Remove Virus with Knoppix 6.1

Kurze Einfuehrung in Linux und die Knoppix Live-DVD

Die DVD ist ein Linux Live System, dh. sie ist bootbar von CD/DVD. Um zu verstehen, wie dies funktioniert, hier eine ganz ganz kurze Beschreibung:

a. Linux hat eine standardisierte Ordner-Struktur, anders als bei Windows wo das ganze System in C:\Windows zu finden ist. Es gibt zahlreiche Verzeichnisse im Root, welche alle eine besondere Funktion haben. In Linux gibt es keinen “Back-slash” \, sondern nur normale “Slashes” /. Es gibt auch keine Laufwerksbuchstaben, alles haengt bei Linux an einem Baum.

b. Eine Live-CD/DVD laesst ja normalerweise keine Schreibzugriffe zu (ist ja ein ROM Medium). Dazu gibt es aber ein spezielles Filesystem (UNIONFS), welches zum nur lesbaren Filesystem noch einen Bereich schafft, der auch beschrieben werden kann. Dieser Bereich wird im RAM des Rechners abgelegt, ausser man bringt dem System vor dem Start mit einer Boot-Option bei, wo der schreibbare Bereich angelegt werden kann, zB. auf einer Partition der Festplatte (darf FAT32 sein, nicht jedoch NTFS). Fuer deinen Zweck waere ein USB Stick das geeignete Medium, allerdings wollen wir zunaechst mal schauen, ob es auch ohne geht. Dazu unten mehr. Falls es doch notwendig sein sollte erlaeutert folgende Seite die verschiedenen Boot-Optionen und wie man sie einstellt: http://www.knoppix.net/wiki/Live_CD_Tips

c. Dein Netbook hat nur 1GB RAM, mein Notebook hingegen 2GB. Ich kann deshalb nicht mit Sicherheit sagen, ob der Vorgang wie unten beschrieben bei dir 1:1 funktioniert.

d. Linux ist eigentlich ein “Kommandozeilen”-Betriebssystem. Die graphische Oberflaeche ist lediglich ein Aufsatz, um die Kommandos einfacher einzugeben. Intern werden Befehle, wie zB. um ein Virus-Scan auszuloesen, in den meisten Programmen in eine Kommandozeile uebersetzt und dann dort ausgefuehrt, ohne dass der Benutzer wirklich was davon merkt.

e. Geraete, wie zB. Harddisks, USB-Sticks, USB-Cams, CD-Laufwerke, etc. sind fuer Linux Dateien und werden genauso behandelt.

f. Da Linux konsequent auf Multiuser und auf Sicherheit ausgelegt ist werden alle Dateien (auch die Geraete) ueber Zugriffsrechte gesteuert. Der User Norbert zB. hat nur eingeschraenkte Zugriffsrechte auf die Dateien von User Bernard und umgekehrt. Welche Zugriffsrechte wirklich gelten koennen ueber Defaults eingestellt werden, einzelne Dateien koennen aber auch spezielle Zugriffsrechte haben (ich kann dir zB. erlauben, eine bestimmte Datei zu Lesen und zu Beschreiben).

g. Ein spezieller User namens Root ist fuer die Systemadministration zustaendig, welcher Zugriff auf alle Dateien und Resourcen hat. Normalerweise erledigt man aber alle Aufgaben als “normaler” User.

h. Achtung: anders als Windows unterscheidet Linux zwischen Gross- und Kleinschrift. Verzeichnis “Vault” und “vault” sind nicht dasselbe!

Dein System nach Viren durchsuchen

Boote zunaechst mal Knoppix ohne Boot-Optionen. Wenn der Bootvorgang abgeschlossen ist muessen wir zunaechst mal deine Laufwerke fuer Knoppix sichtbar machen. Da diese nicht zur Linux-

Umgebung gehoeren sind sie zunaechst mal gar nicht ge-mounted, dh. die Hardware wurde zwar erkannt, aber die Laufwerke stehen dem System nicht als Datei (siehe oben) zur Verfuegung.

a. Am einfachsten geht das ueber die graphische Oberflaeche, indem du den “PCMan File Manager” aufrufst. Entsprechendes Icon befindet sich an 2. Stelle links in der Statuszeile, also gleich neben Knoppix-Start-Button (an derselben Stelle wo sich bei Windows XP der Start-Button befindet). Wenn du den PCMan File Manager geoeffnet hast solltest du alle Partitionen sehen, welche sich auf der Harddisk befinden. Oeffne nun alle Partitionen der Reihe nach, in welchen du nach Viren suchen willst, moeglicherweise aber auch nur eine, naemlich die Systempartition. Beim Zugriff fuehrt der PCMan File Manager ein “mount” Befehl auf diese Partitionen aus, den man auch haendisch vom Terminal ausfuehren kann, es ist aber viel einfacher so. Danach kannst du den PCMan File Manager wieder schliessen, den brauchst du nicht mehr.

b. Ueberpruefe nun via Kommandozeile, dass deine Laufwerke auch wirklich zur Verfuegung stehen. Oeffne ein Terminal-Fenster (Icon an 3. Stelle links in der Statuszeile) und gib den Befehl “mount” ohne “-Zeichen ein, abgeschlossen mit Enter. Dies gibt dir Infos zu allen ge-mounteten Geraeten, also auch deiner Harddisk. Die letzten Zeilen beziehen sich auf deine Harddisk-Parition(en), und zwar steht dort etwas wie ”/dev/sda1 on /media/sda1 ……“, wichtig fuer dich ist nur der Anfang. Dahinter kommen infos, mit welchen Optionen die Laufwerke gemounted wurden, also heisst “rw” zB. read-write, dh. die Partitionen sind aus Knoppix auch beschreibbar. Das ist natuerlich wichtig, damit du bei der Virus-Reparatur deine Aenderungen auch aufs Laufwerk zurueckschreiben kannst. Hintergrund-Info: Ein Windows-System kann lediglich maximal 4 primaere Partitionen haben, oder aber 3 primaere und eine extended Partition. Die extended Partition kann dann wiederum eine Anzahl logischer Laufwerke/Paritionen beinhalten. Die Partitionsnummern sind fest vorgegeben, und zwar 1-4 fuer die primaeren und 5-xxx fuer die logischen Laufwerke/Partitionen (logische Partitionen werden in einem container abgespeichert, welcher wiederum eine primaere Partition darstellt, aber nicht direkt ansprechbar ist). Wenn du also dein Laufwerk C: und D: gemounted hast, dann solltest du bei Angabe des “mount” Befehls eine Zeile fuer sda1 und eine Zeile fuer sda2 (falls D: ein primaeres Laufwerk ist) oder fuer sda5 (falls D: ein logisches Laufwerk ist) sehen. Es spielt fuer Linux keine Rolle, ob das Laufwerk primaer oder logisch ist, aber du musst dir die Geraete-Bezeichnung merken, also etwa sda1, sda5, oder was es bei dir eben ist.

So, wenn dies vorbereitet ist, dann muessen wir noch die Viren-Signaturen auf den aktuellsten Stand bringen. Diejenigen auf der DVD haben den Stand vom 7 Februar 2009, sind also leicht veraltet. Dazu teste zunaechst mal, ob du eine Verbindung zum Internet hast. Dies erkennst du am einfachsten, wenn du den Web Browser startest (Icon an 4. Stelle links in der Statuszeile). Es gibt 2 Moeglichkeiten, warum keine Internet-Verbindung zustande kommt: deine Hardware wird von Knoppix nicht unterstuetzt (glaube ich nicht), oder du brauchst spezielle Settings, um via PPPoE aufs Internet zu kommen. Das ist dann der Fall, wenn du spezielle Software auf deinem Rechner installieren musstest, um aufs Internet zu kommen. Es gibt zahlreiche verschiedene Verfahren, alle hier zu beschreiben fuehrt zu weit, aber wenn dies der Fall ist dann ruf mich mal an, vielleicht kann ich dir am Tel. einfach helfen.

Falls du keine Internet-Verbindung aufbauen kannst, dann musst du von einem anderen Rechner die Signaturen fuer ClamAV herunterladen (www.clamav.net) und vor dem Scannen auf einen USB-Stick kopieren. Den steckst du einfach ins laufende Knoppix-System ein, er wird automatisch erkannt. Welchen Verzeichnis-Namen der Stick erhaelt kannst du wiederum mit dem “mount” Befehl ueberpruefen, aller Voraussicht nach wird dies /media/sdb1 sein.

c. Oeffne wiederum ein Terminal-Fenster und gib den folgenden Befehl ein (ohne ”): “sudo freshclam -v -l /dev/null”. Dies updatet die Virensignaturen. Es gibt versch. Warnings waehrend dem Vorgang, die kannst du alle ignorieren, aber nach Abschluss des Updates musst du im Terminal-Fenster

ueberpruefen, ob die Signatur-Datenbank erfolgreich geladen wurde (es gibt eine entsprechende Meldung). Da die Logdatei normalerweise in einen Bereich geladen wird, welcher nicht beschreibbar ist, wird die graphische Version des Virus-Scanners ClamAV leider die Version/Datum der Viren-Signaturen nicht anzeigen koennen. Auch ist dies der Grund, warum obiger Befehl als Logdatei /dev/null hat, damit wird die Logdatei naemlich ins “Nirwana” geschrieben, also gar nicht angelegt (du siehst, selbst das Nirwana ist eine Datei unter Linux).

d. Nun kannst du im bestehenden Terminal-Fenster mit folgenden Befehlen den Virus-Scan ausloesen (jeweils fuer eine bestimmte Partition, im Bespiel Partition C: auf deiner Harddisk): Nur scannen: “clamscan –recursive /media/sda1” Scannen und ALLE erkannten Viren resp. Dateien beseitigen: “clamscan –recursive –remove /media/sda1” Nur Scannen mit den Signaturen von Datei xyz: “clamscan –recursive –database=/media/sdb1/xyz” Nur Scannen mit Signaturen in Verzeichnis xyz: “clamscan –recursive –database=/media/sdb1/xyz” Im Beispiel habe ich dir gleich den Befehl hingeschrieben, wie du die Signaturen von einem USB-Stick laedtst. Dies kann entweder eine Datei sein (Update woechentlich) oder mehrere Dateien (incremental Updates werden taeglich nachgefuehrt), das kommt halt darauf an, wann du die Signaturen herunterlaedst.

Ich empfehle dir, vorerst mal einen Scan ohne –remove durchzufuehren, es kann naemlich auch sein, dass der Virus-Scanner einen Fehlalarm ausloest (ist zwar selten, gibts aber). Im Falle von –remove werden dann alle Dateien geloescht. Statt –remove kannst du den Befehl auch wie folgt ausloesen: “clamscan –recursive –move=/media/sdb1/vault /media/sda1” (beachte dass zwischen dem Parameter “–move=/media/sdb1/vault” und “/media/sda1” ein Leerschlag steht). In diesem Beispiel wuerden dann alle Dateien mit Virusbefall ins Verzeichnis “vault” deines USB-Sticks geschoben (und von der Harddisk entfernt).

Clamscan kennt noch viele weitere optionale Parameter. Wenn du weiter einsteigen willst kannst du im Terminal-Fenster den Befehl “man clamscan” eingeben, dann wird die Hilfedatei fuer clamscan angezeigt.

So, das ist die “Erste Hilfe - Anleitung zum Entfernen von Viren”. Du kannst die Life-CD auch noch fuer viele weitere Notfaelle einsetzen, zB. um Dateien zu retten, wenn dein System nicht mehr bootbar ist. Ich weiss, es toent etwas kompliziert, aber der Vorgang ist zuverlaessig und vor allem, man weiss ganz genau was passiert. Also, nun hoffe ich, dass du damit deinen Virus erfolgreich entfernen kannst.