17 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 16
- Verschlüsselten Internetzugriffen in den Kapiteln 5 und 6
- Absicherung von FTP-Servern im Kapitel 7
- Passwortverschlüsselung im Kapitel 9
- Firewall im Kapitel 14

In diesem Kapitel finden Sie Informationen, die sich etwas allgemeiner mit dem Thema Sicherheit befassen.

Dazu gehören

- Informationen über Sicherheitsprobleme
- Aktualisieren von Programmen und Systemdateien
- Erkennen von Einbruchsversuchen und Einbrüchen
- 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.

17.1 Informationen über Sicherheitsprobleme

Wenn Sie Murpheys Gesetz glauben, dann 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 in diesem Fall den Internet-Server von Windows-Systemen betrifft, werden Sie sehr häufig in den Logdateien Ihres Webservers finden. Dort tauchen Zeilen auf wie:

```
24.141.103.24 - - [19/Dec/2001:20:57:58 +0100] "GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u685
8%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%
u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u0
0=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 Webserver, 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-Webserver zu befallen, aber ein mit diesem Wurm befallener Rechner versucht nach einem Zufallsprinzip, andere Rechner zu befallen.

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

Im Web gibt es mehrere Webserver und Mailinglisten mit sicherheitsrelevanten Informationen für Linux. Sie sollten diese Informationen regelmäßig lesen und die zugehörigen Mailinglisten abonnieren.

17.1.1 SuSE

Da Sie mit einem SuSE-System arbeiten, ist deren Webserver die naheliegende Informationsquelle für Sicherheitsfragen. Der Vorteil dieser Website besteht darin, dass hier dann auch immer Lösungsvorschläge bzw. Programmaktualisierungen zu finden sind, die sich auf das SuSE-System beziehen.

Unter der URL `http://www.suse.de/de/support/security/index.html` finden Sie die aktuellen Sicherheitsinformationen.

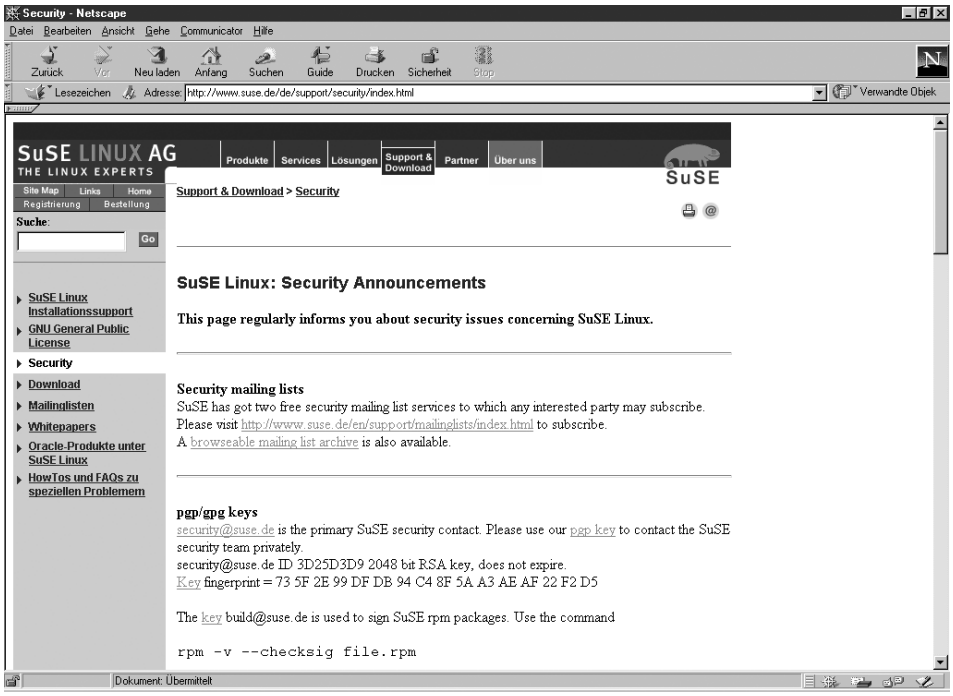

Abbildung 17.1: Sicherheitsinformationen bei SuSE

Für die Information per Mail finden Sie unter der Adresse `http://www.suse.de/de/support/mailinglists/index.html` eine Übersicht über die Mailinglisten von SuSE, die Sie dann von dieser Seite aus auch gleich abonnieren können. Für Sicherheitsfragen interessant sind vor allem die Listen `suse-securitiy-announce@suse.com` und `suse-securitiy@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 beteiligen, die Diskussionssprache ist übrigens Englisch.

17.1.2 Bugtraq/Securityfocus

Unter der URL `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`, die Sie ausgehend von der URL `www.securityfocus.com/cgi-bin/subscribe.pl` abonnieren können. Gerade wenn Sie mit verschiedenen Betriebssystemen zu tun haben, 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.

Alle bekannten Vulnerabilities (ausnutzbare Programmfehler) finden Sie ausgehend von der Seite `http://www.kb.cert.org/vuls/`.

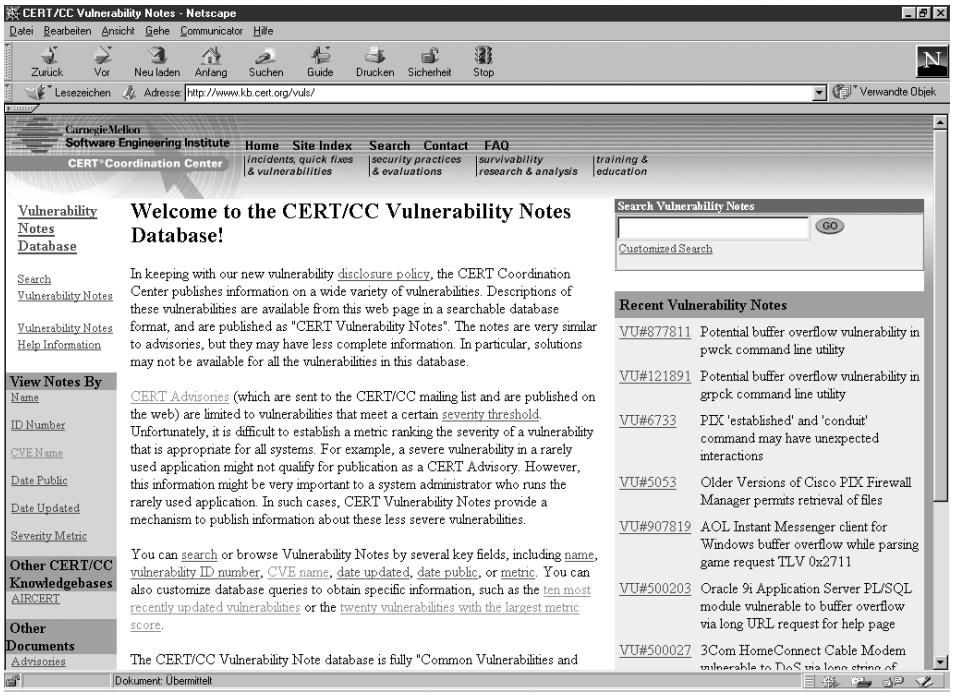

Abbildung 17.3: Vulnerability Informationen beim Cert

Die zugehörigen Lösungsvorschläge (Advisories) finden Sie dann unter der URL `http://www.cert.org/advisories/`.

Wenn Sie Internet-Systeme mit guter Anbindung und vielen Nutzern betreiben, dann 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 diskutiert und löst.

Die FTP-Server, über die SuSE aktualisierte Versionen der Pakete zur Verfügung stellt, haben Sie ja bereits mehrfach kennen gelernt. Nach den bisherigen Beschreibungen haben Sie die verbesserten Pakete immer per Hand geladen und installiert. In den aktuellen Versionen hat SuSE sogar ein automatisiertes Update-Verfahren realisiert, das *YaST Online Update* (YOU).

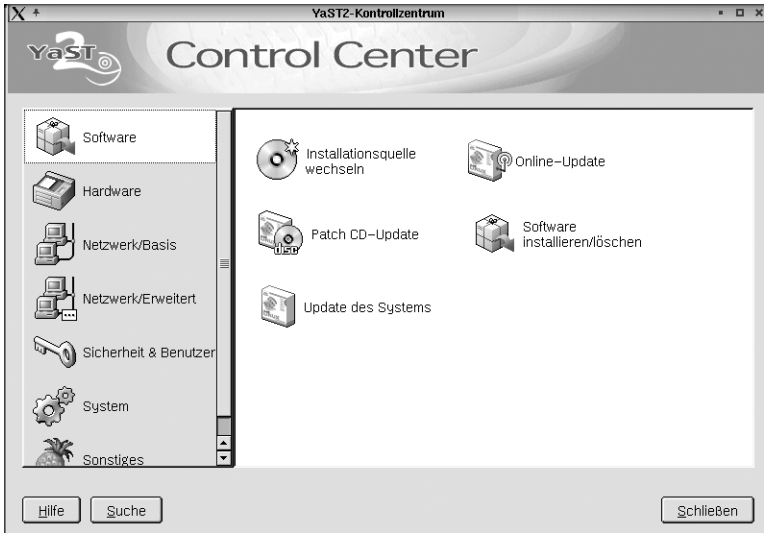

Abbildung 17.4: YaST2: Online Update

Wenn Sie YaST2 starten, dann 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 17.5: YOU: Installationsquelle

Wählen Sie das manuelle Update, da dann nur die wirklich benötigten Pakete geladen werden müssen. Bei der Wahl des automatischen Updates bekamen die Autoren nach dem Laden der File-Liste die etwas abschreckende Meldung, dass mehr als 167 MByte zu laden wären.

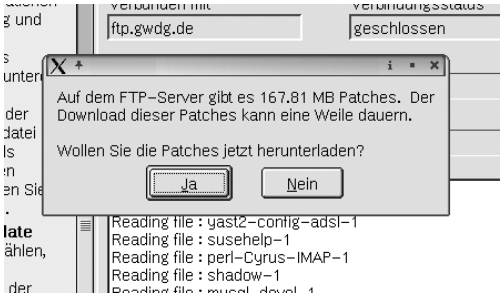

Abbildung 17.6: YOU: Meldung bei automatischem Update

Wenn Sie beim manuellen Update auf *Weiter* klicken, lädt YaST2 eine Liste der zur Verfügung stehenden aktuelleren Pakete. Da 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.

Nach dem Laden und der Installation dieses Paketes müssen Sie das YaST2 Controll Center und das Online-Update neu starten. Sie bekommen dann nach dem Laden der Dateiliste das folgende Auswahlfenster mit den verfügbaren Patches.

Abbildung 17.7: YOU: Liste der verfügbaren Patches

Gehen Sie diese Liste ruhig einmal durch. Mit einem `X` markiert YOU alle bei Ihnen installierten Pakete, die es aktualisieren möchte. In der Bildschirmkopie können Sie erkennen, dass YOU das bereits per Hand aktualisierte Paket `amavis-sendmail` nicht erneut aktualisieren wird, also Ihre individuelle Konfiguration ausgewertet hat.

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

Wenn Sie dann auf *Weiter* klicken, beginnt YOU mit dem Laden der Pakete. Sie sollten unterhalb von `/var/lib/YaST/patches/i386/update/7.3/` über entsprechend viel Festplattenkapazität verfügen, bei den Tests der Autoren immerhin 33MB.

Abbildung 17.8: YOU: Laden der Patches

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

Zum Abschluss des Update-Vorganges fasst YaST2 die erfolgten Aktualisierungen zusammen.

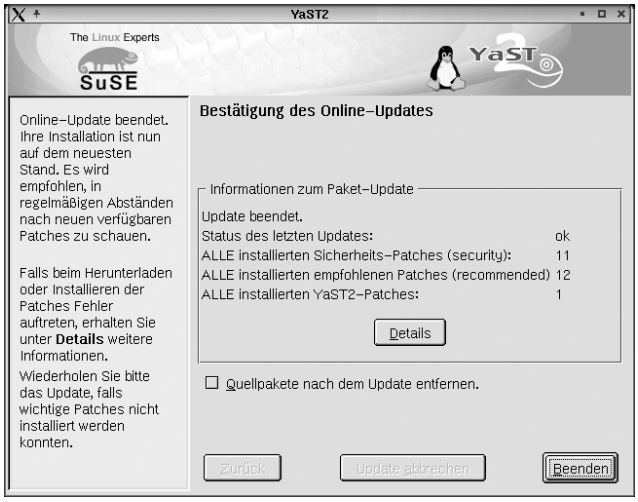

Abbildung 17.9: YOU: Bestätigung des Updates

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!

17.3 Einbruchserkennung

Die Aktualisierung der Programmpakete dient dazu, Einbrüche zu verhindern, indem Sie Programme mit Sicherheitslücken durch korrigierte Versionen ersetzen.

Eine absolute Sicherheit vor Hackern kann aber auch dies nicht bieten. Wenn es dann doch einmal zu einem erfolgreichen Einbruch in Ihr System kommen sollte, sollten Sie diesen möglichst schnell erkennen.

Dieses Erkennen eines Einbruches ist nicht immer ganz einfach, da die Einbrecher oft Systemprogramme durch veränderte Versionen ersetzen. Beliebt sind Veränderungen an den Programmen `ps` und `ls`, so dass diese die Verzeichnisse und Programme der Einbrecher nicht anzeigen.

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

Die Autoren haben mit dem Programm Claymore zur Einbruchserkennung (intrusion detection), das Sie von `http://linux.rice.edu/magic/claymore/` kostenlos laden können, gute Erfahrungen gemacht.

```
wget  http://linux.rice.edu/magic/claymore/claymore.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.

Bevor Sie das Programm konfigurieren und starten können, müssen Sie zuerst sicherstellen, dass das Perl-Modul Digest-MD5 auf Ihrem Rechner installiert ist, was normalerweise nicht der Fall sein dürfte. Installieren Sie das Modul von der SuSE-CD oder dem FTP-Server nach, Sie finden es als `perl-Digest-MD5` in der Serie `perl`.

Nach Installieren des Perl-Modules können Sie Claymore konfigurieren.

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 ist eine Liste der zu überwachenden Programme mit vollständiger Pfadangabe. Die zweite Datei ist die gleiche Liste, erweitert um die jeweiligen Prüfsummen. In diese Prüfsummen geht sowohl der Dateiinhalt als auch das Dateidatum mit ein, so dass Veränderungen sofort zu erkennen sind.

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

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

Eine Liste der zu überwachenden Dateien schlägt das Programm vor, wenn Sie den Parameter `-m` mit angeben. Diese Liste können Sie dann gleich an die richtige Stelle bringen mit:

```
/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 jetzt

```
/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` abgespeicherten Wert.

Sowie es eine Abweichung gibt, erhalten Sie an der Konsole und über die konfigurierbare Mailadresse eine Warnung.

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 Mailadresse für die Warnungen an, möglichst eine auf einem anderen Rechner!

Die Dateinamen für die Listen und das Programm selber sollten Sie ändern, um einem möglichen Einbrecher das Auffinden des Programms zu erschweren.

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

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

veranlassen Sie eine stündliche Überprüfung der Systemdateien.

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 die Passwörter nur verschlüsselt abgelegt sind. Die zugehörige Verschlüsselungsfunktion ist eine Einweg-Funktion, die kein Entschlüsseln vorsieht. Meldet sich ein Benutzer am System an, dann 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 Passwortes ist aber nicht nur von seiner Länge, sondern auch stark vom verwendeten Zeichensatz abhängig. Die folgende Tabelle geht von einer einheitlichen Passwortlänge von 8 Zeichen aus, wobei wieder 10 Millionen Passwörter pro Sekunde geprüft werden.

Zeichensatz	*Zeichen-zahl*	*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	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, das Sie eigentlich nicht alle Kombinationen durchprobieren müssen. Viele Leute benutzen Namen, Telefonnummern oder Ähnliches, einfach weil diese leichter zu merken sind.

Selbst bei einer Passwortlänge von acht Zeichen können Sie daher in wenigen Minuten zum Erfolg kommen, wenn Sie ein Wörterbuch als Grundlage für Ihre Knackversuche nehmen.

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

Hinweis: Schon ein einzelner geknackter Zugang ist ein Sicherheitsrisiko. Wer erst einmal Zugang zu Ihrem System hat, kann 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` der Serie `sec` finden. Installieren Sie dieses Programm. Danach 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
```

Mit den Daten aus dieser Datei lassen Sie `john` nun arbeiten, Sie werden erstaunt sein, wie viele Passwörter er so 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, dann 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.

Sie können `john` übrigens jederzeit unterbrechen, bei einem Neustart setzt er seine Arbeit an der gleichen Stelle fort. 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.

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 dann jeder Ihrer nachlässigen Benutzer verwarnt.

Den Text der Mail an die Benutzer kann man in dem Perl-Programm `mailer` relativ leicht ändern. Im Original handelt es sich um einen englischen Text. Wenn das für Ihre Benutzer ein Problem sein sollte, 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
umgehend ändern, sonst mache ich das ;-)
```

```
Hinweise zur Auswahl eines besseren Passwortes finden sich
unter
http://server/passwort.htm im Intrnet.

Gruss,
        Password Checking Robot
        im Auftrag von U. Debacher
EOF

                SENT=$(($SENT+1))
        done

        echo $SENT messages sent
)
```

Wenn Sie sich ausführlicher mit der Dokumentation von `john` beschäftigen, dann werden Sie noch mehr Möglichkeiten finden, um weitere Passwörter zu knacken. Eventuell veranlasst Sie die Erfahrung ja sogar dazu, 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.