PC-Sicherheit

Was sollte man unbedingt tun, um den PC sicher (besser: „sicherer“) zu machen?

Soviel am Anfang, es gibt keine 100%-e Sicherheit bei der Nutzung des Rechners im Internet! Es sei denn, man zieht den Netzstecker ab, dann gibt es keine Probleme vom Netz, das wäre aber auch nicht im Sinne des Erfinders. Was kann man also tun?

1.
Man sollte immer misstrauisch sein.
Wird etwas im Netz gratis oder zu tollen Preisen angeboten, dann könnte da eine böse Absicht hinter stecken.
Man sollte beim Runterladen von Software nur auf bekannte Firmen zugreifen, wie z.B. „Chip“, „Computer-Bild“ usw. Wenn es da nur kaufbar ist, dann können alle anderen Anbieter, die es gratis anbieten, Hintergedanken haben. (später kommen wir noch auf eine Bewertung solcher Seiten)

2.
Alle Updates des verwendeten Betriebssystems durchführen.
Das sollte per Einstellung automatisch erfolgen, da aber zum festgelegten Zeitpunkt (meist einmal pro Tag um 3.00Uhr) der Rechner vielleicht nicht an ist, sollte man in der Lage sein, selbst den Vorgang anzustoßen. Wenn man wichtige Dinge vorhat, z.B. Online-Banking, dann sollte es vor dieser Verbindung durchgeführt werden.
Windows XP:
Man hört nun: „Windows XP ist abgeschaltet!“ Dass ist so nicht korrekt, die Windows XP-Server bleiben weiterhin, zwar in reduzierter Anzahl, aktiv – die alten Updates bekommt man weiterhin, es wird aber nicht mehr nach Fehlern im bestehenden System gesucht und diese beseitigt. Man kann das System weiterhin nutzen, es wird jedoch bei der Entwicklung neuer Software, nicht mehr berücksichtigt.

3.
Viren-Scanner
Es ist ganz wichtig einen Viren-Scanner auf dem Rechner zu installieren.
Das kann ein kostenloser Scanner, besser ein gekaufter sein. Meist ist die Leistung von gekauften Scannern umfangreicher.
Man bedenke, dass im Internet **mehrere tausend Viren pro Tag „ausgesetzt“** werden, dann könnte sich schon einmal einer auf meinem Rechner breit machen. Hatte man bisher keinen Scanner, dann sollte man nach Installation eines Scanners sofort eine System-Untersuchung damit durchführen. Nicht alle Viren richten sofort Schaden an, sogenannte Trojaner halten sich etwas zurück und brechen unvermittelt zu unbestimmter Zeit aus.
Und man sollte dafür sorgen, dass der Scanner immer „geupdatet“ ist. Das kann man auch immer selbst starten. Bei den freien Scannern erfolgt das automatisch weniger oft als bei den gekauften.

Solche Scanner können also WWW-Seiten beim Runterladen auf Viren untersuchen, die Software auf meinem Rechner untersuchen, den Start von befallenen Programmen verhindern und viel mehr. Das Netz eignet sich ja nicht nur zum Runterladen auch Hochladen ist möglich, also selbst etwas ins Netz zu bringen. Das muss sein, denn sonnst wüsste MicroSoft ja nicht, welche Software neu gemacht werden muss. Fängt nun der Rechner völlig selbst solche Aktion an, dann verhindert das auch der Scanner, ohne meine Erlaubnis bzw. Anweisung darf das kein System auf dem Rechner. Um nun aber noch die notwendigen Aktionen zum und vom Internet durchführen zu können, übernimmt der Scanner nun auch noch die Funktion der „Firewall“ und schaltet die vom System aus und damit haben wir ein weiteres Thema.

4.
Firewall

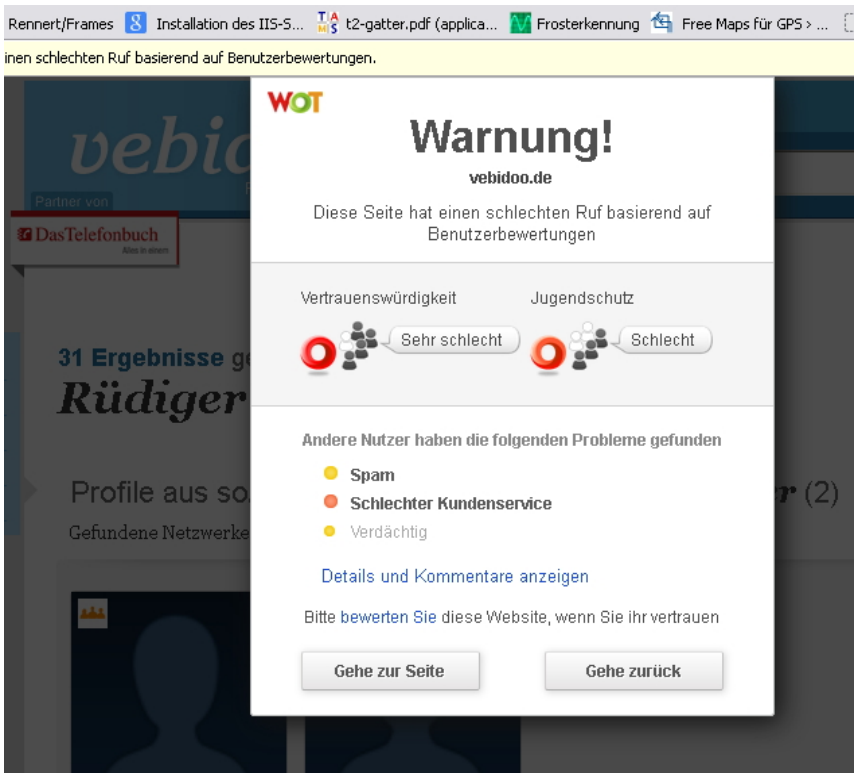
Die Firewall ist ein Programm was die Funktion eines Schutzwalls bzw. Brandmauer hat.
Standardmäßig ist dieses Teil im Windows-Betriebssystem gesetzt (an). Es legt fest, welche
Daten diese Schutzmauer passieren dürfen, in beide Richtungen. Bei Leistungsstarken Viren-Scannern muss sie stark modifiziert werden, deshalb
wird nun die Firewall vom System ausgeschaltet und vom Scanner übernommen, also deinstalliert
man den Viren-Scanner, ist das System schutzlos, man muss sofort die System Firewall einschalten!
Man kann die Firewall auch selbst konfigurieren, dass sollte man besser aber nur dem Profi überlassen!

5.
Verhaltens-Analyse

Mit all den Maßnahmen kann man aber keine hinterhältig angebotenen Verträge fernhalten!
Grundsätzlich gilt, keine Adresse, keine Konto-Nummer, keine Telefon-Nummer und nur in bestimmten Fällen die eMail-Adresse angeben (manchmal
geht es nicht anders).
Die Browser, das ist die Software, die die runtergeladenen WWW-Seiten darstellen, z.B. Internet-Explorer oder Firefox-Explorer, sind eine sehr gefragte Anlaufstelle der Schadsoftware. Deshalb sollten die auch immer mit neuesten Updates auf dem aktuellen Stand gehalten werden (der Internet-Explorer wird beim System-Update mit aktualisiert, Firefox muss man selbst organisieren, weitere auch).
Weiterhin gibt es zu den Explorern Zusatzsoftware, so genante Add-Ons. So ein nützliches Tool ist „WOT“. Hier bewerten Nutzer die WWW-Seite und vergeben rote, gelbe oder grüne Punkte. Hat jemand schon einmal so einen hinterhältigen Vertrag über die Seite erhalten, kann er die mit rot kennzeichnen, z.B. wurde unter „rüdiger renner“ dieser Eintrag bei **Google** gefunden:

Rüdiger Renner - Email, Fotos, Telefonnummern zu **Rüdiger** ...
www.vebidoo.de/**rüdiger**+renner
Rüdiger Rennert/R-TimmiR-Timmi Animationen und Bilder. Bis auf den Radfahrer (finde ich gut) sind fast alle Bilder im Rahmen eines Comics zur Darstellung ...

Ruft man nun so eine Seite auf, dann gibt es
unübersehbar Alarm, den Vorgang kann man nun abbrechen.



Die Seite wird unter:

www.vebidoo.de/rüdiger+renner

angeboten. Bei mir existiert die Originalseite unter:

http://www.u-r-rennert.de/r_man/r_timmi.php

Wer nun diese Seite übernommen hat und wissentlich oder unwissentlich hier fehlerhafte Informationen eingebaut hat, ist mir nicht bekannt, ich war es auf jeden Fall nicht! Es ist natürlich aber ärgerlich. Wenn man aber weiter ermittelt, stellt man fest, dass auch schon:

www.vebidoo.de

dieses Problem aufweist, der ganze Server ist bereits angegriffen worden (weitere Recherchen haben ergeben, dass die „vebidoo“ gezielt solche Aktionen durchführt und juristisch nicht verfolgt werden kann!).
Leider werden nicht alle Seiten so gekennzeichnet, aber in diese Falle läuft man eben auf dieser Seite nicht mehr, also Vorsicht ist weiterhin geboten.

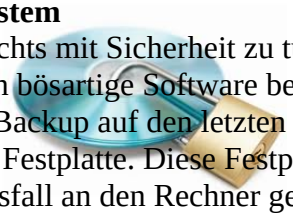
6.
Nutzerrechte

Windows bietet an, dass mehrere Nutzer für einen Rechner angemeldet werden können. Den Nutzern können unterschiedliche Rechte im System zugeordnet werden, der eine darf z.B. nur eigene Programme starten, der andere darf das auch, aber er darf auch neue Software installieren! Der erste Nutzer wird so als Any-User (natürlich wird man einen ordentlichen Namen vergeben) bezeichnet, der andere als Administrator.

Der Nutzen dieser Aktion ist, dass man nur als Any-User arbeitet und nur wenn notwendig sich als Administrator anmeldet (das kann auch für den einmaligen Start eines Programms zutreffen). Schadsoftware braucht meist auch Administratorrechte, dann kommt eben vom System die Mitteilung: “kann das Programm nicht starten“! – Mein Kommentar ist dann: „ist ok.- sollst du ja auch nicht“! Da ja auch der Name der Software genannt wird, kann man dies Ding gezielt entfernen.
Problem ist jedoch das Anlegen der Nutzer. Man sollte dazu einen sehr kompetenten

Rechnernutzer zur Hilfe holen, denn macht man da einen Fehler, hat man im schlimmsten Fall keinen Zugriff mehr auf den Rechner, dann hilft nur den Rechner komplett neu zu installieren, dann ist alles weg. Damit kommt man gleich zu einem neuen Thema.

7.
Backup vom System

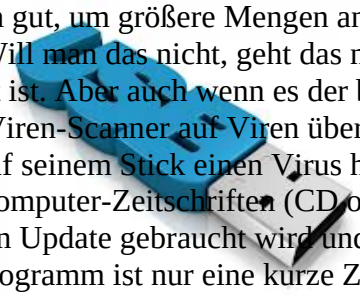


Das hat direkt nichts mit Sicherheit zu tun, aber für den eben beschriebenen Fall, oder wenn das System durch bösartige Software befallen ist, kann man, sofern man hat, das System wieder mit dem Backup auf den letzten Stand bringen. Man braucht dazu so eine Software und eine externe Festplatte. Diese Festplatte wird nur wenn man ein Backup erstellen will oder im Schadensfall an den Rechner gesteckt, damit hat der Rechner in der anderen Zeit keinen Zugriff auf den Speicher – das ist gut so!

8.
Cloud-Systeme

Wenn man unterwegs ist, möchte man zuweilen auch auf die Daten vom Rechner zuhause zugreifen. Das geht sehr gut mit Cloud-Systemen. Die Daten werden zentral auf einem Server gespeichert und jeder vereinbarte Nutzer kann nun diese Daten holen. Nutzer können andere Rechner, Tablet-Pc's oder auch Smartphone sein. Es macht sich gut dort seine wichtigen Daten zu speichern – aber man bedenke, weiß man was der Serverbetreiber mit den Daten sonst noch macht? Also lieber nichts Wichtiges speichern, ein Zettel tut's auch!

9.
Software übernehmen



Cloud-Systeme eignen sich gut, um größere Mengen an Daten oder Software zu übertragen (meist mindest 2GByte). Will man das nicht, geht das natürlich auch mit einem USB-Stick, wenn man am gleichen Ort ist. Aber auch wenn es der beste Freund ist, sollte man den Stick zunächst einmal mit dem Viren-Scanner auf Viren überprüfen. Manchmal weiß der andere gar nicht, dass er auf seinem Stick einen Virus hat!
Software von bekannten Computer-Zeitschriften (CD oder DVD) sind ungefährlich, jedoch kann es sein, dass sofort ein Update gebraucht wird und das ist eventuell wieder kostenpflichtig oder das Programm ist nur eine kurze Zeit kostenfrei. Für CD/DVD's von anderen Leuten gilt das Gleiche wie für Sticks!

10.
LAN/WLAN

Bei der LAN-Nutzung werden Leitungen zur Übertragung der Daten vom „Modem" zum Rechner genutzt, bei WLAN eine Funkverbindung. Solche WLAN-Verbindung kann natürlich auch von anderen abgehört und genutzt werden. Man muss also immer den Sicherheits-Modus eingeschaltet haben (die Kodierung kennen nur Modem und PC).
Ich schalte generell bei Nichtnutzung des Rechners auch das Modem aus!
Ist man unterwegs und kann an einem Ort eben sofort ohne Probleme auf WLAN zugreifen, dann hat der nicht unbedingt vergessen den Sicherheitsmodus einzuschalten, er kann auch so versuchen Schadsoftware zu verteilen!

10.
Bluetooth

Bluetooth ist ebenfalls eine Datenübertragung per Funk (kurze Enfernungen). Auch diese Verbindung kann kodiert werden und ist dann sicherer. Auch Laptops verfügen über so eine Verbindungsmöglichkeit, man sollte sie, wenn sie nicht gebraucht wird, abschalten.

11.
Weitere Probleme

Noch **einmal zu Virenscannern.**

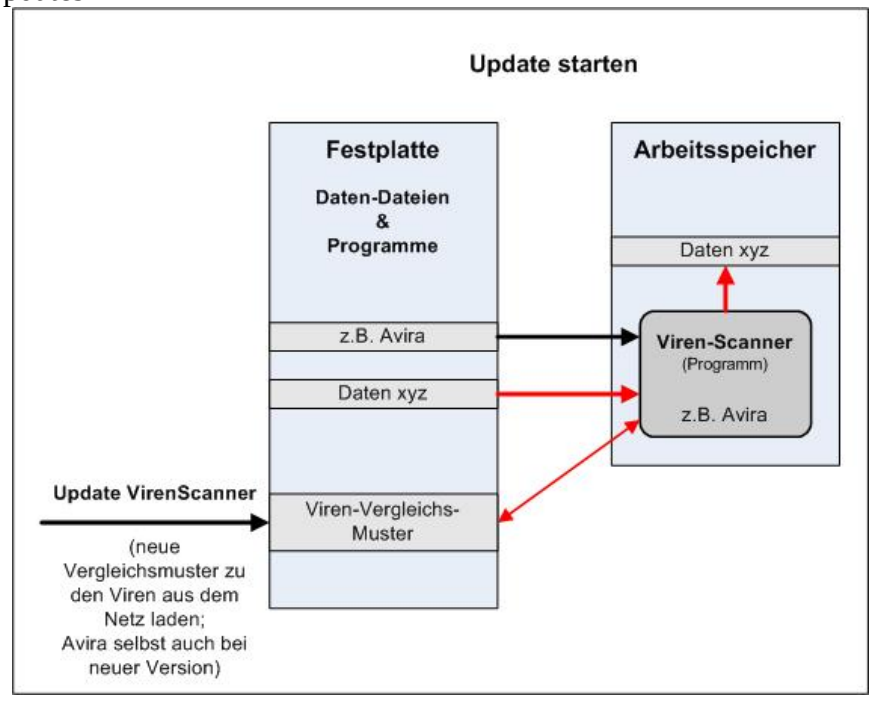
Arbeitsweise eines Viren-Scanners

Meist gibt es zwei wichtige Begriffe bei Viren-Scannern:

Update und
Systemprüfung

Gleich vorneweg – beides ist wichtig, die Updates werden bei richtiger Einstellung automatisch durchgeführt, die Systemprüfung muss man selbst anweisen!
Man sollte aber generell in der Lage sein, Updates selbst anzustoßen.

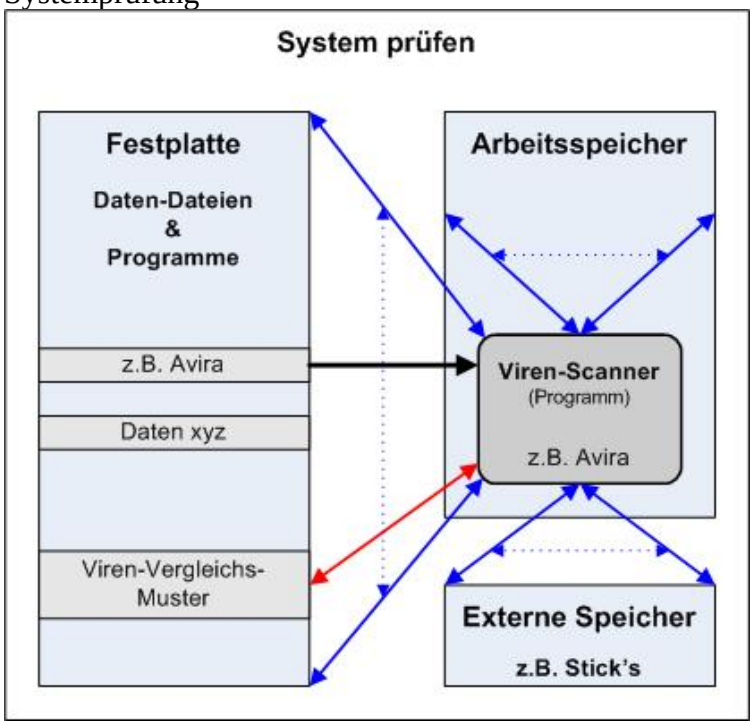
Updates



Um Viren zu finden, vergleicht der Viren-Scanner das zu startende Programm mit den Viren-Vergleichs-Mustern. Die neuen Muster werden beim „VirenScanner-Update“ auf die

Festplatte herunter geladen – folglich kann der Scanner nicht die neusten Viren finden, wenn die neusten Muster nicht heruntergeladen wurden. Man kann auch nicht sagen, dass man das gestern getan hat – die werden minütlich bereitgestellt. Also vor jeder wichtigen Aktion sollte man so ein Update auslösen.

Systemprüfung

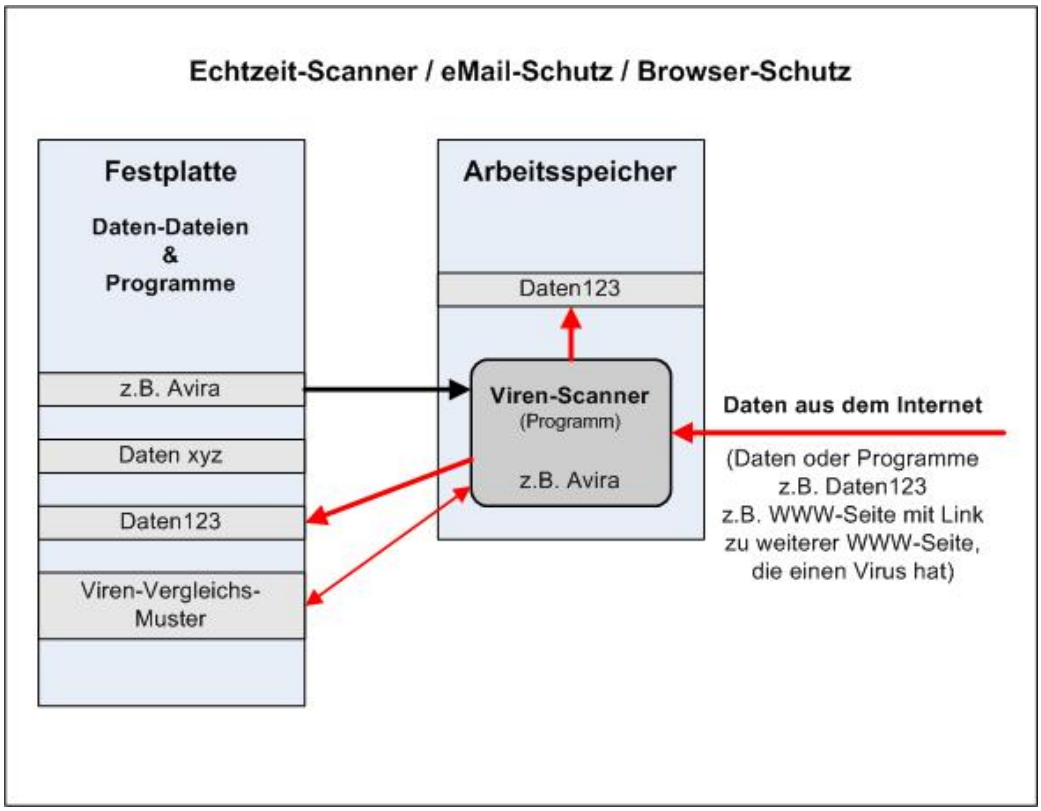


Jetzt werden alle Dateien von allen vorhandenen Speichern (auch Hauptspeicher und so man will auch alle externen Speicher (externe Festplatte, Sticks)) vom Viren-Scanner geholt und kontrolliert. Hat er etwas gefunden, so wird der Name des Programms und des Virus in eine Liste eingetragen. Am Ende des Suchlaufs kann man entscheiden, ob der Virus entfernt werden und selbst in Quarantäne gesteckt werden soll! Das Ganze ist nicht unproblematisch.
Ein verseuchtes Programm sieht etwa so aus:

Programm abc	**Virenkennung**	Programm abc	**Virenprogramm**	Programm abc	Prüf-Bits

Im eigentlichen Programm wird das Virenprogramm eingebunden. Damit das so veränderte Programm nicht als fehlerhaft erkannt wird, muss auch der Prüfteil am Ende des Programms verändert werden. Und damit sich der Virus nicht wieder in sich selbst verpflanzt, muss eine Kennung des Virus abgelegt werden, was eben nun aber auch die Möglichkeit schafft, den Virus zu finden.
Bei der Systemprüfung wird nun alles was Virus ist entfernt, aber der Prüfteil muss erhalten bleiben und neu berechnet werden. Geht da etwas schief, geht eben das Programm auch nicht mehr!
Die Systemprüfung muss nicht jeden Tag durchgeführt werden, denn der Viren-Scanner sollte den Rechner sauber halten. Und die Prüfung dauert schon mal 4 Stunden und mehr!

Echtzeit_Scanner / eMail-Schutz / Browser-Schutz



Das sollte der Viren-Scanner auch leisten.
Generell springen Viren nicht von einem Programm ins andere über, es bedarf immer den Start eines behafteten Programms oder des Virus-Programms selbst. Letztere sind böse. So wie einige Programme automatisch aus einer speziellen Liste heraus gestartet werden, wird ein Virus der dort eingefügt wurde auch gestartet und er verrichtet sein Unwesen und verbreitet sich weiter.
Oder wenn der Virus in einem Systemprogramm steckt, z.B. zur Anzeige des Bildschirms, und da der Bildschirm immer wieder angezeigt wird, hat man ganz schnell den Rechner mit Viren voll.

eMail-Viren
Liest man seine eMail mit „Outlook“, dann werden vom Provider (wo ich mich mit meiner eMail angemeldet habe) nur die Daten geschickt, die Darstellung erfolgt mit „Outlook“. Outlook läuft auf meinem Rechner und muss auch frei von Viren sein, ist oft das Ziel von Viren.
Anders wenn ich die eMail als Web-Seite beim Provider lese, der ist dann dafür juristisch verantwortlich, das keine Viren übermittelt werden, mein Browser muss natürlich auch Virenfrei sein. Meist passiert auf diesem Weg nichts!
Gefährlich wird es, wenn im Anhang eine Datei hängt oder auf eine weitere Web-Seite verwiesen wird. Diese Teile werden nicht vom Provider überprüft.
Bin ich neugierig und öffne diese Seite, habe ich dann den Virus. Hier sollte aber auch ein guter Viren-Scanner eingreifen, den Virus melden und das Öffnen der Datei (Seite) verhindern, das leistet der Echtzeit-Scanner – klar, das geht nur wenn das System aktuell ist. (so hat sich offensichtlich der Virus im Mai 2015 in das Computernetz des Bundestages geschlichen, weil Einige mit nicht aktuellem Virenscanner und neugierig solche Web-Seiten geöffnet haben. Welche Folgen das hat, sieht man)

Weitere Informationen

Wer über eine gekaufte Version eines Virenscanners verfügt, kann sich eine sog. **Rescue-CD** erstellen. Problem kann sein, dass die Viren auch den Virenscanner befallen haben und sich selbst bei der Suche immer auslassen, dann findet man den Viruns nie. Deswegen haben VirenScanner- Firmen so eine Rescue-CD entwickelt. Die Funktion ist, dass der Rechner
mit dem auf der CD vorhandenen Betriebssystem (eine LINUX-Version) hochgefahren wird und der Scanner auch von der CD genommen und gestartet wird – da kommt nun kein Virus von der Festplatte des Rechners mehr ran. Nebenbei kann man auch über Programme der CD Dateien z.B. auch auf einen externen Speicher kopieren, diese werden auch zugleich auf Virenbefall kontrolliert – also von einem nicht mehr funktionsfähigen Windows-System kann man wichtige Dateien retten!
Avira und Kapersky hat z.B. solche CD's.

Von sogenannten „**sozialen Netzwerken**" halte ich wenig (ist meine Meinung)!
Im Telefonbuch möchte man keinen Eintrag haben aber bei Facebook meldet man sich an und posaunt alle seine Daten in die ganze Welt!? Aber auf jeden Fall sollte man wissen, dass Facebook auch eine Menge Einstellungen zulässt, so dass meine Daten geschützt sind, bzw. man nur die unbedingt notwendigen ins Netz stellt.
Wer unbedingt sich im Netz präsentieren will, kann das auch selbst unter Google tun, da kann man kostenlos WWW-Seiten erstellen und seine Neuheiten im Netz präsentieren, da braucht man nur eine eMail-Adresse!

Ein weiteres Problem ist **Skype**. Damit kann man per Computer mit anderen Leuten sprechen und sieht sich auch. Wenn die Partner weit von einander entfernt sind ist das toll. Wer da mithört, weiß man nicht und man sollte auch auf seinen Hintergrund achten: Aber es gibt auch Probleme. Man braucht ja Kamera und Mikrofon am Rechner, die sind in neueren Laptops schon fest eingebaut. Es ist kein Geheimnis, dass Schadsoftware, über solche Systeme eingeschleust werden, auch wenn sie nicht genutzt werden, unbemerkt Kamera und Mikrofon nutzen können, was dadurch für Informationen an unerwünschter Stelle landen können, kann man sich vorstellen.
Es klingt unglaublich, man sollte aber besser beide Teile (Mikrofon und Kamera) mit einem Pflaster zukleben.
Das gilt auch für **Smartphones**, in einer Fernsehsendung wurde
vor kurzem nachgewiesen, dass selbst bei einem ausgeschalteten Telefon das Mikrofon durch Schadsoftware aktiviert werden kann. Laptops werden auch nicht mehr ausgeschaltet, sie gelangen in einen Ruhezustand, womit gleiche Möglichkeiten wie bei einem Smartphone bestehen, es hilft eigentlich nur die Batterien zu entfernen!

Online-Banking
Zunächst einmal ist das Verfahren nicht unsicherer als ein Bankautomat, denn auch da werden Daten und sogar das Geld „gefischt".
Der Rechner zu Hause sollte vor solchen Aktionen immer auf den aktuellen Stand des Betriebssystems und des Virenscanners sein. Das System sollte auch aktuell auf Viren untersucht sein (muss man selbst starten). Man sollte bei der Aktion nicht Administrator-Rechte haben. Aufmerksamkeit ist ganz wichtig, wenn etwas auf den Seiten anders aussieht sollte man sofort abbrechen und neu beginnen, ganz von vorne. Im Zweifelsfall rufe ich bei der Bank an und
frage nach.
Banken bieten verschiedene Verfahren zur Bearbeitung an. TAN's von einer Liste nehmen

ist nicht gut, bessere Verfahren sind Chip-TAN und SMS-TAN. Bei SMS-TAN bekommt man über eine SMS per Telefon die TAN. Das Verfahren ist auch bereits angegriffen worden, ist nicht so sicher wie es scheint. Bei Chip-TAN braucht man ein Extragerät was über den Bildschirm verschlüsselt in 5 Bit mit der Bank kommuniziert. Das Gerät braucht außerdem meine Bankkarte. Da gibt es bisher noch keine negativen Meldungen.
Wenn ich bei dieser Art des Bankings dann die Nachfrage nach TAN's bekomme, dann weiß ich, dass die Seite falsch ist und außerdem habe ich auch keine TAN's.
Der Nachteil ist natürlich, dass man von unterwegs, man wird sicher das Gerät nicht mitnehmen, keine Überweisung tätigen kann, das ist sicher auch nicht notwendig.
Diesen Weg muss man auch nutzen, will man beim Interneteinkauf die Ware sofort bezahlen, die Bank lässt dann keinen anderen Weg zu.
Ein sicheres Verfahren erreicht man mit dem oben bereits besprochenen weiteren Nutzer auf dem Rechner. Der Nutzer bekommt nur Standard-Rechte und der Nutzer führt nur mit dem für ihn relevanten System Aktionen mit der Bank durch, also keine Internetnutzung ganz allgemein. Der Vorteil ist, dass die Möglichkeit Viren einzufangen so kleiner wird.
Wer noch sicherer arbeiten will, sollte eine „**Live CD**" benutzen. Das Betriebssystem befindet sich auf der CD und wird in den Hauptspeicher des Rechners geladen. Alle Teile des Betriebssystems werden nun nur noch von der CD geladen. Die Systeme kennen zumeist auch nicht die Laufwerke des Rechners. Da meist ein Internet-Browser vorhanden ist, kann man nun von hier aus das Online-Banking durchführen. Vieren kann es auf diesem System kaum geben, Phishing an anderer Stelle wird damit jedoch auch nicht ausgeschlossen. Ein solches Live-System ist z.B. „**Knoppix**".

Noch ein Wort zu **eigenen WWW-Seiten**. Es reizt natürlich, selbst Veröffentlichungen im Internet zu machen. Da gibt es verschiedene Wege:
- man baut zu Hause einen Server auf
  dann kann man alles betreiben was man will html, php, mysql, Grafik, CGI usw. aber man muss eine Adresse beschaffen (kaufen) und man muss das Teil selbst von Schadsoftware frei halten – das kann aufwendig sein, man ist ja auch juristisch verantwortlich!
- man kauft Speicherplatz bei einem Provider
  jetzt ist der Provider für die Datensicherheit und Sicherheit allgemein verantwortlich. Solche Probleme, wie unter 5. beschrieben, muss nun der Provider verhindern.
  Ich kann nur das nutzen was im Angebot vereinbart ist. Und ich muss natürlich meine Seiten dort bearbeiten können. Ich zahle etwa 4€ im Monat.
- es gibt z.B. bei Google auch die Möglichkeit Seiten herzustellen. Man ist etwas in der Darstellung eingeschränkt, es reicht aber für den Normalnutzer – und die Seiten sind kostenlos!
  z.B. unsere Seiten zum Senioren ComputerClub:
  https://sites.google.com/site/elmenliha/

- eine neue Variante sind Blogs
  hier kann der Nutzer öffentlich etwas zu seinem gewählten Thema schreiben. Andere Leute können auch dazu direkt Kommentare geben.

Es gibt also viele Wege, im Internet aktiv zu werden, man sollte sich sehr genau überlegen welche Variante sinnvoll ist.