15 Sicherheit im System

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

- Virenschutz in den Kapiteln 3 und 14,
- Verschlüsselten Internet-Zugriffen in den Kapiteln 5 und 6,
- Absicherung von FTP-Servern im Kapitel 7,
- Passwortverschlüsselung im Kapitel 9 und
- Firewalls im Kapitel 12

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 Einbruchsversuchen und Einbrüchen und
- Erkennen schwacher Passwörter.

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

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

15.1 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.

Ein Beispiel für ein solches Problem (*Code Red*), das den Internet-Server von Windows-Systemen betrifft, werden Sie sehr häufig in den Log-Dateien Ihres Web-Servers finden. Dort tauchen Zeilen auf wie:

```
24.141.103.24 - - [09/Jun/2003:20:57:58 +0200] "GET /
default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u
7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090
%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/
1.0" 400 330
```

Hier hat der aufrufende Rechner einen überlangen Parameter an das Programm `/default.ida` übergeben, das auf den Internet-Servern von Windows-Systemen vorhanden ist. Die ersten Zeichen dienen nur dazu, die von Microsoft vorgesehene Länge zu überschreiten. Die Zeichen dahinter sind ein Programmcode.

Viele Programme, wie hier der Web-Server, laufen mit besonderen Rechten und übertragen diese Rechte beim Absturz auf Programmcode, der Teil der Eingabe ist.

Der hier als Beispiel angeführte Wurm *Code Red* ist nicht in der Lage, Apache-Web-Server zu befallen, aber ein mit diesem Wurm befallener Rechner versucht nach einem Zufallsprinzip, andere Rechner zu befallen.

Weitere Informationen zum Wurm Code Red finden Sie im Cert Advisory unter `http://www.cert.org/advisories/CA-2001-19.html`

Auch in der Linux-Welt gibt es Programme mit ähnlichen Sicherheitsproblemen. In der letzten Zeit sind mehrfach Probleme bei FTP-Servern und SSH-Dämonen bekannt geworden. Sie können die Sicherheit bzw. Unsicherheit Ihrer Programme in der Regel nicht ohne weiteres abschätzen, aber versuchen Sie, sich über bekannte Probleme zu informieren.

Im Web bieten mehrere Web-Server und Mailing-Listen Sicherheitsinformationen für Linux. Linux-Systemverwalter sollten diese Informationen regelmäßig lesen und die zugehörigen Mailing-Listen abonnieren.

15.1.1 SuSE

Da Sie mit einem SuSE-System arbeiten, ist deren Web-Server die nahe liegende Informationsquelle für Sicherheitsfragen. Der Vorteil dieser Web-Site besteht darin, dass hier auch Lösungsvorschläge bzw. Aktualisierungen für Programme des SuSE-Systems zu finden sind, auch wenn sie jetzt unter dem Novell-Logo läuft.

An der URL `http://www.novell.com/linux/security/securitysupport.html` finden Sie die aktuellen Sicherheitsinformationen.

Abbildung 15.1: Sicherheitsinformationen bei Novell/SuSE

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

15.1.2 Bugtraq/Securityfocus

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

Abbildung 15.2: Sicherheitsinformationen bei SecurityFocus

Sehr weit verbreitet und beliebt ist die zugehörige Mailing-Liste `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.

15.1.3 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 15.3: Vulnerability Informationen beim Cert

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

15.1.4 Heise Security

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

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.

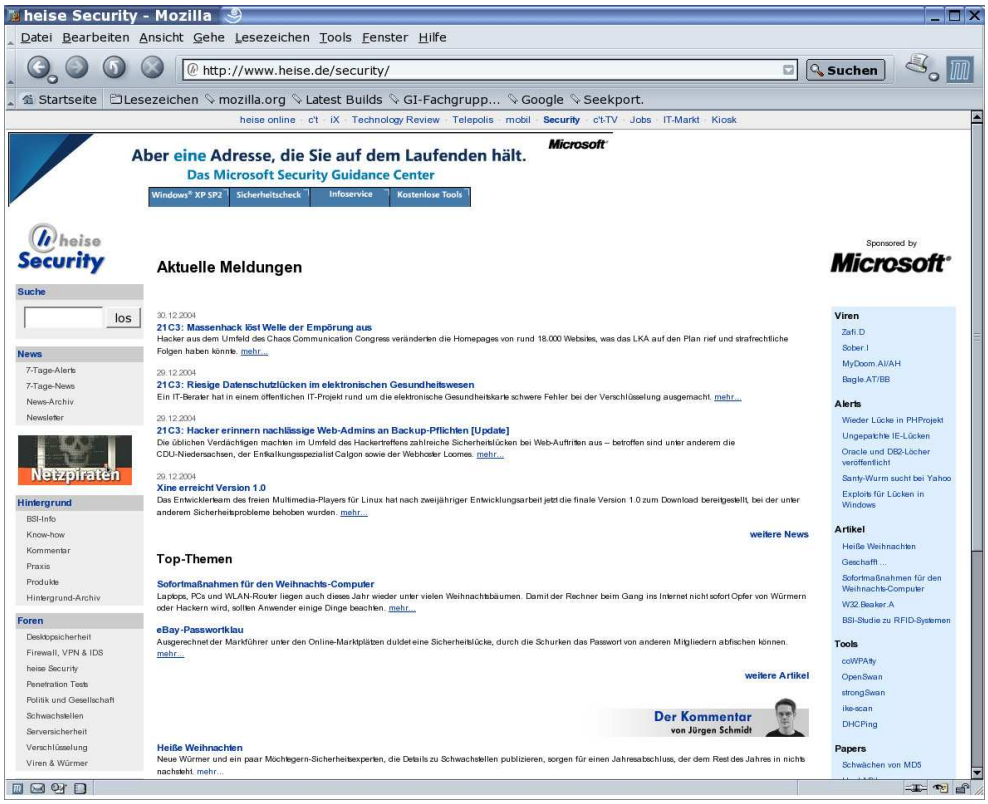

Abbildung 15.4: Heise Security

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

15.2 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 an der Adresse `ftp://ftp.suse.com/pub/suse/i386/update/9.2/rpm/i586/` beziehen, oder einem der anderen FTP-Server mit den SuSE-Dateien (siehe Abschnitt 2.5). 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.

15.2.1 YOU

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

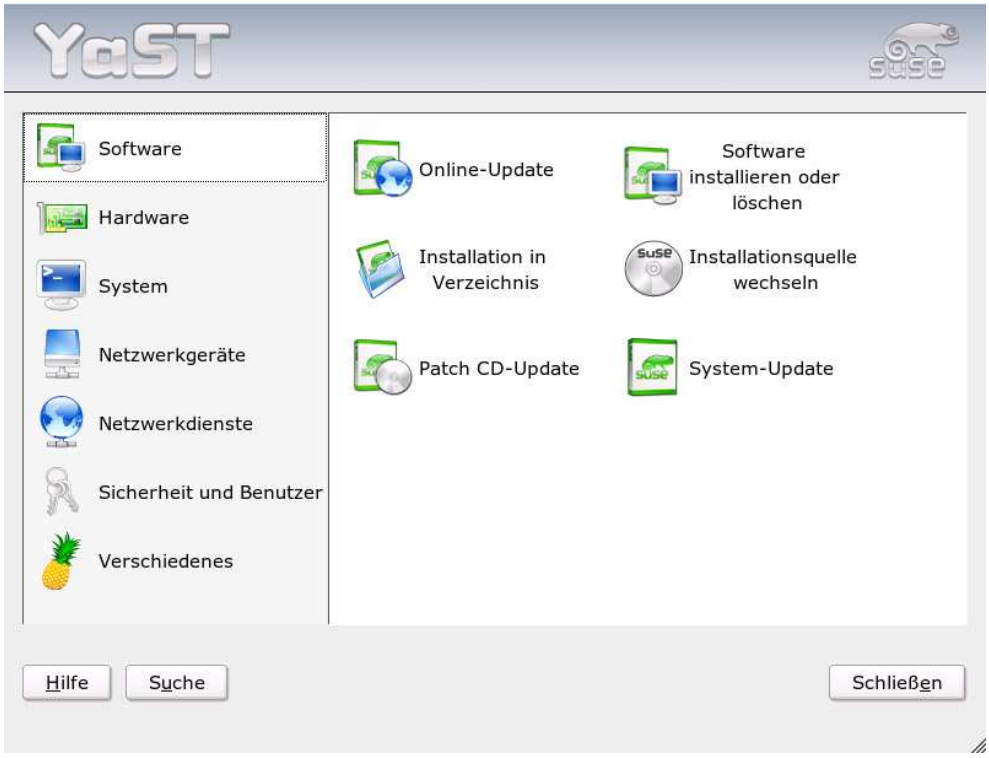

Abbildung 15.5: YaST: Online-Update

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

Hinweis: Das Online-Update kann natürlich nur funktionieren, wenn Ihr Rechner über eine funktionsfähige Internet-Anbindung verfügt.

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

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.

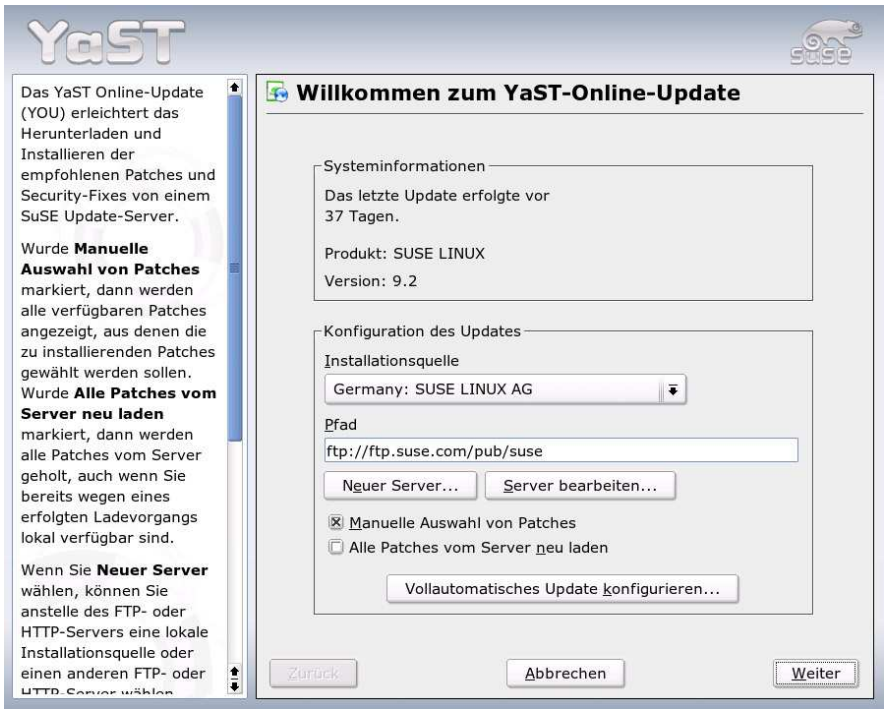

Abbildung 15.6: YOU: Installationsquelle

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

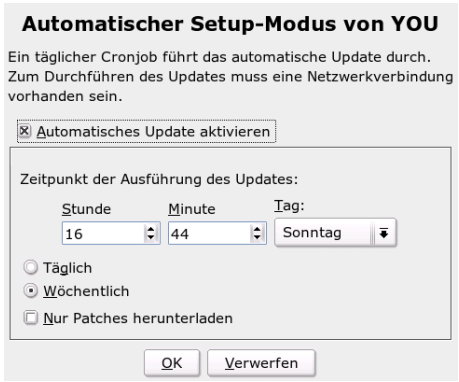

Abbildung 15.7: YOU: Automatisch

Sie sollten sich gut überlegen, ob Sie 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 ändert.

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. Mit der Schaltfläche *Neuer Server*... können Sie Installationsmedien auswählen.

Abbildung 15.8: YOU: Neuer Server

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, das Sie auch installieren müssen. Normalerweise bekommen Sie nach dem Laden der Dateiliste das folgende Auswahlfenster mit den verfügbaren Patches.

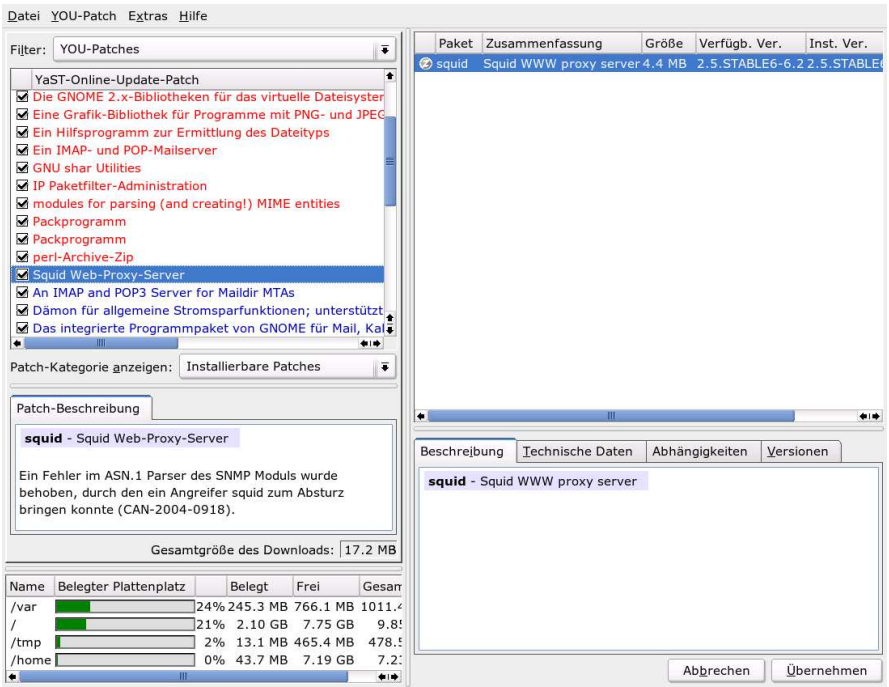

Abbildung 15.9: Liste der verfügbaren Online-Patches

Bitte gehen Sie diese Liste durch. Mit einem Häkchen markiert YOU alle bei Ihnen installierten Pakete, die es aktualisieren möchte. Dabei stellt es alle *sicherheitsrelevanten* Updates in Rot dar und *empfohlene* 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 in der Liste mindestens die Pakete, die Sie bereits aus anderen Quelle aktualisiert haben, wie z. B. den Virenscanner AntiVir.

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

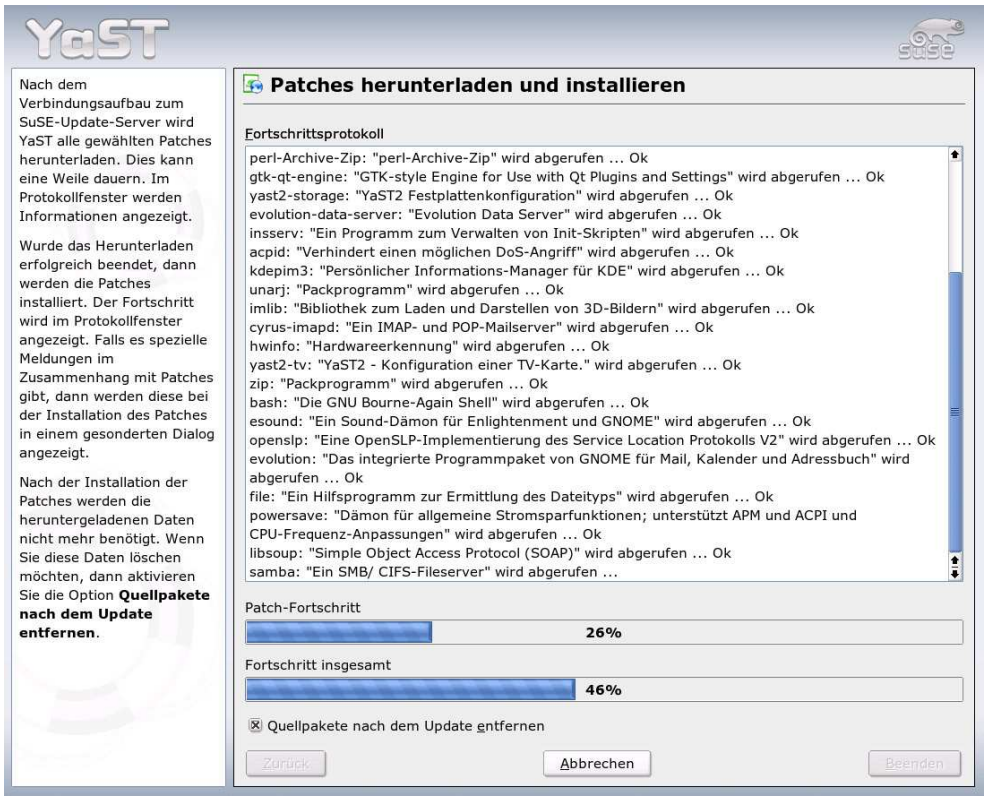

Abbildung 15.10: YOU: Laden der Patches

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

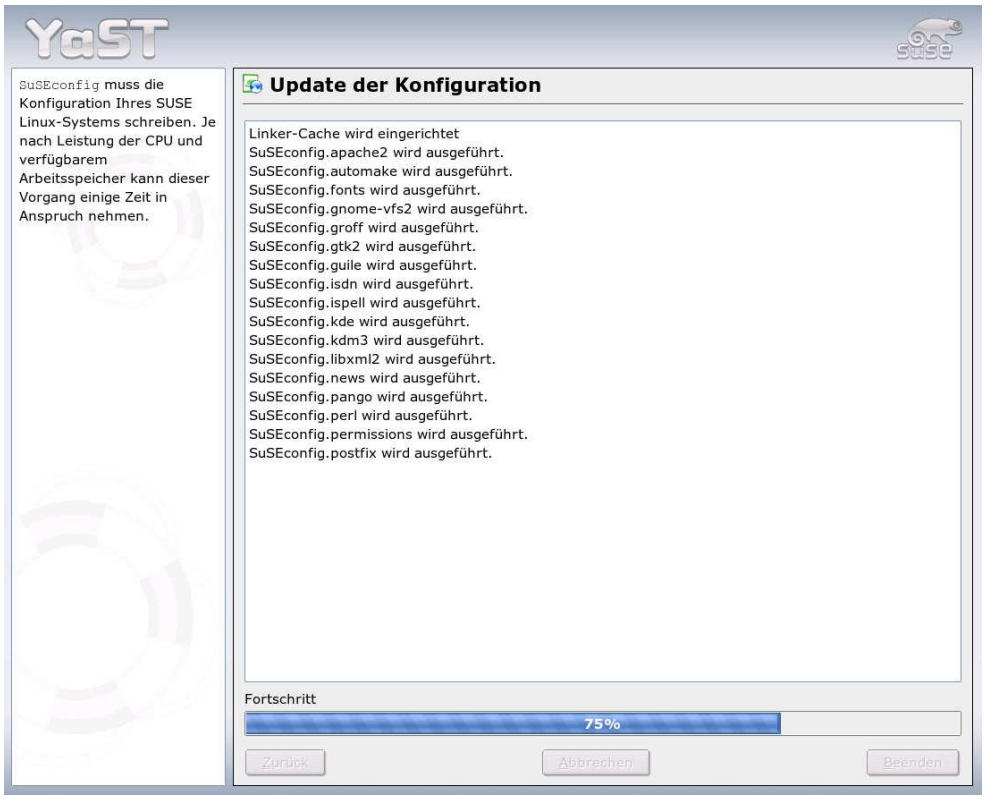

Abbildung 15.11: YOU: Aktualisierung der Konfigurationsdateien

Damit ist Ihr erstes Online-Update abgeschlossen.

Sie sollten das Updaten 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!

15.2.2 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 Web-Site `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 9.2 online aktualisieren kann.

Die momentan aktuelle Version ist 0.12.5, was sich aber bis zum Erscheinen des Buches 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-0.12.5-0.
noarch.rpm
rpm -i  fou4s-0.12.5-0.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 vorzunehmen 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 courier-imap-51818 (2004-11-18) ====
An IMAP and POP3 Server for Maildir MTAs
This update fixes the problem that the authentication daemon
was not started correctly.
================================================================
courier-imap                      3.0.7-3.2     (3.0.7-3      )
                                ↵ [dl] recommended   497kb
```

```
courier-imap-ldap                3.0.7-3.2     (3.0.7-3      )
                                ↵ [dl] recommended     3kb
= Update Information for fetchmsttfonts.sh-51687 (2004-11-25) =
Download Microsoft(r) TrueType Core Fonts
For legal reasons we can't include the Microsoft(r) 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.
================================================================
fetchmsttfonts.sh                script        (N/A          )
                                ↵ [dl] script          0kb
NOTE: Script must be installed using fou4s -i --
interactive: fetchmsttfonts.sh
======== Update Information for samba-51877 (2004-12-17) =======
This update of the samba server fixes several integer overflows
that can be exploited to overflow heap memory. An
attacker can use this bugs to execute arbitrary code remotely.
(CAN-2004-1154)
================================================================
samba                            3.0.9-2.1     (3.0.7-5      )
                                ↵ [dl] security     2838kb
samba-client                     3.0.9-2.1     (3.0.7-5      )
                                ↵ [dl] security     6449kb

======== Update Information for squid-51732 (2004-10-21) =======
Squid WWW proxy server
A bug in the ASN.1 parser of the SNMP module has been fixed
which would have allowed an attacker to crash squid
(CAN-2004-0918).
================================================================
squid                           2.5.STABLE6-6.2 (2.5.STABLE6-6)
                                ↵ [dl] security      467kb
```

Fou4s zeigt hier Updates, aber auch optionale, noch nicht installierte Pakete. 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.

Das automatische Update starten Sie mit:

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

und 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 Internet-Zugriff ausführen. Im einfachsten Fall tragen Sie dazu Proxy-Informationen, Benutzerdaten und ein Passwort in die Konfigurationsdatei von fou4s ein:

`/etc/fou4s.conf` (ab Zeile 74)

```
# 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.

15.3 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. Beliebt sind 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 Versions-Nummer 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, sodass 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 nun

```
/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.

15.4 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 Einweg-Funktion, 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	2.660 Jahre

Tabelle 15.1: 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	*Zeichenzahl*	*Zahl der möglichen Passwörter*	*Zeitbedarf 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 15.2: 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 wenigstenS die unsichersten Kandidaten zu ermahnen.

Beim Knacken und beim Ermahnen der Benutzer kann das Programm `john` helfen, dass Sie bei SuSE im Paket `john` in der Paketgruppe *Produktivität • Sicherheit* finden, aber nur bei der DVD-Version. Nach dem Installieren dieses Programms finden Sie das Programm selbst 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 genügt 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 haben. 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
)
```

Die Dokumentation von `john` nennt noch mehr Möglichkeiten, um weitere Passwörter zu knacken. Eventuell hilft Ihnen diese Erfahrung, selbst sicherere Passwörter zu verwenden.

Machen Sie 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.

15.5 Portscanner

Im Kapitel 12 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 *Portscannerr* 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 *Produktivität • Netzwerk • Diagnostik* im Paket *nmap* finden. Installieren Sie dieses Programm nach.

Um Ihren eigenen Rechner testen zu können, benötigen 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 3.70 ( http://www.insecure.org/nmap/ )
at 2004-12-30 16:50 CET
Interesting ports on boss.lokales-netz.de (192.168.1.2):
(The 1644 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  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
443/tcp  open  https
600/tcp  open  ipcserver
631/tcp  open  ipp
781/tcp  open  hp-collector
962/tcp  open  unknown
1026/tcp open  LSA-or-nterm
2049/tcp open  nfs

Nmap run completed -- 1 IP address (1 host up)
scanned in 2.346 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 1657 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.