die Sandbox benutzt, um dort Programme abgeschottet von allen anderen, laufen zu lassen. Wird die Sandbox beendet, wird dieser Speicher gelöscht und alles was du getan hast, kann wieder rückgängig gemacht werden.
Dies funktioniert mit so ziemlich allen Programmen, außer mit Antiviren, Firewall und anderen Sicherheitsprogrammen, da diese recht tief im Betriebssystem verwurzelt sind.
Wenn du also ein Programm heruntergeladen hast und es nur probieren möchtest, ist es sicher eine gute Idee, dies in der Sandbox zu tun, weil es relativ gefahrlos ist und wenn dir das Programm nicht gefällt, musst du es nicht mühsam deinstallieren! Wenn das Programm gefährlich wäre oder sonst was tut, was dir nicht passt, ist nichts vertan.
Mit Hilfe der Sandbox kannst du alles, was du getan hast wieder rückgängig machen, wenn du willst!

Und wo gibt es sowas?
Eigentlich bin ich ja ein Fan von Open Source und Freeware.
Ich habe schon einiges ausprobiert, aber meines Wissens ist das einzige brauchbare Sandboxing-Programm **Sandboxie** http://www.sandboxie.com/, welches leider kommerzieller Natur ist. Man korrigiere mich, falls ich mich irre!
Es kann alles, was nötig ist und kann **selbst nach Ablauf der 30 Tägigen Testlizenz immer noch verwendet werden**. Zwar stehen danach nicht mehr alle Funktionen zur Verfügung, doch für unsere Zwecke reicht das vollkommen aus!
Wenn du vollends von Sandboxie überzeugt bist, oder du die "Kauf mich" Hinweise satt hast, kannst du natürlich auch eine Lizenz erwerben.

Ich denke €30 ist ein recht fairer Preis für eine lebenslange Lizenz (ich bekomme übrigens nichts bezahlt für dieses Kapitel, falls das jemand glaubt) und wahrscheinlich habt ihr schon mal mehr Geld für irgendeinen anderen Blödsinn ausgegeben…

Und wie funktioniert das alles?
Wenn du Sandboxie installiert hast, kommt eine **sehr informative Einleitung**, die du unbedingt lesen und verstehen solltest. Diese erklärt, was eine Sandbox tut und wie sie funktioniert.
Weiters kommt einmal gleich dein Standard-Browser (hoffentlich der Firefox ;)) automatisch in die Sandbox und ein Verknüpfung dazu wird auf dem Desktop abgelegt. Wenn du diese öffnest, geht gleich einmal der Browser in der Sandbox auf und du kannst dich mit der Funktionalität vertraut machen.
Eigentlich merkt man nur am **gelben Rahmen** um das Programm (wenn du mit der Maus über den **oberen Rand** fährst), dass es in der Sandbox läuft.
Im **Infobereich der Taskleiste** hast du jetzt ein Sandboxie Symbol, wo du Kontrolle über deine Sandbox(en) hast. Mit "Inhalte löschen" bekommst du eine Übersicht über alle Änderungen (Dateien, Einstellungen usw.) und du bist in der Lage die eine Datei zu behalten, aber die andere zu löschen!
Du hast alles in der Hand!
Selbst wenn ein Programm irgendwo versteckt Dateien anlegen würde, könntest du das sehen, und natürlich verhindern.
Willst du ein heruntergeladenes Programm in der Sandbox testen, genügt ein Rechtsklick auf diese Datei und ein Klick auf "**in der Sandbox starten**"

Dies ist meiner Ansicht nach die einzige praktikable Möglichkeit für (fortgeschrittene) Laien, um Programme zu testen, bzw. mit einem abgeschottetem Browser zu surfen!
In der heutigen Zeit, wo so viele Gefahren für Rechner im Internet lauern, ist es die einzige Möglichkeit Erfahrungen zu sammeln, ohne sich ständig die Finger zu verbrennen, soll heißen den Rechner komplett zu vermurxen!

Nachschlag:

Parallelinstallation
Es ist möglich, mehrere Betriebssysteme auf einem Rechner zu installieren. Diese können dann beim Start des Rechners ausgewählt werden, es kann aber immer nur eines gestartet werden. Eignet sich, wenn man z.B. zusätzlich zu Windows ein Linux basiertes Betriebssystem installieren möchte. Eine Parallelinstallation hat den Vorteil, dass das System alle System-Ressourcen alleine zur Verfügung hat, dafür muss immer der Rechner heruntergefahren und neu gestartet werden, wenn man damit arbeiten will.

Virtualisierung
https://de.wikipedia.org/wiki/Virtualisierung_%28Informatik%29

Virtuelle Maschinen (VMs)
Wer experimentierfreudig ist und gerne mehr darüber diese Thematik erfahren will, dem kann ich die freie Virtualisierungslösung **Oracle Virtual Box** https://www.virtualbox.org/ empfehlen.
Als Übung kannst du dir hier eine Version von **Knoppix** http://www.knopper.net/knoppix/ herunterladen und versuchen diese in einer VM zu installieren!
Bedenke, dass hier ein **halbwegs schneller Rechner mit viel Hauptspeicher** von Vorteil ist!
Bedenke weiters, dass du wahrscheinlich sehr **viele Beschreibungen** wirst lesen müssen…

Kapitel 19: Die Cloud

In diesem Kapitel geht es um die **Cloud**, wie **Datenspeicher und Rechenzentren im Internet** recht salopp genannt werden.
Es bedeutet in etwa, dass man seine Daten irgendwo im Internet speichern kann und auch Rechenleistung ins Internet ausgelagert werden kann.
Dies bringt natürlich gewisse Vorteile mit sich, aber auch Nachteile, auf die ich näher eingehen werde.

Die Idee dahinter
Das Prinzip ist nicht neu, denn in der Anfangszeit der Computer was es gar nicht möglich einen solchen daheim zu haben, außer man verfügte über eine Lagerhalle, einen industriellen Stromanschluss und einen Riesenhaufen Geld.
Rechner gab es eigentlich nur beim **Militär und in Forschungseinrichtungen**.
Benutzer hatte einen so genannten **Terminal** (grob gesagt ein Monitor mit Tastatur) der abgesetzt vom Rechner mit einem Kabel verbunden war. Man hatte ein Benutzerkonto und bekam einen **gewissen Teil der Rechnerleistung und des Speichers** zuerkannt.
Später wurde die Verkabelung durch einen Netzwerkanschluss, der Terminal durch einen kleinen PC ausgetauscht und man konnte sogar Daten vom Server herunterladen, jedoch die rechenintensiven Teile der Anwendung lagen letztendlich beim Server.
Mit dem **Siegeszug des Personal Computer** erhöhte sich die Rechnerleistung immer mehr und die Server wurden meist nur mehr verwendet, um die Daten zentral speichern zu können. Die Rechenleistung wurde jedoch meist dem lokalen Computer überlassen, da dieser nun über genügend Leistung und Speicher verfügte.
Je nach den technischen Gegebenheiten änderte sich die Philosophie der Client - Server Beziehung und wer welche Aufgaben in welchem Ausmaß übernehmen sollte.
Im Privatbereich gab es damals eigentlich sowieso keinen Grund, Daten wo anders als auf seinem Gerät zu bearbeiten und zu speichern (mangels Internet).

Warum jetzt eigentlich wieder?
Die große Verbreitung von Smartphones, Tablets und ihre Apps gemeinsam mit dem Internet sorgten für eine Renaissance unter dem Namen "**Cloud Speicher**" bzw. "**Cloud Computing**".
Die Idee ist nun, einen zentralen Ort für seine Daten, bzw. hohe Rechenleistung zu haben, auf die ich von jedem meiner Geräte Zugriff habe.
Ich muss mir nun **keine Sorgen mehr um Backup und Datensicherheit** machen, denn das macht alles **der Betreiber der Cloud** für mich, oder? Ich benötige lediglich einen Internetanschluss (ist heute nicht mehr außergewöhnlich) für meine Geräte

und alles ist gut!
Viele Anbieter stellen sogar die Möglichkeit in Aussicht, einfach alles komplett in der Cloud zu speichern…

Ist das eigentlich nicht eh super?
Die Cloud bietet natürlich den Vorteil, **jederzeit an jedem Ort** (mit Internet natürlich) auf meine **Daten zugreifen** zu können. Dies ist jedoch auch **gleichzeitig der Nachteil**, weil die Daten dadurch **nicht mehr alleine in meiner Gewalt** sind.
Passiert an zentraler Stelle ein Fehler, hat dies oft recht weitreichende Auswirkungen und es kann recht schnell zu Datenverlust kommen.
Außer man hat doch noch irgendwo ein Backup der Daten!
In den letzten Jahren gab es einige schwerwiegende Ausfälle bei großen Betreibern, die es sogar in die Medien schafften. Die Daten waren dabei zum Teil unwiederbringlich verloren und das, obwohl die Betreiber bestimmt sämtliche Maßnahmen zur Datensicherung berücksichtigt haben.

Leider ist die **Datenmenge oft schon so groß, dass eine Wiederherstellung in einer vernünftigen Zeit (Stunden) gar nicht mehr möglich ist!**
Sollte jemand von Daten in der Cloud beruflich abhängig sein, so kann dies sogar bis zum Bankrott führen, denn fast niemand kann sich heute einen tagelangen Ausfall leisten.
Mit steigender Menge der Daten, die ich in die Cloud lege, steigt auch das Risiko und die Abhängigkeit vom Anbieter.

Risiko für Firmen
Momentan ist es Mode, die **eigene Server-Infrastruktur zu verkleinern**, und alles in die Cloud auszulagern. Sämtliche Office Anwendungen können heutzutage **komplett online bedient** werden, was Vorteile, aber auch Nachteile mit sich bringt.
Zum einen ist es meiner Meinung nach **moralisch verwerflich**, da für die Firmen eigentlich nur die **Vergrößerung des Profits durch Verringerung des Personals** im Vordergrund steht. Denn wenn man die ganze Office-IT in die Cloud legt, braucht man nur mehr für die Dienstleistung an sich zu bezahlen, braucht aber **keine eigenen Server, keinen Platz dafür und auch kein Personal**.
Für viele Firmen ist dies eigentlich bereits schon Grund genug, dies so schnell wie möglich umzusetzen, obwohl die **Auslagerung aller Daten einer Firma datenschutzrechtlich äußerst bedenklich ist**.
Weiters macht man sich **total vom Internet abhängig**, da bei einem Ausfall eventuell gar nichts mehr gearbeitet werden kann...
Auch andere wichtige Fragen stellen sich:
Was ist nach Ablauf des Vertrages? Wenn das Service dann doch viel mehr kostet? Was passiert, wenn der Dienst eingestellt wird? Was passiert dann mit den Firmendaten? Wie bekommt man die Daten wieder? Wem gibt man die Daten als nächstes, weil es gibt ja keine eigene Infrastruktur mehr, auf die man sie speichern

kann? Sind die Dienste miteinander kompatibel? Was passiert bei einem Ausfall, wie schnell ist alles wieder verfügbar? Was ist, wenn die Daten zerstört werden, wie schnell können sie wiederhergestellt werden?
Nun, man sieht recht schön, dass es **außer des Einsparungspotentials auch noch andere Dinge zu berücksichtigen** gibt!

Risiko für Privatpersonen
Die Cloud ist natürlich auch für Privatpersonen eine Option. Die meisten Anbieter verdienen ihr Geld sowieso mit Großkunden und "verschenken" ihr Service für Privatpersonen, z.B. indem nur eine gewisse Kapazität verfügbar ist.
Die meisten Leute denken, dass dies eine **gute Methode ist, um gewisse Daten "in Sicherheit"** zu wissen, bzw. dass dies quasi ein Backup der Daten ersetzt. Doch leider ist das nur eine **trügerische Sicherheit**, denn man ist vor Datenverlust nicht gefeit, wie ich auch schon am eigenem Leib erfahren musste. Weiters muss man bedenken, dass man möglicherweise **private, vertrauliche oder sensible Informationen im Internet ablegt und das meist noch unverschlüsselt**.
Eine weitere Krankheit ist **das Passwort vergessen** (was euch ja hoffentlich nicht mehr passieren kann), denn ein Konto für einen Cloud-Dienst ist recht schnell angelegt. Am Rechner läuft die Software mit gespeichertem Passwort und solange dieser OK ist, hat man auch kein Problem.
Außer der PC wird von heute auf morgen kaputt und man hat keinen Zugriff mehr auf die Dateien.
Hat man nun wichtige Daten in der Cloud gespeichert, **sind sie zwar grundsätzlich noch da**, wenn man aber das Kennwort nicht mehr weiß, ist guter Rat teuer…

Wer hat aller Zugriff?
Eine weitere Frage ist wie immer, wer außer mir noch Zugriff auf die Daten hat.
Wie in einigen vorherigen Kapiteln besprochen kann es natürlich sein, dass meine Daten auch missbräuchlich verwendet werden können, von wem auch immer.
Weiters steigt das Risiko eines Datenverlustes durch Hackerangriffe, da solche Rechen und Daten-Zentren für böse Hacker natürlich ein wunderbares Ziel mit schier unendlichen Möglichkeiten darstellen!

Was kann man tun?
Nun, da es auch Vorteile bietet, habe ich selbst auch Daten in der Cloud. E-Mails, Bilder, Projekte, usw. sind dadurch für mich überall und jederzeit erreichbar.
Jedoch achte ich darauf, dass **sensible Informationen** (z.B. Passwörter und persönliche Dokumente) **nur verschlüsselt** gespeichert sind und von sämtlichen Daten auch ein **regelmäßiges Backup** gemacht wird.
Ich bin dadurch **nicht von der Cloud abhängig**, d.h. wenn der Service versagt, kompromittiert oder beendet wird, existieren meine Daten trotzdem unbeschadet weiter.

Für Daten in der Cloud gilt: Wenn es unverschlüsselt gespeichert wird, dann nur Informationen, die du auch in einer Fußgängerzone an Wildfremde verteilen würdest!

In den richtigen Händen kann eine Cloud Anwendung sinnvoll und gut sein, so viel steht fest. Jedoch sollte man wie immer **Vorsicht walten lassen** und sich nicht zu sehr davon abhängig machen!
Ein **Backup** ist sowieso unerlässlich, auch wenn eh alles in der Cloud ist.
Manchmal ist vielleicht auch zu bedenken, **welche Daten** wirklich überall und jederzeit zur Verfügung stehen müssen…

Nachschlag:
Ich mache in meinen Ausführungen keinen Unterschied zwischen Speichern von Daten und Auslagerung von Rechenleistung, da heute meist beide recht großzügig als Cloud bezeichnet werden.

File Hosting
https://de.wikipedia.org/wiki/Filehosting
https://de.wikipedia.org/wiki/Online-Datensicherung

Cloud Computing
https://de.wikipedia.org/wiki/Cloud_Computing

Wer sich mit Verschlüsselung von Daten vertraut machen will, dem empfehle ich **Veracrypt** https://veracrypt.codeplex.com/, den Nachfolger der bekannten Verschlüsselungssoftware **Truecrypt**. https://de.wikipedia.org/wiki/TrueCrypt
Folgendes sei aber gleich gesagt, es ist eine sehr, sehr umfangreiche Materie…

Kapitel 20: Juhu! Ich bin endlich sicher!

Wahnsinn, das ist das zwanzigste Kapitel, du hast es geschafft!
Nachdem du alle Kapitel und die dazugehörigen Portionen des Nachschlags brav gelesen hast, bist du jetzt endlich sicher unterwegs im Internet!
Juhu!

Als aufmerksamer Leser ist dir sicher klar, dass das leider nicht wahr sein kann, denn **es gibt keine wirkliche Sicherheit. Das ist das einzig sichere!**
Alles was ich hier aufgeschrieben habe ist nur ein Standardschutz, denn zu 100% sicher ist ein Rechner nur, wenn er ausgeschalten ist und bleibt!
Klingt blöd, ist aber so.

Alle hier aufgeführten Schutzprogramme haben garantiert Fehler, und sind wahrscheinlich angreifbar. Es muss sich nur jemand die Mühe machen und die Fehler finden. Und tatsächlich sind Menschen ständig auf der Suche nach Schwachstellen, oder finden diese vielleicht zufällig.

Die Guten verständigen die Hersteller. Diese könnten dann agieren und den Fehler ausbügeln, was sie leider nicht immer (gleich) tun.
Oftmals verstreichen viele **Monate(!)**, manchmal sogar **Jahre (!!)** bis bekannte, oft kritische Sicherheitslücken von den Herstellern ausgebessert werden. Oftmals reicht es den Guten dann auch irgendwann und sie **drohen mit der Veröffentlichung der Schwachstelle** im Internet, weil dies oft der einzige Weg ist, ein Unternehmen zu einer Aktion zu bewegen.

Die Bösen verständigen niemanden. Sie horten diese Schwachstellen, um sie für ihre nächste Attacke zu verwenden. Diese Schwachstellen nennt man dann **Zero-Day-Exploit**, weil der Hersteller 0 Tage Zeit hat, sich eine Lösung für das Problem zu überlegen.

Aus Erfahrung weiß man, dass es **oft die großen Hersteller** sind, die sich mit der Bereitstellung eines Patches für die betroffene Software recht lange Zeit lassen. Und das obwohl besagte Firmen oft Heerscharen von Programmierern angestellt haben.
Doch diese Firmen **wägen einfach die Kosten gegen das Risiko** ab und das Risiko für eine große Firma ist in diesem Fall halt relativ klein.
Kleine Firmen können sich ein solches Gebaren nicht leisten, denn schließlich geht es um **den guten Ruf!**
Open Source Communities lassen meist auch nicht lange auf eine Lösung von gravierenden Problemen warten, denn auch hier geht es um den guten Ruf.
Außerdem geht es **um den Stolz** der Programmierer, denn niemand möchte sein Werk fehlerbehaftet wissen…

Eigentlich müsste man ob der vielen Gefahren der Windows Welt den Rücken kehren und sich **um eine Alternative umsehen**. Doch leider ist dies aus diversen Gründen oft nicht möglich.
Ich verstehe auch warum, denn es gibt viele Prügel, die einem da in den Weg geworfen werden.
Sei es die **berufliche Abhängigkeit** von gewissen Softwareprodukten, oder einfach nur das **aufgebaute Wissen** über Windows, oder vielleicht weil **alle Leute die man kennt, nur Windows verwenden.**
Windows hat sich eben als Desktop Betriebssystem für die meisten durchgesetzt, denn Microsoft hatte die geniale Idee eine **Lizenz für ihre Software gemeinsam mit Geräten eines Marktführers von PC Hardware zu vertreiben**.
Das war der Grund für die rasende Verbreitung.
Wer sich ein Gerät kaufte, hatte Microsoft **automatisch an Bord** und die Hersteller anderer Betriebssysteme und Software haben leider den Startschuss im Dornröschenschlaf verpasst.
Für Firmen ist die große Verbreitung sogar teilweise ein Grund dafür, um Windows zu verwenden, weil der **Einschulungsaufwand relativ klein** ist, da jeder Windows kennt. Paradoxerweise gilt dies auch umgekehrt, denn viele verwenden zuhause Windows, weil sie es von der Arbeit kennen ;)

Für mich selbst bestehen solche Probleme nicht, denn ich muss mich von Berufswegen mit relativ vielen unterschiedlichen Betriebssystemen auseinandersetzen. Daher habe ich auch bereits vor Jahren den Entschluss gefasst, privat von Windows weg zu gehen.
Dies hat mich **relativ viel Vorbereitungsarbeit** gekostet, weil ich mich vorab schon Informiert habe, wie ich die von mir verwendete Software sinnvoll ersetzen kann.
Doch das ist für die meisten Leute einfach nicht möglich, weil sie **weder die Zeit noch das notwendige Wissen** dafür haben und so bleibt ihnen halt nichts Anderes übrig, als weiterhin dabei zu bleiben.

Dies soll auch absolut kein Ratschlag sein, auf ein anderes System zu wechseln, denn auch hier müsste man **immer Vorsicht walten lassen**.
Es würde sich auch nichts an den Gefahren ändern, denn die Rechnung ist einfach: **Würden alle was anderes verwenden, dann wäre dies das Ziel der bösen Buben.**
Das einzig wirklich wirksame wäre **eine gute Mischung**, aber das ist leider nur eine Utopie.
Eines wird sich immer gegen alle andere durchsetzen können und das ist dann der Marktführer und dieser wird auch die Prügel einstecken müssen!
Dies wird auch so lange sein, so lange wir in einer **marktorientierten Wettbewerbsgesellschaft** leben…

Zum Abschluss noch ein Gleichnis:
Es ist falsch zu behaupten, dass wenn du einen Regenmantel an hast, du auch gegen Meteoriteneinschläge geschützt bist.
Ein Regenmantel schützt dich eben nur vor Regen und das auch nicht ewig, denn irgendwann wirst du trotzdem nass...
Wenn du aber aufpasst und auch hin und wieder den Blick schweifen lässt, kannst du vielleicht den Meteoriten schon von weiten kommen sehen und ihm möglicherweise auch ausweichen!

Nachschlag:
Exploit
https://de.wikipedia.org/wiki/Exploit

BSI für Bürger
https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html

Bleib Virenfrei
https://www.bleib-virenfrei.de/

Kapitel 21: Diese Seite verwendet Cookies

Vielleicht ist es euch ja auch schon aufgefallen: Beim Besuch von manchen Webseiten bekommt man über dem Inhalt eine lustige Warnung präsentiert, die so oder ähnlich lautet:

> „*Diese Website verwendet Cookies von [BLA BLA BLA], um ihre Dienste bereitzustellen, Anzeigen zu personalisieren und Zugriffe zu analysieren. Informationen darüber, wie du die Website verwendest, werden an [BLA BLA BLA] weitergegeben. Durch die Nutzung dieser Website erklärst du dich damit einverstanden, dass sie Cookies verwendet.*“

Wie ich nun herausgefunden habe, handelt es sich dabei um die **Umsetzung einer total wichtigen EU Regulierung**, nach welcher ein Internet User explizit zustimmen muss, dass auf seinem Rechner Cookies gespeichert werden.

Scheinbar halten sich viele große Anbieter (Google zum Beispiel) an diese Regel und präsentieren nun eine Warnung, die nur mit dem Drücken von „OK“ verschwindet.

Automatisch blockierte Cookies
Wenn man aber Cookies automatisch blockiert oder löscht, bekommt man diese Meldungen bei jedem Besuch der Seite.
Da ihr als brave, aufmerksame Leser vermutlich auch einen **Adblocker und Ghostery** verwendet, werden diese Meldungen immer wieder kommen; Es handelt sich dabei nämlich meistens um so genannte **Tracking Cookies**, die dazu verwendet werden, den Besucher wieder zu erkennen und sein Benutzerverhalten zu speichern.
Ghostery sollte bei richtiger Einstellung solche Cookies eigentlich blockieren…

Blödsinn
Die Vorgehensweise, die Benutzer permanent mit solchen Meldungen zu bombardieren, ist meiner Meinung nach abzulehnen, weil man so dazu verleitet wird, ohne nachzudenken auf „OK“ zu drücken, weil einem solche Meldungen auf die Nerven gehen.
Ignoriert man die Meldung, bleibt sie immer über der Webseite kleben und verschandelt so das Layout der Seite, was dann (wahrscheinlich gewollt) genau dazu führt, doch irgendwann auf „OK“ zu drücken, um die ewigen Meldungen los zu werden.

Was kann man dagegen tun?
Ich bin bei meinen Recherchen auf die Seite http://www.kiboke-studio.hr/i-dont-care-about-cookies/ gestoßen, wo genau für diese Problematik Abhilfe geschaffen wird. Man kann sich entweder eine Browser Erweiterung installieren, die in Zukunft solche Meldungen unterdrückt, oder einen Filtersatz für unseren Adblocker, der im Prinzip das gleiche macht.
Die von mir empfohlene Firefox Erweiterung **uBlock Origin** kann das übrigens auch, man muss diese Option nur aktivieren:
Dashboard > Vorgegebene Filter > EU: Prebake - Filter Obtrusive Cookie Notices

Mir persönlich gefällt die Filterliste für den Adblocker recht gut, da man sich so keine zusätzliche Erweiterung installieren muss, aber das ist freilich Geschmackssache. Grundsätzlich wäre zu sagen, dass zu viele Erweiterungen den Browser verlangsamen können, zu viele Filterlisten im Adblocker allerdings auch; Ihr müsst das selbst abwägen, was für euch die bessere Lösung ist!

Nachschlag:
https://de.wikipedia.org/wiki/HTTP-Cookie#Tracking

Kapitel 22: Daten sicher löschen

Nicht alles was du auf deinem Rechner löschst, ist auch tatsächlich weg.
Das heißt, wenn du bei einer Datei auf löschen drückst, wandert sie zunächst in den Papierkorb. Dort verweilt sie, bis du den Papierkorb leerst, oder du sie wieder herausholst.
Wenn du den Papierkorb dann ausleerst, sind die Dateien zwar für dich verschwunden, jedoch immer noch auf deiner Festplatte, da **nur der Verzeichniseintrag gelöscht wurde, nicht aber die Datei selbst!**
Auch das formatieren von Festplatten ist nicht immer eine sichere Lösung, wie ich noch aufzeigen werde…
Daher geht es in diesem Kapitel um das sichere Löschen von Daten auf deinem PC bzw. USB Stick, externe Festplatte und dergleichen.

Was hat das mit Sicherheit im Internet zu tun?
Nun, es hat mit dem Internet direkt nichts zu tun, jedoch sieht die Sache ganz anders aus, wenn man sein Gerät verkaufen oder entsorgen möchte. Denn auf jedem PC befinden sich **IMMER** eine Menge persönlicher Daten.

Ist mir doch Wurscht
Auch wenn man denkt, auf seinem System befindet sich nichts wichtiges, ist das meistens eine Fehleinschätzung. Auf einem PC befinden sich viele interessante Daten, wenn man weiß, was man damit anfangen kann. Alleine wenn ich darüber nachdenke, wie ein Fremder meine Mails liest, läuft mir ein kalter Schauer über den Rücken, auch wenn sich in meinen E-Mails keine moralisch verwerflichen Daten befinden ;)

Was man alles auf einem Computer finden könnte:

*** Persönliche Daten**
Viele Leute verwenden Outlook oder ähnliche E-Mail Programme. Daher ist das Programm dementsprechend konfiguriert und hat ziemlich sicher das Passwort deines Mailkontos auf dem Rechner gespeichert.
Hoffentlich verschlüsselt, aber das ist eigentlich egal, denn wenn jemand einfach dein Mailprogramm startet, kann derjenige deine Mails abrufen!
Und nicht nur das. auf diesem Wege könnte man versuchen bei vielen anderen Konten (Social Media, Instant Messenger, Online Speicher, Ebay, usw.) das Kennwort zurückzusetzen, da man ja dann das Mail mit dem dementsprechenden Kennwort-zurücksetzen-Link empfangen kann!

Aus Emails könnte jemand, auch wenn keine Zugangsdaten gespeichert wurden, trotzdem recht einfach Zugang zu deinen Systemen erlangen. Da Tier oder Kindernamen, Namen des Partners, Geburtstage und der gleichen oft als Kennwort für alles Mögliche verwendet werden, ist dies ein Einfallstor für geknackte Passwörter aller Art.

*** Passwortlisten im Klartext**
Manche Leute speichern sich alle möglichen Zugangsdaten und Passwörter in ein Textdokument auf ihrem Computer ab und "verstecken" diese Datei dann irgendwo auf der Festplatte. Habe ich selbst gesehen. Könnt ihr das Klatschen meiner Hand auf meiner Stirn hören? Für diesen Zweck gibt es einen Passwort-Tresor. Ihr erinnert euch vielleicht an **KeePass?**

*** Fotos und Videos**
Bitte, es geht hier gar nicht um peinliche Fotos, Nacktfotos oder gar Privat-Pornos. Wenn jemand dein Aussehen kopieren würde, und viel über dich weiß (wegen deiner Mails), könnte der oder diejenige damit schon einiges anstellen. Du würdest staunen, wie dreist Identitätsdiebe sind und wie wenig ähnlich dir jemand sehen muss, um trotzdem als du durchzugehen…

Deswegen sicher Löschen
Ich denke, wir sind uns nun einig: Wenn du einen Rechner verkaufen oder wegwerfen willst, musst du deine Daten unbedingt löschen, und zwar nicht nur die "Eigenen Dateien" sondern wirklich ALLES.
Fest steht, wenn du deinen Rechner nur neu aufsetzt und die Festplatte gewöhnlich formatierst, sind die Daten nicht richtig weg!

Und ab hier wird es ein wenig technisch…
Beim schnellen Formatieren (Standardeinstellung) wird eigentlich nur das gesamte "Inhaltsverzeichnis" der Festplatte gelöscht, die Daten liegen noch unangetastet herum. Mit der Gratis Software **PC Inspector File Recovery** ist es möglich, ziemlich alles was gespeichert war, wiederherzustellen!
http://www.pcinspector.de/default.htm
Daher sollte man unbedingt die langsame Formatierungsmethode verwenden, um die vorhandenen Dateien wirklich zu überschreiben.
Bei älteren magnetischen Datenträgern (Herstellungsdatum vor 2001) von geringerer Kapazität (< 15 Gigabyte) konnten Daten, die vor dem Überschreiben auf der Platte waren, immer noch wiederhergestellt werden!
Dazu war zwar Spezial Software und auch Hardware vonnöten, aber es war theoretisch noch möglich.

Heutzutage ist die Datendichte auf den Magnetplatten so hoch, dass nach dem einmaligen Überschreiben beim langsamen Formatieren quasi nichts mehr zu retten ist.

Bei SSD (Solid State Drive) Festplatten sieht es anders aus, hier gibt es von Haus aus keinen Restmagnetismus, den man ausnützen könnte. Ein einmaliges vollständiges Überschreiben mit Zufallsdaten reicht normalerweise aus, damit die Daten zerstört sind.
Normalerweise deswegen, weil eine SSD in Wirklichkeit mehr Speicher hat, als draufsteht. Dies ist notwendig, weil die Speicherzellen nicht endlos überschrieben werden können und der Festplattencontroller automatisch die Belegung des Speichers rotiert um eine gleichmäßige "Abnützung" und eine längere Lebensdauer des Mediums zu erreichen. Auch hier könnte man mit Spezialsoftware Daten wiederherstellen.

Man kann sich nicht mehr den eigenen Ast absägen…
Ein weiteres Problem ist, dass man nicht die gesamte Platte während des Normalbetriebs löschen kann, weil sich ja das Betriebssystem darauf befindet. Moderne Betriebssysteme lassen es mittlerweile nicht mehr zu, dass du den Ast auf dem du selbst sitzt absägen kannst…

Auf Werkseinstellung zurücksetzen
Viele aktuelle Geräte haben bereits einen integrierten Wiederherstellungsmodus, mit dem der gesamte Rechner wieder in den Auslieferungszustand gebracht werden kann, inklusive sicheren löschen.
Leider hat man als Normalsterblicher keine Kontrolle darüber, wie "sicher" diese Methode ist…
Deswegen müssen wir, wenn wir ganz sicher sein wollen, wieder ein wenig in die Trickkiste greifen…

Boot Medium
Für das totale löschen einer in einem Gerät verbauten Platte empfehle ich Dariks Boot and Nuke, kurz **DBAN**. https://sourceforge.net/projects/dban/files/dban/
Die Vorgehensweise ist ähnlich wie bei einem Antivirus Boot-Medium.
Du lädst dir die ISO Datei der letzten Version herunter und brennst sie auf eine CD, oder einen USB Stick. Wenn du dann von der CD startest, kannst du die Festplatte auswählen und mit verschiedenen Optionen löschen.
Grundsätzlich sollte ein **einfaches überschreiben mit Zufallsdaten** ausreichend sein, egal ob bei HDD oder SSD Platten.
Dies kann abhängig von Kapazität, Geschwindigkeit und Art der Platte einige Stunden bis Tage dauern.

ACHTUNG: Dies löscht die komplette Festplatte Ratzeputz, inklusive aller Rettungspartitionen! Wenn du keine Installations-DVD hast, kannst du den Rechner

danach nicht mehr in den Auslieferungszustand zurücksetzen!
Daher nur verwenden, wenn du den Rechner wegwerfen, oder ohne Betriebssystem verkaufen willst!

Für den täglichen Gebrauch
Für einzelne Dateien oder nicht Systempartitionen und externe Laufwerke (USB-Sticks oder Festplatten) empfehle ich das Programm **Eraser**. http://eraser.heidi.ie/
Damit kann man bequem Dateien sicher löschen und sogar automatische Löschaufgaben planen.
Aber Vorsicht ist geboten, wenn du mit sensiblen Daten arbeitest. Denn es werden nur die ausgewählten Dateien gelöscht, nicht aber die temporären Dateien, die Programme wie z.B. Microsoft Word und viele andere während des Bearbeitens anlegt und danach wieder "löscht". Es handelt sich dabei im Prinzip um versteckte Kopien deiner Dateien mit anderem Namen.
Um solche gänzlich los zu werden muss man den unbelegten Speicherplatz der Platte löschen, was mit Eraser ebenfalls möglich ist.
Mehr Informationen in der Beschreibung http://eraser.heidi.ie/help/

Physische Vernichtung
Wer allerdings komplett auf Nummer Sicher gehen will, muss schon zu drastischeren Methoden greifen.
D.h. der Datenträger wird richtig zerstört und damit meine ich entweder Shreddern oder noch besser schmelzen. USB Sticks kann man übrigens leicht mit einigen Hammerschlägen zerstören.

CDs und DVDs
Auch selbst gebrannte Medien, die als Datensicherung dienen, sollten nicht einfach weggeworfen, sondern auch unbrauchbar gemacht werden. Am besten eignet sich dazu ein Mikrowellenofen, einige Sekunden und einige Blitze später ist die CD oder DVD zerstört. Ich muss nicht extra auf die Brandgefahr hinweisen, oder?
Ansonsten wäre auch Shreddern angesagt.

Ist das nicht alles sehr kompliziert und auch recht paranoid?
Es mag vielleicht so erscheinen, jedoch haben mich schlechte Erfahrungen (meistens die anderer) gelehrt, mit gespeicherten Daten immer vorsichtig umzugehen.

Daher rate ich bei Weitergabe von PC, Notebook, Festplatte, usw. an dritte diese gründlich zu löschen, um Datenmissbrauch vorzubeugen!
Möglicherweise kann dir auch ein sachverständiger Freund dabei helfen, wenn du dich selbst nicht so recht heraussiehst ;)

Nachschlag:
https://de.wikipedia.org/wiki/Social_Engineering_(Sicherheit)
https://de.wikipedia.org/wiki/Identit%C3%A4tsdiebstahl
https://de.wikipedia.org/wiki/Festplattenlaufwerk
https://de.wikipedia.org/wiki/Solid-State-Drive
https://de.wikipedia.org/wiki/Datenvernichtung

Kapitel 23: Kurz URLs

Meine braven Leser werden bestimmt wissen, was ein **URL** ist, oder?
Zur Auffrischung, URL bedeutet **Uniform Resource Locator** und ist die eindeutige Internetadresse zu einem Dokument im Internet.
Außerdem sehen wir uns ja sowieso jeden Link, den wir in Browser anklicken vorher etwas genauer an, oder?

Vielleicht ist euch aufmerksamen Internetbenutzern schon aufgefallen, dass es **total kurze Internetadressen** wie diese gibt:
http://goo.gl/uQ8g4R
oder
http://bit.ly/29ukqtz

Das sind gekürzte URLs von unterschiedlichsten Internetservices um lange URLs wie z.B. http://meinelustigeinternetseite.com/blabla/blablabla/nochmehrblablabla/undnochmehrblablabla/jetztkommtendlichdieseite.html zu kürzen.
Aus verständlichen Gründen, denn wer möchte so eine lange URL eintippen?
Auch der verbreitete Einsatz von Smartphones (kleinere Displays) und Kurznachricht-Dienste wie Twitter oder Facebook und dergleichen, haben den Einsatz von Kurz URLs sogar teilweise notwendig gemacht. Hier geht es schließlich um die Kürze der Nachricht.
Mit den Kurz-URL-Services ist man somit in der Lage, diese Probleme zu lösen.

Wie funktioniert das?
Im Prinzip ist es recht einfach: Der Anbieter des Kurz-URL-Dienstes speichert die tatsächliche URL in seiner Datenbank und übersetzt ab sofort die generierte Zahlen-Buchstaben-Wurst und leitet den Benutzer der kurzen URL auf das Ziel der langen URL um.

Das ist ja eigentlich voll praktisch!
Natürlich ist sowas total praktisch, auch ich habe bereits solche Dienste in Anspruch genommen.
Aber: Was wäre, wenn ich diesen Link http://malwareseite.com/virus.exe als diesen http://alturl.com/n5imd "tarnen" würde?
Dieses Prinzip ist in der Vergangenheit schon oft genutzt worden, um bekannte gefährliche URLs zu verschleiern, bzw. auch um Mail-Virenscanner, die eigentlich Links zu ausführbaren Dateien löschen sollten, zu verwirren.

Natürlich gibt es noch einen Nachteil: Wenn der URL-Kürzer seine Dienste beendet, sprich es gibt die Seite nicht mehr, ist es unmöglich, die tatsächliche URL jemals wieder herauszufinden! Das ist zwar ärgerlich, aber wenigstens ungefährlich.
Aber man stelle sich vor, jemand hackt sich in so ein System und manipuliert die

Datenbank des Kurz-URL-Services. Ich glaube, ich muss nicht extra darauf hinweisen, dass dies recht katastrophale Auswirkungen hätte.

Was kann man dagegen tun?
Manche dieser Kurz-URL-Dienste bieten an, das Ziel anzeigen zu lassen, bevor man auf die tatsächliche Seite geht. Es gibt aber **zig solche Dienste** und es ist total lästig, jedes Mal vorher auf deren Seite zu gehen, um das Ziel zu überprüfen. Deswegen gibt es auch Seiten, die recht viele unterschiedliche gekürzte URLs auf einmal überprüfen können.
http://checkshorturl.com ist so eine Seite, auf der man sich das Ziel der Kurz-URLs übersetzen lassen kann.
Eine weitere Möglichkeit ist die URL auf **http://virustotal.com** überprüfen zu lassen, denn auch hier gibt es einen URL Tester. Es wird zwar nicht angezeigt, wohin die URL führt, dafür aber mit welchen Gefahren man rechnen muss, wenn man die Adresse besucht.

Tipps für Webseiten Betreiber
* Es ist eine gute Idee, sich bei der Auswahl des Seitennamens für etwas relativ kurzes zu entscheiden.
http://trockenlegung.at ist OK, http://www.atg-mauerwerks-trockenlegung.at (mein Lieblingsbeispiel) ist nicht OK.
* Keine zu tief verschachtelte Seitenstruktur. http://meineseite/unterseite ist OK. http://meineseite/unterseite/nocheineunterseite/nocheineunterseite/undnocheineunterseite ist nicht OK.
* Verwendet besser keine Kurz-URL-Dienste um URLs zu kürzen. Bleibt transparent! Seiten mit zu vielen Kurz-URLs werden üblicherweise als unseriös betrachtet.

Seid gewarnt!
Gebt **IMMER** acht und denkt nach, **BEVOR** ihr auf einen Link klickt.
Egal ob gekürzt oder nicht...
Das erspart viel Ärger!

Nachschlag:
https://de.wikipedia.org/wiki/Uniform_Resource_Locator
https://de.wikipedia.org/wiki/Kurz-URL-Dienst

Kapitel 24: Adobe Flash

In diesem Kapitel möchte ich mein Leser auf die **Gefahren von Adobe Flash** hinweisen. Es handelt sich dabei um ein Plugin für den Browser, der es ermöglicht **Animationen abzuspielen**.
Dieses Produkt existiert seit dem Jahr 2003 und hieß einst Macromedia Flash und wurde 2007 von der Firma Adobe (bekannt durch Photoshop, Adobe Reader u.a.) gekauft und weiterentwickelt.

Alles was bunt ist
Teilweise wurden ganze Internetseiten mit dieser Technik entwickelt, vor allem solche, die recht bunt mit vielen bewegten Objekten und anderen, für den Inhalt der Seite nicht wichtigen Elementen, versehen sind.
Viele **Online-Spiele** bauen auf Adobe Flash auf und benötigen das Plugin um zu funktionieren.
Auch **Werbung** basiert oft auf Flash, da ja hier oft animierte Inhalte zur Anwendung kommen.
Mittlerweile gibt es schon seit einiger Zeit **HTML5**, ein **Webstandard** welcher ebenfalls animierte Objekte generieren kann und von den allen modernen Browsern unterstützt wird. Dies sollte in absehbarer Zukunft Adobe Flash ersetzen, wie ich hoffe. Viele Internetportale wie z.B. YouTube haben schon reagiert und unterstützen bereits seit geraumer Zeit HTML5 und benötigen Flash nicht mehr zwingend.

Was ist denn so gefährlich an Adobe Flash?
An sich ist das Plugin harmlos, denn es tut genau das was es soll, es zeigt animierte Inhalte, bzw. Videos an. Auch die Firma Adobe ist grundsätzlich vertrauenswürdig. Leider ist Flash seit einiger Zeit eine Art "Stiefkind" von Adobe, denn es gab die letzten Jahre schon **mehrmals aktiv von Hackern ausgenutzte Sicherheitslücken**, so genannte Zero Day Exploits.
Obwohl der Firma Adobe bekannt, wurden oder konnten diese Sicherheitslücken **nicht zeitnahe geschlossen** werden und man lief Gefahr, sich im Internet relativ leicht Malware einzufangen.
Es wurden auch einige Male mehrere Sicherheitslücken geschlossen, dafür aber neue aufgerissen, die danach bald ebenfalls zu Zero Day Exploits wurden.
Das Problem ist, dass Flash auf **relativ viele Ressourcen des Betriebssystems** Zugriff hat, bzw. erlangen kann. Nicht nur Audio (Ein- so wie Ausgänge!) und Video kann gesteuert werden. Was viel schlimmer ist, es kann teilweise auf das Dateisystem des Rechners zugegriffen werden. Ist das Flash Plugin fehlerhaft, könnte der Angreifer auch Dateien manipulieren, auf die Flash normalerweise nicht zugreifen dürfte und somit den ganzen Computer unter seine Kontrolle bringen.

Deinstallieren hilft
Sicherheitsexperten rieten in der Vergangenheit häufig, das Flash Plugin zu deaktivieren, bzw. zu deinstallieren, um die Gefahr einer Verseuchung zu bannen. Das Problem ist nur, der "normale" Nutzer hört oder liest eher wenig von IT-Sicherheitsexperten und bekommt gar nicht mit, was los ist und warum. Meine Leser ausgenommen ;)
Leider ist es auch manchmal so, dass man von Flash sogar beruflich abhängig ist. Denn es gibt relativ viele webbasierende Programme, die auf Flash aufbauen, bzw. Flash benötigt um richtig zu funktionieren. Dann kann man nicht so einfach das Plugin deinstallieren, weil man sonst nicht mehr arbeiten kann.
Fakt ist, Adobe Flash ist veraltet und gefährlich, man sollte es tunlichst nicht mehr verwenden.
Dies betrifft uns User, sowie auch Web-Entwickler, die auf diese sterbende Technologie besser nicht mehr setzen sollten!

Firefox hat Flash schon öfter blockiert
Vielleicht ist es meinen Lesern, die ja hoffentlich Mozilla Firefox zum Surfen verwenden, sogar schon aufgefallen, dass das Flash Plugin manchmal automatisch deaktiviert wurde. Und zwar weil es veraltet war und eines Sicherheitsupdates bedurfte. Flash versagte dann den Dienst und das Plugin musste für jede Seite mit Flashinhalten separat aktiviert werden. Dies hatte den Sinn, dass eine böse Seite einem kein Schadprogramm unterjubeln konnte, indem es präparierten Flash-Inhalt anbot.
Zukünftige Releases von Mozilla Firefox werden sogar Flash von Haus aus blockieren. Man wird es zwar weiterhin benutzen können, wird jedoch darauf hingewiesen, dass man sich in Gefahr begibt, wenn man Flash benutzt.

Was also tun?
Ich würde jedem, der von Flash nicht beruflich abhängig ist raten, das Plugin bald zu deinstallieren, da es relativ gefährlich ist.
Wer nur online Spiele spielt, sollte sich vielleicht um Alternativen die mit HTML5 laufen umsehen. Dies gibt es auf alle Fälle. Ich denke, man sollte nicht die Sicherheit seines Rechners wegen ein paar primitiven Spielen "aufs Spiel" setzen.
Wenn man von Flash-basierender Software beruflich abhängig ist, sollte man sich rasch um eine Alternative umsehen. Dies ist zwar bestimmt mit Kosten verbunden (wegen Kauf oder Upgrade von Software). Dies ist aber sicher billiger, als ein Totalausfall wegen durch Virenbefall unbenutzbarer Rechner.

Totgesagte leben länger

Leider wird auch Adobe Flash das Schicksal einer **Zombie Software** ereilen, so ähnlich wie der **Internet Explorer 6**, der auch nicht tot zu kriegen ist. Obwohl es seit 2014 keine Updates für IE6 gibt, ist er aber immer noch im Umlauf, da es ja auch noch viele PCs gibt, die unter Windows XP laufen, welches auch keine Updates mehr erfährt.

Bei Adobe Flash wird es wahrscheinlich ähnlich sein, denn viele Leute wissen ja gar nicht, was auf ihrem Rechner installiert ist...

Nachschlag:

http://www.heise.de/newsticker/meldung/Firefox-blockt-ab-August-Flash-teilweise-3274488.html
https://de.wikipedia.org/wiki/Adobe_Flash
https://de.wikipedia.org/wiki/Exploit#Zero-Day-Exploit
https://de.wikipedia.org/wiki/HTML5
https://de.wikipedia.org/wiki/Internet_Explorer#Version_6

Kapitel 25: Elektronische Wahl

Normalerweise schreibe ich nicht über Politik, aber in diesem Fall möchte ich eine Ausnahme machen.
Nach dem nun bei der **Bundespräsidentenwahl 2016 in Österreich**, sagen wir mal ganz salopp, viel Scheiße passiert ist, werden nun Stimmen aus der [Zensiert, Name der Partei jedoch der Redaktion bekannt] laut, die statt der Briefwahl ein elektronisches Wahlsystem (E-Voting) vorschlagen.

Nun, dies ist gelinde gesagt, eine Schnaps-Idee

Selbst und geheim
Das größte Problem, welches die Gegner von E-Voting erschnüffeln, ist das Problem, dass nicht festgestellt werden kann, ob der Wähler auch tatsächlich selbst und wirklich geheim wählt!
Um es mit auch für junge Menschen verständlich auszudrücken:

ROFL, ROFL!!!!

Leider ist das Problem aber ein ganz anderes, denn man kann einer elektronischen Wahl grundsätzlich und überhaupt nicht trauen!
Aber wieso, werden da viele sagen, Computer verzählen sich nicht, oder?

Warum die Wahl mittels Stimmzettel so sicher ist
Die Wahl per Stimmzettel ist total simpel. Es gibt Stimmzettel, die werden vom Wähler angekreuzt, in eine verschlossene Wahlurne geworfen und letztendlich ausgezählt. Das alles vor sehr vielen Zeugen um möglichst viel Sicherheit und Authentizität zu erreichen.
Es bedürfte eines sehr großen Aufwandes, eine Wahl per Stimmzettel zu manipulieren.
Es müssten total viele eingeweihte Verbündete (Mitwisser) geben um Wahlergebnisse ernsthaft zu manipulieren. Und man stelle sich vor, viele Menschen wüssten über eine Verschwörung Bescheid, irgendjemand würde plappern oder Informationen an die Presse weitergeben und die Wahl wäre hinfällig.

Und das Beste ist, man kann die Stimmzettel jederzeit wieder auszählen, falls es Zweifel gäbe.
Nicht umsonst wird diese Form der Wahl schon so lange verwendet, auch wenn sie bestimmt nicht ganz perfekt ist.

Warum eine elektronische Wahl so unsicher ist
Eine einzelne Person, nennen wir sie mal "der böse Hacker" könnte die Wahlergebnisse ändern.

Aber warum sollte das jemand tun?

Ja warum denn bitte nicht!
Tagtäglich werden sogar recht komplexe Sicherheits-Systeme aufgebrochen und das meist von Menschen, die es nur tun, weil sie es können.
Jetzt stelle man sich vor, jemand würde aus, sagen wir einmal, wirtschaftlichen Interessen handeln, wäre da der Antrieb nicht noch viel größer? **Wahlergebnisse** gehen dann gut **für den Höchstbietenden** aus!
Und das Beste ist, nur eine kleine Anzahl von Mitwissern wäre erforderlich, um ein landesweites elektronisches Wahlsystem zu manipulieren. Wohlgemerkt, wir reden nicht von ein paar manipulierten Stimmen, sondern von einem komplett manipulierten Wahlergebnis.
Egal welchen Aufwand in Sachen Sicherheit man betreiben würde, das System würde dadurch nur noch komplexer und daher noch leichter zu manipulieren.
Denn man sollte immer bedenken, je komplizierter ein Mechanismus ist, desto kleiner kann die Schraube sein, die letztendlich zur Katastrophe führt.

Bitte Finger weg vom E-Voting
Eine Wahl hat immer mit Vertrauen zu tun.
Ich vertraue lieber auf tausende Wahlhelfer, die Menschen sind und ein Gewissen haben, als tausenden Wahlcomputern, denen das Wahlergebnis vollkommen egal ist, aber dafür unbemerkt und im großen Stil von einer oder wenigen Personen manipuliert werden können.

Ich hoffe auf das Schneeball-System (jeder kennt jemanden, der wiederum jemanden kennt) um Politikern bewusst zu machen, dass eine elektronische Wahl, ganz egal, wie sie auch aussehen möge, total schlecht wäre.
Nicht alles was mit Computern erledigt wird, ist auch automatisch gut erledigt, wie wir alle wissen.
Also bitte redet darüber, so viel wie möglich, dann dringt es bestimmt auch in höhere Sphären vor!

Nachschlag:
Hier ist ein Video von Tom Scott auf dem Kanal Computerphile, welches ganz im Detail erklärt, warum E-Voting so schlecht ist:
https://www.youtube.com/watch?v=w3_0x6oaDmI

Kapitel 26: Was deine Suchmaschine über dich weiß

In diesem Kapitel behandle ich ein Thema, welches von den meisten Computer oder Smartphone-Benutzern komplett unterschätzt wird:
Die Suchmaschine!

Sie ist ein sehr mächtiges Werkzeug, denn wie soll man denn bitte sonst in den unendlichen Weiten des Internets finden, wonach einem gerade zumute ist?
Als in den Neunziger-Jahren das Internet so richtig in Fahrt kam, reichte eine Liste mit bekannten Webseiten auf der Startseite seines Internetproviders einfach nicht mehr aus, um im Internet zu navigieren. Die Webseiten schossen wie die sprichwörtlichen Schwammerl aus der Erde und das Internet wurde zu einem Dschungel aus Webseiten, in dem etwas sinnvolles zu finden nicht mehr möglich war.
Zwei Studenten gründeten daraufhin eine kleine Firma in einer Garage, ihr kennt den Namen der Firma vielleicht, es ist **Google…**

Warum Größe so gefährlich ist
Anfangs war Google eine kleine Suchmaschine unter vielen, vielleicht erinnert sich noch wer an Altavista, Excite, Lycos, Yahoo...
Doch rasch hat sich Google zur meist benutzten Suchmaschine etabliert, was auch seinen Grund hatte; Denn die Suchmaschine war die schnellste und die Ergebnisse waren die Besten, wie man neidlos gestehen muss. Die meisten anderen Suchmaschinen wurden durch Fusionen oder Einkäufe anderer Firmen immer mehr dezimiert und fristen heute neben dem Riesen Google trotzdem nur ein Nischendasein.

Doch das rasche Wachstum hat auch seine Schattenseiten, denn Google ging an die Börse und nun musste natürlich immer mehr Geld verdient werden. Am besten geht das im Internet natürlich mit Werbung, wie könnte es anders sein.
Und natürlich kann man auch als Geschäftstreibender dafür zahlen, um bei den Suchergebnissen ganz oben gezeigt zu werden.
Der so genannte PageRank wurde geschaffen, welcher indirekt den Wert einer Internetseite bestimmt. Wie dieser berechnet wird, ist natürlich streng geheim!
Zudem hat Google auch noch jede Menge andere Produkte geschaffen, wie z.B. Android, Docs, Drive, Maps und viele mehr. Wer gerne wissen will, was alles, siehe im Nachschlag.

Nun, Wachstum und Größe alleine ist noch keine Gefahr, doch die Macht die damit einher geht, sehr wohl. Denn man bedenke, dieser Konzern weiß, wonach du suchst und was du dir wünschst! Er identifiziert dich und speichert dein Benutzerverhalten, er arbeitet mit anderen großen Unternehmen zusammen und auch mit Geheimdiensten. Und dies alles ist kein Geheimnis!

Was alles gespeichert wird
Jede Suchmaschine speichert im Prinzip alle Daten die sie über deinen Browser herausfinden kann, wie z.B. IP-Adresse, welchen Rechner (oder Smartphone) du verwendest, welche Leistungseckdaten dein Gerät hat, wie groß dein Bildschirm ist, den Webbrowser, ob du Cookies von befreundeten Webdiensten gespeichert hast und natürlich deine Suchanfrage. All diese Daten werden dafür verwendet, um dich eindeutig zu identifizieren, auch wenn du gar nicht angemeldet bist.

Noch schlimmer ist es, wenn du mit deinem Google-Konto auf deinem Smartphone eingeloggt bist, denn dann bist du ja ohnehin schon über deine Telefonnummer identifizierbar. Aber auch dein Standort, solltest du die Standortdienste deines Smartphones aktiviert haben, wird gespeichert und zur Generierung von Daten verwendet.

Wofür werden die Daten verwendet
Die gespeicherten Daten werden hauptsächlich für Werbung (eh klar) verwendet, aber natürlich auch für verschiedenste Informationsdienste (Welches Lokal / Geschäft / Freund ist in meiner Nähe). Aber auch Verkehrsdienst-Meldungen können durch Bekanntgabe deines Standortes angezeigt werden.
Keine Frage, natürlich haben Suchmaschinen und Informationsdienste auch einen hohen praktischen Nutzen!

Doch den hauptsächlichen Nutzen hat die Suchmaschine selbst, denn diese generiert aus deinen Daten wieder Daten und verknüpft diese mit anderen Daten um damit noch mehr Daten für noch mehr Werbung und noch mehr Information zu generieren.

Google hat zwar ein gewisses Weltverbesserungs-Image, was ja auch teilweise richtig sein mag. Viel Gehirnschmalz wird hier aufgewandt, um neue Technologien zu entwickeln, die sich in Zukunft positiv auf die Menschheit auswirken können.
Man darf jedoch nicht vergessen, dass Google trotzdem ein profitorientiertes und den Aktionären verpflichtetes Unternehmen ist.

Filterblase
Ein weiterer negativer Effekt ist die so genannte Filterblase. Weil die Suchmaschine dich (wieder)erkennt, präsentiert sie dir auch auf dich zugeschnittenen Suchergebnisse. D.h., wenn wir beide einen Suchbegriff eingeben, bekommen wir unterschiedliche Antworten, weil die Suchmaschine aufgrund unseres bisherigen Suchverhaltens darauf eingeht, was uns voraussichtlich mehr interessieren könnte.

Dies bedeutet, dass wir beide in einer jeweils anderen Filterblase eingesperrt sind und wir nur das zu sehen bekommen, was uns möglicherweise mehr interessiert. Denn dadurch kann natürlich auch mehr zielgerichtete Werbung gemacht werden und die Chance, dass wir aktiv auf die Werbung reagieren ist wesentlich größer.
Ich würde mal behaupten, die Suchergebnisse sind dadurch verfälscht, weil die Suchmaschine so viel über uns weiß und für uns bestimmt, was wir sehen sollen und was nicht.

Du kannst dies übrigens ganz leicht ausprobieren, indem du eine(n) Freund(in) anrufst und ihr beide die gleiche Frage in die Suchleiste von Google eingebt. Vergleicht nun die erste Seite der Suchergebnisse…

Ist mir doch egal
Ich habe ja schon mehrmals über die "Ich habe ja nichts zu verbergen!" Thematik geschrieben und hier ist es genau das gleiche. Jedem ist es egal, was die Mächtigen über einen wissen, jedoch man bedenke: Die Mächtigen leiten die Geschicke der Welt und somit betrifft es letztendlich auch DICH!

Im Prinzip ist die Thematik die gleiche wie bei den sozialen Netzwerken:

- Alles was du in der Suchleiste eingibst wird analysiert, katalogisiert und gespeichert. Für immer!
- Dein Suchergebnis ist eigentlich nur das Abfallprodukt einer Milliarden-Dollar-Werbe-Maschinerie.
- Mit steigendem Kapital einer Firma steigt auch der Einfluss auf Politik und Wirtschaft.
  Falls es noch niemanden aufgefallen ist: In der vom Geld regierten Welt haben Großkonzerne die Macht und nicht unsere Politiker!
- Es ist ziemlich sicher, dass deine Suchmaschine mehr über dich weiß, als dein(e) Freund(in), Partner(in) oder deine Familie.
- Du bist in deiner eigenen Filterblase eingesperrt und wirst nur mit den Informationen gemästet, die aus dir einen noch besseren Konsumenten machen. Du bist in Wahrheit ein Informations-Schaf.

Was man dagegen tun
Die Lösung ist recht einfach, verwende nicht die Suchmaschinen des Platzhirschen.

- Verwende **Metasuchmaschinen**.
  Eine Metasuchmaschine tut eigentlich nichts anderes, als deine Eingabe an andere Suchmaschinen weiter zu geben und dir dann die Ergebnisse zu präsentieren. Der Trick dabei ist, dass dich die ursprüngliche Suchmaschine nicht identifizieren kann, weil sie nur die Daten der Metasuchmaschine sieht.
- **Verwende nicht die Google Suchleiste auf dem Smartphone**, sondern öffne den Webbrowser und gib deine Suchanfrage in eine Metasuchmaschine ein.

Meine momentan bevorzugte Metasuchmaschine ist **DuckDuckGo**:
https://duckduckgo.com/

Natürlich werdet ihr euch fragen, wie wird denn diese Suchmaschine finanziert?
Ja, freilich auch mit Werbung.
Jedoch nur mit Relevanz zum eingegebenen Suchbegriff, anstatt mit personalisierter Werbung.

Aber ich denke, Werbung stellt ja für euch sowieso längst kein Problem mehr dar, oder?
DuckDuckGo verspricht außerdem, keine Daten über dich zu speichern. Wir werden sehen, ob das auch in Zukunft so bleibt…

Nachschlag:
https://de.wikipedia.org/wiki/Liste_von_Google-Produkten
https://de.wikipedia.org/wiki/Alphabet_Inc.
https://de.wikipedia.org/wiki/PageRank
https://de.wikipedia.org/wiki/Filterblase
https://de.wikipedia.org/wiki/Metasuchmaschine
https://de.wikipedia.org/wiki/DuckDuckGo

Kapitel 27: Das Smartphone

Bei meinem Werk "Sicher im Internet" geht es ja eigentlich um Personalcomputer. Jedoch benutzen heute viele Menschen teilweise gar keine PCs oder Notebooks mehr, sondern eher Tablet-Computer, bzw. überhaupt nur mehr Smartphones.

Da diese ja zumeist immer mit dem Internet via Mobilfunk oder WLAN verbunden sind, stellen diese eine besondere Gefahr für die Privatsphäre und die Sicherheit der persönlichen Daten dar.
Deswegen möchte ich das Thema Smartphone in diesem Kapitel etwas genauer beleuchten.

Warum ist das Smartphone ein Sicherheitsrisiko?
Auf jedem Smartphone befinden sich j**ede Menge schützenswerte Daten**, quasi das gesamte Leben wird mit dem Smartphone verwaltet. Termine, Kontakte, E-Mails, Kurznachrichten, Wege und Karten, Zugangsdaten, persönliche Daten, Fotos, das gesamte soziale Umfeld, deine geografische Position, all das ist auf fast jedem Gerät zu finden.

All diese Daten sind natürlich sehr interessant und wertvoll. Einerseits für die Produzenten der Geräte, den Hersteller des Betriebssystems, den Herstellern der ganzen installierten Apps und natürlich nicht zu vergessen, die bösen Buben des Internets.

Jeder möchte vom Kuchen mitnaschen und Geld verdienen.
Und das alles, obwohl du für das Gerät freiwillig so viel geblecht hast...

Sperre und Verschlüsselung
Viele Benutzer sperren ihr Smartphone leider gar nicht oder nur unzureichend. Wird es liegen gelassen, hat jeder der will Zugriff auf die Daten. Deshalb **immer eine Displaysperre einrichten** und auch aktivieren, wenn du das Gerät öfter wo liegen lässt.

Sollte dein Smartphone Verschlüsselung der Daten anbieten, solltest du diese aktivieren. Dies geht meistens mit dem Einrichten der Displaysperre einher.

Sichern der Daten
Wenn dein Smartphone gestohlen wird oder verloren geht, dann kann der Dieb oder Finder hoffentlich nichts damit anfangen, weil das Gerät doch hoffentlich verschlüsselt ist, oder?
Jedoch sind deine Daten nun weg. Vor Cloud-Backups hab ich ja schon in einem vorherigen Kapitel gewarnt, weil diese sicherheitstechnisch auch nicht das Gelbe vom Ei sind.

Daher solltest du regelmässig alles was wichtig ist auch **wo anders sichern**. Für manche Smartphones gibt es sogar irgendwelche Backup Programme, die alles wichtige auf dem PC sichern können. Ich habe damit bisher nie wirklich gute Erfahrungen gemacht, ausserdem hilft das Backup meist nur, das gleiche Gerät wieder herzustellen. Wenn du ein anderes neues Gerät hast, hilft dir das herzlich wenig.

Was man aber immer machen kann, ist das Smartphone als Datenspeicher mit dem PC zu verbinden und **einfach alles herunter kopieren**. So kann man im Zweifelsfall bestimmen, was von den Daten aufs neue Gerät soll und was nicht.

Fragwürdige Updatepolitik der Hersteller
Ein sehr großes Problem sind die Sicherheitsupdates des Betriebssystems, oder genauer gesagt, das Ausbleiben selbiger. Da es sich eingebürgert hat, das Smartphone **fast jährlich** gegen das neue, bessere, schnellere und modernere Nachfolgemodell auszutauschen, gibt es für die Hersteller meist keine Veranlassung das Betriebssystem mit Updates zu versorgen. Dies kostet schliesslich viel Geld, denn man müsste Entwickler haben, die sich mit den "Altgeräten" befassen. Da besteht meist kein Interesse, ausserdem wartet der Nachfolger schon auf seine Erscheinung!

Das Nachfolgemodell hat auch das Nachfolgebetriebssystem installiert und das ist dann ja bestimmt sicherer, oder?
Leider zeigt die Erfahrung, dass die neuen Versionen der Betriebssysteme meistens noch unter **gravierenden Kinderkrankheiten und Sicherheitslücken** bei ihrer Veröffentlichung leiden. Zu oft bleiben diese **unbehandelt** und das Smartphone ist mit allen seinen schützenswerten Daten während seiner gesamten Lebensdauer unnötigen Risiken ausgesetzt.

Übrigens: Mittlerweile ist nicht mehr Microsoft Windows das am meisten angegriffene Betriebssystem, sondern **Android von Google**. Grund dafür ist natürlich die weite Verbreitung.

Apps mit unnötigen Berechtigungen
Was auch noch erwähnenswert ist, sind die meist ungewöhnlich **umfangreichen Berechtigungen** der installierten Apps.
Man stelle sich die Frage: Benötigt eine simple Taschenlampen App wirklich die Berechtigung zum Lesen aller Nachrichten, Kontakte und deinen Standort?
Oder ein einfaches Spiel?
Oder vielleicht die brandneue Ringtone App?

Viele gratis angebotenen Programme beinhalten nicht nur Werbung, sondern wollen auch **alles auf deinem Smartphone lesen** können.
Bedenke folgendes: Das Gerät hängt immer im Internet. Was werden die Programme mit den gefundenen Daten wohl tun?

Und bedenke weiters, nicht nur deine eigenen Daten sind betroffen, denn mit dem Adressbuch verrätst du natürlich auch noch die Kontaktdaten und möglicherweise auch Wohnadressen **deiner Freunde und deiner Familie**.

Zumeist werden die so gewonnenen Daten nur für Werbung benutzt, man muss aber auch leider davon ausgehen, dass immer wieder Daten an dunkle Kanäle verkauft werden.

Zusätzlich ist noch zu sagen, dass in einem Smartphone **Mikrofon und Kameras** verbaut sind. **Mithören und auch mitsehen können nicht ausgeschlossen werden**, wenn du die Berechtigungen der Apps nicht genau hinterfragst.

Anonymitätsverlust
Viele glauben, wenn sie im Internet auf einem Computer (vielleicht nicht mal der eigene) unterwegs sind, dass sie dort unerkannt lesen und schreiben können was sie wollen. Wie ich aber bereits aufgezeigt habe, ist das ohnehin nur eine Illusion.

Aber in Verbindung mit einem Smartphone, welches die richtige App installiert hat, kann man über einen unhörbaren Ton, den eine Werbung auf einer manipulierten Webseite über die PC oder Notebook Lautsprecher aussendet, relativ einfach erkannt werden.
Denn wie schon gesagt, das **Smartphone lauscht vielleicht mit** und es enthält nicht nur deine Telefonnummer, sondern auch alle deine ganzen persönlichen Daten. Dadurch ist ein Rückschluss auf deine Person zu 100% möglich.

Verwendung in der Öffentlichkeit
Heute ist es ganz normal, dass man jederzeit und überall mit dem Smartphone in der Hand herumläuft und sich den von anderen produzierten Blödsinn in jeder freien Minute anzusehen oder anzuhören. Man sollte aber auch bedenken, dass man das alles nicht nur selbst sehen kann. **Jeder neben dir kann das auch!**

Ich bin immer sehr interessiert, was sich die Leute so alles ansehen.
Das gibt sehr viel Aufschluss über die Persönlichkeit eines Menschen...

Sicherheits-Apps
Ich möchte auch noch explizit vor so genannten Sicherheits-Apps warnen, die immer wieder gerne gratis, aber auch in Bezahlversionen verfügbar sind.

Viele dieser Apps tun entweder gar nichts, ausser Geld zu kosten, oder sie sind selbst eher Problem als Lösung, da sie Zugriff auf alle deine Daten haben.

Nichts kann ein Gerät besser schützen, als ein **aktuelles Betriebssystem** und ein **achtsamer, sicherheitsbewusster Benutzer**.

Online Banking
Wie ich in vorherigen Kapiteln bereits erwähnt habe, **rate ich eindringlichst davon ab, auf dem Smartphone Online Banking zu betreiben**. Wenn eine deiner belanglosen Apps ein Trojanisches Pferd enthält, sind dann nicht nur deine persönlichen Daten weg, sondern **auch dein Geld**. Und das bekommst du garantiert nie wieder, auch dann nicht, wenn du den Fall der Polizei übergibst.

Was kann man dagegen tun?
Nun, ich rate dazu, etwas Verstand walten zu lassen:

- Muss man wirklich dauernd jede erlebte Kleinigkeit der ganzen Welt via Facebook oder Whatsapp mitteilen?
- Muss man wirklich dauernd jede erlebte Kleinigkeit seiner "Freunde" auf Facebook oder Whatsapp ansehen?
- Muss man permanent Selfies inklusive Duckface auf Instagram posten?
- Muss man wirklich rund um die Uhr erreichbar sein?
- Müssen alle deine Fitnessdaten inklusive GPS Koordinaten im Internet gepostet werden?
- Hinterfrage die Berechtigungen deiner Apps, jedes neuere Smartphone Betriebssystem erlauben dir die volle Kontrolle über die App-Berechtigungen zu verwalten. Sollte deine Taschenlampen App nicht mehr richtig funktionieren, wenn sie nicht mehr auf deinen Standort zugreifen kann, dann ist es Zeit, diese zu deinstallieren!
- Gehe sparsam mit deinen Daten um, je weniger gespeichert sind, umso weniger kann passieren.
- Deaktiviere WLAN, Bluetooth, NFC, Standort und überhaupt alle Dienste, die du gerade nicht benötigst. Dies schont nicht nur die Akkulaufzeit, sondern verringert auch die Angriffsmöglichkeiten.
- Bedenke bereits vor dem Kauf, wie viel Aussicht es für Aktualisierungen des Betriebssystems gibt. Es gibt hin und wieder wirklich Geräte, die langlebig sind und wo auch das Betriebssystem für längere Zeit garantiert Updates erfährt.

Dies erfordert zwar einiges an Recherche, aber es lohnt sich, sowas zu hinterfragen. Vielleicht können dir Freunde bei der Auswahl behilflich sein, die sich ein wenig mit der Materie auskennen.

Nachschlag:
Sound Beacons
https://www.heise.de/newsticker/meldung/Datenschutz-Werbe-Tracker-ueberwinden-Geraetegrenzen-2921817.html

Datenschutz am Smartphone
http://help.orf.at/stories/2802909/

Kapitel 28: Mails von deiner Bank

Dies ist ein Nachtrag zu den Themen E-Mails und E-Banking.

Österreichische Banken (vielleicht auch in anderen Ländern?) sind jetzt auf die glorreiche Idee gekommen, ihre E-Banking Benutzer jetzt auch mit dem total modernen Medium **E-Mail** zu informieren.
Früher war es üblich, die Benutzer nur per Telefon, Brief und der so genannten Postbox (ein Bereich innerhalb des E-Bankings) mit Nachrichten oder Werbung zu beglücken.
Damit ist jetzt aber Schluss und ich erkläre euch, warum das eine schlechte Idee ist.

Änderung der AGBs
Die Banken haben in ihrer jährlichen Änderung der AGBs einfach „per Mail“ bei den Benachrichtigungsmöglichkeiten hinzugefügt. Das wars. Stillschweigen bedeutet „Ich bin einverstanden“, Ablehnung bedeutet, „du kannst gerne kündigen, wenn dir was nicht passt“.
Gut, das machen eh alle so, aber ein Bankkonto ändert man nicht mal so schnell, wie z.B. den Mobilfunkanbieter.
Außerdem, welche Alternative hat man, wenn es alle Banken gleichtun?

Auswirkung
Früher hat es mal geheißen: „Banken senden niemals eine Mail, in der sie auffordern, auf irgendwelche Links zu drücken, oder irgendwo Benutzerdaten einzugeben“.
Das könnt ihr nun vergessen.
So gesehen bei einer Mail der Hausbank meiner lieben Frau.
Sie hat ein Werbemail für das Zahlen mit dem Smartphone bekommen, auf der sich **sage und schreibe 16 (sechzehn!) Weblinks** zum Draufklicken befanden.

OK, es steht nirgends, dass man draufklicken soll, aber es ist ja eine Einladung, oder?

Nun werden die Menschen trainiert, auf bunte Mails von Banken zu reagieren und die weiterführenden Information im Internet zu lesen.
Das Problem ist aber, **wie viele Menschen kennt ihr persönlich, die die Authentizität einer E-Mail oder einer Webseite bestätigen können?**

Ein Beispiel am Rande: In der Türkei gab es vor nicht allzu langer Zeit einen Fall, wo man Anhänger der Opposition mit gefälschten Mails, die zum Downloaden einer **angeblichen Protest-App** aufrief, die **in Wirklichkeit ein Trojaner** war.
Was das bedeutet, könnt ihr euch wahrscheinlich denken.

Man hat es jetzt den E-Mail Betrügern noch leichter gemacht, eine **noch größere Anzahl an zukünftigen Betrugsopfern** zu bekommen.

Hintergrund
Ich denke mal, die Banken haben das gemacht, um die trostlosen Benachrichtigungen in der Postbox zu umgehen, die wahrscheinlich eh keiner liest, weil die Information so nicht sofort verfügbar ist.
Ob das wirklich so ist, kann natürlich nur ein Insider im Bankwesen sagen, da ich aber selbst in einem großen Unternehmen arbeite, weiß ich, auf welche großartigen Gedanken und Visionen die Vordenker und Lenker so kommen.
Sicherheitsbedenken werden da zugunsten der schönen Werbung einfach abgewedelt…

Aufweichung bei der Passwort-Komplexität
Zusätzlich möchte ich noch erwähnen, dass alle meine Banken mich vor längerer Zeit per AGB dazu „gezwungen“ haben, die Kennwörter für das E-Banking zu ändern.
Und zwar so, dass die ersten paar Stellen numerisch sein müssen, der Rest darf gnädigerweise auch Buchstaben und Sonderzeichen enthalten.

Dadurch hat das Kennwort wesentlich an Komplexität eingebüßt und ist dadurch wesentlich leichter zu erraten.

Und wieso?
Na, damit das Anmelden bei den E-Banking-Apps nicht so schwer ist, denn wer möchte schon dauernd Sonderzeichen in sein Smartphone eintippen?
Bei der Komponente, die die aufgrund der schlechten Update-Politik der Hersteller die größte Angriffsfläche für Schwachstellen ist und auch den größten Anreiz für Hacker bietet, nämlich dem Smartphone, muss man nur ein paar Zahlen eingeben, um sich zu authentifizieren.
Sieht denn da vielleicht noch jemand die Ironie und den Schwachsinn?

Darum kein E-Banking am Smartphone
Ich kann nur immer wieder gebetsmühlenartig bitten und betteln.

Bitte benutzt keine E-Banking-App (und am besten gar nichts was mit Bank im Entferntesten zu tun hat) auf dem nicht so Smartphone.

Danke.

Kapitel 29: Verschlüsseln aber mit Hintertür?

Nach dem Terroranschlag in Wien wurden jetzt wieder Stimmen laut, die sich für eine **Aufweichung der Ende zu Ende Verschlüsselung bei Instant-Messenger** wie Telegram, WhatsApp oder Signal stark machen.
Ungeachtet dessen, dass es beim Terroranschlag in Wien **keinerlei Bezug zu verschlüsselter Kommunikation** über Instant-Messenger Dienste gab.

Was ist eigentlich eine Ende zu Ende Verschlüsselung
Vereinfacht dargestellt heißt das, dass ein Programm auf dem Gerät von Albert sich einen kryptographischen Schlüssel mit dem Gerät von Berta ausmacht und danach alle Nachrichten über das Internet verschlüsselt zwischen den Geräten von Albert und Berta überträgt. Zusätzlich wechseln die Geräte den kryptographischen Schlüssel zyklisch um dadurch die Verschlüsselung noch sicherer zu gestalten.
Nun kann auf den Transportweg im Internet niemand mehr mitlesen und auch der Anbieter des Dienstes kann die Nachrichten nicht mehr im Klartext sehen.

Wie will man eine Aufweichung der Verschlüsselung erreichen?
Hier soll die Ende zu Ende Verschlüsselung so gestaltet werden, dass der Anbieter des Dienstes quasi einen Generalschlüssel zum Brechen der Verschlüsselung in der Hinterhand hält.
Das bedeutet, dass Ermittlungsbehörden (welche auch immer), vom Dienstbetreiber den Schlüssel erhalten um so die Nachrichten dann trotz verschlüsseltem Transport abfangen und entschlüsseln zu können.

Warum das keine gute Idee ist
Würde man die Verschlüsselungsmethoden absichtlich aufweichen, öffnet man dadurch Tür und Tor für Missbrauch und Kriminalität. Denn wenn man künstlich Schwachstellen in Verschlüsselungsalgorithmen einbaut, ist die Wahrscheinlichkeit recht groß, dass dies nicht nur von Ermittlungsbehörden genutzt werden kann, sondern auch von Internet-Kriminellen.
Die Verschlüsselung von Internet Kommunikation sollte so wie das Briefgeheimnis behandelt und in Ruhe gelassen werden.
Außerdem geht es dabei nicht nur um eventuelle Mitleser, sondern auch um die Garantie, dass die Nachricht von einem zum anderen Gerät zweifelsfrei ohne Manipulation angekommen ist.

Aber ich habe ja nichts zu verbergen
Über diese Aussage hab ich mich schon mehrmals ausführlich ausgelassen.
Es geht hier um ein wenig mehr, als das Empfinden der Unwichtigkeit der eigenen Kommunikation.
Es geht hier um **Vertraulichkeit** von Informationen.
Wer möchte schon, dass Nachrichten während des Transportes mitgelesen oder gefälscht werden können?
Wie sieht es mit Industriespionage aus?
Was ist mit Whistleblowern und Journalisten?
Was ist mit Dissidenten in unterdrückten Ländern ohne Demokratie wie wir sie kennen?
Viel hängt von der Vertraulichkeit von Nachrichten ab.

Aber es könnte helfen, Verbrechen zu verhindern
Nun, es ist schon lange erwiesen, dass sämtliche Schnüffeleien und Abhöraktionen von diversen Staaten und Organisationen kaum bis gar nicht zur Verbrechens-, bzw. Terrorismusbekämpfung beitragen.
Die meisten Verbrechen werden nach wie vor durch gute Ermittlungsarbeit aufgeklärt bzw. abgewendet.
Weiters ist davon auszugehen, dass **Verbrecher und Terroristen nach wie vor verschlüsselt kommunizieren** werden, nur wir Normalos eben nicht.Denn die sicheren Algorithmen gibt es ja bereits und das ist nicht mehr zu verhindern.
Vertrauliche Kommunikationswege für Verbrecher und Terroristen steht daher weiterhin nichts im Wege.
Trotzdem ist es der feuchte Traum von vielen Politikern, Organisationen und Firmen, eine allumfassende Überwachung zu haben.
Doch ich befürchte, dass die gewonnenen Erkenntnisse meistens zu rein wirtschaftlichen Zwecken verwendet werden.
Denn **Wissen ist Macht**.

Nachwort
Es war ein langer Weg, bis es wirklich gute Verschlüsselung gab.
Auch war es ein langer Weg, bis diese überall im Internet Einzug gehalten hat.
Fast jede Webseite bietet heute https Transportverschlüsselung an.
Ziemlich alle Instant-Messenger bieten von Haus aus Ende zu Ende Verschlüsselung an.
Sogar DNS Abfragen können mittlerweile über DoH (DNS over https) oder DoT (DNS over TLS) gemacht werden.
Verschlüsselung ist ein recht komplexes Thema, bei dem sich nur recht wenige Menschen wirklich gut auskennen.

Ich wäre dafür, dass sich weiterhin Experten mit dem Thema befassen und nicht irgendwelche Bürokraten und Sesselfurzer, die keine Ahnung haben, wovon sie eigentlich reden und was sie da fordern…

Nachschlag

https://netzpolitik.org/2020/hintertueren-zu-verschluesselter-kommunikation-wirtschaft-und-zivilgesellschaft-stellen-sich-gegen-plaene-der-eu-staaten/
https://krawutzi.wordpress.com/2016/02/18/manifest-fuer-alle-die-was-zu-verbergen-haben/
https://de.wikipedia.org/wiki/DNS_over_HTTPS
https://de.wikipedia.org/wiki/DNS_over_TLS

Kapitel 30: Das Internet of Things (IoT)

Mit diesem Kapitel möchte ich auf die Gefahren von „**Internet of Things**“ Geräten, kurz **IoT** hinweisen.

Was ist eigentlich IoT?
Als IoT Geräte bezeichnet man in der Regel **Kleingeräte**, die per WLAN Verbindung mit deinem Heimnetzwerk und natürlich auch dem Internet kommunizieren können.
Zum Großteil sind hier **Smart Home** Geräte gemeint: Lampen, bzw. Leuchtmittel, Thermostate, Lichtschalter, Steckdosen, Türsprechanlagen und Türspione, Türschlösser und viele mehr.
Aber auch diverse **Heim Assistenten** wie Amazon Echo oder Google Home gehören natürlich auch dazu.
Kurzum, alles was nicht offensichtlich ein Computer ist, aber mit dem Heimnetzwerk verbunden ist, ist ein IoT Gerät.

Natürlich haben solche Geräte einen gewissen Komfort-Gewinn, jedoch sollte man aber auch den **allmählichen Verlust der Privatsphäre** innerhalb der eigenen Wohnung auch bedenken…
Denn viele dieser Geräte können (oder werden) auch dazu verwendet, dich auszuspionieren.

Wie funktionieren solche IoT Geräte?
Ich habe selbst einmal einen Versuch mit einer per Mobiltelefon-App gesteuerten Steckdose gemacht.
Lange Rede kurzer Sinn, ich wollte meine Kaffeemaschine bereits von unterwegs einschalten, damit sie auf Betriebstemperatur ist, wenn ich nach Hause komme.
Die Steckdose, die ich gekauft hatte, wurde per WLAN **vom Mobiltelefon aus konfiguriert** um Zugriff ins WLAN zu erlangen.
Hört sich paradox an, ist aber so. Die **Mobiltelefon-APP** startet einen Hotspot am Mobiltelefon, mit dem sich die Steckdose verbindet und dann die Grundkonfiguration (die Verbindung in mein richtiges WLAN) zu machen.
Danach soll die Steckdose nicht nur geschaltet werden können, wenn mein Mobiltelefon und die Steckdose im gleichen WLAN sind, sondern auch aus dem Internet. Denn die Steckdose baut eine **Verbindung zu einem Server irgendwo in der Cloud** auf, mit dem die Steckdose mit Mobiltelefon-APP auch ohne WLAN Verbindung von überall aus steuerbar ist.
Hört sich recht kompliziert an, oder?

Ja, ist es auch und außerdem gibt es da einiges zu bedenken:

- Ich muss der Mobiltelefon-APP trauen, dass sie nicht mein WLAN samt Kennwort weiß ich wo hin sendet.
- Ich muss der Steckdose vertrauen, dass diese nicht mein WLAN samt Kennwort weiß ich wo hin sendet.
- Ich muss darauf vertrauen, dass das Gerät nicht mit anderen Geräten in meinem WLAN spricht und nach außen verrät, was noch so alles in meiner Wohnung am WLAN hängt.
- Ich muss darauf vertrauen, dass das Gerät nicht unauffällig ein Mikrofon oder Kamera verbaut hat.
- Ich muss darauf vertrauen, dass das Gerät nicht als Trojanisches Pferd fungiert bzw. aufgrund von Sicherheitslücken dazu missbraucht werden kann.

Zum Glück war mein Gerät so eine Reinfall, dass ich von der Idee der IoT Geräte relativ schnell geheilt war.

Aber es ist doch voll praktisch!
Keine Frage, dass solche Geräte voll praktisch sind.
Was man aber mit Sicherheit auch sagen kann, ist dass IoT Geräte ein Internet Sicherheits-Albtraum sind!

Ich spinne jetzt einmal ein paar Gedanken:
Angenommen, dass es sehr, sehr viele dieser Geräte gibt, die von teils dubiosen Herstellern in China billigst hergestellt werden und das ist definitiv so.
Und weiter angenommen, dass sich eine nicht allzu demokratische Regierung in China dazu entschließt, nicht nur die eigenen Bürger zu überwachen, sondern auch alle anderen, mittels der in der Welt befindlichen IoT Geräte, da ja jederzeit per Internet erreichbar sind?
Das könnte nämlich relativ leicht passieren, oder passiert es vielleicht eh schon?

Das hört sich aber schon ein wenig nach Verschwörung an, oder?
Klar, aber es ist definitiv im Bereich des möglichen.
Aber selbst wenn dieser schlimmste Fall nicht eintritt, gibt es immer noch zu bedenken, dass dein **WLAN nicht bei der Wohnungstüre aufhört**. Viele IoT Geräte sind nicht wirklich wartbar und haben (eventuell) schwere Sicherheitslücken.
Sollte ein Gerät verwundbar sein, könnte jemand (Polizei, böser Nachbar, Verbrecher, Chinesen) dadurch Zugriff auf dein Netzwerk und alle darin befindlichen Geräten verschaffen.
Oder vielleicht überhaupt gleich **Zutritt zu deiner Wohnung?**

Natürlich sind auch **Firmen** immer mehr durch die **schnell ansteigende Anzahl solcher IoT Geräte** in Gefahr.
Denn diese Geräte könnten zum **Vorbereiten von großen Hacker-Angriffen** als Hintertür verwendet werden, oder einfach nur zum Guten alten **ausspionieren von Industriegeheimnissen**.

Wen das noch nicht genügend abgeschreckt hat, der lese noch mehr darüber im Nachschlag…

Nachschlag:
https://de.wikipedia.org/wiki/Internet_der_Dinge
https://sicherheitskultur.at/iot.htm
https://www.heise.de/hintergrund/Lebensgefaehrliches-Internet-der-Dinge-3562468.html

Das ENDE

Vielen Dank für Euer Interesse

Herr Johannes bei den Furzen
https://krawutzi.wordpress.com/
https://krawutzi.wordpress.com/sicher-im-internet/