Aktueller Überblick über freie Software und ihre Macher

Projekteküche

Auch im vergangenen Monat hat sich viel getan in der Welt der freien Software. Wir haben die Leckerbissen herausgepickt: Das IDS Samhain, Linux auf dem Linksys WRT54G Wireless Router sowie Updates für Debian GNU/Linux Woody. Feinschmecker bekommen diesmal türkisches Lahmacun. Martin Loschwitz

Abbildung 1: KDE 3.2 wartet mit vielen Verbesserungen auf. Die Entwickler haben nicht nur den Programmumfang erheblich vergrößert, es gibt auch neue Artworks, etwa das hier gezeigte Plastik-Theme.

Wenn die KDE-Entwickler ihren Zeitplan einhalten, steht KDE 3.2 beim Erscheinen dieses Heftes schon auf den Download-Servern bereit (geplantes Release-Datum ist der 2. Februar). Die neue Version lockt mit aktualisierten Menüs und Programmen sowie verbesserter Performance. Das Plastik-Theme poliert KDE grafisch auf. Mit der sich anbahnenden Integration von KDE und Gnome [1] ist auch für die fernere Zukunft einiges zu erwarten.

Samhain

Server vor Einbrüchen schützen gestaltet sich zunehmend schwieriger. Die Einbrüche in die Server des Debian- und weiterer Open-Source-Projekte (siehe [14]) machen es wieder deutlich: Sicherheitslücken haben fatale Folgen, die Server waren für mehrere Wochen nicht erreichbar. Während sich Programme wie Apache oder Sendmail im laufenden Betrieb updaten lassen, muss der Admin bei einem Update des Kernels, wie es bei den angesprochenen Angriffen nötig war, das System neu booten.

Noch schwieriger ist die Pflege mehrerer Computer: In Zentren, in denen ein Rechner kaum dem anderen gleicht, sind die Kernel vielfach für jedes Gerät und spezielle Aufgaben unterschiedlich konfiguriert. Großflächige Updates über ein Paketsystem sind damit unmöglich. Meist handelt es sich bei Sicherheitsproblemen im Kernel um lokale Verwundbarkeiten. Ein Angreifer kann den Rechner nur kompromittieren, wenn er Log-in-Zugang hat. Die Gefahr verringert sich, wenn es keine oder nur vertrauenswürdige lokale Benutzer gibt.

Viel gefährlicher sind solche Probleme, wenn auf einen Rechner viele Benutzer Zugriff haben, deren Integrität nicht immer gewährleistet ist. Administratoren, die mehrere solcher Rechner zu pflegen haben, können es kaum verhindern, dass eines der installierten Programme mal eine Sicherheitslücke hat. Das Risiko steigt zusätzlich, wenn ein Exploit kursiert. Kurzum: Totale Sicherheit gibt es nicht und Eingriffe ins System lassen sich niemals hundertprozentig ausschließen.

Einbruchserkennung

Wichtig ist also, dass das System einen Einbruch so schnell wie möglich erkennt. MD5-Checksummen von Dateien erstellen ist eine von vielen Möglichkeiten, um Einbrüche nachträglich zu entdecken. Das System ständig auf verdächtige Dateien hin zu prüfen ist allerdings extrem aufwändig. Daher gibt es fertige Lösungen, die diese Aufgaben übernehmen, so genannte File Integrity Checker, die zur Kategorie der Intrusion-Detection-Systeme (IDS) gehören. Bekannte Beispiele sind Tripwire [2] und die freie Alternative Aide [3].

Das von den Samhain Labs entwickelte IDS Samhain [4] funktioniert, ähnlich wie Aide, auf einer Vielzahl von unterschiedlichen Plattformen: Linux, FreeBSD, AIX 4, HP-UX 10.20, Solaris (2.6 und 2.8), Unixware 7.1.0 und Alpha/True64. Auch auf OpenBSD soll Samhain laufen, die Entwickler bestätigen dies aber nicht offiziell.

Bereits bei der Auswahl der Logdateien ist Samhain sehr flexibel: Es kann Logfiles auf einem zentralen Server sammeln. Das ist für große Netzwerke praktisch. Die Verbindung zwischen Client und Server ist dabei verschlüsselt. Eine andere Möglichkeit besteht darin, Logdateien per E-Mail zu senden. Samhain verwendet dazu einen eigenen Mailserver, um Beeinflussungen durch externe Mailserver zu verhindern. Außerdem hat der Anwender die Möglichkeit, Logdaten in einer PostgreSQL- oder MySQL-Datenbank zu speichern, aber auch klassisch in lokalen Dateien, die mit Signaturen geschützt sind.

Selbstschutz

Die Files, die Samhain überwachen soll, legt der Administrator in einer Liste fest. Dort sind Eigenschaften wie eine SHA1-Checksumme und Timestamps gespeichert. Auch diese Datei schützt das Programm mit einer GnuPG-Signatur vor Modifikationen. Ein System zur Einbruchserkennung muss sich auch selbst gegen Angriffe schützen. Wenn der Angreifer das IDS modifiziert, ist das komplette System nichtig.

Einen entsprechenden Schutz bietet Samhain mit GnuPG-signierten Logdateien und einem in die Binaries einkompilierten 64-Bit-Schlüssel. Dieser wird vor dem Kompilieren automatisch generiert und ist in jeder E-Mail und jedem Logeintrag enthalten. Stimmt eine Nachricht nicht mit diesem Key überein, weist der Mailserver sie zurück.

Samhain verfügt über eine Daemon-Funktion. Es läuft dann nach dem Start im Hintergrund und kann sich sogar verstecken, um von Dritten unbemerkt zu arbeiten. Findet der Angreifer kein IDS, wird er auch nicht versuchen, es auszuhebeln, getreu dem Motto „Security by obscurity“. Ein eigenes Kernelmodul verwischt sämtliche Spuren, die Samhain hinterlässt.

Das Webinterface Beltane [5], ebenfalls von den Samhain Labs entwickelt, erleichtert die Konfiguration von Samhain-Installationen in großen Netzen. Es bringt allerdings einige Einschränkungen mit sich: So setzt es eine Datenbank voraus, aus der es die Logdaten erhält. Nähere Informationen gibt es in der Samhain-FAQ [6] und auf der Website von Beltane.

Plumpe Einbrüche lassen sich meist bereits an einigen wenigen Besonderheiten feststellen – Panic-Meldungen im Logfile des Kernels sind immer ein Grund zur Beunruhigung. Wer aber erweiterte Sicherheit will, kommt um einen File Integrity Checker nicht herum. Für diesen Zweck ist Samhain mit seinem großen Funktionsumfang einen Blick wert.

Linux auf dem WRT54G

Der Siegeszug von Linux beschränkt sich nicht nur auf Desktop-Computer und Server. So ist es bereits seit längerem möglich, Linux auf der D-Box 2 zu installieren, um sich der unbeliebten Betanova-Software auf diesem Premiere-Decoder zu entledigen. Auf manche Hardware installieren die Hersteller heutzutage sogar schon Linux ab Werk.

Die meisten Benutzer interessiert die Firmware eines Geräts allerdings wenig. Für sie zählt lediglich, dass es so funktioniert, wie vom Hersteller versprochen. Auf dem 20. Chaos Communication Congress (kurz 20C3, [7]) spielte die Firmware von Computerhardware jedoch eine große Rolle – es gab unter anderem Vorträge darüber, wie man die installierte Firmware eines Geräts identifiziert.

Immer öfter versuchen nämlich Hardwarehersteller, die Vorteile von Linux zu nutzen, und passen den Sourcecode an ihre Geräte an, geben ihn dann aber nicht wieder heraus. Auf diese Weise halten sie die Interna ihrer Hardware geheim. Die GPL ist in dieser Hinsicht allerdings ziemlich eindeutig: Wer ein unter der GPL lizenziertes Programm als Binary vertreibt, muss den Sourcecode veröffentlichen.

Öffentliche Firmware

Die Firma Linksys gehört nicht zu diesen schwarzen Schafen: Auf der Website lässt sich unter [8] der Sourcecode zur Firmware des Wireless-LAN-Routers WRT54G herunterladen. So kam es, dass sich nach seiner Veröffentlichung viele findige Tüftler daran machten, die Software genauer zu untersuchen. Denn bekanntlich gibt sich in der Welt der freien Software kaum jemand lange mit dem zufrieden, was er erreicht hat. Immer wieder versuchen die Programmierer, noch ein Quäntchen Performance mehr oder noch eine kleine Verbesserung beim Speicherhandling aus der Software herauszuquetschen.

Die Hardware des Routers ist nicht spektakulär. Im Innern stecken ein Mips-Prozessor und 4 MByte Flashspeicher. Das Gerät kommt mit zwei externen Antennen, die sich allerdings nicht durch stärkere Modelle ersetzen lassen. Wie das G im Namen bereits ahnen lässt, ist Unterstützung für Wireless LAN mit 54 MBit/s (alias IEEE 802.11g) integriert. Außerdem fungiert das Gerät als Router mit NAT-Funktion, um ein Netzwerk ans Internet anzuschließen.

Interessanterweise lässt sich auf dem WRT54G auch ohne eigens angepasste Firmware einiges verändern. Das Einspielen eines neuen, eventuell sogar selbst erstellten Firmware-Image ist nämlich immer mit einem gewissen Risiko verbunden. Wird etwa der Access Point während des Flashvorgangs vom Strom getrennt, erleidet das Gerät unter Umständen erheblichen Schaden. Auch

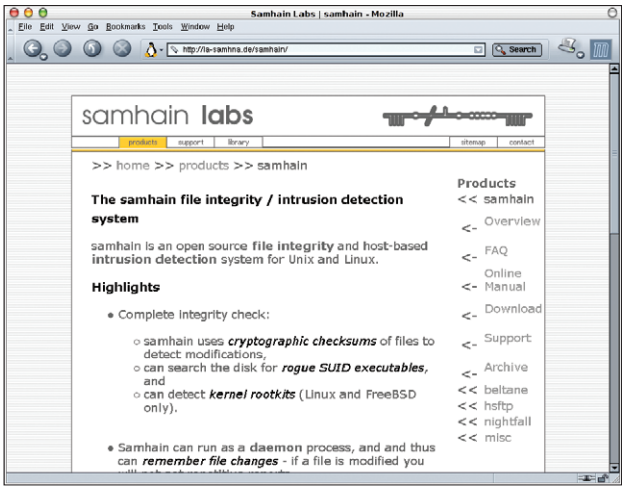

Abbildung 2: Das Intrusion-Detection-System (IDS) Samhain (hier die Projekt-Homepage) erkennt Manipulationen an Dateien. Dazu bietet es viele Funktionen.

dann, wenn das Flashen eines Image reibungslos abläuft, ist nicht sichergestellt, dass es funktioniert.

Wer die Firmware nicht komplett ersetzen möchte, nutzt einen Fehler in älteren Revisionen der mitgelieferten Firmware aus (ab 1.30.7, jedoch nicht in der Serie 1.41.x): Im Webinterface des Konfigurationsprogramms gibt es die Funktion, andere Rechner anzupingen. Die Datei »Ping.asp« greift dazu auf das Shellkommando »ping« zurück, hinter dem sich Busybox [9] verbirgt. In fehlerhaften Firmwareversionen lässt sich in das Feld für die IP-Adresse ein beliebiges Shellkommando eingeben etwa »`ps ax > /tmp/ping.log 2 > &1`«.

Shell-Zugriff mit den Wrt54gtools

Auf Dauer ist es allerdings recht unbequem, mit dem Webinterface zu hantieren. Was läge da näher, als eine Shell zu installieren? Die Wrt54gtools [10] von C. J. Collier enthalten eine Shell sowie einen Telnet-Daemon, mit dem sich dann Kommandos starten lassen. Auf diese Weise behebt der Benutzer zum Beispiel Fehler in der Firmware des WRT54G, etwa den im »ROUTER«-Modus, der Probleme beim Übergang von der WAN- zur LAN-Schnittstelle bereitet. Es ist sogar denkbar, einen SSH-Daemon auf dem Gerät zu installieren. Ob das sinnvoll ist, ist in Anbetracht der sehr langsamen Mips-CPU aber fragwürdig.

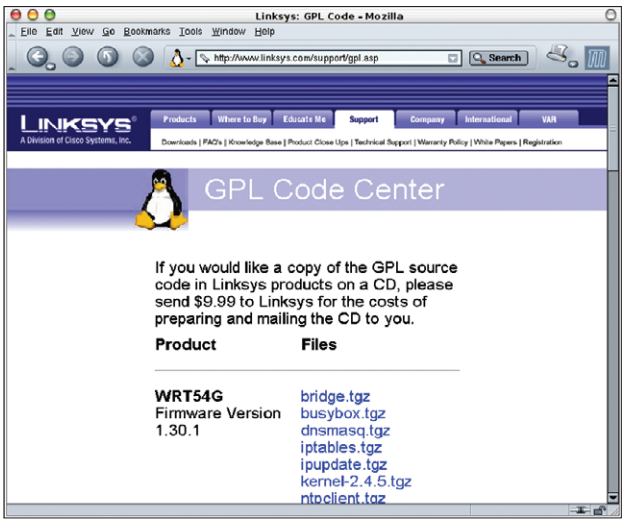

Abbildung 3: Die Firma Linksys ist einer der wenigen Hardwarehersteller, die ihre modifizierte Linux-Firmware im Sourcecode verfügbar machen. Erfahrene Linuxer bauen sich so ihr eigenes Linux-System für den WLAN-Router WRT54G.

Doch auch mit dem Web-basierten Konfigurations-Interface lässt sich so manche Einstellung des Access Points verändern. Die Parameter »wl_antdiv« sowie »wl_txant« beeinflussen die Leistung der Antennen und »et0macaddr« ändert die MAC-Adresse des Access Points. Wer mit Webinterfaces auf Kriegsfuß steht, für den gibt es das Programm »wl« auf dem Router. Es ist sogar möglich, den bekannten WLAN-Paket-Sniffer Kismet zu installieren (siehe [11]).

Um die Firmware aus den Sourcen zu kompilieren, benötigt der Anwender lediglich ein Linux-System mit einem GCC, der Binaries für die Mips-Architektur erstellt. Dann ergibt sich jedoch wieder das Risiko eines Geräteschadens beim Update der Firmware.

Wer einen ordentlichen Access Point für die eigenen vier Wände sucht, dürfte mit dem WRT54G gut bedient sein. Durch Linux als Betriebssystem und dazu noch einen Fehler im Webinterface bietet das Gerät Vorteile, die es sehr attraktiv machen. Die Möglichkeit, ein eigenes, an die persönlichen Wünsche angepasstes Firmware-Image aufzuspielen, lässt viele Tüftlerherzen höher schlagen.

Debian GNU/Linux Woody aufmöbeln

Die neue Version von Debian GNU/Linux (3.1, Codename Sarge) kommt bestimmt – irgendwann. Wer bis dahin ein aktuelles Betriebssystem auf Basis der stabilen Woody-Release einsetzen möchte, hat also offiziell schlechte Karten. Mittlerweile gibt es jedoch Projekte, die dem abhelfen wollen. Auch einzelne Entwickler haben inzwischen veralteter Software in Woody den Kampf angesagt.

Der Ansatz ist immer derselbe: Die Entwickler kompilieren Pakete aus dem Unstable-Zweig (Sid) für Woody. Diese Methode hat einen Vorteil gegenüber einem Upgrade auf Debian GNU/Linux Testing – man bringt lediglich ein spezifisches Programm (und seine Abhängigkeiten) auf den aktuellen Stand. Das Basissystem, also Pakete wie Libc6, sind von solchen Updates nicht betroffen. Sollte es Probleme mit einem Programm geben, ist es leicht wieder zu entfernen. Downgrades von Testing auf Stable hingegen sind mit einiger Bastelei verbunden.

Linux 2.6 gibt es auch für Woody

In technischer Hinsicht ist das Portieren eines Pakets von Sid auf Woody meist kein Problem. Oft genügt es, das Paket einfach auf einem Woody-System erneut zu erstellen. Gelegentlich sind dazu zwar weitere Pakete erforderlich, die der Entwickler vorher bauen muss, bei kleinen Abhängigkeitsketten hält sich der Aufwand aber in Grenzen. Der erste Freiwillige, der bereits frühzeitig, nämlich kurz nach der Release von Woody damit begann, Pakete von Unstable nach Stable zu portieren, ist Adrian Bunk. Er war selbst Entwickler bei Debian, hat das Projekt allerdings verlassen, weil er mit dem Release-Management nicht einverstanden war.

Bunk führt mit seinen Portierungen nun fast schon eine Tradition fort. Benutzer, die Linux 2.4 auf Debian GNU/Linux 2.2 (Codename Potato) verwenden wollten, erinnern sich vermutlich noch gut an seinen Namen. Mit Potato war es nämlich nicht möglich, den Kernel 2.4 zu benutzen. Er benötigte aktuelle Modutils, die für Potato einfach nicht verfügbar waren. Adrian Bunk portierte seinerzeit kurzerhand die Pakete von Unstable nach Stable. Derartige Probleme sind mittlerweile Geschichte, denn mit Woody sind aktuelle 2.4er Kernel ja kein Problem mehr. Bunk beschloss aber offensichtlich, auch Woody mit Backports verschiedener Pakete zu versorgen – und das in viel größerem Stil, als es noch bei Potato der Fall war.

Seine Website ist in zwei Bereiche aufgeteilt, zum einen die Pakete, die Bunk als „sehr stark getestet“ und „stabil“ einstuft, zum anderen einige Pakete, die als „nicht so stark getestet“ markiert sind.

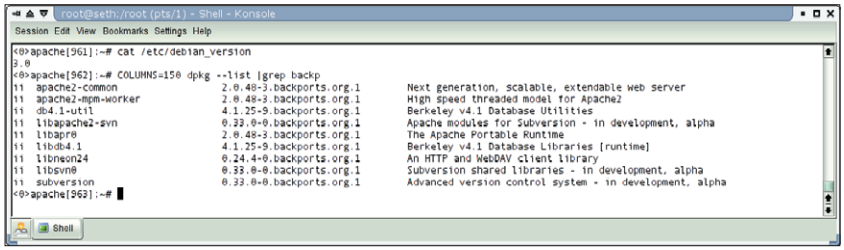

Abbildung 4: Dpkg liefert den Beweis: Dank des Backports-Projekts von Norbert Tretkowski laufen Apache 2 und Subversion auf einem Debian-Woody-System. Auch XFree86 4.2 und Mozilla 1.5 gibt es nun für Woody.

Die beiden Kategorien enthalten Pakete wie GCC 3.3, Mozilla 1.2 und Open Office 1.0.3. Bei den weniger stark getesteten Paketen finden sich – es lässt sich fast schon ahnen – die Pakete, die zum Betreiben von Linux 2.6 auf Woody notwendig sind (unter anderem die »module-init-tools«).

Das zweite Projekt hat Norbert Tretkowski, ein offizieller Debian-Entwickler, ins Leben gerufen. Der Name ist hier Programm: Das Backports-Projekt [12] erstellt Backports von sehr vielen Unstable-Paketen auf Woody. Der Umfang an Paketen ist wesentlich größer als bei Adrian Bunk. Fast jedes bekannte Programm ist hier vertreten, dazu zählen XFree86 4.2, Vim, Mozilla 1.5 und Apache 2. Eine Aufteilung in verschiedene Stränge hat Norbert Tretkowski nicht vorgenommen.

Der Trick mit den Abhängigkeiten

Das tut der Sache aber keinen Abbruch. Wer die Backports per Apt ins System einspielen möchte, muss nämlich für jedes Paket einen Eintrag in der »/etc /apt/sources.list« vornehmen. Der Trick ist dabei, dass die »Packages.gz«-Datei, die im Verzeichnis für jedes Paket existiert, die kompletten Abhängigkeiten dieses Pakets enthält. Deswegen installiert Apt dann, wenn der Anwender ein Paket explizit einträgt, alle Abhängigkeiten ohne besonderen Befehl mit. Noch ein kurzer Hinweis: Wer die Services von Backports verwenden möchte, möge bitte einen der zahlreichen Mirror-Server von [13] verwenden, um den Hauptserver zu entlasten.

Eines der wichtigsten Updates für die meisten Desktop-Anwender ist wohl KDE 3. Die Version 3.0 kam etwa zehn Tage vor der Release von Woody heraus, weshalb sie nicht mehr den Weg auf die Woody-CDs fand. Doch das ist kein Problem, da jeder KDE-Mirror jeweils aktuelle Pakete auch für Woody bereithält. Den größten Anteil an der Arbeit daran trägt Ralf Nolden. Er pflegt auch die Debian-spezifischen Dateien im CVS-Tree des KDE-Projekts mit.

Es ist mittlerweile also nicht mehr zwangsläufig so, dass auf aktuelle Software verzichten muss, wer Woody installiert hat. Allerdings sollten es interessierte Anwender lieber nicht übertreiben. Vermutlich kollidieren einige Pakete von Adrian Bunk mit denen von Backports, was zu Inkonsistenzen im System führen könnte.

Lahmacun (türkische Pizza)

Zutaten für den Hefeteig: 1 kg Mehl, 42 g Hefe, zirka ein halber Liter Milch, etwas Salz, eine Prise Zucker, eine Tasse Öl.

Zutaten für den Belag: 500 g gehacktes Fleisch, fünf bis sechs Zwiebeln, vier Knoblauchzehen, ein Bund Petersilie, eine Dose geschälte Tomaten, 200 bis 300 g Öl, zwei Esslöffel Margarine, Tomatenmark, Paprikamark (gibt es im türkischen Lebensmittelgeschäft), Salz, Pfeffer.

Zubereitung des Teigs: Das Mehl in eine Schüssel geben, die Hefe in die Mitte des Mehlhaufens. Mit lauwarmer Milch, Öl, Salz sowie dem Zucker verkneten. Danach mindestens eineinhalb Stunden zugedeckt stehen lassen.

Zubereitung des Belags: Zwiebeln, Knoblauch, Petersilie und Tomaten klein schneiden und mit dem Fleisch, der Margarine, dem Tomatenmark und dem Paprikamark sowie mit Salz und Pfeffer vermischen.

Nach eineinhalb Stunden den Teig nochmals durchkneten und dann je nach Vorliebe entweder kreisförmig oder quadratisch auf dem Backblech dünn ausrollen. Danach den Belag gleichmäßig auf dem Teig verteilen. Anschließend in einen vorgeheizten Backofen bei 250°C Ober- und Unterhitze schieben. Die Backzeit sollte vor Ort selbst bestimmt werden, sechs Minuten sind aber der empfohlene Mindestwert.

Guten Appetit und bis zum nächsten Mal

Während also der Ofen die Pizza auf Betriebstemperatur bringt, noch der obligatorische Aufruf: Wer ein Tool schätzt oder entwickelt hat und es an dieser Stelle vorgestellt sehen möchte, schickt eine E-Mail an [15]. Alle Hinweise sind willkommen. *(mwe)* ■

Infos

[1] GTK+-Programme und KDE: [https://www.linux-community.de/Neues/story?storyid=11629]
[2] Tripwire: [http://www.tripwire.org/]
[3] Aide: [http://www.cs.tut.fi/~rammer/aide.html]
[4] Samhain: [http://la-samhna.de/samhain/]
[5] Beltane: [http://la-samhna.de/beltane/]
[6] Die Samhain-FAQ: [http://la-samhna.de/samhain/s_faq.html]
[7] 20. Chaos Communication Congress: [http://www.ccc.de/congress/2003/]
[8] GPL Download Center von Linksys: [http://www.linksys.com/support/gpl.asp]
[9] Busybox: [http://www.busybox.net/]
[10] Wrt54gtools: [http://www.seattlewireless.net/index.cgi/Wrt54gTools]
[11] Kismet auf dem WRT54G: [http://www.seattlewireless.net/index.cgi/LinksysWrt54g#head-2755b98d6bf5b10da8a5d1cff01df93b319e51a6]
[12] Backports für Debian: [http://www.backports.org/]
[13] Spiegelserver von Backports: [http://www.backports.org/mirrors.html]
[14] Einbruch in Debian-Server: Linux-Magazin 03/04, Editorial und News
[15] Hinweise und Vorschläge: [projektekueche@linux-magazin.de]

Der Autor

Martin Loschwitz ist Schüler aus Niederkrüchten und hilft in seiner Freizeit, die Debian-GNU/-Linux-Distribution weiterzuentwickeln. Zurzeit arbeitet er am Debian-Desktop-Projekt.