

## 17 Sicherheit im System

Beim Durcharbeiten dieses Buchs konnten Sie bereits mehrfach Hinweise auf Sicherheitsaspekte lesen, so z. B. Informationen zu

- Virenschutz in den Kapiteln 3 und 16,
- verschlüsselten Internetzugriffen in den Kapiteln 5 und 6,
- Absicherung von FTP-Servern im Kapitel 7,
- Passwortverschlüsselung im Kapitel 9 und
- Firewalls im Kapitel 14.

Die Informationen des Ihnen hier vorliegenden Kapitels befassen sich etwas allgemeiner mit dem Thema Sicherheit.

Dazu gehören:

- Informationen über Sicherheitsprobleme,
- Aktualisieren von Programmen und Systemdateien,
- erkennen von Einbruchversuchen und Einbrüchen und
- erkennen schwacher Passwörter.

Sie müssen sich aber immer darüber im Klaren sein, dass Sicherheit, vor allem wenn Internetverbindung besteht, kein Zustand ist, sondern eine dauernde anstrengende Arbeit.

Scheuen Sie diese Arbeit, werden Sie bzw. Ihre Organisation vielleicht bald in der Schadensstatistik vorkommen.

### 17.1 Informationen über Sicherheitsprobleme

Wenn Sie Murpheys Gesetz glauben, gibt es keine fehlerfreien Programme. Das betrifft leider auch die Linux-Welt, obwohl hier zumindest Systemabstürze selten sind. Viele Programme haben aber kleine Fehler, die sich im normalen Betrieb nicht bemerkbar machen. Sie können z. B. nur Eingaben von maximal 255 Zeichen Länge verkraften und stürzen bei längeren Eingaben ab. Das ist so lange kein Problem, wie bei der bestimmungsgemäßen Nutzung nur kurze Eingaben auftauchen. Eventuell wird dieses Problem nie jemand bemerken. Hacker suchen aber gezielt nach solchen Fehlern und überschwemmen die Programme mit unsinnigen Eingaben.



Unter der URL <http://www.suse.de/de/security/> finden Sie die aktuellen Sicherheitsinformationen.

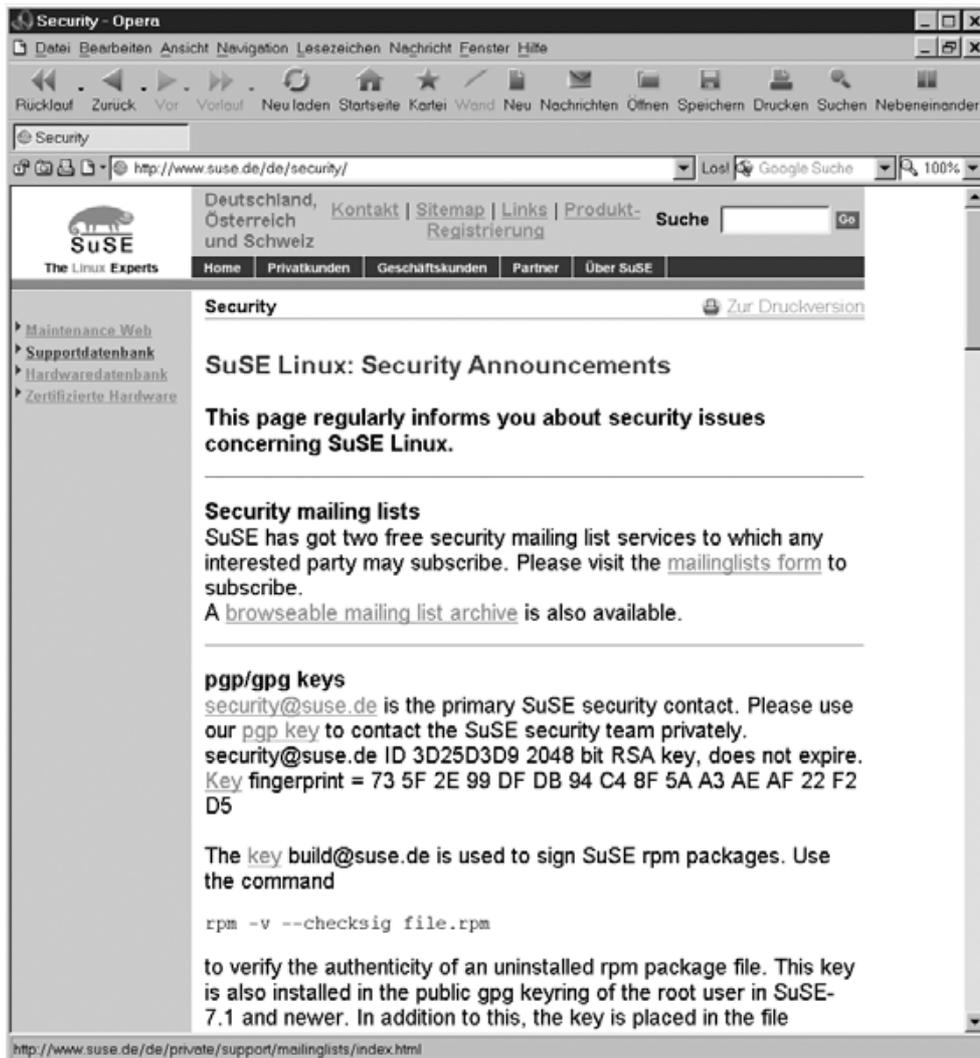


Abbildung 17.1: Sicherheitsinformationen bei SuSE

Für die Information per Mail finden Sie an der Adresse <http://www.suse.de/de/private/support/maillinglists/> eine Übersicht über die Mailinglisten von SuSE, die Sie von dieser Seite aus abonnieren können. Sicherheitsfragen behandeln vor allem die Listen `suse-security-announce@suse.com` und `suse-security@suse.com`. Über die Liste `security-announce` macht SuSE selber auf Probleme aufmerksam, in der Liste `security` können Sie auch Fragen stellen und sich an Diskussionen in englischer Sprache beteiligen.

### 17.1.2 Bugtraq/Securityfocus

An der Adresse <http://www.securityfocus.com/> finden Sie unabhängige Sicherheitsinformationen für verschiedene Betriebssysteme sowie Virusinformationen.

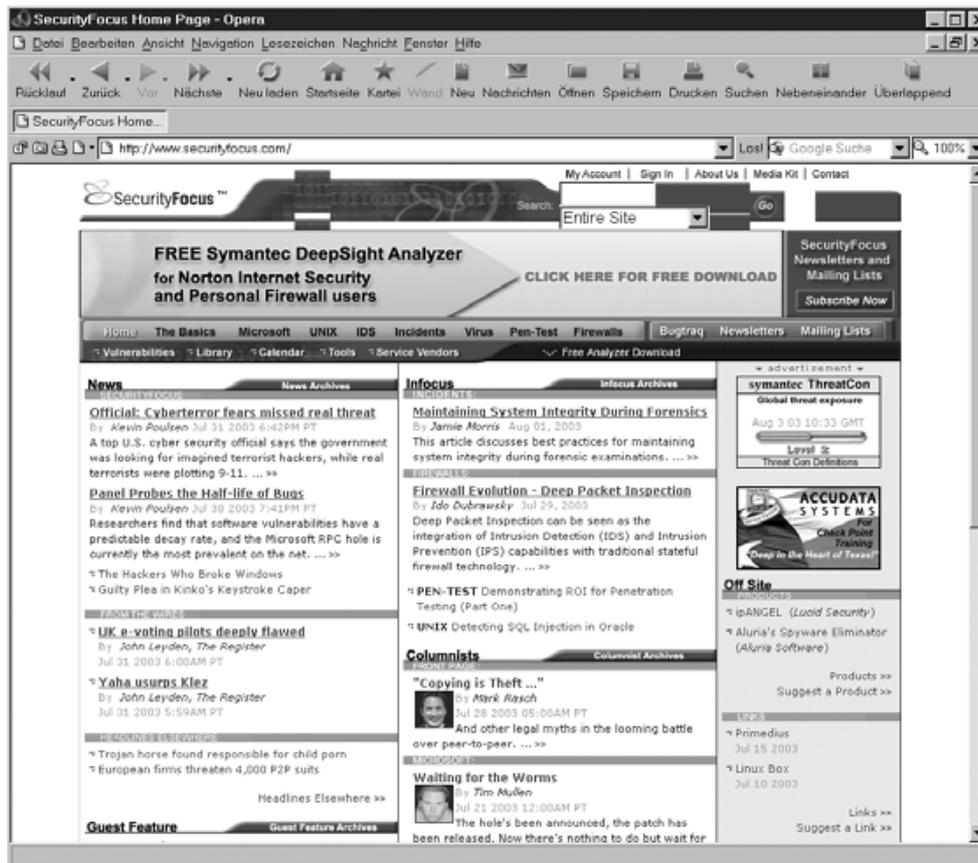


Abbildung 17.2: Sicherheitsinformationen bei SecurityFocus

Sehr weit verbreitet und beliebt ist die zugehörige Mailingliste [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com), die Sie an der URL <http://www.securityfocus.com/subscribe> abonnieren können. Wenn Sie Systeme mit verschiedenen Betriebssystemen betreuen, ist diese Liste eine wichtige Ergänzung zu der SuSE-Liste. Außerdem sind hier aktuelle Informationen meist deutlich schneller vorhanden.

### 17.1.3 Cert

Eine sehr anerkannte Institution in Sicherheitsfragen ist das CERT Coordination Center an der Carnegie Mellon University.

Eine Übersicht bekannter ausnutzbarer Programmfehler (Vulnerabilities) finden Sie ausgehend von der Seite <http://www.kb.cert.org/vuls/>.

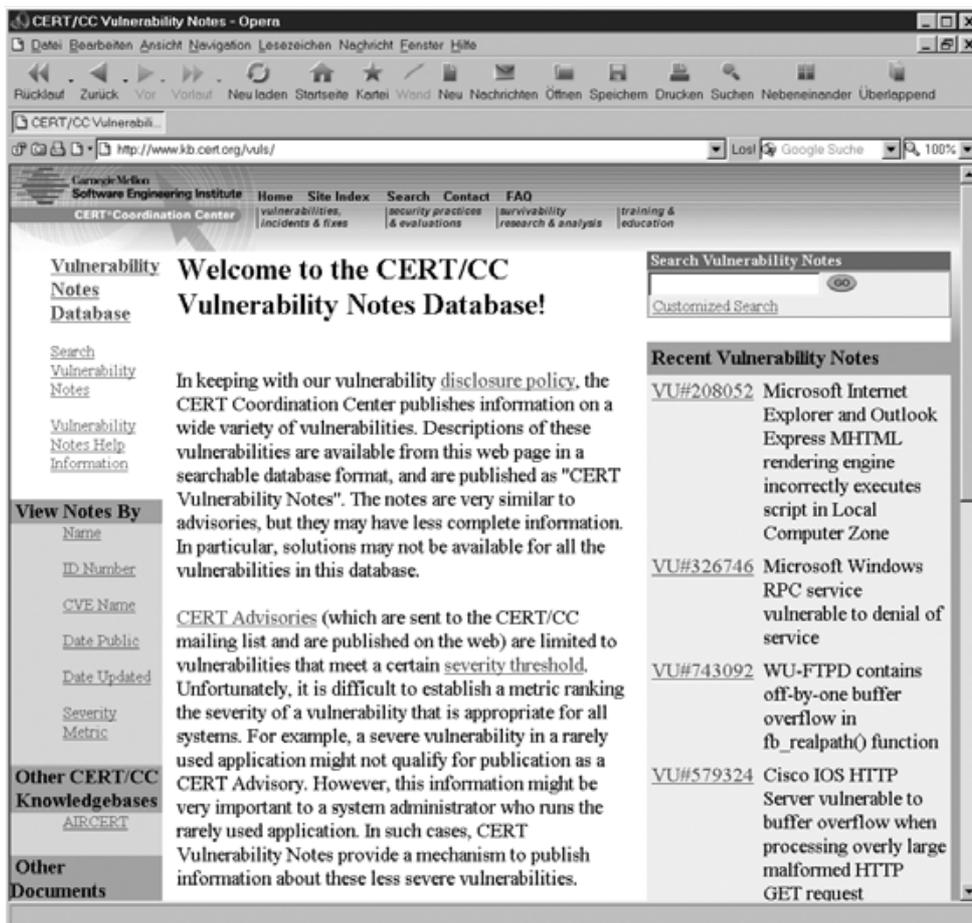


Abbildung 17.3: Vulnerability Informationen beim Cert

Die zugehörigen Lösungsvorschläge (Advisories) stehen an der URL <http://www.cert.org/advisories/>.

### 17.1.4 Heise Security

Relativ neu ist das Angebot des Heise-Verlags an der URL <http://www.heise.de> bzw. <http://www.heise.de/security/>.

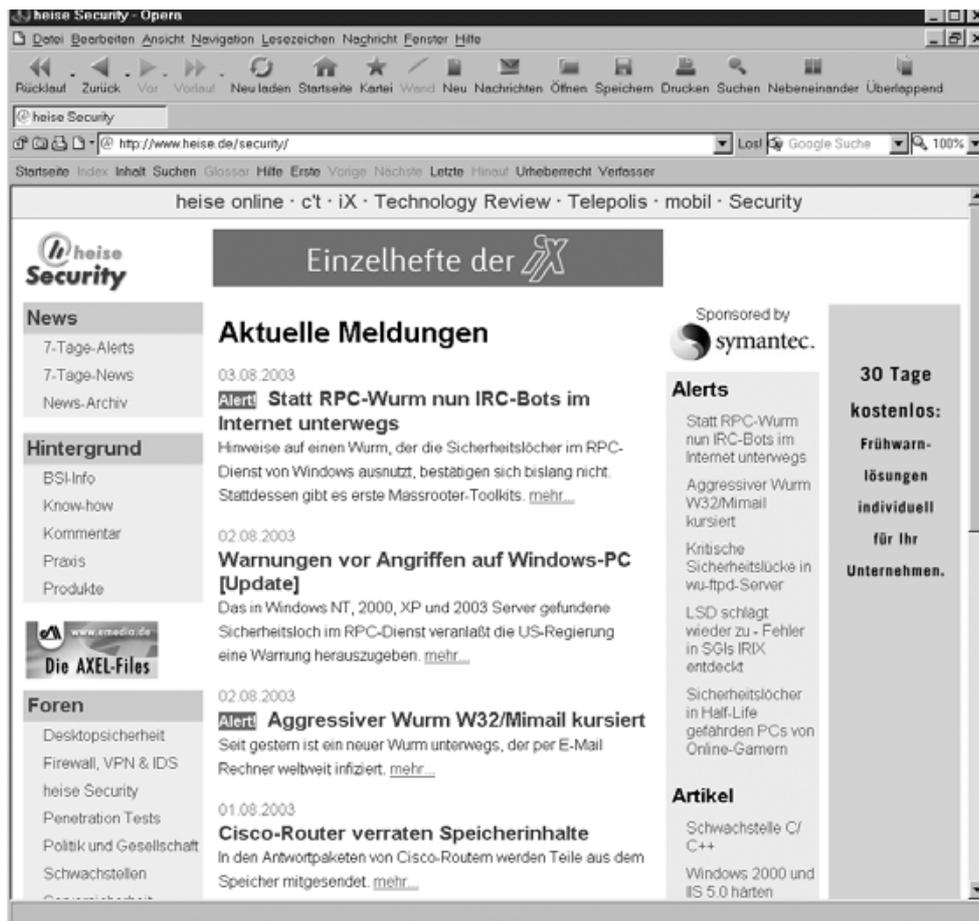


Abbildung 17.4: Heise Security

Die deutschsprachigen Heise-Seiten sind auf den hiesigen Markt abgestimmt. Sie finden hier aktuelle Sicherheitsmeldungen, eine Fülle von Hintergrundinformationen zum Thema Sicherheit und Diskussionsforen zum Thema. Unter der Rubrik *Dienste* können Sie Ihren Browser auf Sicherheitsmängel testen.

Wenn Sie Internetsysteme mit guter Anbindung und vielen Nutzern betreiben, sollten Sie Stammgast auf diesen Seiten werden.

## 17.2 Programme und Systemdateien aktualisieren

Die Programme und Systemdateien, die Sie von der SuSE-CD installieren, sind naturgemäß schon einige Wochen alt. In der Zwischenzeit wurden eventuell Fehler gefunden bzw. bereinigt. Der Vorteil der Linux-Gemeinde besteht ja gerade darin, dass sie Sicherheitsprobleme nicht verschweigt, sondern offen diskutiert und löst.

Sie könnten die verfügbaren Patches direkt vom FTP-Server unter `ftp://ftp.suse.com/pub/suse/i386/update/8.2/rpm/i586/` beziehen. Die hier angebotenen rpm-Pakete kann man nicht zur Neuinstallation nutzen, da SuSE in diese Pakete jeweils nur die korrigierten Dateien packt, um den Download-Umfang zu reduzieren.

### 17.2.1 YOU

Einfacher als Laden vom FTP-Server ist SuSEs automatisiertes Update-Verfahren, das *YaST Online Update* (YOU).

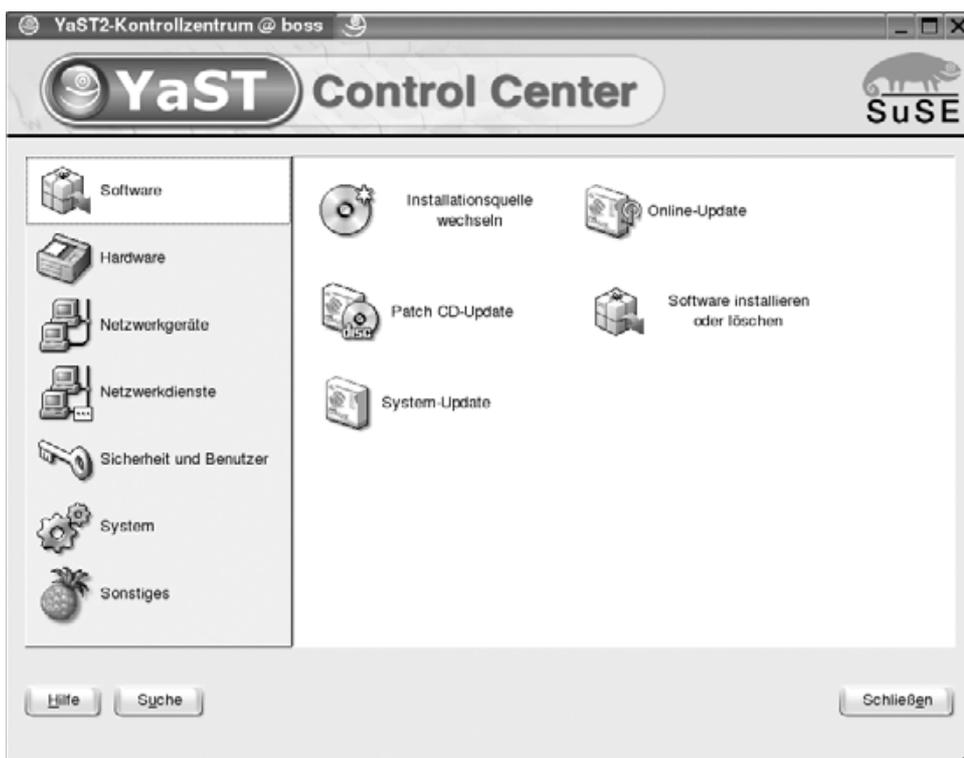


Abbildung 17.5: YaST: Online Update

Wenn Sie YaST starten, finden Sie das Online-Update in der Rubrik *Software*.

**Hinweis:** Das Online-Update kann natürlich nur klappen, wenn Ihr Rechner über eine funktionsfähige Internetanbindung verfügt.

Nach dem Start des Programms müssen Sie einen FTP-Server auswählen und sich zwischen automatischem und manuellem Update entscheiden.

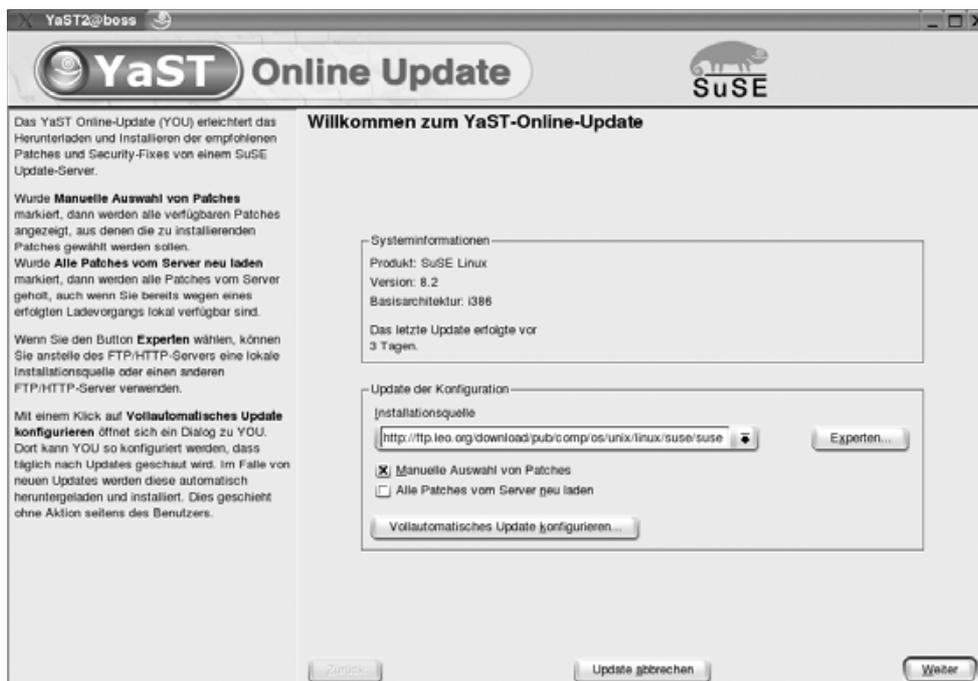


Abbildung 17.6: YOU: Installationsquelle

Um nur die wirklich benötigten Pakete zu laden, wählen Sie das manuelle Update. In der Auswahlliste *Installationsquelle* können Sie den FTP-Server bestimmen, von dem Sie die Dateien beziehen möchten. Viele Server, speziell im Hochschulbereich, spiegeln die SuSE-Server und eignen sich daher ebenfalls als Update-Quelle. Meist sind sie sogar deutlich schneller als die SuSE-Server.

Über den Button *Vollautomatisches Update konfigurieren* können Sie einen Cron-job einrichten lassen, der Ihr System automatisch jeden Tag aktualisiert, sofern eine Internetverbindung vorliegt.



Abbildung 17.7: YOU: Automatisch

Sie sollten sich das aber gut überlegen, ob Sie dem YOU so weit vertrauen, dass es Ihr System ohne Kontrolle aktualisieren darf. Das manuelle Update ist zwar etwas lästiger, aber Sie wissen auch genau, was YOU an Ihrem System verändert.

Falls Sie mehrere Rechner mit gleichen SuSE-Versionen aktualisieren wollen, ist es einfacher, die Pakete einmal zu laden und dann per NFS oder Datenträger auf den anderen Rechnern einzuspielen. Dazu dient der Button *Experten...* über den Sie zu einer Auswahl der Installationsmedien kommen.

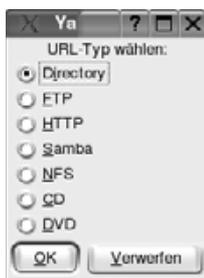


Abbildung 17.8: YOU: Experten

Wenn Sie beim manuellen Update auf *Weiter* klicken, lädt YaST eine Liste der zur Verfügung stehenden aktuelleren Pakete. Falls ein Update für das Online-Update zur Verfügung steht – auch das kann mal passieren –, sehen Sie nur ein einziges Paket, welches Sie auch installieren müssen. Normalerweise bekommen Sie nach dem Laden der Dateiliste das folgende Auswahlfenster mit den verfügbaren Patches.

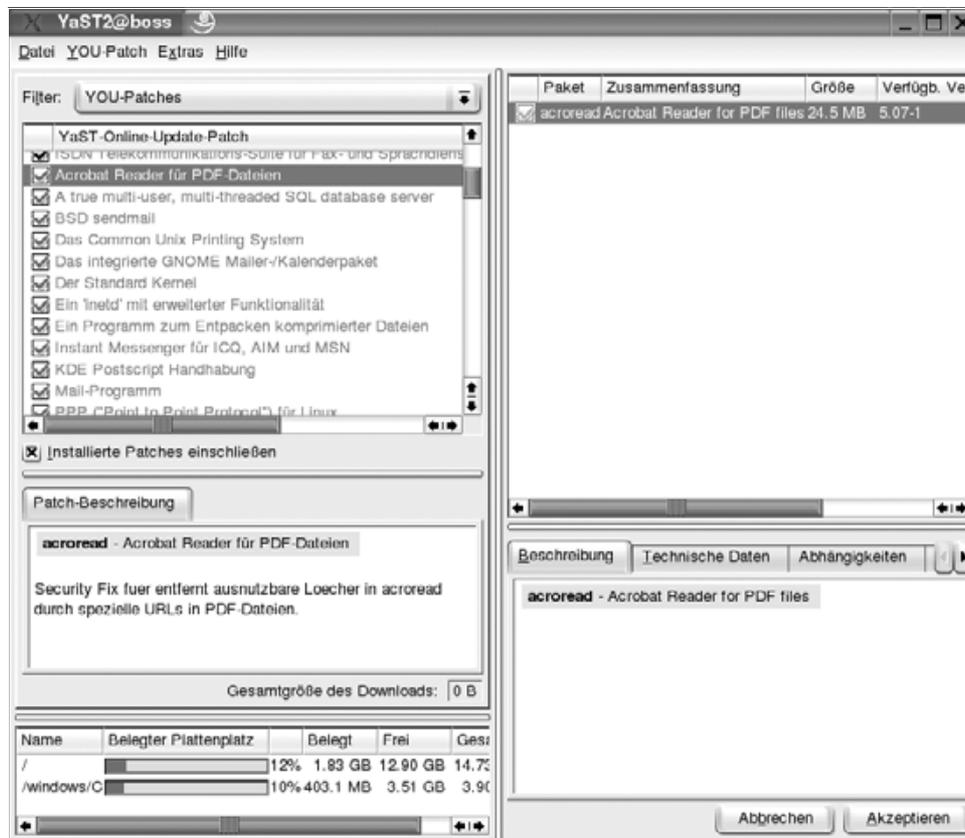


Abbildung 17.9: YOU: Liste der verfügbaren Patches

Gehen Sie diese Liste ruhig einmal durch. Mit einem Häkchen markiert YOU alle bei Ihnen installierten Pakete, die es aktualisieren möchte. Dabei sind alle *sicherheitsrelevanten* Updates in Rot dargestellt, *empfohlene* Updates in Blau. Zusätzlich gibt es noch *optionale* Updates in Schwarz, dabei ist z. B. ein Paket mit Microsoft-Schriften, die SuSE nicht direkt ausliefern kann.

Entfernen Sie hier auf alle Fälle die Pakete, die Sie bereits aus anderen Quelle aktualisiert haben, wie z. B. den Virenschanner AntiVir.

Wenn Sie dann auf *Weiter* klicken, beginnt YOU mit dem Laden der Pakete. Sie sollten unterhalb von `/var/lib/YaST2/you/` über entsprechend viel Festplattenkapazität verfügen, bei den Tests der Autoren immerhin einige Megabyte.

Nach dem Laden aller Pakete beginnt YaST, diese Pakete zu installieren und aktualisiert gegebenenfalls auch die Konfigurationsdateien.

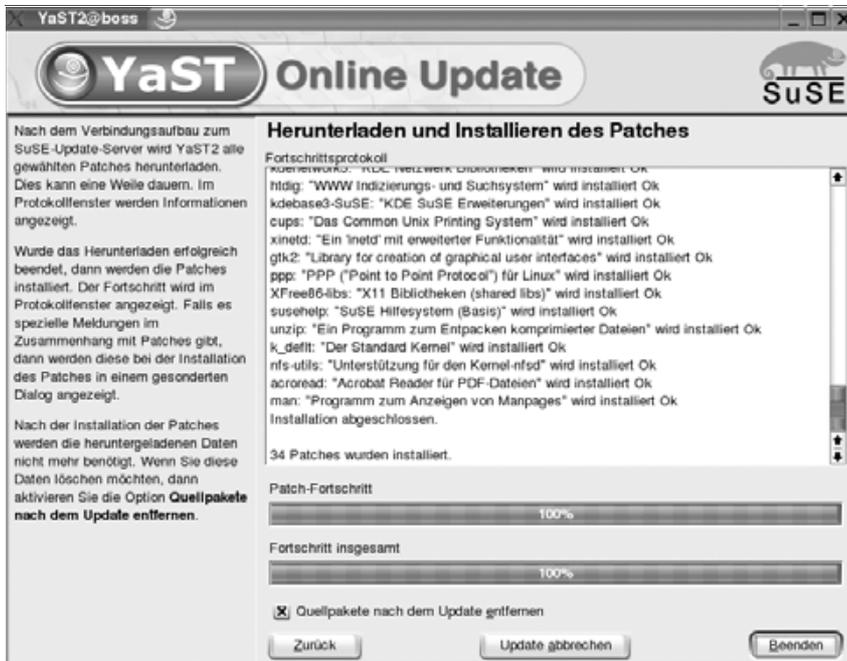


Abbildung 17.10: YOU: Laden der Patches



Abbildung 17.11: YOU: Aktualisierung der Konfigurationsdateien

Damit ist Ihr erstes Online-Update abgeschlossen.

Sie müssen den Update-Vorgang regelmäßig wiederholen, da SuSE immer wieder neue Pakete zur Verfügung stellt. Die weiteren Updates gehen dann auch wesentlich schneller, da nur die in der Zwischenzeit erneuerten Pakete zu laden sind. Machen Sie doch das Update zu einer regelmäßigen Einrichtung!

### 17.2.2 *fou4s*

Das YaST Online Update ist ein recht schweres Geschütz. Die Autoren haben schon mehrfach Server betreut, vor allem solche mit wenig Speicher, auf denen das Programm irgendwann nicht mehr laufen wollte. Das Problem tritt hauptsächlich bei der textbasierten Version von YaST auf.

Auf Servern, die man per SSH aus der Ferne betreut, ist es nicht immer sinnvoll, nur für das regelmäßige Online-Update eine grafische Anwendung zu starten.

Hier bietet sich das Programm *Fast OnlineUpdate for SuSE* (*fou4s*) an, das Sie kostenlos von der Website <http://fou4s.gaugusch.at/> beziehen können. Der Autor Markus Gaugusch hat hier ein nützliches kleines Werkzeug geschaffen, das die SuSE-Versionen von 7.1 bis 8.2 online aktualisieren kann.

Die momentan aktuelle Version ist 0.9.3, was sich aber bis zum Erscheinen des Buchs sicherlich noch ändern wird. Laden Sie das rpm-Archiv des Programmpakets in ein beliebiges Verzeichnis und installieren Sie es von dort.

```
wget http://fou4s.gaugusch.at/download/fou4s-0.9.3-0.noarch.rpm
rpm -i fou4s-0.9.3-0.noarch.rpm
```

Danach ist das Programm ohne weitere Konfigurationshandlungen einsatzbereit. In der Voreinstellung bezieht *fou4s* alle Informationen vom Server <ftp.gwdg.de>, Sie können aber jederzeit mit dem Befehl

```
/usr/sbin/fou4s --server
```

einen beliebigen anderen Server auswählen, der die SuSE-Dateien spiegelt.

Sodann rufen Sie mit dem folgenden Befehl die Beschreibungsdateien für die Patches vom ausgewählten Server ab:

```
/usr/sbin/fou4s -u
```

Jetzt können Sie abfragen, welche Updates und Veränderungen für Ihr System anstehen:

```
/usr/sbin/fou4s -ev
```

Der Schalter `-e` steht dabei für *Evaluation*, `fou4s` prüft, was zu tun wäre, nimmt aber noch keinerlei Updates oder Änderungen vor. Der Schalter `-v` steht für *verbose* und erhöht die Informationsmenge.

Eine typische Ausgabe könnte folgendermaßen aussehen. Zuerst überprüft `fou4s` die vorhandenen Informationen über Patches, dann bietet es diejenigen Patches zum Download an, die für den Linux-Rechner relevant sind.

```
boss:~ # fou4s -ev
ftp.gwdg.de: Checking [#####] 100 %

=== Update Information for XFree86-server-37046 (2003-06-25) ===
X Window System server and modules
Hardware cursor position on Intel i845/i855/
i865 chipsets fixed. Xvideo
performance improved dramatically.
=====
New XFree86-server 4.3.0-63 (old 4.3.0-
15) [optional, 989kB] [d1]
NOTE: Package XFree86-server contains pre-install information.
You must use interactive mode to install this package.

===== Update Information for fetchmsttfonts-3 (2003-06-25) =====
Download Microsoft(c) TrueType Core Fonts
For legal reasons we can't include the Microsoft(c) TrueType
Core Fonts in our product. This patch downloads these fonts and
installs them on your system. Please note that about 4 MByte
data are downloaded therefore. License for the fonts will be
installed as /usr/share/doc/corefonts/EULA.html.
=====
New fetchmsttfonts script (old none) [script, 0kB] [d1]
NOTE: Script fetchmsttfonts must be installed in interactive
mode.

===== Update Information for fetchnvidia-1 (2003-06-25) =====
Download NVIDIA(c) Graphics Driver
For legal reasons we can't include the graphics driver of NVIDIA
(c) in our product. This patch downloads this driver and
installs it on your system. Please note that about 6 MByte data
are downloaded therefore. License for the driver and the install
er itself will be copied to /usr/share/doc/nvidia.
=====
New fetchnvidia script (old none) [script, 0kB] [d1]
NOTE: Script fetchnvidia must be installed in interactive mode.
Checking for deleted files ...
```

Sie sehen hier drei optionale Pakete im Angebot, die bisher noch nicht installiert wurden. Zu jedem der Pakete sehen Sie die Beschreibung von SuSE. Im vorliegenden Fall ist fou4s auch nicht bereit diese Pakete automatisch zu installieren, sondern fordert ein interaktives Update.

Sie können auch gleich das automatische Update starten mit:

```
/usr/sbin/fou4s -i
```

oder das interaktive mit

```
/usr/sbin/fou4s -i --interactive
```

Leser, die Programmen nicht blind vertrauen, werden das interaktive Update vorziehen, das für jedes Paket mehrere Optionen anbietet.

Mit einem Tastendruck auf

- [Y]es            lassen Sie das Paket aktualisieren,
- [N]o            lassen Sie das Paket bei diesem Durchlauf nicht aktualisieren,
- [S]kip          legen Sie fest, dass fou4s das Paket jetzt und zukünftig nicht aktualisiert,
- [D]escription   lassen Sie sich die Beschreibung anzeigen.

Da fou4s mit Proxy-Servern zusammenarbeiten kann, können Sie Online-Updates ohne direkten Internetzugriff ausführen. Im einfachsten Fall tragen Sie dazu Proxy-Informationen, Benutzerdaten und ein Passwort in die Konfigurationsdatei von fou4s ein:

/etc/fou4s.conf (ab Zeile 56)

```
# HTTP Proxy to use for downloads - must begin with
# http:// and end with / !!!
Proxy=http://router.lokales-netz.de:3128/
#
# Proxy username (default: none)
ProxyUser=debacher
#
# Proxy password (default: none)
ProxyPasswd=geheim
#
```

Die Autoren setzen Fou4s auf den von ihnen betreuten Servern häufiger ein als YOU.

## 17.3 Einbruchserkennung

Das Aktualisieren von Programmpaketen dient dazu, Einbrüche dadurch zu erschweren, dass Sie Programme mit bekannten Sicherheitslücken durch korrigierte Versionen ersetzen.

Eine absolute Sicherheit vor Hackern kann aber auch dies nicht bieten. Wenn es zu Einbrüchen in den von Ihnen betreuten Systemen kommen sollte, sollten Sie diese möglichst schnell erkennen.

Einbrüche lassen sich nicht immer ganz einfach erkennen, da die Einbrecher oft Systemprogramme durch veränderte Versionen ersetzen. Beliebte Veränderungen an den Programmen `ps` und `ls`, damit diese die Verzeichnisse und Programme der Einbrecher nicht anzeigen.

Ein recht einfaches, aber durchaus wirkungsvolles System der Einbruchserkennung besteht daher darin, Prüfsummen der wichtigsten Systemdateien zu erstellen und diese regelmäßig zu vergleichen. Wenn Einbrecher Systemdateien verändern, ändern sich die Prüfsummen, was eindeutig auf einen Einbruch hinweist.

Die Autoren haben mit dem Programm Claymore zur Einbruchserkennung (intrusion detection), das Sie von <http://www.securityfocus.com/tools/1675> kostenlos laden können, gute Erfahrungen gemacht.

```
wget http://www.securityfocus.com/data/tools/claymore03.tar.gz
```

Das Perl-Programmpaket ist sehr klein. Entpacken Sie das Archiv mit

```
tar xvfz claymore.tar.gz
```

Dabei entsteht ein Verzeichnis `claymore-0.3` (die Versionsnummer kann sich ändern), in das Sie mit

```
cd claymore-0.3
```

wechseln.

Kopieren Sie das Programm in das Verzeichnis `/root/bin`

```
cp claymore.pl /root/bin
```

Das Programm arbeitet mit zwei Dateien

- `light.list`
- `light.db`

Die erste Datei enthält eine Liste der zu überwachenden Programme mit vollständiger Pfadangabe und die zweite Datei zusätzlich die jeweiligen Prüfsummen. In diese Prüfsummen gehen sowohl der Dateiinhalt als auch das Dateidatum mit ein, so dass Veränderungen sofort zu erkennen sind.

Beide Dateien legt das Programm im Home-Verzeichnis des aufrufenden Benutzers ab, also in `/root/claymore-0.3`. Legen Sie also bitte dieses Verzeichnis an.

```
mkdir /root/claymore-0.3
```

Das Programm schlägt eine Liste der zu überwachenden Dateien vor, wenn Sie den Parameter `-m` mit angeben. Diese Liste können Sie so an die richtige Stelle bringen:

```
/root/bin/claymore.pl -m > /root/claymore-0.3/light.list
```

Dann müssen Sie die Datei mit den Prüfsummen initialisieren:

```
/root/bin/claymore.pl -r
```

Das dauert jetzt etwas, da sehr viele Dateien in der Liste stehen.

Jedes Mal, wenn Sie hinfert

```
/root/bin/claymore.pl
```

aufrufen, erzeugt das Programm für jede Datei in der `light.list` eine Prüfsumme und vergleicht diese mit dem in der Datei `light.db` gespeicherten Wert.

Sowie es eine Abweichung gibt, warnt Claymore an der Konsole und an die konfigurierbare Mail-Adresse.

In dem Programm können Sie ein paar Einstellungen leicht verändern, vor allem den Mail-Empfänger für die Virenwarnungen.

`claymore.pl` (Auszug ab Zeile 21)

```
#####
# info to customize
$USER = ''; # (optional) address to email warnings, try
    ↓ 'root@localhost'
#####
# PATHs, these should be adjusted to match your system
$DB_FILE = "$ENV{'HOME'}/claymore-$::VERSION/light.db";
$LIST_FILE = "$ENV{'HOME'}/claymore-$::VERSION/light.list";
$MAIL = '/bin/mail';
```

Geben Sie in der Variablen `$USER` eine sinnvolle Mail-Adresse für die Warnungen an, möglichst eine auf einem anderen Rechner!

Um Einbrechern das Auffinden des Programms zu erschweren, sollten Sie die Dateinamen für die Listen und das Programm selbst ändern,

Wenn das Programm zu Ihrer Zufriedenheit konfiguriert ist, sollten Sie es per Crontab regelmäßig aufrufen lassen. Mit

```
05 * * * * /root/bin/claymore.pl
```

veranlassen Sie eine stündliche Überprüfung der Systemdateien.

Sie müssen nun aber bei jedem Online-Update daran denken, dass Sie die Datenbank von Claymore mit

```
/root/bin/claymore.pl -r
```

neu erzeugen, da Sie sonst nach dem Update stündlich eine Fehlermeldung bekommen.

**Hinweis:** Auch das Programm Claymore und ähnliche Programme bieten keine absolute Sicherheit. Allein schon diese Beschreibung macht das System unsicherer, weil bekannter.

## 17.4 Erkennen schwacher Passwörter

Passwörter in Unix-Systemen können normalerweise noch nicht einmal die Systemverwalter ermitteln, weil Linux die Passwörter nur verschlüsselt ablegt. Die zugehörige Verschlüsselungsfunktion ist eine Einwegfunktion, die kein Entschlüsseln vorsieht. Meldet sich ein Benutzer am System an, verschlüsselt Unix dieses Passwort und vergleicht es mit der in der Shadow-Datei abgelegten Version. Eine Entschlüsselung ist also nicht notwendig.

Es gibt trotzdem theoretisch ein einfaches Verfahren, die Passwörter zu knacken: Sie probieren einfach alle Möglichkeiten durch. Der Aufwand hierfür hängt sehr von der Passwortlänge ab, wie Sie an der folgenden Tabelle sehen können. Diese Tabelle geht davon aus, dass 62 verschiedene Zeichen zur Verfügung stehen, die 26 lateinischen Buchstaben einmal klein, einmal groß und die zehn Ziffern. Weiter geht die Berechnung davon aus, dass Sie 10 Millionen Kennwörter pro Sekunde überprüfen können.

| Passwortlänge | Zahl der möglichen Passwörter | Zeitbedarf zum Knacken |
|---------------|-------------------------------|------------------------|
| 1             | 62                            | keiner                 |
| 2             | 3844                          | keiner                 |
| 3             | 238.328                       | keiner                 |
| 4             | 14.776.336                    | 1,4 Sekunden           |
| 5             | 916.132.832                   | 1,5 Minuten            |
| 6             | 56.800.235.584                | 1,5 Stunden            |
| 7             | 3.521.614.606.208             | 4 Tage                 |
| 8             | 218.340.105.584.896           | 8 Monate               |
| 9             | 13.537.086.546.263.552        | 43 Jahre               |
| 10            | 839.299.365.868.340.224       | 2660 Jahre             |

Tabelle 17.1: Sicherheit in Abhängigkeit von der Passwortlänge

Die Sicherheit eines Passworts hängt nicht nur von seiner Länge, sondern auch stark vom verwendeten Zeichensatz ab. Die folgende Tabelle geht von einer einheitlichen Passwortlänge von 8 Zeichen aus, wobei wieder 10 Millionen Passwörter pro Sekunde geprüft werden.

| Zeichensatz            | Zeichen-<br>zahl | Zahl der möglichen Passwörter | Zeitbedarf<br>zum Knacken |
|------------------------|------------------|-------------------------------|---------------------------|
| 8-Bit ASCII            | 256              | 18.446.744.073.709.551.616    | 58.500 Jahre              |
| 7-Bit ASCII            | 128              | 72.057.594.037.927.936        | 228 Jahre                 |
| Buchstaben und Ziffern | 62               | 218.340.105.584.896           | 8 Monate                  |
| nur Buchstaben         | 52               | 53.459.728.531.456            | 62 Tage                   |
| nur Kleinbuchstaben    | 26               | 208.827.064.576               | 6 Stunden                 |
| Wörter aus Wörterbuch  | -                | ca. 250.000                   | nahezu keiner             |

**Tabelle 17.2: Sicherheit in Abhängigkeit vom Zeichensatz bei jeweils 8 Zeichen**

Da viele Benutzer Passwörter mit deutlich weniger als acht Zeichen benutzen, gibt es eine durchaus realistische Chance, diese Passwörter zu knacken. Die Chance erhöht sich noch dadurch, dass Einbrecher nicht alle Kombinationen durchprobieren müssen. Viele Anwender benutzen Namen, Telefonnummern oder Ähnliches, die sie sich leicht merken können.

Wenn Sie Knack-Tests ein Wörterbuch zu Grunde legen, können Sie bei einer Passwortlänge von acht Zeichen bereits in wenigen Minuten Erfolg haben.

Sie können damit zwar nicht die Passwörter aller Benutzer knacken, aber 50% innerhalb weniger Minuten sind ein durchaus realistischer Wert.

**Hinweis:** Schon ein einzelner geknackter Zugang ist ein Sicherheitsrisiko. Einbrecher, die einen Zugang zu Ihrem System haben, können dort nach weiteren Schwachpunkten suchen.

Sie sollten daher regelmäßig versuchen, die Passwörter Ihrer Benutzer zu knacken, um wenigsten die unsichersten Kandidaten zu ermahnen.

Beim Knacken und beim Ermahnen der Benutzer kann das Programm `john` helfen, dass Sie bei SuSE im Paket `john` auf der *CD4* bzw. in der Paketgruppe *Productivity • Security* finden. Nach dem Installieren dieses Programms finden Sie das Programm selber unter `/usr/sbin/john` und seine Komponenten unter `/var/lib/john/`.

Das Programm kann mit einem Wörterbuch arbeiten, es liefert auch eine englische Version mit. Sie müssten hier erst ein deutsches Wörterbuch erstellen. Hinweise dazu finden Sie im Verzeichnis `/usr/share/doc/packages/john/`.

Dieser Aufwand ist sogar unnötig, meist langt es sogar, mit den Daten in den Benutzerdateien zu arbeiten. Damit können Sie Passwörter knacken, die aus Namen oder Variationen davon bestehen.

Wechseln Sie in das Verzeichnis `/var/lib/john/`.

```
cd /var/lib/john
```

Nun lassen Sie aus `passwd` und `shadow` eine einheitliche Datei montieren, im Beispiel heißt sie `passwd.john`:

```
unshadow /etc/passwd /etc/shadow > passwd.john
```

Wenn Sie `john` mit den Daten aus dieser Datei arbeiten lassen, werden Sie staunen, wie viele Passwörter er ermittelt.

```
john -single passwd.john
```

Mit diesem Befehl nutzt `john` nur die Benutzerdatenbank als Grundlage, keines der zusätzlich verfügbaren Wörterbücher.

Wenn Sie bereits viele Benutzer angelegt haben, dauert das Knacken schon eine Weile. Wenn Sie den Fortschritt kontrollieren wollen, drücken Sie einmal die Leertaste, worauf `john` den aktuellen Stand anzeigt.

```
Loaded 1037 passwords with 426 different salts (Standard DES
                                         ↵ [24/32 4K])
Burak          (bs1002)
laura          (lc1001)
sandra         (kj1002)
laura          (lt1002)
christi        (sw1002)
gast0          (gast)
ahmad-fa       (ak1005)
ann-kath       (ag1005)
wolf-die       (wm1004)
walter         (ja1001)
guesses: 10  time: 0:00:00:05 71% c/
s: 370569  trying: &tc3001& - *j5c*
```

Hier hat `john` nach knapp 5 Sekunden bereits 10 von etwa 1000 Passwörtern geknackt. Bei dem Datenbestand aus dem Beispiel hatte `john` nach knapp 2 Minuten bereits mehr als 70 Passwörter geknackt und das im einfachsten Modus.

Wenn Sie `john` unterbrechen, setzt er bei einem Neustart seine Arbeit an der Stelle fort, wo Sie ihn unterbrochen hatten. Die bereits geknackten Passwörter hält er in der Datei `john.pot` fest. Falls Sie erneut alle Passwörter testen wollen, müssen Sie diese Datei vorher löschen.

Das Ergebnis der Arbeit von `john`, eine Liste der Benutzerdaten inklusive Passwort im Klartext, können Sie mit

```
john -show passwd.john
```

ansehen. `John` zeigt dabei nur die Accounts, deren Passwort `john` ermitteln konnte.

Wenn `john` mit der Arbeit fertig ist, können Sie ihn auch veranlassen, eine Mail an alle Benutzer zu schicken, deren Passwörter er knacken konnte. Dazu finden Sie im Verzeichnis ein Programm `mailer`, das Sie zuerst mit

```
chmod u+x mailer
```

ausführbar machen und dann folgendermaßen aufrufen:

```
./mailer passwd.john
```

Damit ist jeder Ihrer nachlässigen Benutzer verwarnt.

Den im Original englischen Text der Mail an die Benutzer kann man in dem Perl-Programm `mailer` relativ leicht ändern. Wenn englischsprachige Warnungen einige Ihrer Benutzer überfordern könnten, sollten Sie den Text übersetzen.

```
#!/bin/bash
#
# This file is part of John the Ripper password cracker,
# Copyright (c) 1996-98 by Solar Designer
#
if [ $# -ne 1 ]; then
    echo "Usage: $0 PASSWORD-FILE"
    exit 0
fi

# There's no need to mail users with these shells
SHELLS=-,/bin/false,/dev/null,/bin/sync

# Look for John in the same directory with this script
DIR="`echo "$0" | sed 's,/[^/]*$,,'`"

# Let's start
$DIR/john -show "$1" -shells:$SHELLS | sed -n 's/:.*//p' |
(
    SENT=0

    while read LOGIN; do
        echo Sending mail to "$LOGIN"...
# You'll probably want to edit the message below
        mail -s 'Unsicheres Passwort' "$LOGIN" << EOF
```

```
Hallo!

Das Passwort für den Account "$LOGIN" ist unsicher. Bitte ändern
Sie es umgehend, sonst macht das Ihr Systembetreuer;-)

Gruss,
    Password Checking Robot
    im Auftrag Ihres Systembetreuers
EOF
    SENT=$(( $SENT+1 ))
    done
    echo $SENT messages sent
)
```

Wenn Sie sich ausführlicher mit der Dokumentation von `john` beschäftigen, werden Sie noch mehr Möglichkeiten finden, um weitere Passwörter zu knacken. Eventuell hilft Ihnen diese Erfahrung, Ihre eigenen Passwörter zu ändern.

Machen Sie sich und auch Ihren Benutzern immer wieder klar, dass Sicherheit kein Zustand ist, sondern ein anstrengender Prozess. Ein Teil dieses Prozesses ist u. a. die Wahl geeigneter Passwörter.

## 17.5 Portscanner

Im Kapitel 14 konnten Sie lesen, wie Sie einzelne Ports gezielt für den Zugriff aus dem Internet sperren können. Je weniger Dienste Sie anbieten, je weniger Ports also offen sind, desto geringer ist die Chance für Angreifer, in Ihr System einzudringen.

Sie sollten sich nicht darauf verlassen, dass Ihr Firewall-System wie gewünscht funktioniert, sondern es gezielt kontrollieren. Dazu kann ein *Portscanner* für Sie den Zustand aller Ports ermitteln.

Ein sehr weit verbreiteter Portscanner ist das Programm *nmap*, das Sie bei SuSE auf *CD4* bzw. in der Paketgruppe *Productivity • Networking • Diagnostic* im Paket *nmap* finden. Installieren Sie dieses Programm nach.

Um Ihren eigenen Rechner testen zu können, brauchen Sie ein anderes Gerät, von dem aus Sie *nmap* benutzen können.

Wenn Sie mit den Voreinstellungen arbeiten wollen, reicht *nmap* die Angabe der Rechneradresse, entweder als Name oder als IP.

```
nmap 192.168.1.2
```

Nun ist das Programm eine Weile beschäftigt. Je stärker ein System abgeschottet ist, desto länger benötigt *nmap* für seine Untersuchungen. Sie bekommen dann eine Ausgabe der folgenden Art:

```

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on boss.lokales-netz.de (192.168.1.2):
(The 1587 ports scanned but not shown below are in state:
└─ closed)
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
25/tcp    open       smtp
53/tcp    open       domain
80/tcp    open       http
110/tcp   open       pop-3
111/tcp   open       sunrpc
443/tcp   open       https
658/tcp   open       unknown
809/tcp   open       unknown
1024/tcp  open       kdm
1025/tcp  open       NFS-or-IIS
3128/tcp  open       squid-http
6000/tcp  open       X11

Nmap run completed -- 1 IP address (1 host up)
└─ scanned in 6 seconds

```

Hier im Beispiel sind recht viele Ports offen. Das ist zunächst nicht weiter tragisch, da der Scan innerhalb des lokalen Netzes erfolgte.

Ein Scan über das Internet dürfte aber auf keinen Fall derartig viele offene Ports zeigen. Im Idealfall zeigt der Scan, dass alle Ports geschlossen sind, zumindest wenn Sie keinerlei Dienste nach außen anbieten wollen. Ansonsten dürfen nur genau die Ports offen sein, die zu benötigten Diensten gehören.

```

(The 1599 ports scanned but not shown below are in state:
└─ filtered)
Port      State      Service
22/tcp    open       ssh
80/tcp    open       http

Nmap run completed -- 1 IP address (1 host up)
└─ scanned in 169 seconds

```

Bei diesem System ist nur der Web-Server und der SSH-Zugang erreichbar.

Speziell bei Konfigurationsarbeiten am Firewall-System sollten Sie Ihren Rechner regelmäßig von einem anderen System aus scannen.

**Hinweis:** Portscans auf fremde Rechner gelten zumindest als unfreundliche Aktionen. Manche Provider ahnden übermäßige Scan-Aktivitäten mit dem Trennen der Verbindung.