

05. Februar 2012, 15:37 Uhr

Umstieg auf Linux

Nie wieder Viren

Von *Frank Patalong*

Linux? Bloß nicht! Viele Nutzer scheuen das Betriebssystem. Nur was für Experten, lautet das Urteil. Eine Fehleinschätzung, denn der Windows-Rivale hat sich zum Normalverbraucher-System gemausert. Der Rechner läuft stabil, schnell und vor allem virensicher. Ein Erfahrungsbericht.

Am Morgen des 5. Januar 2012 flackerte der Bildschirm meines PC kurz auf. Für Bruchteile einer Sekunde sah man, wie sich ein Internet-Explorer-Fenster öffnete und dann komplett über den Bildschirm legte. Der produktive Teil meines Arbeitstages war damit beendet.

Ich recherchierte gerade im Web, eine der geöffneten Seiten muss verseucht gewesen sein. Sie schleuste die neueste Version des sogenannten BKA-oder UKash-Virus auf meinem Rechner ein und schoss ihn regelrecht ab. Binnen Sekunden war Windows unbrauchbar geworden, verweigerte mir jeden Zugriff. Den sollte ich gegen Zahlung von 100 Euro wieder bekommen, behauptete die sich als Polizei-Warnung verkaufende Erpressungssoftware. Wer das glaubt und zahlt, wird ärmer, aber nicht selig.

Die Infiltrierungsmethode nennt sich Drive-by, man fängt sich einen Schädling ein, während man sich eine Web-Seite ansieht. Es reicht, dass der Rechner in diesem Augenblick nicht ausreichend geschützt ist, was häufig der Fall ist.

Schutz ist ein relativer Begriff

Der Schutz ist durch Sicherheitslücken der installierten Software begrenzt. Zu jedem gegebenen Zeitpunkt haben wir etliche Programme installiert, die bisher nicht geflickte Sicherheitslecks aufweisen - vom Browser über den PDF-Reader, die Office-Software bis hin zu diversen Skripten (Java, Flash etc.), die das bevorzugte Einfallstor für Viren sind. Und gegen neu auftretende Schadsoftware gibt es so oder so zunächst keinen Schutz - egal, wie gründlich man sich absichert.

Mein PC hängt beispielsweise hinter einem Router, der vieles abfängt. Ich arbeite ohne Admin-Rechte. Der Rechner ist durch Firewall und Virenschutzsoftware abgesichert, die jede Stunde auf neuesten Stand gebracht werden. Sicherheitsupdates der Software sind selbstverständlich. "Mein" BKA-Virus kam trotzdem durch.

Es ist zum Mäuse melken, zum in die Tischplatte beißen, zum aus der Haut fahren. Wir **Windows**-Nutzer leben mit diesem Mist seit über zwanzig Jahren. Wir haben es als Teil der PC-Normalität akzeptieren gelernt, nehmen es hin wie Schlechtwetter. Warum eigentlich?

Weit über 95 Prozent aller Virenprobleme betreffen einzig und allein unsere Windows-Rechner. **Apple**-Fans lachen sich eins und behaupten, das läge an schlechter Software. Hauptsächlich liegt es wohl eher daran, dass sich die Verseuchung für Kriminelle lohnt: Windows läuft auf rund 90 Prozent aller PC.

Aber was ist, wenn auf dem von einem Erpressungstrojaner blockierten Rechner einmal wirklich kostbare Daten verschüttet liegen? Dann muss man sich etwas einfallen lassen.

Rettungsversuche - mein Leben als PC-Hotline

Weil Freunde und Nachbarn mich für eine Art PC-Hotline halten, habe ich immer diverse Rettungstools bereit liegen. So gehe ich bei einem akuten Virenbefall vor:

- Ich versuche die Säuberung mit Hilfe einer sogenannten Rettungs-, Rescue- oder Live-CD, bei der das Betriebssystem von der CD oder DVD bootet. PC-Zeitschriften wie "c't" oder "PC Welt"

legen ihren Ausgaben so etwas mehrmals im Jahr bei, ansonsten kann man - wenn man noch Zugang zu einem anderen Rechner hat - auch selbst eine herunterladen und brennen (siehe Linkverzeichnis). Oft entscheide ich mich für die "Desinfec't"-DVD der PC-Zeitschrift "c't", die gleich vier aktuelle Virens Scanner mitbringt: Avira, Bitdefender, ClamAV und Kaspersky.

- Die automatisch online aktualisierten Virens Scanner untersuchen dann einer nach dem anderen den befallenen Rechner - ein Prozess, der Stunden dauern kann.
- Wieder unter Windows lasse ich einen spezialisierten Adware-Scanner folgen. Danach ist der Tag gelaufen - und normalerweise wieder alles im grünen Bereich.

Normalerweise. Es hat sich vieles getan an der Cybercrime-Front. Bei den Erpressungsviren funktioniert die oben geschilderte Routine nicht mehr. Sie sind zugleich primitiv und perfide. Scanner, Entfernungstools und selbst Live-CDs verpuffen bei den neueren Varianten, weil die ihre Schadwirkung schon bestens getarnt im sogenannten Boot-Sektor der Festplatte entfalten. Der oben geschilderte, meist sehr erfolgreiche Virencleaner geht völlig an ihnen vorbei.

Bei den Erpressern hilft nur Handarbeit

Hier hilft nur die Bereinigung auf Registry-Ebene, **wie wir sie vor kurzem geschildert haben**. Auch das klingt beruhigender, als es ist: Die gegen den BKA-Virus empfohlenen Methoden sind Stoff für Fortgeschrittene und dürften Otto Normalverbraucher meist völlig überfordern. Verschiedene Virenvarianten erfordern unterschiedliche Maßnahmen. Damit die wirken, muss man die jeweilige Variante richtig erkennen. Und selbst dann gilt: Was auch immer der Virus auf dem Rechner an möglicherweise verborgenen Schäden verursacht hat, ist nicht behoben. Möglich, dass Hintertüren ins Betriebssystem offen bleiben.

Der letzte Schritt, um den Rechner wirklich wieder abzudichten, lautet darum eigentlich: Man sollte seine Daten exportieren und sichern - und dann die Festplatte komplett formatieren und Windows neu installieren. Anders gesagt: alles kaputt hauen und neu aufbauen. Wer all das selbst nicht kann und die Hilfe eines Fachmanns braucht, ist schnell dreistellige Summen los.

Wie gesagt, es ist zum Mäuse melken. Ich hatte die Nase voll. Genug davon, als ehrenamtlicher Virenfeuerwehrmann immer wieder Abende in den Sand zu setzen. Genug davon, alle paar Jahre auch selbst den GAU zu erleben.

In der Stunde der PC-Not fällt mir seit Jahren vor allem eines ein: **Linux**. Und vielleicht war es nun an der Zeit, Linux nicht mehr nur als Notsystem einzusetzen, sondern als sichere Alternative neben meinem mit viel zu viel Mühe bereinigtem Windows fest zu installieren?

Das geht ganz problemlos. Es kann allerdings unerwartete Nebenwirkungen haben.

Keimendes Linux-Fieber - die Bekehrung des Schornsteinfegers

"Och, das ist ja chic", sagte meine Tochter, als sie meinen neuen PC-Desktop sah. Sie meinte natürlich vor allem den Bildschirmhintergrund, aber auch, wie aufgeräumt alles aussah. Installiert hatte ich das Linux-System Ubuntu 11.10.

Hier die augenfälligen Unterschiede zu Windows im Schnelldurchlauf:

- Die Startleiste mit den wichtigsten Programm- und Dateisystem-Einträgen ist nicht unten zu finden, sondern links. Die üblichen kleinen Symbole, wie beispielsweise Uhr, Aus-Knopf oder Lautsprechersteuerung, findet man oben statt unten rechts.
- Was in der Startleiste zu sehen ist, hängt davon ab, was man besonders oft oder am aktuellen Tag gebraucht hat, es wechselt. Immer zu sehen ist der Internetbrowser Firefox, das Office-Paket LibreOffice, der Software-Shop (vergleichbar mit einem App-Store) und der sogenannte Dash am Seitenkopf oben links. Den könnte man mit dem Start-Button bei Windows vergleichen.

Die meisten Programme unter Linux unterscheiden sich kaum von ihren Windows-Versionen oder Entsprechungen. Äußerst komfortabel ist, dass so gut wie alles vorinstalliert scheint. Selbst wenn etwas fehlt, ist die Nachinstallation von Programmen oder Codecs zur Darstellung von Videos ein Kinderspiel. Alle meine unter Windows angelegten Dateien (Texte, Bilder, Filme etc.) sind zugänglich und nutzbar.

Die große Schwäche: Linux ist kein Spielplatz

Was nicht bedeutet, dass Linux aus Verbrauchersicht keine Schwächen hätte. Nach zehnminütiger Einarbeitung probierte meine Tochter die Software für einen Tag aus. Dann fragte sie: "Kann ich damit auch Sims spielen?"

Kommt drauf an, sagte ich und dämpfte damit ihre Begeisterung merklich. Kommerzielle Spiele gibt es nur selten in Linux-Versionen, gerade die populärsten sind nicht darunter. Viele Windows-Programme lassen sich - oft unter Leistungseinbußen - mit Emulatoren (eine Art "Übersetzer-Programm") aus Linux heraus nutzen: Ob das aber klappt oder nicht, ist auch von der eingesetzten Hardware abhängig. Browserspiele laufen natürlich. Generell muss man aber sagen: Linux-Rechner sind nichts für Leute, die PC zum Spielen nutzen.

Arbeitsaufgaben, Internet und "sachliche" Hobbys, aber auch Multimediaanwendungen vom Filmkonsum über Grafiksoftware bis zum DVD-Schnitt bedient Linux dagegen vorzüglich. "Schade", sagte meine Tochter, eigentlich sei dieses Ubuntu "viel besser als mein Windows". Was sie meint: Es ist einfacher - und deutlich schneller.

Domino-Effekte: wenn einer anfängt...

Am Abend rief mich ein Freund an, er ist Schornsteinfeger. "Hör mal", sagte er, "ich krieg' diesen BKA-Mist nicht runter."

"Spielst Du eigentlich an der Kiste?", fragte ich. Er verneinte. Ich machte ihm einen naheliegenden Vorschlag, um ihn (und mich!) von seinem Virenproblem zu erlösen.

"Meinste, das krieg' ich hin?", fragte er zurück.

Vor ein paar Jahren hätte ich gezögert. Egal, was Linux-Fans da behaupten, die meisten Distributionen (so nennt man die verschiedenen Linux-Ausprägungen) sind Stoff für Leute, die wissen, was sie tun - und nicht für normale Anwender. Nach ein paar Tagen Ubuntu sehe ich da aber keine Probleme mehr. Gerade die unter Linux-Fans heiß umstrittene neue Unity-Arbeitsoberfläche ist es, was das System für Normal-User interessant macht: die ist einfach, übersichtlich und intuitiv zu bedienen - das kann locker auch mit Apple konkurrieren.

Ein paar Abende später installiere ich Ubuntu auf dem Laptop meines Freundes, neben der Windows-Partition, die erhalten bleibt. Alles geht ganz einfach, nach 20 Minuten sind wir durch. Wir testen den Rechner, im Internet, dann mit einem 24 Gigabyte großen HD-Video im mkv-Format. Das Bild fließt ruckelfrei und gestochen scharf. Codecs, Nachinstallationen, Probleme? Fehlanzeige.

In den folgenden Tagen warte ich auf den ersten Hilferuf. Er kommt nicht.

"Spitze", sagt mir mein Linux-Schornsteinfeger, als wir uns eine Woche später treffen, "das Ding ist jetzt viel schneller!" Er grinst wie ein Honigkuchenpferd, Probleme hat er offenkundig keine. "Sag mal", sagt Stefan, ein weiterer Freund: "Meinst Du wirklich, man kann das inzwischen versuchen?"

Ich verspreche ihm, eine Installations-DVD mitzubringen. Ein paar Tage darauf fragt der Nächste. Um mich herum entsteht ein kleiner, virenfreier Linux-Cluster. Vielleicht sind meine Tage als ehrenamtliche Viren-Hotline gezählt.

URL:

<http://www.spiegel.de/netzwelt/gadgets/0,1518,812304,00.html>

MEHR AUF SPIEGEL ONLINE:

"BKA"-Virus: So werden Sie Lösegeld-Trojaner wieder los (23.01.2012)

<http://www.spiegel.de/netzwelt/web/0,1518,809770,00.html>

"Rockiger Satchbook" im Test: Hier läuft Linux auf dem Laptop (30.01.2012)

<http://www.spiegel.de/netzwelt/gadgets/0,1518,811764,00.html>

Tipps für mehr Sicherheit: So schützen sich Profis vor Computer-Kriminellen

(19.01.2012)

<http://www.spiegel.de/netzwelt/web/0,1518,808814,00.html>

Software-Test: Die besten Fotooverwarter für Linux (19.11.2011)

<http://www.spiegel.de/netzwelt/gadgets/0,1518,796830,00.html>

MEHR IM INTERNET

Live- und Recuesystem: Microsoft Windows Defender Offlöine (Beta)

<http://windows.microsoft.com/en-US/windows/what-is-windows-defender-offline>

Gezielte Entsperrung gegen Erpresser-Software: Kaspersky-Tool "Windows Unlocker"

<http://support.kaspersky.com/de/viruses/solutions?qid=208641247>

Live-Rettungssystem "Desinfec't": Aus Lizenzgründen nur per Heftnachbestellung (3,70 Euro)

http://www.heise-shop.de/heise-zeitschriften-verlag/ct-8-2011_pid_14746734.html

Live-DVD-Systeme: Linux-Rescue-System mit Avira-Scanner

<http://www.avira.com/de/support-download-avira-antivir-rescue-system>

Ad- und Spyware-Entfernungsprogramm: SuperAntiSpyware

<http://www.superantispyware.com>

Schadsoftware-Entfernungstool: Malwarebytes Anti-Malware

<http://fileforum.betanews.com/download/Malwarebytes-AntiMalware/1186760019/1>

Viren-Entfernungstool: Stinger

<http://www.mcafee.com/de/downloads/free-tools/stinger.aspx>

Live- und Recuesystem: Knoppix-Linux-DVD mit F-Secure-Scanner

http://www.f-secure.com/en/web/labs_global/removal/rescue-cd

SPIEGEL ONLINE ist nicht verantwortlich

für die Inhalte externer Internetseiten.

© SPIEGEL ONLINE 2012

Alle Rechte vorbehalten

Vervielfältigung nur mit Genehmigung der SPIEGELnet GmbH