Erschienen in EasyLinux 11/2005

Sicherheitsrisiken unter Linux

Verfehlte Schutzimpfung

von Achim Leitner

Persönliche Firewalls, Dialer-Schutzprogramme und Virenscanner gehören auf Windows-Systemen zur Standardausstattung sicherheitsbewusster Anwender. Ihre Linux-Kollegen dürfen sich auch ohne diese teuren Helfer ins Internet wagen.

Per Internet Explorer und Outlook Express ohne Viren-Schutzprogramm ins Web: Dieser Windows-Spaß gilt gemeinhin als fahrlässig, und das zu Recht. Linux-Anwender hingegen verzichten auf Virenscanner, dennoch sind Angriffe auf diese Systeme weitaus seltener. Es stellt sich die Frage, warum dem so ist und ob Antiviren-Software nicht auch für den Pinguin Pflicht sein sollte.

Um es vorweg zu nehmen: Theoretisch könnten diese Programme tatsächlich auch Ihrem Linux-Systemen etwas zusätzlichen Schutz gewähren. Praktisch können Sie aber auch sehr gut darauf verzichten. Bevor Sie auch nur über Virenabwehr nachdenken, sind andere Maßnahmen wesentlich wichtiger und wirksamer: Updates, sichere Konfiguration und vorsichtiger Umgang mit Mail und Web.

Der Begriff "Virus" hat heute seine enge Definition verloren und dient vermehrt als Oberbegriff für sämtliche schädliche Software. Dieser bedauerliche Bedeutungswechsel führt zu Verwirrung und Mehrdeutigkeiten: Wer von einem Virus spricht, meint vielleicht einen Wurm oder ein trojanisches Pferd, vielleicht aber auch einen echten Virus. Der folgende Text bleibt daher bei der engen Definition: Nur ein Virus heißt Virus, der Oberbegriff lautet Malware oder Schadprogramm.

Dabei ist die Unterscheidung ganz leicht: Viren verändern ein vorhandenes Programm und sorgen dafür, dass jeder Start dieses Programms auch den Viren-Code ausführt. Wie ihre biologischen Vorbilder brauchen Viren den Wirt. Die Technik funktioniert zwar unter Linux, wie einige wenige real existierende Viren beweisen, eine Epidemie ist aber weitgehend ausgeschlossen und bisher auch ausgeblieben. Die Gründe dafür liegen in Technik und Organisation von Linux und dessen Anwendern.

Virengefahr

Um sich weiter zu verbreiten, infiziert ein Virus fremde Software. Unter älteren Windows-Versionen hat er dabei freie Hand, Linux bremst Viren aber aus. So lange Sie als normaler User und nicht als Root arbeiten, dürfen die Programme und damit auch die Viren weder System-Software noch fremde Programmdateien überschreiben.

Dem Virus fehlt damit ein Ausbreitungsweg: Er kann keine Programme infizieren, selbst wenn ihn jemand einschleppt. Dazu kommt, dass sich Linux-Anwender kaum gegenseitig Software zuschicken. Daran wird sich künftig nichts ändern: So lange die Programme frei verfügbar sind bleiben Warez (Raubkopien) uninteressant. Originalsoftware lädt man leichter und schneller von der Distributions-CD, einer Heft-CD oder der Originalseite der Entwickler. So lange Sie als Linux-Anwender keine Programme starten, die aus dunklen Quellen stammen, findet kein Virus den Weg auf Ihren Rechner.

Sehr sinnvoll sind Linux-Virenscanner in gemischten Umgebungen: Läuft das Schutzprogramm auf einem Datei- oder Mail-Server, der auch Windows-Clients bedient, dann schützt Linux die Windows-Rechner vor den Gefahren.

Abb. 1: Bei Open Office (hier Version 1.1.4 auf Suse Linux 9.3) bestimmen Sie selbst, ob es Makros ausführen soll und wenn ja, in welchen Dateien sich die Makros befinden müssen. Führen sie Makros nur aus, wenn Sie sicher sind dass der Code unbedenklich ist.

Makros

Makro-Viren funktionieren ähnlich wie Viren, nur befallen sie keine Programme, sondern Dokumente. Das klappt, so lange die Bearbeitungssoftware über Makro-Funktionen verfügt. Es sind durchaus Viren denkbar, die sich in Open-Office-Dateien einnisten. Allerdings warnt Open Office den Benutzer, bevor es ein Makro aus einer unbekannten Quelle ausführt. Welche Quellen als bekannt und sicher gelten, können Sie selbst bestimmen (Abbildung 1).

Wenn Sie ein Dokument öffnen, das Makros enthält, aber sich außerhalb der Pfadliste im Dateisystem befindet, dann fragt Open Office nach, bevor es das Makro ausführt. So behalten Sie die Kontrolle -- seien Sie aber vorsichtig und klicken nicht unüberlegt auf Ja-Ich-Will-Makros-Ausführen-Schaltflächen. So lange Sie keine fremden Open-Office-Dateien öffnen und die darin enthaltenen Makros absichtlich zulassen, kann auch kein Virus Ihre Dateien befallen. Word-Makro-Viren haben sowieso keine Chance, da Open Office keine Microsoft-Makros (weder Word Basic noch VBA) ausführt.

Würmer

Die nächste wichtige Schädlingsart sind Würmer. Im Gegensatz zu Viren benötigen sie kein Wirtsprogramm, sie funktionieren selbständig und breiten sich eigenmächtig aus. Dazu missbrauchen sie fremde Programme und deren Sicherheitslücken. Der bekannteste Wurmträger ist wohl das E-Mail-Programm Outlook unter Windows.

Ein typischer E-Mail-Wurm versendet sich an alle Personen aus dem Adressbuch. Dem Empfänger schadet das nur, wenn er sorglos den E-Mail-Anhang öffnet oder wenn der Wurm eine Sicherheitslücke des Mail-Programms ausnutzt. Beides könnte auch unter Linux geschehen. Aber die Hürden, die sich dem Wurm in den Weg stellen, sind zahlreicher und höher:

- Linux-Anwender benutzen viele verschiedene Mail-Programme, es herrscht nicht die unter Windows übliche Outlook-Monokultur. Ein E-Mail-Wurm würde sich beträchtlich langsamer ausbreiten, da er bei vielen Empfängern unwirksam wäre.
- Linux-Mail-Programme zeigen den vollen Dateinamen und geben dem Benutzer mehr Informationen, welcher Dateityp tatsächlich im Anhang steckt. Damit hat es ein Wurm schwer, wenn er den Benutzer austricksen und ihn dazu verleiten will, schädliche Anhänge zu öffnen.
- Die meisten E-Mail-Programme ignorieren HTML-Anhänge oder benutzen sichere Programm-Module, um den HTML-Code anzuzeigen. Outlook verwendet dazu die selben Software-Komponenten wie der Internet Explorer und ist folglich für ähnliche Sicherheitslücken anfällig.

Dennoch gilt unter Linux ebenso wie unter Windows: Öffnen Sie keine Anhänge von suspekten E-Mails. Und vor allem: Starten Sie keine unerwartet eintreffenden Programme. Damit würden Sie einen eventuellen Wurm selbst in ihren Rechner einsetzen. Der hätte dann zwar immer noch nicht die volle Kontrolle über den Computer, weil Sie ja als normaler Benutzer und nicht als Root arbeiten, dennoch bereitet der Schädling Ärger.

Wine-Gefahr

Recht interessant ist die Frage, ob Windows-Viren und -Würmer mit Hilfe der Kompatibilitätssoftare Wine auch unter Linux laufen. Wine emuliert zwar kein vollständiges Windows, es gaukelt aber einzelnen Programmen eine Microsoft-Umgebung vor. Sollten die Windows-Programme virenverseucht sein, ist es kurioserweise besser, je schlechter Wine arbeitet: Die meisten Viren scheitern an der unvollständigen Simulation. Dennoch gab es bereits Fälle, in denen Windows-Viren unter Wine begrenzt lauffähig waren.

Im Januar 2005 nahm Matt Moen diese Kuriosität zum Anlass für einen bissigen Artikel [2] auf Newsforge: Er testete fünf Windows-Viren unter Wine. Ein Teil lief tatsächlich, aber keiner richtete ernsten Schaden an.

Wie schwer die potenziellen Folgen ausfallen hängt davon ab, ob die Schad-Software für Wine optimiert ist oder nur zufällig läuft. Je nach Wine-Konfiguration hat die Malware problemlos Zugriff auf Ihr Home-Verzeichnis oder weitere Bereiche des Rechners. Daher gilt: Sie sollten auch unter Linux sehr vorsichtig mit bekannt anfälliger Windows-Software sein. Ältere Internet-Explorer-Versionen laufen zwar unter Wine (Abbildung 2), durch die vielen Sicherheitsprobleme ist vom Einsatz aber dringend abzuraten.

Abb. 2: Dank Wine laufen ältere Versionen von Microsofts Internet Explorer auch auf Linux. Der Einsatz ist aber sehr bedenklich, da Windows-Schad-Software auch Linux angreifen könnte.

Je nach Dateiverknüpfung ist es sogar möglich, per Mail-Anhang versandte Windows-Würmer von Linux-Mail-Programmen aus zu starten: Ist für EXE-Dateien Wine als Betrachter eingestellt, dann kann ein Klick auf solche Anhänge erschreckende Folgen nach sich ziehen.

Während Wine nur einzelne Windows-Programme ausführt, gibt es andere Software die das komplette Microsoft-Betriebssystem als Gastsystem unter Linux startet: VMware, Win4lin, Virtual PC oder Qemu. In diesen Biotopen finden auch Schädlinge ihre gewohnte Umgebung vor und breiten sich ungehindert aus. Wenn per Samba-Mount oder ähnlichen Techniken aus dem Emulator heraus Zugriff auf das

Linux-System besteht, dann könnten Schädlinge sogar dort Dateien manipulieren.

Saubermänner

Ob ein Programm schädlich ist oder nicht lässt sich nur sehr schwer feststellen. Bei einem einfachen E-Mail-Wurm ist die Sachlage noch recht eindeutig. Manche bösartigen Funktionen verstecken sich aber gut getarnt in harmlos wirkenden Programmen. Diese Kategorie heißt trojanisches Pferd.

Oft weiß nicht einmal der Programmierer von den verborgenen Programmteilen in seiner Software. Eventuell hat ein Angreifer den Computer des Entwicklers geknackt und unbemerkt Zusatzfunktionen in seine Software eingefügt. In anderen Fällen ist es der Autor selbst, der dunkle Ziele verfolgt. Bei Open-Source-Software stehen die Chancen aber gut, dass andere Entwickler verborgene Fallen aufdecken und die Linux-Gemeinde warnen. Die Erfahrung zeigt, dass dies sehr schnell klappt.

Gegenwehr

Der prinzipbedingt hohe Schutz bleibt nur erhalten, wenn alle Computer mit den neuesten Sicherheitskorrekturen ausgestattet sind. Wer darauf verzichtet, diese "Patch" oder "Update" genannten Korrekturen einzuspielen, setzt sich und andere einer unnötig hohen Gefahr aus. Ist ein Rechner erst einmal geknackt, nutzen ihn die Cyber-Gauner für weitere Attacken auf neue Opfer.

Beim Aktualisieren [5] helfen Ihnen die modernen Distributionen. Deren Online-Update-Funktion sagt Ihnen, wenn es für ein installiertes Paket eine neue Version gibt. Ist die Ursache eine Sicherheitslücke, dann sollten Sie das Update möglichst rasch einspielen. Wer Online-Updates nicht einspielt, sei es weil er keine, nur eine teure oder eine langsame Internetverbindung besitzt, ist mit den Update-DVDs in jeder EasyLinux-Ausgabe gut beraten.

Alte Bekannte

Heikel sind vor allem Sicherheitslücken in einem Server-Programm. Dieses Stück Software wartet darauf, dass sich ein anderes Programm (ein Client) mit ihm in Verbindung setzt (siehe Abbildung 3). Ein typischer Server ist zum Beispiel Apache (Web-Server), dazu passen Firefox oder Konqueror als Client.

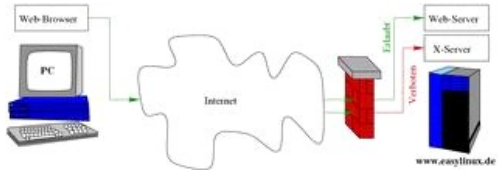

Abb. 3: Eine Firewall verhindert, dass Clients verbotene Verbindungen zu einem Server herstellen. Was erlaubt ist und was nicht gibt der Administrator vor.

Über das Internet kann sich jeder mit einem Server verbinden und sein Unwesen treiben. Als Täter kommen Menschen mit dunklen Absichten in Frage (meist als Cracker tituliert) oder ein Stück Software -- letzteres zählt als weitere Wurmvariante. Zu großer Verbreitung gebracht haben es Ramen und Lion. Der Ramen-Wurm [3] griff 2001 den Wu-FTP-Server an, während der Lion-Wurm [4] eine Sicherheitslücke im DNS-Server Bind nutzte. In beiden Fällen waren die Lücken bereits länger bekannt, nur hatten die Betreiber vieler Unix- und Linux-Computer die Updates nicht eingespielt.

Um sich vor unerwarteten Angriffswellen zu schützen, verwenden viele Netze so genannte Firewalls. Diese Schutzwälle lassen nur Datenpakete passieren, die bestimmten Kriterien genügen. Diese Kriterien aufzustellen ist bei großen Firewalls eine komplexe Aufgabe für Firewall-Administratoren. Für kleine Heimnetze oder einzelne Rechner bringen die meisten Linux-Distributionen einfache Konfigurationsprogramme mit.

Eines ist allen Firewalls gemein: Wenn sie eine Verbindung zulassen, dann müssen sich weiterhin die Client- und Server-Programme selbst schützen. Der beste Schutz ist, nur die benötigten Programme zu installieren und zu starten und Sicherheits-Updates immer einzuspielen.

Falsch gewählt

Linux blieb bislang von der Plage der Dialer-Programme verschont. Diese ändern mehr oder weniger heimlich die Einwahlnummer ins Internet. Wer per ISDN oder Modem online geht, zahlt dann eine wesentlich höhere Verbindungsgebühr. Dialer müssten sich unter Linux aber erst Root-Rechte verschaffen, um die Einwahlnummer zu ändern, und sie müssten für jede Distribution und Einwahltechniken die passende Stelle im System finden.

Die Vielfalt der Linux-Distributionen stellt Dialer-Programmen hohe Hürden in den Weg. Gänzlich unmöglich sind solche Angriffe auf Ihren Geldbeutel aber nicht. Ein gesundes Misstrauen gegenüber obskuren Wunderprogrammen, Internet-Beschleunigern und ähnlichen Software-Trickkisten aus dunklen Quellen bewahrt Sie vor unangenehmen Überraschungen.

Kein Kraut gewachsen ist gegen die moderne Form des Bauernfängers, das so genannte Phishing. Im großen Stil fälschen Internet-Kriminelle E-Mails, die ihre Empfänger auffordern, die Zugriffsdaten auf das Bankkonto oder den E-Bay-Account zu ändern. Die Adressen in diesen Mail sind natürlich gefälscht, die Webseiten auf die sie verweisen oft täuschend echt nachgebaut. Dagegen hilft nur ein großes Maß an Misstrauen: Glauben Sie keinen Empfehlungen aus unerwartet eintreffenden Mails und verwenden Sie beim Online-Banking ausschließlich ein Lesezeichen (Bookmark), um zur Bank-Seite zu navigieren. Das vermeidet Tippfehler und Verwechslungen mit ähnlich klingenden Namen, die zu Sites von Online-Räubern führen.

Gute Selbstverteidigung

Mit Linux benutzen Sie eine solide Basis, die sich gegen Eindringlinge aus dem Untergrund der Datennetze wehrt. Ihre Mithilfe vorausgesetzt, ist diese Abwehr auch sehr erfolgreich: So gilt Linux zu Recht als sicheres Betriebssystem mit verantwortungsvollen Benutzern, das getrost auf Virenscanner & Co verzichten kann. (fjl)

Infos

[1] Makro-Viren (englisch): Peter Seebach, "Macro virsues", August 2002, http://www.plethora.net/~seebs/ops/ibm/cranky18.html
[2] Windows-Viren unter Linux: Matt Moen, "Running Windows viruses with Wine", 26.01.2005, Newsforge, http://os.newsforge.com/article.pl?sid=05/01/25/1430222
[3] Ramen-Wurm: http://www.linux-community.de/story?storyid=848
[4] Lion-Wurm: http://www.linux-community.de/story?storyid=1196
[5] Updates einspielen: Achim Leitner, "Patches, Updates und Advisories -- so bleibt Linux sicher", EasyLinux 12/2004, S. 34

Dieser Online-Artikel kann Links enthalten, die auf nicht mehr vorhandene Seiten verweisen. Wir ändern solche "broken links" nur in wenigen Ausnahmefällen. Der Online-Artikel soll möglichst unverändert der gedruckten Fassung entsprechen.